VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

BEZPEČNOSTNÍ GAP ANALÝZA VE FIREMNÍM PROSTŘEDÍ
SECURITY GAP ANALYSIS IN ENTERPRISE ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Vojtěch Sommer

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Sedlák

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Vojtěch Sommer**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

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:

Bezpečnostní GAP analýza ve firemním prostředí

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:

Prvním cílem je navrhnout opatření proti bezpečnostním hrozbám ve vybraném firemním prostředí. Návrh opatření bude vypracován na základě analýzy současného stavu, která bude provedena na základě normy ISO/IEC 27 002. Tato norma je úzce spjata s doporučením ISMS. Dále norma úzce souvisí se souborem konceptů a postupů ITIL, podle kterého se vybraná společnost řídí. Odborné termíny, techniky, technologie a principy použité v analýze a návrhu práce jsou popsány již na začátku v části teoretická východiska práce. Návrh opatření by měl rovněž sloužit jako zpětná vazba pro společnost, kde analýza probíhala.
Druhým cílem této práce je osobní přínos pro autora. Díky diplomové práci by autor měl mít možnost seznámit se s novým druhem problematiky, kterou zatím měl možnost poznat jen z teoretického hlediska.

Základní literární prameny:

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

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

DOUCEK, P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

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

Abstrakt

Diplomová práce se zabývá úrovní bezpečnosti informací ve vybraném firemním prostředí. Pro tento účel bude vypracována bezpečnostní GAP analýza, která vychází z doporučené normy ISO/IEC 27002. Na základě provedené analýzy bude předložen návrh bezpečnostních opatření, díky kterému by se mělo snížit riziko hrozeb pod akceptovatelnou hranici, a zároveň by společnost neměla být nadále v rozporu s již zmíněnou normou.

Abstract

The diploma thesis deals with the level of information security in a selected company environment. For this purpose, a security GAP analysis will be performed in accordance with the recommended standard ISO/IEC 27002. The results of this analysis will then set a baseline to the proposed security precautions which should reduce the risk of threats bellow the acceptable level and they should also no longer be against the mentioned standard.

Klíčová slova

Bezpečnost, řízení, odpovědnost, aktiva, informační bezpečnost, riziko, systém, šifrování

Key words

Security, management, responsibility, assets, information security, risk, system, encryption

Bibliografická citace

SOMMER, Vojtěch. *Bezpečnostní GAP analýza ve firemním prostředí* [online]. Brno, 2020 [cit. 2020-05-11]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/127746. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná a 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 1. března 2020

_____

podpis studenta

Poděkování

Rád bych poděkoval Ing. Petru Sedlákovi za cenné rady a pevné vedení mé diplomové práce. Dále bych chtěl poděkovat všem kolegům působícím ve společnosti, kde jsem měl možnost vypracovat tuto diplomovou práci.

OBSAH

ÚVOD

V současném světě se nachází nespočet technologií všude mezi námi. Předpokládaný trend napovídá, že toto množství dále poroste. Tento vývoj je pochopitelný, neboť takové technologie lidem ulehčují práci i život. Na co se ovšem často zapomíná, je bezpečnost všech těchto technologií. Bezpečnost je často o krok pozadu a domnívám se, že právě bezpečnost všech informačních a komunikačních technologií bude získávat větší váhu. Proto je třeba tvořit a rozvíjet soubor doporučení a norem zabývajících se bezpečností informací a jimi by se měly řídit všechny společnosti, organizace ale i lidé, kteří tyto nástroje používají. Pokud nebudou aplikována opatření, která jsou popsána například v souboru norem ISO/IEC 27000, pak může dojít k velkým škodám nejen na majetku, ale i na životech.

Z důvodů popsaných výše jsem se rozhodl provést analýzu bezpečnostních mezer podle ISO/IEC 27002 ve společnosti, která je celá postavena na práci s nejmodernějšími technologickými nástroji v oblasti informačních a komunikačních technologií.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Diplomová práce má dva hlavní cíle. Prvním cílem je navrhnout opatření proti bezpečnostním hrozbám ve vybraném firemním prostředí. Návrh opatření bude vypracován na základě analýzy současného stavu, která bude provedena v souladu s normou ISO/IEC 27002. Tato norma je úzce spjata s doporučením ISMS a úzce souvisí se souborem konceptů a postupů ITIL, jímž se vybraná společnost řídí. Odborné termíny, techniky, technologie a principy použité v analýze a návrhu práce jsou popsány již na začátku v části Teoretická východiska práce. Návrh opatření by měl rovněž sloužit jako zpětná vazba pro společnost, kde analýza probíhala.

Druhým cílem této práce je osobní přínos pro autora. Diplomová práce by měla autorovi umožnit seznámení se s novým druhem problematiky, kterou měl zatím možnost poznat jen z teoretického hlediska.

2 TEORETICKÁ VÝCHODISKA PRÁCE

Teoretická východiska této diplomové práce čerpají z použitých odborných termínů, metod a praktik v dalších částech práce. Vzhledem k tomu, že se práce zabývá informační bezpečností a dále obecně bezpečností v oblasti informačních a komunikačních technologií, budou zde teoreticky popsány i obory, které s takovou problematikou přímo souvisí. Mezi tyto obory lze například zařadit projektové řízení, správu sítí či správu systémů.

2.1 Definice základních pojmů a termínů

V této části budou stručně představeny některé pojmy a termíny, které se budou dále používat a jejichž znalost je nezbytná pro lepší pochopení problematiky.

Síťová infrastruktura

Jedná se o pojem, který zahrnuje nejen všechny síťové prvky, ale i zařízení použitá při vytváření ICT prostředí. [1]

ICT (Information and Communication Technology)

S větším nástupem komunikačních technologií bylo přidáno písmeno C (Communication – komunikace) do původní zkratky IT, aby byly zdůrazněny komunikační technologie pro přenos informací, dat či hlasu. [2]

Přenos dat

Přenos dat, také označovaný jako digitální komunikace, je přenos digitálních zpráv nebo digitalizovaného analogového signálu pomocí fyzického dvoubodového nebo vícebodového přenosového média, kterým může být například metalický kabel, optický kabel nebo bezdrátový přenos. [1]

Počítačová síť

Počítačová síť je součástí síťové infrastruktury sloužící k realizaci komunikačního prostředí mezi uživateli. [1]

Důvěrnost

Zajištění přístupu k informacím a jejich poskytnutí pouze oprávněným osobám. Důvěrnost informace lze chápat jako stav, kdy je informace poskytována jen oprávněným uživatelům. [1] [3]

Integrita

Zajištění správnosti a úplnosti dat. [1]

Dostupnost

Zajištění dostupnosti informací pro oprávněné uživatele v okamžiku potřeby. [1]

Aktivum

Jedná se o jakoukoliv věc v organizaci, která má nějakou cenu. Může mít hmotnou i nehmotnou podobu. [1]

Hrozba

Hrozbou nazýváme možnost působení vlivů na zranitelná místa aktiv způsobujících změny vlastností informačních aktiv. [3]

Zranitelnost

Zranitelnost je jakékoliv slabé místo aktiva. [1]

Opatření

Jakákoliv aktivita, zařízení, technika či postup snižující sílu hrozby nebo zabránění účinku. [1]

Riziko

Riziko je pravděpodobnost, s jakou přeroste bezpečnostní hrozba v bezpečnostní incident. [1] [3]

Bezpečnostní incident

Bezpečnostní incident lze chápat jako stav aktiva s narušenými vlastnostmi po působení bezpečnostní události. Bezpečnostní incident znamená vždy změnu vlastností aktiva bez ohledu na jeho dopad. [3]

Dopad

Dopad je vznik škody v důsledku hrozby. [1]

Standard

Standard je zdokumentovaná úmluva obsahující technické specifikace nebo podobná přesně stanovená kritéria důsledně používaná jako pravidla, směrnice, resp. jako definice charakteristických vlastností zabezpečující, že materiály, výrobky, procesy, služby apod. jsou takové, jak se zamýšlelo. [3]

Norma

Norma je pouze doporučení pro daný standard nebo řešení. Jedná se tedy o doporučení použitelných standardů k realizaci požadovaného kompatibilního řešení. [3]

Audit

Audit je nezávislý a dokumentovaný proces s hodnocením kritérií. [1]

ISO (International Organization for Standardization)

Posláním organizace zvané ISO je podporování rozvoje standardizačních a s tím spojených aktivit ve světě se zaměřením na usnadnění mezinárodních směn zboží a služeb a na spolupráci ve sféře intelektuálních, vědeckých, technologických a ekonomických aktivit. [4]

IEC (International Electrotechnical Commission)

IEC je celosvětová organizace, která připravuje a vydává mezinárodní normy z oblastí elektrotechnických, elektronických a jim příbuzných. [4]

NIST (National Institute for Standards and Technology)

Vládní standardizační orgán s posláním v oblastech vývoje a podpory standardů, měřicích technik a technologií za účelem zvýšení produktivity, usnadnění obchodu a zlepšení života. [4]

2.2 Knihovna ITIL

Každý zaměstnanec, který nastoupí do společnosti, kde byla zpracovávána tato diplomová práce, je nucen projít ITIL školením, jímž se celá organizace řídí. Proto je důležité porozumět knihovně ITIL.

2.2.1 Historie ITIL

Koncept ITIL se objevil v 80. letech minulého století, kdy si britská vláda uvědomila, že poskytovaná úroveň IT služeb není dostačující. Z toho důvodu byla pověřena CCTA (Central Computer and Telecommunications Agency), nyní nazývaná OGC (Office of Government Commerce), aby vyvinula rámce pro efektivní a finančně odpovědné využívání IT zdrojů v britské vládě a soukromém sektoru. [5]

Nejstarší verze ITIL byla původně nazývána GITIM (Government Information Technology Infrastructure Management). Tato původní verze se samozřejmě velmi lišila od současné verze ITIL, ale koncepčně byla velmi podobná. Zaměřovala se na podporu a poskytování služeb. [5]

Velké společnosti a vládní agentury v Evropě přijaly tento rámec na začátku 90. let velmi rychle. ITIL se rychle šířil a byl používán vládními i nevládními organizacemi. Díky popularitě se ITIL vyvíjel společně s vývojem nových informačních technologií.[5]

V roce 2000 se společnost CCTA sloučila s OGC. Ve stejném roce společnost Microsoft použila ITIL jako základ pro vývoj svého proprietárního rámce Microsoft Operations Framework (MOF). Na přelomu století rovněž OGC kompletně přepracovává celou knihovnu a v roce 2001 je vydána ITIL verze 2. Následně se během několika let stala knihovna zdaleka nejpoužívanějším přístupem osvědčených postupů v oblasti správy IT služeb po celém světě. V roce 2007 vyšla knihovna verze 3, která byla v těsnějším sepjetí s ISO 20000. V této verzi byly doplněny procesy, jako je řízení

majetku, řízení lidských zdrojů či řízení projektu. V únoru 2019 vyšla zatím poslední verze 4, která je doplněna o 13 nových procesů. [5] [6]

2.2.2 Popis

Knihovna ITIL je založena na nejlepších zkušenostech z praxe ITSM neboli IT Service Managementu. ITSM je definováno britskou normou BS 15000 (ISO 20000), ale záběr tzv. „best practices“ knihovny je širší. Knihovna ITIL ve verzi 3 se rozděluje do několika hlavních oblastí popsaných níže. [6]

Service Strategy

Tato část poskytuje praktický rámec k návrhu, vývoji a implementaci řízení služeb nejen z pohledu organizačního, ale i jako zdroje strategické výhody. Publikace obsahuje definice služeb, strategie ITSM a plánování přidané hodnoty, IT správa, definice typů poskytovatelů služeb a obchodních strategií. [7]

Service Design

Rámec pro návrh a vývoj služeb a procesů jejich řízení. Zahrnuje principy a metody pro převod strategických cílů do portfolia služeb. Nesoustředí se pouze na nové služby, ale obsahuje i procesy změny a průběžné zlepšování stávajících služeb. [7]

Service Transition

Postupy, jak požadavky definované v rámci Service Strategy efektivně realizovat v průběhu Service Operation za současného řízení rizik poruch a výpadků služeb. Poskytuje rámec pro řízení komplexní problematiky spojené se změnami ve službách a v procesech jejich řízení. Tento rámec využívá kombinace postupů Release Managementu, Programme Managementu a Risk Managementu a převádí je do praktického kontextu řízení služeb jakožto celku. [7]

Service Operation

Postupy pro řízení služeb v produkčním prostředí, dosažení výkonnosti a účinnosti v dodávce služeb a jejich podpoře tak, aby bylo docíleno přidané hodnoty pro obě strany, tedy pro zákazníka i pro poskytovatele služby. [7]

Continual Service Improvement

Obsahuje prostředky pro vytváření a udržování přidané hodnoty služby pro zákazníka způsobem zvyšující se kvality služeb a efektivity provozu. [7]

2.3 Information Technology Service Management (ITSM)

ITSM neboli řízení IT služeb vychází z rámce ITIL, ve kterém byl poprvé použit, ale není s ním výhradně spojený. Jako v případě ITIL se jedná o souhrn nejlepších postupů pro řízení procesů služeb ICT. ITSM je druh řízení ICT využívající principů řízení na bázi služeb a zahrnuje pohledy zákazníků i poskytovatelů. Audit IT procesů za využití ITSM umožňuje vedení společnosti zjistit nedostatky v oblasti řízení IT procesů. [12]

Společnost, kde byla vypracována tato diplomová práce, funguje podle rámce ITIL a využívá ITSM nástroj, kde každý proces má nastavené SLA.

2.3.1 Service Level Agreement (SLA)

SLA je dohoda o úrovni poskytovaných služeb a představuje formalizovaný popis služby, kterou dodává dodavatel svému zákazníkovi. SLA se rozděluje do tří částí:

- Časová dostupnost (jak často je služba dostupná – např. forma 24/7 nebo 99,7 % v roce)
- Cena
- Rychlost odezvy a řešení potíží se službou (např. v analyzované společnosti při tzv. „major incidentu“ se musí do pěti minut začít řešit problém). [15]

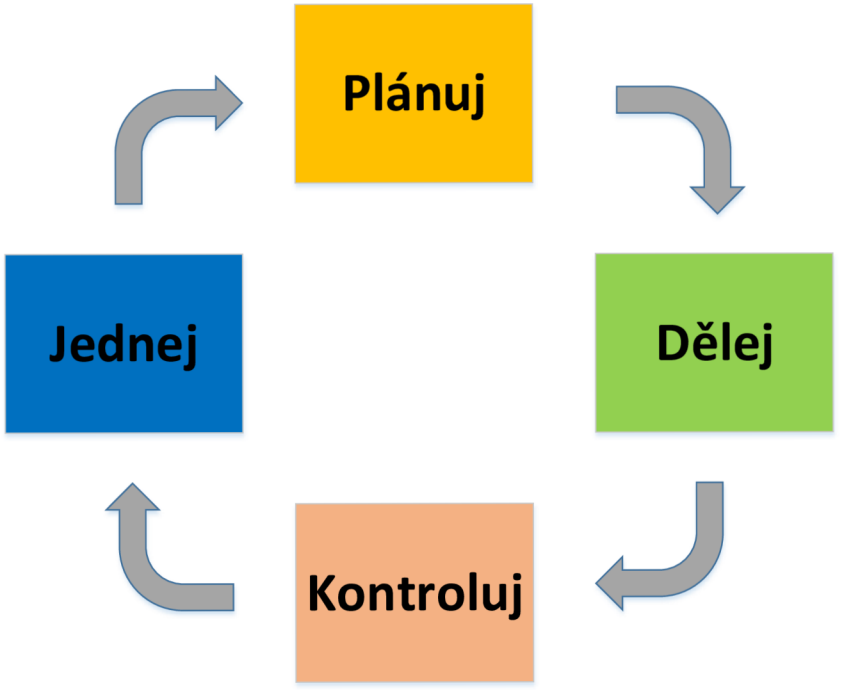
V případě analyzované společnosti se často využívá SLA v nástroji ITSM pro stanovení hranice (neboli deadline), dokdy musí být daná ICT služba poskytnuta. Díky tomu je dosaženo optimální dohody mezi zákazníkem a dodavatelem, neboť mají přesně definované hranice sjednaných služeb, a to pomocí parametrů, jako jsou kvalita a rozsah.

SLA rovněž definuje způsob řešení podpory, komunikační kanály, řešení nestandardních situací, stanovení odpovědností apod. [15]

2.4 Demingův cyklus PDCA

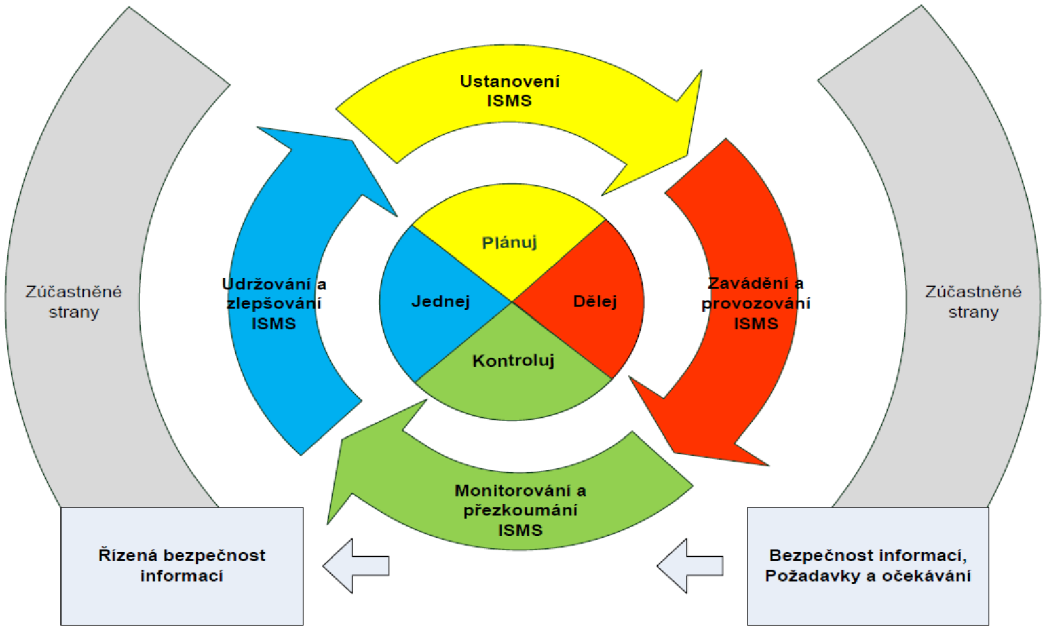
PDCA cyklus je metoda postupného zlepšování kvality výrobků, služeb, procesů, aplikací či dat probíhající formou opakovaného provádění čtyř základních činností. [1]

- Plan (plánuj)
  - Naplánování zamýšleného zlepšení
- Do (dělej)
  - Provedení plánu
- Check (kontroluj)
  - Ověření výsledku realizace oproti původnímu záměru
- Act (jednej)
  - Provedení úprav na základě ověření a následná implementace zlepšení. [1]



Obrázek č. 1: PDCA cyklus
(Zdroj: Vlastní zpracování v programu Visio)

PDCA cyklus byl vytvořen Walterem Shewhartem v roce 1930. Následně byl vylepšen panem Demingem (Demingův cyklus). W. Edwards Deming byl americký statistik, který definoval 7 smrtelných chorob firem, a je spolutvůrcem TQM (Total Quality Management). [1]



Obrázek č. 2: Demingův model pro ISMS (čtyřfázová forma)
(Zdroj: 1)

Pro účel ISMS (Information Security Management System) byl vytvořen Demingův model ve čtyřfázové formě:

identifikovat procesy

popsat a zdokumentovat procesy

na základě dokumentace řídit procesy

následně optimalizovat procesy

ustanovení ISMS,

zavádění a provoz ISMS,

monitorování a přezkoumání ISMS,

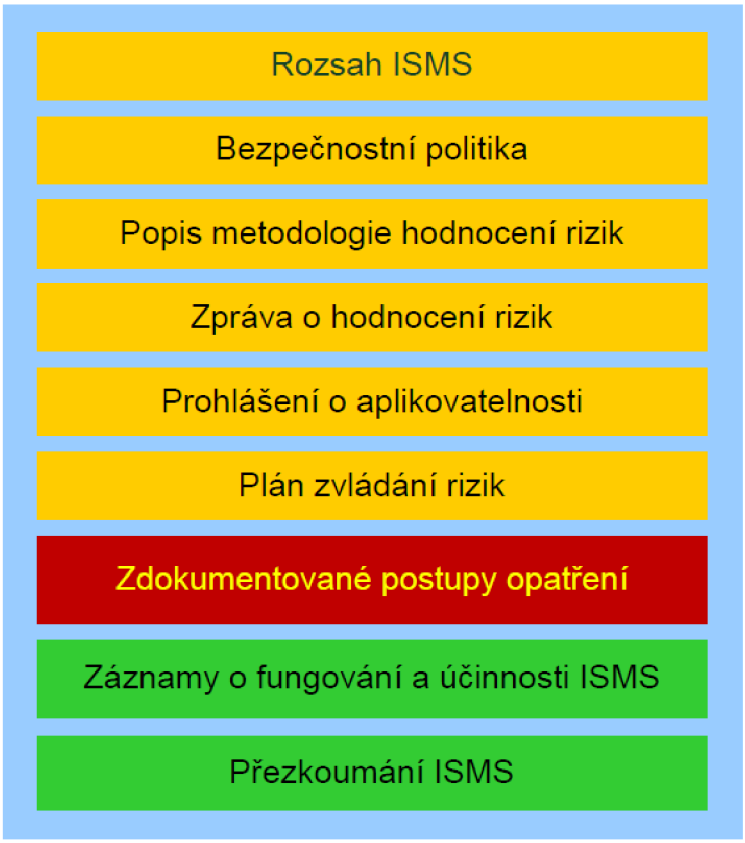
údržba a zlepšování ISMS. [1]

2.5 Information Security Management System (ISMS)

Systém managementu bezpečnosti informací představuje systematický a řízený proces trvalého zlepšování bezpečnosti informací podle mezinárodní normy ISO/IEC 27001. Jedná se o řízení bezpečnosti informací se všemi atributy, které tento obor obnáší.

ISMS model je založen právě na výše zmíněném Demingově modelu skládajícím se ze čtyř etap. [8]

Každá organizace, která se chystá zavést tento systém, musí vést a pravidelně aktualizovat povinnou dokumentaci dle ISO/IEC 27001. Obsah této dokumentace je zobrazen na obrázku níže. [8]



Obrázek č. 3: Povinná dokumentace dle ISO/IEC 27001
(Zdroj: 8)

2.5.1 Bezpečnost informací

Bezpečnost informací je systematický proces trvalého zlepšování ochrany cenných informací (aktiv) ve všech formách výskytu. Bezpečnost informací má 3 cíle:

- Dostupnost
- Integrita
- Důvěrnost [8]

Bezpečnost informací je vyžadována v mnoha případech; mezi nejdůležitější patří:

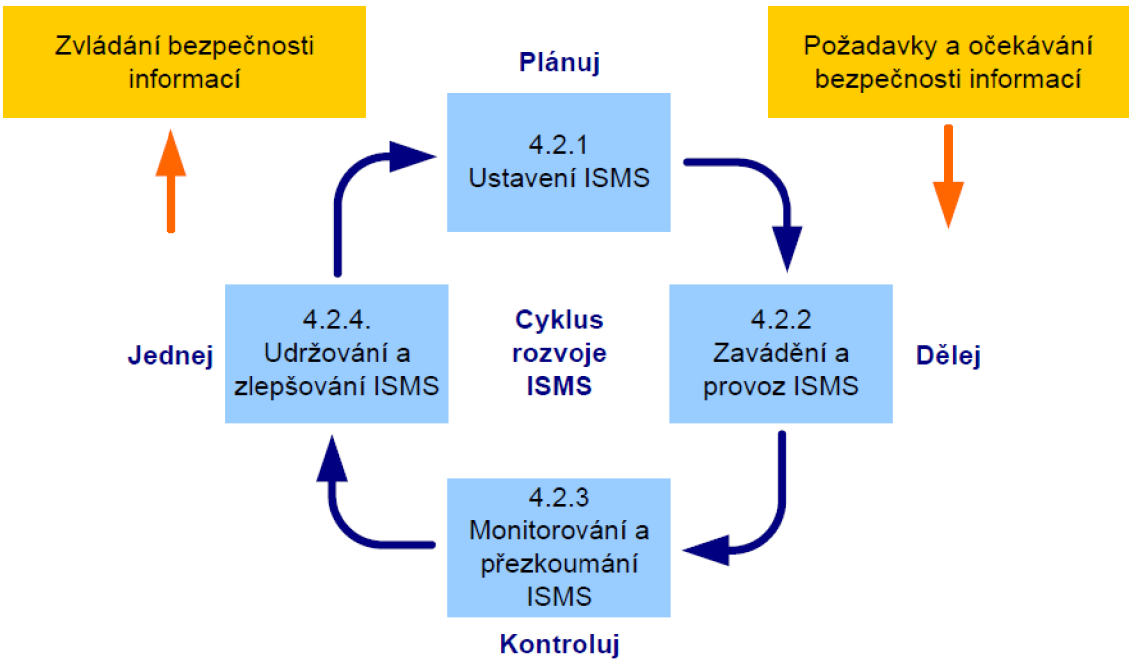
- Zákony a regulační orgány
    - Ochrana osobních údajů (GDPR)
    - IS veřejné správy (ISVS)
    - Kritická informační infrastruktura (Kybernetický zákon)
    - Mezinárodní prostředí
- Kontinuita podnikání
    - Dostupnost a spolehlivost
    - Schopnost prezentace ochrany informací
    - Ochrana know-how
- Vztahy důvěry a jejich udržení
    - Vytváření holdingů
    - Požadavky partnerů
    - Důvěra klientů a zákazníků [8]

2.5.2 Přínosy zavedení ISMS v organizaci

Přínosů pro organizace je po zavedení ISMS mnoho. Společnosti se často prezentují certifikací, že splňují ISMS, čímž imponují svým partnerům a mohou se tak dostat k zajímavějším zakázkám. Díky ISMS jsou rovněž v oblasti bezpečnosti kompatibilní s ostatními organizacemi. Mezi další výhody patří například splnění požadavků na ochranu osobních údajů (GDPR) nebo splnění požadavků Kybernetického zákona z pohledu KI (Kritické Infrastruktury). [8]

2.5.3 Postup pro zavedení a provozování ISMS

Systém řízení bezpečnosti informací se vytváří a následně i řídí podle požadavků normy ISO/IEC 27001. [8]



Obrázek č. 4: Zavedení a provozování ISMS
(Zdroj: 8)

2.5.3.1 Ustanovení ISMS

V první fázi zavedení a provozování ISMS je třeba určit rozsah a hranice ISMS podle zaměření a činnosti organizace a jejího organizačního uspořádání. Dále je nutno zpracovat politiky podle ISO/IEC 27001. Následně je třeba zpracovat metodiky hodnocení rizik a určení kritérií pro akceptaci rizik. Dalším bodem ustavení ISMS je identifikace všech informačních aktiv a identifikace a hodnocení rizik ohrožení informačních aktiv. V závěru první fáze je třeba vypracovat prohlášení o aplikovatelnosti opatření a nechat ho schválit vedením organizace. [3]

Prohlášení o aplikovatelnosti je jeden z nejdůležitějších dokumentů ISMS, ve kterém jsou upřesněna bezpečnostní opatření, která bude organizace v rámci ISMS zohledňovat. [3]

2.5.3.2 Zavedení ISMS

V tomto kroku je třeba se zaměřit na bezpečnostní opatření, která byla navržena při ustanovení ISMS. To znamená hlubší rozpracování plánů včetně specifikace časových

termínů, odpovědných osob apod. Kromě upřesnění plánů je třeba zdokumentovat plán zvládání rizik a zavést ho. Další kroky, které se musí uskutečnit v této fázi, jsou:

- Zavedení plánovaných bezpečnostních opatření
- Vytvoření příručky bezpečnosti informací podle ISO/IEC 27002
- Vytvoření programu budování bezpečnostního povědomí (Security awareness)
- Zaškolení všech uživatelů, kterých se oblast týká
- Zavedení měření účinnosti bezpečnostních opatření a sledování stanovených bezpečnostních ukazatelů
- Zavedení a upřesnění postupů pro detekci a reakci na bezpečnostní incidenty
- Řízení zdrojů, dokumentů a záznamů ISMS. [3] [11]

2.5.3.3 Monitorování a přezkoumání ISMS

V tomto úkolu je nejdůležitější získávání zpětné vazby. Z toho důvodu by měla být provedena kontrola všech aplikovaných opatření a jejich důsledků na ISMS. Rovněž by měla proběhnout kontrola odpovědných osob a manažerů, zda plní své povinnosti. Součástí tohoto úkolu je také provedení interního auditu ISMS. Nashromážděná data by měla být následně předložena vedení společnosti, aby bylo ověřeno, že realizace ISMS je v souladu s potřebami organizace. [11]

2.5.3.4 Údržba a zlepšování ISMS

Posledním úkolem při zavádění a provozování ISMS je údržba a zlepšování. V tomto bodě by měl probíhat sběr dat a podnětů pro zlepšení ISMS a na základě těchto podnětů následně implementovat změny. [11]

2.6 International Organization for Standardization (ISO)

Posláním ISO je podporování rozvoje standardizačních a s tím spojených aktivit ve světě se zaměřením na usnadnění mezinárodních směn zboží a služeb a na spolupráci ve sféře intelektuálních, vědeckých, technologických a ekonomických aktivit. [4]

Obrázek č. 5: Logo ISO
(Zdroj: 9)

ISO organizace neboli Mezinárodní organizace pro normalizaci vznikla v Londýně v roce 1946, kdy se sešlo 65 delegátů z 25 zemí, aby projednali budoucnost mezinárodních standardů. Následně byla v roce 1947 založena organizace ISO, ve které pracovalo 67 skupin technických expertů, kteří se zaměřovali na specifické subjekty. [9]

2.6.1 Přehled norem

S přihlédnutím k zaměření této diplomová práce bude níže uveden přehled norem, které souvisí s informační bezpečností nebo s bezpečností v oblasti informačních technologií:

- ISO/IEC 27000 – Základy (přehled) a slovník
- ISO/IEC 27001 – Požadavky
- ISO/IEC 27002 – Soubor postupů (dříve ISO 17799)
- ISO/IEC 27003 – Návod pro implementaci
- ISO/IEC 27004 – Metriky a měření účinnosti opatření
- ISO/IEC 27005 – Management rizik
- ISO/IEC 27006 – Požadavky na místa provádějící audit a certifikaci
- ISO/IEC 27007 – Směrnice pro audit
- ISO/IEC TR 27008 – Doporučení auditorům
- ISO/IEC 27xxx – Specifikace pro oborové činnosti organizace. [4]

2.7 National Institute of Standards and Technology (NIST)

Alternativou k ISO je tzv. NIST neboli Národní institut standardů a technologie. Tento institut vznikl v USA v roce 1901 a v současnosti je součástí amerického ministerstva obchodu. NIST byl založen americkým Kongresem a jeho úkolem bylo odstranění infrastruktury druhořadého měření, které zaostávalo za schopnostmi Velké Británie, Německa a dalších ekonomických konkurentů. [10]

Obecným úkolem NIST je podpora inovací a průmyslové konkurenceschopnosti USA, zlepšování vědeckých měření, standardů či technologií a zlepšování kvality života. Oblastí bezpečnosti ICT se pak zabývá CSD (Computer Security Division), tedy Divize počítačové bezpečnosti. [10] [4]

Divize CSD se dále rozděluje do těchto skupin:

- šifrovací technologie
- zabezpečení systémů a aplikací
- bezpečnostní komponenty a mechanizmy
- bezpečnostní inženýrství a risk management
- bezpečnostní testování, validace a měření. [11]

2.8 European Union Agency for Network and Information Security (ENISA)

ENISA neboli Evropská agentura pro síťovou a informační bezpečnost je středobodem pro odborné znalosti v oblasti bezpečnosti počítačových sítí a bezpečnosti informací pro Evropskou unii (EU), její členské státy, občany a soukromý sektor. Agentura spolupracuje s těmito skupinami subjektů, aby vytvořila rady a doporučení na základě nejlepších praktik v oblasti informační bezpečnosti. [14]

Obrázek č. 6: Oficiální logo agentury ENISA
(Zdroj: 14)

ENISA napomáhá členským státům EU implementovat legislativu a pracuje na zlepšení odolnosti vůči kritické informační infrastruktuře a počítačovým sítím. Agentura byla založena v roce 2004. ENISA má dvě sídla, přičemž jsou obě v Řecku, první v Aténách a druhá ve městě Heraklion. Od roku 2019 tato agentura pracuje na přípravě evropského schématu kybernetické certifikace, které umožní získat certifikaci na produkty, procesy a služby podporující digitální jednotný trh. Tento úkol je nazýván Cybersecurity Act. [14]

2.9 CCTA Risk Analysis and Management Method (CRAMM)

Metodika CRAMM je soubor softwarových nástrojů pro zavedení a podporu systémů řízení informační bezpečnosti. Tato metodika je určena k identifikaci a ohodnocení aktiv, analýzu rizik informačních systémů a sítí, pro návrh bezpečnostních opatření, stanovení havarijních požadavků na IS (informační systémy) a navrhování řešení havarijních situací. Metodika se skládá z velké databáze opatření, která je nazývána knihovna opatření. V této knihovně je zahrnuto bezpečnostní opatření pro pokrytí rizik. V nejnovější verzi CRAMM 5.2 je rovněž obsažena norma ISO/IEC 27001:2005. [3]

Pomocí této metodiky, která je podporována softwarovými nástroji, se může společnost či organizace připravit na certifikaci ISO/IEC 27001. Příprava probíhá hodnocením rizik IS, navržením efektivních opatření pro zlepšení informační bezpečnosti, provedením analýzy současného stavu podle ISO/IEC 27001, řízením informačních rizik a vytvářením bezpečnostní dokumentace havarijních plánů a plánů pro zajištění kontinuity při provozu. [3]

2.9.1 CRAMM Expert

Tato metodika je detailním pojetím klasické CRAMM metody, kdy provádění analýzy dělíme do 3 částí:

1. Identifikace aktiv, vytvoření modelů aktiv na základě výslechu osob odpovědných za daná aktiva (např. Service Owner) a přiřazení hodnoty k aktivu, tedy jak velký vliv a možný dopad může dané aktivum mít na provoz a cíle organizace v případě ohrožení aktiva.
2. Identifikace hrozeb a zranitelností systémů a výpočet míry rizika.
3. V této části jsou navržena opatření, která sníží hodnotu rizik. Následně je třeba vypracovat podklady pro implementaci takových opatření doporučených k realizaci. [3]

2.9.2 CRAMM Express

Tato metoda umožní provést velmi rychlou analýzu rizik systému během několika hodin, a to bez porušení zásad základní metodiky CRAMM. Je vhodné ji použít na začátku projektu, čímž získáme rychlý a kvalitní přehled o celém systému. Tento model je uzpůsoben tak, že všechny body analýzy lze následně převést do stejné metodiky ve variantě Expert a provést detailní analýzu v každé dílčí části. [3]

Postup analýzy:

- Zjištění hodnot dat pomocí vodítek hodnocení
- Rychlé zhodnocení hrozeb a zranitelností
- Stanovení míry rizik a výpis opatření. [3]

2.9.3 Výběr opatření

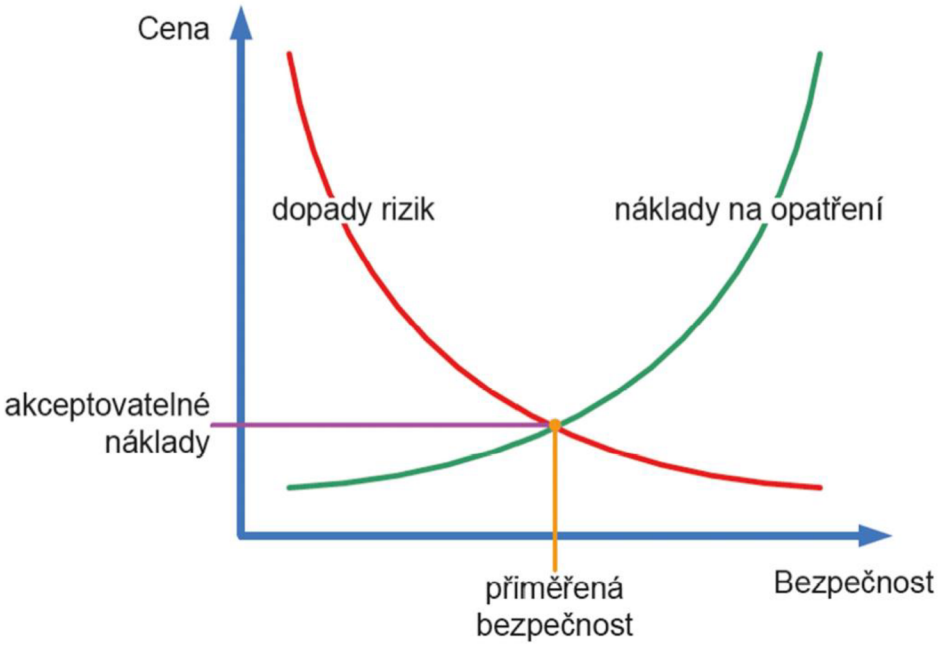
Výběr opatření je výsledný výstup analýzy podle CRAMM Expert. Tato opatření jsou vybírána podle knihovny bezpečnostních opatření, kde zahrnují 5 oblastí:

- IT bezpečnost
- Komunikační bezpečnost

- Personální bezpečnost
- Administrativní bezpečnost
- Fyzická bezpečnost. [3]

2.9.3.1 Přiměřená bezpečnost

Při výběru opatření by měla být vždy zohledňována přiměřená bezpečnost, tedy rozhodnutí, jak vysoké zdroje (např. lidské, finanční) budeme investovat do bezpečnosti a zda pro účel podnikání je tak vysoká či nízká míra bezpečnosti vyhovující. Proto úroveň bezpečnosti je vždy individuální nejen v případě organizací, ale i jedinců. Jak je vidět na obrázku níže, křivky mají stejný průběh jako křivka poptávky a nabídky. Úroveň bezpečnosti by měla stanovit bezpečnostní politika organizace a při změnách dotýkajících se rizik společnosti by měla být vždy zohledněna přiměřená bezpečnost. [3]



Obrázek č. 7: Přiměřená bezpečnost
(Zdroj: 3)

2.10 RACI matice

RACI matice neboli matice odpovědnosti je nástroj, díky kterému lze snadno identifikovat role a odpovědnosti v rámci projektu, procesu nebo v rámci organizace.

Název matice vychází ze čtyř slov, z jejichž počátečních písmen je složeno slovo RACI. Tyto čtyři slova definují vybranému subjektu jeho odpovědnost vůči procesu, projektu či organizaci.

- R – Responsible (Odpovědný)
    - Definuje kdo je odpovědný za vykonání svěřeného úkolu. Každý proces nebo projekt musí mít přidělenou osobu či skupinu, která bude ústředním bodem a koordinátorem celého procesu.
- A – Accountable (Odpovědný za celý úkol)
    - Tato pozice definuje osobu či jiný subjekt, který je odpovědný za celý úkol. Tento subjekt odpovídá za vše, co je v daném projektu vykonáno. V praxi se jedná o osobu, která se před předáním projektu podepíše za celý projekt a nese odpovědnost za veškeré nedostatky v takovém projektu. Takovou osobou tedy bývají vedoucí pracovníci. Každý proces by měl obsahovat právě jedno A.
- C – Consulted (Konzultováno)
    - V některých projektech je třeba využít znalostí a zkušeností osob, které nepatří do skupin prvních dvou písmen popisovaného modelu. Pro tento účel tedy vznikl termín Consulted, tedy konzultace se zkušenou osobou. V rámci projektu či procesu je nutno definovat takovou zkušenou osobu, aby v případě potřeby bylo dohledatelné, na koho se lze obrátit.
- I – Informed (Informován)
    - Do projektů a procesů bývají často zapojeny i osoby, které nejsou nijak zapojeny do žádného úkolu, ovšem měli by být informovány o některých změnách, která s daným procesem souvisí. Z toho důvodu je třeba definovat všechny tyto subjekty.

V některých případech se lze potkat i s RASCI modelem. Tento model je rozšířen o písmeno S – Support (Podpora). Podpora se vytahuje ke všem pracovníkům, kteří se na projektu podílejí. Zde je nutno podotknout, že člověk na úrovni podpory, který úkol vykonává, nemusí nést odpovědnost za výsledek. [16] [17]

2.11 Bezpečnostní opatření

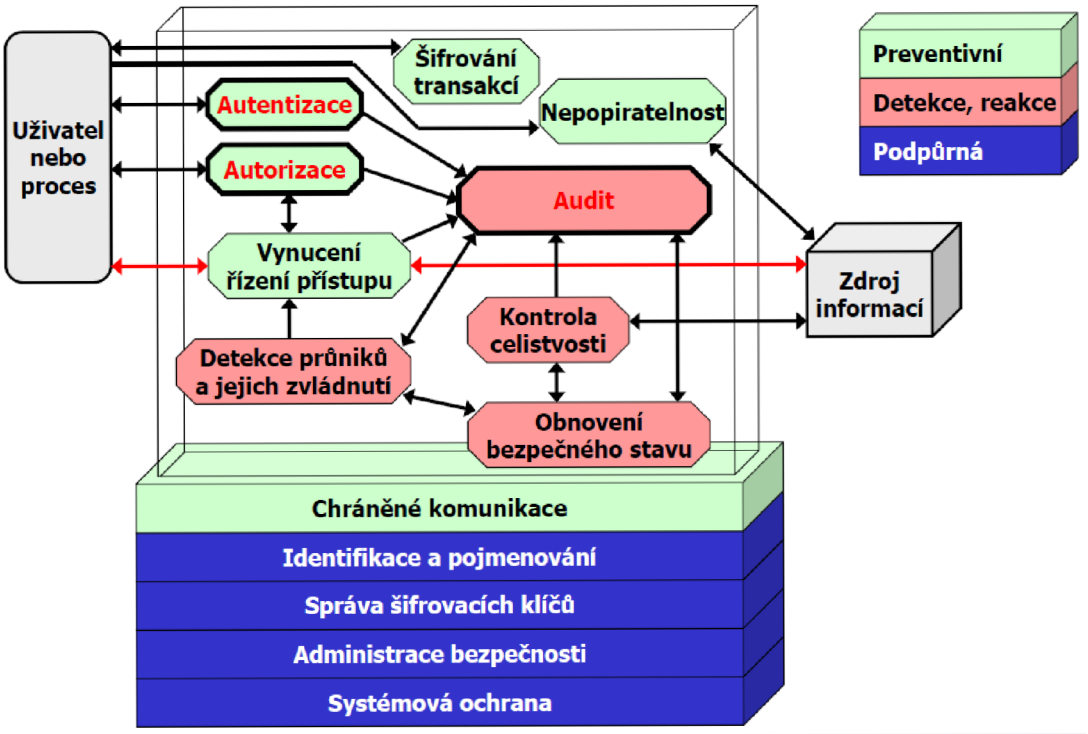
Bezpečnostní opatření může být proces, procedura či technický prostředek speciálně určený pro zmírnění působení hrozeb na organizaci či snížení zranitelnosti nebo dopadu hrozby. Tato opatření dělíme:

- Prevence
- Detekce a reakce
- Podpůrná. [3]

Bezpečnostní opatření informační bezpečnosti se dále rozdělují do těchto skupin:

- Řízení a správa bezpečnosti
- Technologická bezpečnost
- Bezpečnost provozního prostředí. [3]

Bezpečnostní opatření lze vybrat ze dvou variant. První možností je opatření pomocí metody CRAMM, kde lze čerpat z knihovny opatření. Alternativou pro opatření je ISO/IEC 27002 (od kapitoly A.4 po A.18). [3]



Obrázek č. 8: Technologická bezpečnostní opatření
(Zdroj: 3)

Mezi nejdůležitější všeobecná základní bezpečnostní opatření patří:

- Řízení a politiky bezpečnosti ICT
- Řešení incidentů
- Personální opatření
- Provozní problémy
- Kontrola bezpečnostní shody
- Fyzická bezpečnost
- Plánování kontinuity činnosti společnosti. [3]

Obrázek č. 9: Bezpečnostní opatření podle ISO/IEC 27002
(Zdroj: 3)

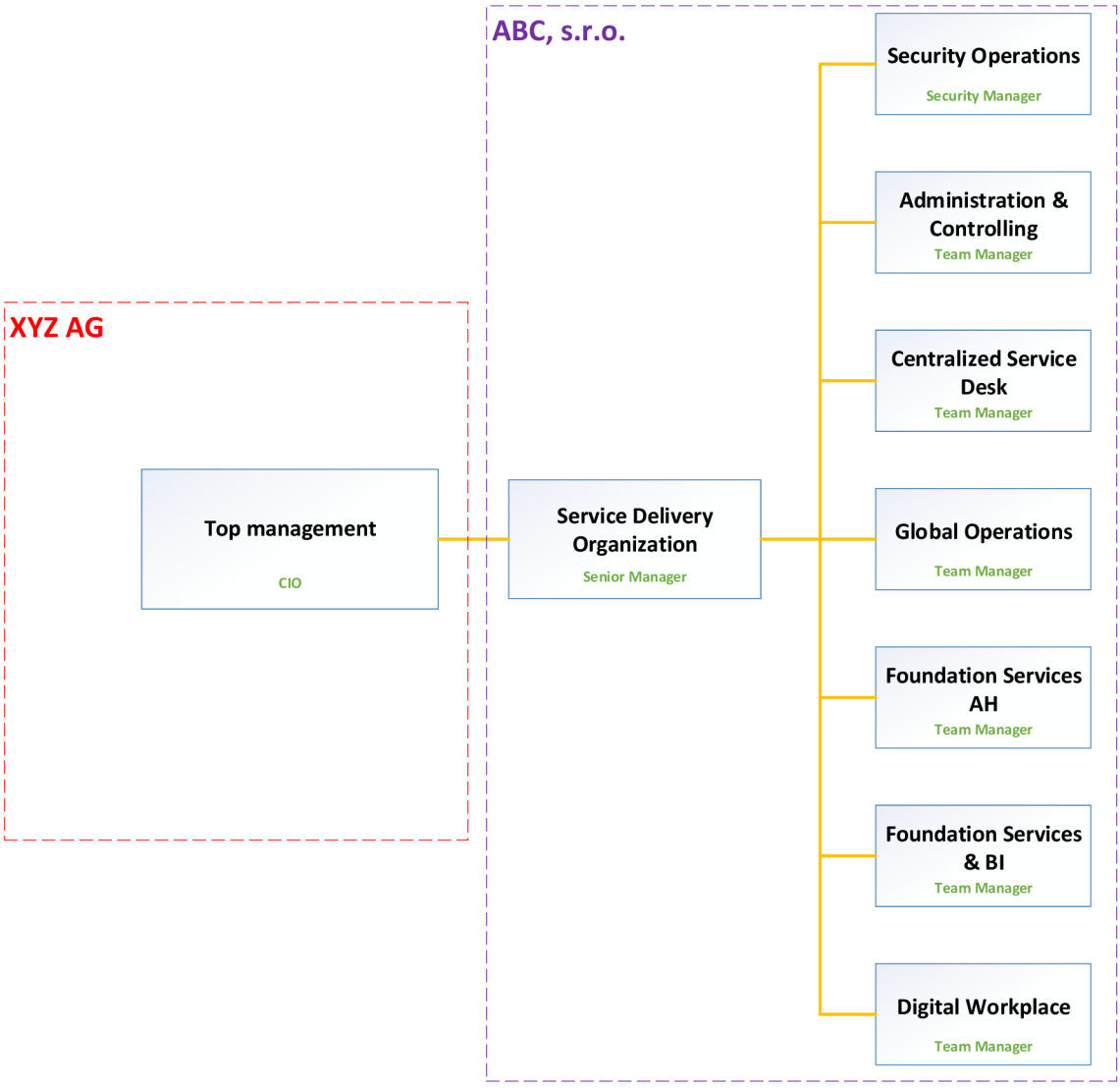
V této diplomové práci bude vypracována bezpečnostní GAP analýza podle normy ISO/IEC 27002:2013. Tato norma obsahuje 113 bezpečnostních opatření rozdělených do 14 oblastí. Tyto oblasti definují 35 kontrolních cílů opatření, které mají za úkol ochranu bezpečnostních aktiv proti narušení důvěrnosti, dostupnosti a integrity. Díky těmto cílům má organizace kvalitní základ pro bezpečnostní politiku. [3][13]

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Společnost

ABC, s.r.o. je dceřinou společností společnosti DEF, a.s., která je vlastněna společností XYZ AG. XYZ Group (dále jen XYZ) je jedním z největších výrobců stavebních materiálů. Tato původem německá společnost se zabývá především výrobou cementu, asfaltu, betonu, betonových výrobků a těžbou kamene. Dceřiná společnost ABC, s.r.o. (dále jen ABC) je mladá společnost, která byla zapsána do obchodního rejstříku dne 19. dubna 2017. Původ ABC pramení v ICT oddělení DEF, a.s., kde úkolem oddělení byla zodpovědnost nejen za vlastní ICT infrastrukturu, ale i za další společnosti, které pod XYZ patří. Ovšem ve velmi krátké době se skupina XYZ rychle rozrostla a stala se jednou z největších společností ve svém oboru, která po celém světě zaměstnává téměř 60 000 lidí ve více než 60 zemích světa. Díky tomu vznikla ABC, která byla nucena řídit čím dál větší množství firemních sítí různých velikostí. Společnost ABC je tedy ve skupině vedena jako tzv. „Service Delivery Organization“. Posláním této společnosti je podpora ICT infrastruktur a aplikací tzv. 24x7.

3.1.1 Organizační struktura společnosti



Graf č. 1: Organizační struktura společnosti
(Zdroj: Interní dokumenty společnosti ABC, s.r.o.)

Společnosti ABC, za kterou zodpovídá Senior Manager (jednatel společnosti), je rozdělena do sedmi oddělení, které spolu úzce spolupracují. Každé takové oddělení vede týmový manažer (Team Manager), který má pod sebou dále Team Leadery a ti zase různé specialisty. Společnost ABC, byť se může zdát její organizační struktura velmi jednoduchá, má kolem 180 zaměstnanců. Takto vysoké číslo je podpořeno skutečností, že některá oddělení pracují v třísměnném provozu.

3.1.2 Cenová politika společnosti

Vzhledem k tomu, že společnost ABC spadá pod XYZ Group a stará se o infrastruktury a aplikace, které do této skupiny patří, je zřejmé, že hlavní motivací nebude co nejvyšší zisk. Neboť všechny společnosti mají stejného většinového vlastníka a taková motivace by tedy byla kontraproduktivní. Díky nižším sazbám, které ABC účtuje společnostem, je tedy dosaženo rovnováhy, kdy ABC není ztrátová a ostatní společnosti mají nižší náklady, než kdyby takovéto služby řešily outsourcingem mimo organizaci nebo samy zaměstnávaly všechny potřebné specialisty, které by například nebyly schopny vytížit. Společnost ABC se ovšem musí řídit doporučeními ze strany finančních úřadů a cena služeb tak odpovídá nákladům navýšeným o 5 % marži.

3.1.3 Serverová infrastruktura pro vlastní účely

Společnost ABC má mnoho aplikací a systémů, které pro své fungování potřebují nejen kvalitní prostředí, ale i infrastrukturu. Proto má společnost pro všechny tyto účely vybudovanou velmi kvalitní počítačovou síť, která je vysoce funkční nejen při kabelovém, ale i při bezdrátovém připojení. V případě bezdrátového připojení je ovšem nutno počítat s určitými restrikcemi z bezpečnostních důvodů. Běh aplikací a systémů zajišťují servery, kde část z nich je umístěna v budově společnosti ABC a ostatní servery jsou umístěny v datacentrech. Fyzické servery dále obsahují mnoho virtuálních strojů, které ve většině případů obsahují operační systém Windows Server. Ovšem ani Linux OS není výjimkou. Za řízení těchto částí společnosti jsou zodpovědná jednotlivá oddělení, podle jejich specializace.

3.1.4 Serverová infrastruktura pro zákazníky

Působení zákazníků v 60 zemích světa vede společnost ABC k řešení vybudování datových center s nejvýhodnější lokací. Z toho důvodu má společnost vybudováno několik datových center umístěných v regionech Severní Ameriky, Evropy a Asie. V těchto datacentrech běží více než 8 000 serverů. Všechny servery jsou neustále monitorovány několika systémy a v případě poruchy některého ze serverů dostanou ihned příslušní specialisté zprávu o chybě.

3.2 Analýza současného stavu podle ISO 27002

Tato kapitola se bude zabývat analýzou současného stavu podle ISO/IEC 27002. Dále budou řešeny jednotlivé kapitoly a podkapitoly z tohoto standardu s ohledem na to, zda se společnost danou problematikou zabývá.

3.2.1 Politiky bezpečnosti informací

3.2.1.1 Pokyny managementu organizace k bezpečnosti informací

- Politiky pro bezpečnost informací (Policies for information security)
  - Politiky bezpečnosti informací jsou ve společnosti definovány bezpečnostními experty. Tyto politiky byly a v případě změn jsou schváleny vedením a následně sdíleny na SharePointu všem zainteresovaným stranám.
- Přezkoumání politik pro bezpečnost informací (Review of the policies for information security)
  - Politiky pro bezpečnost informací jsou v periodickém cyklu přezkoumávány. Přezkoumány jsou i v případě, že dojde ke změnám, které by tyto politiky mohly ovlivnit, a následně musí být opět schváleny vedením.

3.2.1.2 Organizace bezpečnosti informací

- Role a odpovědnosti bezpečnosti informací (Information security roles and responsibilities)
  - Společnost přiděluje odpovědnosti za bezpečnost informací v souladu s politikami bezpečnosti informací (3.2.1.1) a identifikuje odpovědnosti za ochranu jednotlivých aktiv a za provádění specifických postupů v oblasti bezpečnosti informací.
- Princip oddělení povinností (Segregation of duties)
  - Společnost odděluje oblasti působnosti. Například při vytváření major a high incidentů je potřeba schválení od Country Operations Managera.
- Kontakt s autoritami (Contact with authorities)
  - V případě úniku osobních dat musí společnost kontaktovat příslušný orgán do 72 hodin (dle GDPR).

- Kontakt se zvláštními zájmovými skupinami (Contact with special interest groups)
    - Bezpečnostní specialisté se účastní školení, případně jsou v kontaktu přímo se společnostmi nabízejícími některá bezpečnostní řešení (např. Endpoint security).
- Bezpečnost informací v řízení projektů (Information security in project management)
    - Security team je zahrnut do projektového managementu. Například při nasazování nové služby se provádí penetrační testy, bezpečností posouzení, validace designových dokumentů apod.

3.2.1.3 Mobilní zařízení a práce na dálku

- Politika mobilních zařízení (Mobile devices and teleworking)
    - Řešeno pomocí Mobile Device Managementu.
- Práce na dálku (Teleworking)
    - Pro práci z domu se používá šifrovaná komunikace pomocí VPN, dále jsou nastaveny restrikce pro prohlížení webových stránek. Z důvodu bezpečnosti není možné si vzdáleně pročítat e-maily na počítači, pokud uživatel není připojen na VPN.

3.2.2 Bezpečnost lidských zdrojů

3.2.2.1 Před vznikem pracovního poměru

- Prověřování (Screening)
    - Společnost nabírá nové zaměstnance sama a také pomocí náborářských agentur. Společnost provádí náběr zaměstnanců řádně a dodržuje postupy včetně prověřování, ovšem náborářská agentura takové prověřování s nejvyšší pravděpodobností neprovádí.
- Podmínky pracovního poměru (Terms and conditions of employment)
    - Při podepisování pracovních smluv se podepisuje NDA (Non-Disclosure Agreement).

- Všechny podmínky a odpovědnosti zaměstnance i zaměstnavatele jsou náležitě popsány v pracovních smlouvách.

3.2.2.2 Během pracovního poměru

- Odpovědnosti managementu organizace (Management responsibilities)
  - Management vyžaduje, schvaluje a podporuje nasazení kontrol, zda zaměstnanci aplikují bezpečnost informací dle zavedených politik a postupů organizace.
- Povědomí, vzdělávání a školení o bezpečnosti informací (Information security awareness, education and training)
  - Provádí se bezpečnostní školení. Při implementaci nových technologií jsou proškoleni ti zaměstnanci, kteří budou technologie používat. Zde je prostor pro zlepšení, neboť dokumentace již není nejnovější.
- Disciplinární řízení (Disciplinary process)
  - V případě narušení bezpečnosti informací řeší disciplinární proces právní oddělení.

3.2.2.3 Ukončení a změna pracovního poměru

- Odpovědnosti při ukončení nebo změně pracovního poměru (Termination or change of employment responsibilities)
  - Při ukončení pracovního poměru přebírá výpověď personální oddělení. Za předání a vrácení aktiv je zodpovědný nadřízený zaměstnance.
  - V případě změny pracovního poměru se například úprava práv provádí ručně, a proto zde představuje riziko lidský faktor.

3.2.3 Řízení aktiv

3.2.3.1 Odpovědnost za rizika

- Seznam aktiv (Inventory of assets)
  - Za aktiva každé země je odpovědný tzv. COM neboli Country Operations Manager. Ten by měl na všechna aktiva dohlížet a udržovat v nich pořádek.

Security manažeři následně provádí kontroly aktiv a nejasnosti konzultují s Country Operations Managery.

- Vlastnictví aktiv (Ownership of assets)
  - Všechna aktiva mají svého vlastníka, který je odpovědný za správu a řízení aktiva.
  - Vlastník aktiv je klíčová osoba, která rozhoduje, jak bude dané aktivum chráněno.
  - Vlastník aktiva by měl zhodnotit důležitost aktiva z pohledu podnikání a informační bezpečnosti a relevantně klasifikovat aktivum. Díky tomu se určí úroveň ochrany. Všechny tyto kroky se mohou konzultovat se Security Managerem.
  - V případě, že odchází zaměstnanec, kterému bylo přiděleno aktivum typu počítač, má možnost počítač odkoupit. Takový počítač je sice přeinstalován, ovšem je použit přednastavený obraz disku, který již obsahuje aplikace určené výhradně pro zaměstnance. Takový počítač by neměl být odprodán zaměstnanci.
- Přípustné použití aktiv (Acceptable use of assets)
  - Uvedeno v tzv. Job description, tedy v dokumentu o popisu práce, který je novému zaměstnanci předložen při podpisu pracovní smlouvy. Jedná se již o interní dokument.
- Vrácení aktiv (Return of assets)
  - Manažer zaměstnance, který opouští organizaci, je zodpovědný za vrácení všech aktiv. Tento krok je stvrzen dokumentem o vrácení aktiv.

3.2.3.2 Klasifikace informací

- Klasifikace informací (Classification of information)
  - Klasifikace informací je popsána v dokumentu „Umbrela document – Group Information Security Standards“. Informace jsou děleny do 4 kategorií na Confidential, Restricted, Internal a Public.
- Označování informací (Labelling of information)
  - Provádí se na základě tabulky níže.

Tabulka č. 1: Klasifikace informací
(Zdroj: Interní dokumentace společnosti ABC)

	Klasifikace informací			
Popis stavů	Veřejné	Interní	S omezeným přístupem	**Důvěrné**
Popis a označení informací	Veřejné nebo (P)	Interní nebo (I)	S omezeným přístupem nebo (R)	**Důvěrné nebo (C)**
Označení dokumentu	Není požadováno	Není požadováno	Na první straně	**Na všech stranách**
Popis stran	Ne	Ne	Formát: číslo strany/počet stran celkem	**Formát: číslo strany/počet stran celkem**
Verzování a stav dokumentu	Ne	Na první straně	Na první straně	**Na první straně**
Popis elektronických dokumentů za využití metadat	Není požadováno	Není požadováno	Doporučeno	**Vyžadováno**
Popis média	Ano	Ne	Pouze úložná média	**Všechna média**

- Manipulace s aktivy
  - Všichni vlastníci a uživatelé aktiv se musí řídit pravidly manipulace s aktivy, která jsou popsána v interním dokumentu „Asset Management Standard“.

3.2.3.3 Manipulace s médii

- Správa výměnných médií (Management of removable media)
  - Společnost provádí zálohy dat na magnetické pásky typu LTO. Data na páskách jsou šifrována a za ukládání záloh na pásky je odpovědné oddělení Storage and backup.
- Přeprava fyzických médií (Disposal of media)
  - Vzhledem k tomu, že některé systémy, které ABC používá, běží v datacentrech, zálohy z těchto systémů se provádí formou uložení do jiného

datacentra. Tím je snížena manipulace s fyzickými médii na minimum, a jsou tedy minimalizována i další spojená rizika jako poškození nebo krádež.

3.2.4 Řízení přístupu

3.2.4.1 Požadavky organizace na řízení přístupu

- Politika řízení přístupu (Access control policy)
  - Vlastník aktiva by měl v kooperaci se Security manažerem definovat přesná pravidla, přístupová práva, restrikce a omezení pro každou uživatelskou roli spolu s určením detailů a kontrol, které reflektují možná bezpečnostní rizika spojená s udělenými právy.
- Přístup k sítím a síťovým službám (Access to networks and network services)
  - Uživatelé by se měli připojovat do firemní sítě pouze s právy a zařízeními, která jim byla přidělena a určena.
  - V rámci organizace každý uživatel dostane podle pracovní pozice přidělen pracovní laptop a pracovní telefon. Dále jsou každému zaměstnanci přidělena specifická práva, na která má nárok.

3.2.4.2 Správa a řízení přístupu uživatelů

- Registrace a zrušení registrace uživatele (User registration and de-registration)
  - Registrační a odregistrační proces pro řízení přístupu uživatele za využití jednoznačných identifikátorů (dále jen ID) v sobě zahrnuje: Použití unikátních ID, okamžité vypnutí a odebrání ID v případě opuštění organizace, periodické kontroly a identifikace ID a případné vypnutí ID, kontroly na zneužití ID jinými uživateli.
  - V rámci organizace je proces odebrání přístupů v případě odchodu zaměstnance kvalitně zpracován. Mírné nedostatky se jeví při změně pracovní pozice v rámci organizace, kdy zaměstnanec dostává práva na nové pozici, ale již mu zpravidla nejsou odebrána práva, kterými disponoval na původní pracovní pozici.
- Zřízení přístupu uživatele (User access provisioning)

- Zřízení nebo odebrání přístupu uživatele je proces, který musí být: schválen nadřízeným uživatele, schválen majitelem aktiva, ověřen, zda úroveň přístupu je adekvátní požadavkům, a změna práv musí být zaevidována.

- Řízení privilegovaných přístupových práv (Management of privileged access rights)
  - Přidělení privilegovaných práv je omezeno jen na vybrané pracovní pozice a kontrolováno v pravidelných cyklech.
  - Stejně jako v předchozím bodě musí být udělení privilegovaných práv schváleno nadřízeným uživatele a majitelem aktiva.
  - V některých případech existuje pouze jeden privilegovaný účet pro celé oddělení a není tak možné sledovat, který z uživatelů provedl změny.
- Řízení tajných autentizačních informací uživatelů (Management of secret authentication information of users)
  - Uživatel nesmí nikomu sdělovat své přihlašovací údaje.
  - Uživatel je povinen změnit si přihlašovací údaje po prvním přihlášení.
- Přezkoumání přístupových práv (Review of user access rights)
  - Majitel aktiva je povinen provádět kontroly přístupových práv v pravidelných cyklech.
- Odebrání nebo úprava přístupových práv (Removal or adjustment of access rights)
  - Odebrání nebo úprava přístupových práv by vždy měla být provedena ke dni ukončení pracovního poměru, změně smluvního vztahu nebo jiné změně, která vyvolá změnu přístupových práv.

3.2.4.3 Odpovědnost uživatelů

- Použití tajných autentizačních informací (Use of secret authentication information)
  - Uživatel je povinen řídit se pravidly organizace o ochraně autentizačních informací. Mezi taková pravidla patří: ochrana uživatelského hesla, nezapisovat heslo do dokumentu nebo na papír, pokud takový dokument nemůže být dostatečně zabezpečen, při odhalení okamžitě změnit heslo, dodržet pravidla na kvalitu hesla.

- Pravidla na kvalitu hesla pro běžného uživatele jsou převzata ze standardu organizace NIST, tedy heslo musí obsahovat minimálně 8 znaků a alespoň 1 malé nebo velké písmeno, číslici a jeden speciální znak (dolar, procento apod.). Více informací o pravidlech pro hesla bude popsáno dále v tabulce č. 2: Systém řízení hesel, která se vztahuje k Řízení přístupu k systémům a aplikacím.

3.2.4.4 Řízení přístupu k systémům a aplikacím

- Omezení přístupu k informacím (Information access restriction)
  - Omezení přístupu k informacím chrání aktiva před nesprávným přístupem bez řádného povolení.
  - Takové omezení se v celé infrastruktuře dodržuje s výjimkou nového ITSM nástroje Hellshare, zde byly nalezeny slabiny v oblasti řízení přístupu, což má za následek nedokonalé omezení přístupu k informacím.
- Bezpečné postupy přihlášení (Secure log-on procedures)
  - Přístup do systémů a aplikací je řízen pomocí zabezpečené přihlašovací procedury.
  - Ve společnosti jsou vysoké požadavky na komplexitu hesel.
  - Hesla se mohou v některých systémech opakovat.
- Systém správy hesel (Password management system)
  - Systém správy hesel je interaktivní a řídí se podle tabulky č. 2, čímž je vždy dosaženo silného hesla.
  - Předchozí bod ovšem neplatí pro hesla do specifických systémů, která se ukládají do nástroje KeyPass. Tento nástroj není vůbec centrálně řízen.

Tabulka č. 2: Systém řízení hesel
(Zdroj: Interní dokumentace společnosti ABC)

Password management system parameter		Domain controllers	DBs	The others (recommended setup)
Minimal length of end user passwords		8 characters	8 characters	8 characters
Minimal length of privilege account passwords		15 characters	15 characters	15 characters
Complexity of end user passwords	sort A - upper case letter (A-Z)	at least one character from at least three	at least one not more than 4 same characters	at least one character
	sort B - lower case letter (a-z)			at least one character

	sort C - numbers (0-9)	sorts (A, B, C or D)	at least one character	at least one character
	sort D - non-alphanumeric characters (e.g. !, $, *, +, /, -, …)			
	Complexity checking	enabled	enabled	enabled
Password regular change period[1]		90 days	90 days	90 days
Previously used password prevention		10 previous passwords		7 previous passwords
Minimal password life time		1 day	not used	1 day
Force end users to change password at the first log-on		enabled	disabled	enabled
Number of unsuccessful log-ons to lock the account		5 attempts	/	5 attempts
Time when automatically locked account be unlocked		60 minutes		30 minutes

- Použití privilegovaných obslužných programů (Use of privileged utility programs)
  - Obslužné programy ve společnosti existují, ale pravomoc s nimi pracovat má jen velmi úzká skupina proškolených specialistů.
  - Z těchto programů se samozřejmě vedou logy, neboť se jedná o silné nástroje, které dokážou napáchat nemalé škody.
- Řízení přístupu ke zdrojovému kódu programu (Access control to program source code)
  - Přístup ke zdrojovému kódu programů je striktně kontrolován, aby se zamezilo nevyžádaným funkcionalitám programů.

3.2.5 Kryptografie

3.2.5.1 Kryptografická opatření

- Politika použití kryptografických opatření (Policy on the use of cryptographic controls)
  - Kryptografická opatření se používají napříč organizací na většině zařízení. Největší důraz na šifrování zařízení s úložištěm je kladen na zařízení, která opouští perimetr organizace.
  - Šifrování se rovněž používá pro komunikaci.

- Správa klíčů (Key management)
  - Správa klíčů je postavena na dohodnutých standardech, procedurách a zabezpečovacích metodách, které zajišťují kvalitní zabezpečení po celou dobu životnosti.

3.2.6 Fyzická bezpečnost a bezpečnost prostředí

Fyzická bezpečnost je oblast, kterou se organizace zabývá pouze částečně. Proto tato oblast a její nedostatky nebudou zahrnuty v návrhu opatření.

3.2.6.1 Zabezpečení oblasti

- Fyzický bezpečnostní perimetr (Physical security perimeter)
  - Ochrana perimetru je řešena pomocí vstupových karet. Každý zaměstnanec má svoji kartu a nese za ni odpovědnost.
  - Majetek a vybavení společnosti disponuje adekvátní fyzickou ochranou, například zámky na všech skřínkách.
  - Systémy uchovávající citlivé nebo kritické informace jsou chráněny, aby se zabránilo neoprávněnému přístupu.
- Fyzické kontroly vstupu (Physical entry controls)
  - Jak bylo v předchozím bodu zmíněno, fyzická ochrana před vstupem do společnosti je řešena pomocí vstupových karet. Jiné kontroly se zde neprovádí. Jsou zde oddělené recepce. Vstup do kanceláří společnosti je kontrolován separátním systémem se vstupovými kartami.
- Zabezpečení kanceláří, místností a vybavení (Securing offices, rooms and facilities)
  - Za klíče od všech kanceláří a místností, které musí být zabezpečeny, jsou odpovědné Office Administrátorky. V případě, že chce některý ze zaměstnanců navštívit jednu z uzamčených místností, Office Administrátorka je povinna navštívit místnost s ním.
- Ochrana před vnějšími a přírodním hrozbami (Protecting against external and environmental threats)

- Za tento bod nese odpovědnost majitel budovy, kde společnost sídlí. Majitel je rovněž odpovědný za fyzické zabezpečení přístupu do budovy. Dále je odpovědný za splnění všech bezpečnostních norem pro vznik požáru, živelních hrozeb či jiných událostí. Majitel budovy je rovněž odpovědný za dodávku běžných potřeb, jako je teplo, voda, plyn, odvětrávání či klimatizace a podobných věcí či služeb. Společnost ABC se nachází v zabezpečené části budovy a řeší tedy jen zabezpečení uvnitř svého prostoru.

- Práce v zabezpečených oblastech (Working in secure areas)
  - Všichni zaměstnanci jsou školeni na BOZP. V rámci školení jsou všichni zaměstnanci informováni o nebezpečích a nástrahách, se kterými se můžou ve společnosti potkat.
- Oblasti pro nakládku a vykládku (Delivery and loading ares)
  - Společnost se tímto bodem nezabývá. Vzhledem k oblasti podnikání tyto oblasti nepotřebuje.

3.2.6.2 Zařízení

- Umístění zařízení a jeho ochrana (Equipment siting and protecting)
  - Vzhledem k zaměření společnosti se v prostorách nenachází mnoho nebezpečných zařízení či zařízení, která mohou poškozovat životní prostředí.
  - Servery jsou v datacentrech a přístup je řešen dle pravidel a norem datacentra.
- Podpůrné služby (Supporting utilities)
  - Společnost vlastní záložní zdroje, které v případě výpadku elektřiny udržují kritická zařízení v běhu po nezbytně nutnou dobu.
  - V případě výpadku internetových služeb má společnost zavedenou záložní linku.
- Bezpečnost kabelových rozvodů (Cabling security)
  - Jakýkoliv síťový prvek určený pro připojení koncového zařízení do interní sítě je chráněný vůči fyzického přístupu.
- Bezpečnost zařízení a aktiv mimo prostory organizace (Security of equipment and assets off-premises)
  - Všichni zaměstnanci se musí řídit nařízením o způsobu chování na veřejných sítích a to tak, že nesmí sdílet žádné informace o organizaci a jejím podnikání.

- V případě služebních cest se zaměstnanci musí řídit interním dokumentem o způsobu chování se k aktivům mimo organizaci, jako je laptop, telefon, způsob komunikace (VPN apod.)
- Tato pravidla jsou v organizaci dobře nastavena a komunikována s každým, koho se týkají.

- Bezpečná likvidace nebo opakované použití zařízení (Secure disposal or re-use of equipment)
  - Veškeré počítače nebo jiná zařízení s paměťovým médiem jsou při vyřazení naformátována tak, aby nemohlo dojít k pozdějšímu čtení z těchto paměťových médií.
  - V případě poškozených nebo vyřazených paměťových médií je likvidace řešena prostřednictvím specializované společnosti.
- Neobsluhovaná uživatelská zařízení (Unattended user equipment)
  - Uživatel je povinen zabezpečit své zařízení před nežádoucím zneužitím jinou osobou v případě nepřítomnosti u uživatelského zařízení.
- Zásada prázdného stolu a prázdné obrazovky monitoru (Clear desk and clear screen policy)
  - Veškeré citlivé a kritické informace v papírové formě nebo na paměťovém médiu by měly být uzamčeny v bezpečném prostoru (např. ve skříncе nebo v trezoru). Počítače, servery a podobná zařízení by měly být v odhlášeném nebo zamčeném stavu, aby nedošlo k neoprávněnému použití. Ovšem po pracovní době lze na stolech zaměstnanců často nalezneme dokumenty, které lze klasifikovat jako citlivé.

3.2.7 Bezpečnost provozu

3.2.7.1 Provozní postupy a odpovědnosti

- Dokumentace provozních postupů (Documented operating procedures)
  - Manažeři jednotlivých oddělení jsou zodpovědní za definování procedur, které musí být zadokumentovány v interní KB neboli Knowledge Base, tedy znalostní databázi společnosti.

- Interní dokumentace není vždy aktualizovaná a v některých případech chybí úplně. Je to způsobeno vytížeností vlastníků aktiv, kteří za dokumentaci odpovídají, anebo rychlým vývojem v oblasti informačních technologií.
- Operativní týmy jsou kontrolovány pomocí tiketů, které jsou obsluhovány ITSM (IT Service Management) nástrojem.

- Řízení změn (Change management)
  - V rámci organizace je zvolen Change Manager, který je zodpovědný za všechny změny. Veškeré navržené změny jsou každý týden ve stanovený den prodiskutovány a případně schváleny a komunikovány všem zaměstnancům.
  - Change Manager definuje pravidla pro testování, verifikaci potřeb IT bezpečnosti a zpětné procedury pro návrat do bodu před změnou.
- Řízení kapacit (Capacity management)
  - Řízení kapacit je kontrolováno dle standardu ITIL, kterým se řídí celá organizace. Proces je nastaven tak, aby se vyhnulo jakýmkoliv výpadkům technických, lidských nebo informačních zdrojů.
- Princip oddělení prostředí vývoje, testování a provozu (Separation of development, testing and operational enviroments)
  - IT operativa je oddělena od vývojové a testovací části. Vývoj a testování jsou prováděny na rozdílném technickém řešení s pomocí jiných osob než v operativním oddělení.

3.2.7.2 Ochrana před malwarem

- Opatření na ochranu proti malwaru (Controls against malware)
  - Antivirová ochrana na koncových stanicích je řešena pomocí programu McAfee. Ve společnosti jsou zaměstnáni bezpečnostní specialisté, kteří jsou dále zaměřeni na koncové stanice a servery, počítačové sítě nebo e-mailovou komunikaci.
  - Část uživatelů jsou lokálními administrátory na svých počítačích a mohou si instalovat, co chtějí. Nejsou omezeni pouze na instalaci schváleného softwaru.

3.2.7.3 Zálohování

- Zálohování informací (Information backup)
  - Ve společnosti jsou stanovena pravidla a procedury, jakým způsobem, v jakých cyklech, jaká data a na jakých zařízeních se budou zálohovat. K těmto účelů je v ABC dedikovaný specializovaný tým „Storage and Backup".

3.2.7.4 Zaznamenávání formou logů a monitorování

- Zaznamenávání událostí formou logů (Event logging)
  - Logy z různých zařízení jsou zaznamenávány do systému.
  - Operativní a technická oddělení mají stanovené procedury, jak s tímto systémem a logy ze všech zařízení zacházet.
- Ochrana logů (Protection of log information)
  - Systém pro práci s logy plní funkci ochrany logů. Každý oprávněný uživatel je nucen přihlásit se svými přihlašovacími údaji.
- Logy o činnosti administrátorů a operátorů (Administrator and operator logs)
  - Všechny akce a změny administrátorů a operátorů jsou zaznamenány do logů.
  - Podle interní dokumentace by se kontroly logů měly provádět v pravidelných intervalech.
- Synchronizace hodin (Clock synchronization)
  - Pro správné pochopení logů je synchronizace hodin klíčový faktor. Proto jsou všechny zdroje hodin definovány ve firemní znalostní databázi (Knowledge Base, dále jen KB).

3.2.7.5 Řízení a kontrola provozního softwaru

- Instalace softwaru na provozních systémech (Installation of software on operational systems)
  - Pro instalaci softwaru na provozních systémech jsou využity procesy change managementu a release managementu.
  - Instalace softwaru na provozních systémech, která není schválena v rámci change managementu, je striktně zakázaná.

3.2.7.6 Správa a řízení technických zranitelností

- Správa a řízení technických zranitelností (Management of technical vulnerabilities)
  - Technické zranitelnosti jsou analyzovány specialisty a případně konzultovány s bezpečnostním oddělením. Záplaty na tyto zranitelnosti jsou testovány, schváleny a následně implementovány.
  - Na firewallech lze dohledat mnoho pravidel, která již nejsou využívána. Chybí proces kontroly pravidel.
- Omezení instalace softwaru (Restrictions on software installation)
  - Právo instalovat software v provozním IT prostředí by mělo být omezeno na vedoucí pozice provozních a technických týmů. Instalace softwaru by měla být řízena v rámci změny nebo podle oficiálního procesu.
  - Nikdo z uživatelů není oprávněn instalovat si žádný jiný software než ten schválený. Všechen schválený software podporovaný dedikovaným týmem naleznou uživatelé v aplikaci „Software Center“.
  - Skutečnost je taková, že techničtí specialisté pracující na druhé a třetí úrovni podpory mají kromě klasického účtu ještě privilegovaný účet, pomocí kterého jsou schopni instalovat aplikace na svá lokální zařízení. Této možnosti často využívají a instalují si neschválený software.

3.2.7.7 Hlediska auditu informačních systémů

- Opatření k auditu informačních systémů (Information systems audit controls)
  - Během auditů se musí dodržovat stanovená pravidla, která nijak neomezí provoz infrastruktury.
  - Způsob provedení auditu nebo technických testů musí být schválen osobou odpovědnou za skupinu IT Operations.
  - Požadavky auditu na přístupy do systémů a k datům musí být schváleny odpovědnými týmy.
  - Audity by se měly provádět pouze formou read-only neboli pouze čtením dat či přístupem do systému.

- V případě auditů a testů, které mohou mít vliv na dostupnost služby, je nutno provádět tyto akce mimo běžnou pracovní dobu. Všechny zainteresované strany musí být informovány.
- Po skončení auditu nebo technických testů musí být ihned zakázány účty, které byly pro tento účel vytvořeny.

3.2.8 Bezpečnost komunikací

3.2.8.1 Správa bezpečnosti sítě

- Opatření v sítích (Network controls)
  - Opatření v sítích jsou definována vedoucími síťovými specialisty. Podle těchto definic jsou sítě řízeny a spravovány.
  - Chybí zde ovšem pravidelné kontroly například na firewallech.
  - Síťoví specialisté disponují nástroji určenými ke kontrolám síťových prvků.
  - Byly nalezeny procesní nesrovnalosti při vytváření pravidel na firewallech.
- Bezpečnost síťových služeb (Security of network services)
  - Síťové prvky jsou nastaveny podle vhodných bezpečnostních mechanismů a nástrojů, aby se na těchto síťových prvcích daly provádět bezpečnostní kontroly.
  - Všechna vzdálená připojení by měla být schválena IT Security Operational Managerem. Veškerá komunikace musí být šifrovaná, a to nejen vzdálená připojení, ale i všechny bezdrátové sítě.
  - Bezdrátové sítě jsou vhodně zabezpečeny, aby se předešlo nepovolenému přístupu.
  - Záložní linka je řešena pomocí DMVPN. Poskytovatelem tohoto připojení je O2.
- Princip oddělení v sítích (Segregation in networks)
  - Síť je rozdělena na virtuální lokální sítě známé jako VLAN. Toto rozdělení silně zvyšuje zabezpečení a snižuje broadcastovou doménu.
  - Každá lokální síť má přidělený rozsah podsítě.

3.2.8.2 Přenos informací

- Politiky a postupy při přenosu informací (Information transfer policies and procedures)
  - Přenos mezi zařízeními bývá téměř vždy šifrovaný.
  - Elektronická komunikace je kontrolována před malwarem. Provádí se automatické kontroly všech příloh.
  - Při úniku dat, vyzrazení informací nebo jiné bezpečnostní události je zaměstnancům doručena zpráva o přijetí vhodných opatření.
  - Uživatelé obchází politiky, které zakazují kopírování textu například na firemních telefonech, tak, že si text přepošlou na svůj osobní e-mail a odtud ho zkopírují.
- Elektronické předávání zpráv (Electronic messaging)
  - Elektronické předávání zpráv probíhá nejčastěji formou e-mailů nebo instant messagingu. Tyto typy zpráv jsou všechny důkladně analyzovány před hrozbami.
  - Jsou povolené vybrané nástroje pro komunikaci v rámci organizace (Teams, Outlook, Skype etc.) a vně organizace (Yammer), ostatní nejsou povolené. Uživatelé si pak mohou přečíst přesná pravidla používání elektronického předávání zpráv v interním dokumentu „End user Security Standard“.
- Dohody o důvěrnosti nebo mlčenlivosti
  - Každý zaměstnanec je povinen podepsat dohodu o odpovědnosti a dále souhlas o ochraně osobních údajů sestavené na základě 101/2000 Sb. Nesmí tedy vynášet informace, které by mohly jakýmkoliv způsobem poškodit společnost či její podnikání.

3.2.9 Akvizice, vývoj a údržba systému

3.2.9.1 Bezpečnostní požadavky informačních systémů

Vzhledem k tomu, že bezpečnostní tým dozoruje a případně upravuje procesy projektového managementu, aby byly splněny bezpečnostní normy, jsou zahrnuty bezpečnostní požadavky v analýzách nových systémů nebo na úpravu stávajících systémů.

Všechny systémy podléhají tzv. golden image, tedy jakémusi perfektnímu modelu systému, na který jsou následně nabalovány další balíky dle potřeby. Tyto systémy rovněž podléhají pravidelným kontrolám, tzv. hardeningu.

Systémy jsou pravidelně udržovány formou tzv. patch waves a skenů.

Bezpečnostní požadavky zahrnují jednoznačnou identifikaci a autorizaci koncového uživatele (bez rozdílu, zda se jedná o interního, nebo externího uživatele).

- Veškeré přístupy jsou upraveny podle Access Control policy v bodě 3.2.4.1.
    - Řeší se diverze účtů na skupiny: standardní, privilegovaný a technický/servisní účet.
    - Zaměstnanci jsou obeznámeni s tím, jak tyto druhy účtů používat.

3.2.9.2 Bezpečnost v procesech vývoje a podpory

- Postupy řízení změn systémů (System change control procedures)
    - Tyto postupy jsou definovány a řízeny Change Managerem. Tento manažer se postupy musí řídit a následně musí změnu nechat schválit.
    - Tento proces by měl zahrnovat posouzení rizik, analýzu dopadů změn a specifikaci nutných opatření.
- Technické přezkoumání aplikací po změnách provozní platformy (Technical reviw of applications after operating platform changes)
    - V rámci organizace probíhají změny provozního softwaru jen minimálně. Organizace se tak snaží zamezit jakýmkoliv nepříznivým dopadům na provoz nebo bezpečnost organizace. Řídí se tak pravidlem „neměň to, co funguje“. V případě, že je taková změna nutná, musí být přezkoumány a otestovány aplikace kritické pro činnost organizace.
- Vývoj zajišťovaný externími zdroji (Outsourced development)
    - Ta část vývoje, která je řešena externími dodavateli, je kontrolována pověřenými osobami z ABC. Dané osoby následně musí kontrolovat vývoj, zda splňuje všechny bezpečnostní požadavky.
- Testování bezpečnosti systému (System security testing)

- Všechny systémy jsou testovány před uvedením do provozu, viz. Bod 3.2.9.1 Bezpečnostní požadavky informačních systémů.

- Testovací akceptace systému (System acceptance testing)
  - Testovací akceptace systémů je zahrnuta v rámci Proof of Concept (POC), která je součástí řízení projektu v oblasti projektového managementu.

3.2.10 Vztahy s dodavateli

3.2.10.1 Bezpečnost informací ve vztazích s dodavateli

- Politika bezpečnosti informací pro oblast vztahů s dodavateli (Information security in supplier relationships)
  - Dodavatelé mají pouze nezbytně nutný přístup do systémů, aby byla zajištěna maximální možná bezpečnost informací. Další podmínky v rámci bezpečnosti informací upravují smluvní podmínky.
- Řešení bezpečnosti v rámci smluv s dodavateli (Addressing security within supplier agreemets)
  - Řeší se formou TOM (Technical and Organizational measures) dokumentů. Součástí jsou: soulad s GDPR, technická a netechnická opatření, práva a povinnosti atd.
- Řetězec dodavatelů informačních a komunikačních technologií (Information and communication technology supply chain)
  - Obsah tohoto bodu je zahrnut v bodě předchozím.
  - Společnost ABC má smluvně ošetřeny procesy a postupy s dodavateli služeb v oblasti ICT. V případě poruchy služby, kterou má na starosti dodavatel, je stanoveno, dokdy musí dodavatel poslat notifikaci o poruše a dokdy musí vyřešit závadu. Dále je dohodnut způsob komunikace a předávání informací. Tento způsob komunikace musí odpovídat bezpečnosti informací.

3.2.10.2 Řízení dodávky služeb dodavetelem

- Monitorování a přezkoumávání služeb dodavatelů (Monitoring and review of supplier delivery)

- Monitorování služeb probíhá na denní bázi, neboť poskytované služby (např. informační systém, síťové připojení atd.) jsou neustále monitorovány a používány zaměstnanci.
- Přezkoumání služeb probíhá vždy na konci smluvního období, nebo v průběhu smluvní doby v případě častých problémů se službou.

- Řízení změn služeb dodavatelů (Managing changes to supplier services)
  - Provádí se na základě přezkoumání služeb.

3.2.11 Řízení incidentů bezpečnosti informací

3.2.11.1 Řízení incidentů bezpečnosti informací a zlepšování

- Odpovědnosti a postupy (Responsibilities and procedures)
  - Odpovědnosti a postupy při řízení incidentů bezpečnosti informací a zlepšování jsou popsány v interním dokumentu „Information security incident response standard“. Dokument obsahuje RACI matici, kde lze přehledně vidět jednotlivé odpovědnosti v případě bezpečnostního incidentu.

Tabulka č. 3: RACI matice odpovědností a postupů v případě bezpečnostního incidentu
(Zdroj: Interní dokumenty společnosti ABC)

RACI table[1]	Security Operation	Asset owner/s	Operations Manager/s	DPO (Data Protection Officer)	Security Operation	ABC
First assessment of reported event or weakness	A/R					
Detail assessment and preparation of response plan	A/R	C	C	C	I	

Decision on less serious information security incident	A/R	C	C/I	C/I		
Decision on serious	R	A/R	C	C	C	
Decision on critical	R	R	A/R	C	R	C
Response on information security incident	R	R	I	A/C	I	
Lesson learn	R	R	R	C/I	A/R	C/I
Collect the evidence	R	R	R	C/I	A/R	C/I

- Podávání zpráv o událostech bezpečnosti informací (Reporting information security events)
  - Podávání zpráv o událostech bezpečnosti informací by mělo být prováděno, co nejdříve to je možné a za využití dohodnutého komunikačního nástroje (e-mail).
- Podávání zpráv o slabých místech bezpečnosti informací (Reporting information security weaknesses)
  - Zaměstnanci jsou povinni podat zprávu o slabých místech bezpečnosti informací. Standardní postup pro oznámení takovéto situace je vytvoření tzv. tiketu a přidělení takového tiketu na bezpečnostní oddělení nebo poslání e-

mailu s popisem slabého místa. Dále se také může zavolat na Service Desk anebo zavolat na tzv. „Security hotline“.

- Posuzování a rozhodování o událostech bezpečnosti informací (Assessment of and decision on information security events)
  - Rozhoduje Security Manager.
- Ponaučení z incidentů bezpečnosti informací (Learning from information security incidents)
  - Na základě vyhodnocení incidentu vyhotoví bezpečnostní manažer zprávu, ve které uvede, jaké kroky musí být provedeny, aby se incident neopakoval.
- Shromažďování důkazů (Collection of evidence)
  - V organizaci jsou definovány procedury pro shromažďování důkazů. Každý, koho se bezpečnostní incident týká, je povinen vypracoval protokol o takové události.

3.2.12 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

3.2.12.1 Kontinuita bezpečnosti informací

- Plánování kontinuity bezpečnosti informací (Planning information security continuity)
  - Vše běží na základě PDCA cyklu.
- Implementace kontinuity bezpečnosti informací (Implementing information security continuity)
    - V současné době probíhá ve společnosti implementace kontinuity bezpečnosti informací tak, aby byla zaručena business continuity.
- Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací (Verify, review and evaluate information security continuity)
    - Je součástí PDCA cyklu (C – Control).

3.2.13 Soulad s požadavky

3.2.13.1 Soulad se zákonnými a smluvními požadavky

- Identifikace příslušné legislativy a smluvních požadavků (Identification of applicable legislation and contractual requirements)
  - Pro tento účel využívá společnost ABC právní oddělení mateřské společnosti.
- Práva k duševnímu vlastnictví (Intellectual property rights)
  - Informace nebo software třetích stran chráněné autorskými právy nesmí být používány ani ukládány v rozporu s právy duševního vlastnictví.
- Ochrana záznamů (Protection of records)
  - Záznamy musí být bezpečně chráněny před ztrátou, zničením a poškozením dle místních zákonů a regulačních požadavků.
- Soukromí a ochrana osobních údajů (Privacy and protection of personally identifiable information)
  - Všichni zaměstnanci, kteří pracují s osobními údaji, musí být proškoleni dle platné legislativy. Dále byla zavedena technická a organizační opatření tak, aby rovněž splňovala legislativu.
- Regulace kryptografických opatření (Regulation of cryptographic controls)
  - Pro účely ochrany jsou zvoleny takové kryptografické nástroje a protokoly, aby byla zajištěna maximální ochrana informací. Šifrování se provádí nejen při přenosech dat, ale také pro ochranu dat na pevných discích v počítačích a mobilních telefonech.

3.2.13.2 Přezkoumání bezpečnosti informací

- Nezávislé přezkoumání bezpečnosti informací (Independent review of information security)
  - Ve společnosti se provádí interní i externí (nezávislé) audity.
- Soulad s bezpečnostními politikami a normami (Compliance with security policies and standards)
  - Soulad s bezpečnostními politikami a normami zkoumá bezpečnostní oddělení ve společnosti ABC. V případě nálezu podá odpovědné osobě výzvu na opravu.
- Přezkoumání technického souladu (Technical compliance review)
  - V organizaci jsou prováděny penetrační testy, které by měly odhalit případný technický nesoulad.

- V ABC se dále provádí interní testy zranitelnsoti (vulnerability), konfigurační testy (compliance), aby byla zaručena tzv. hardening security baseline.

4 VLASTNÍ NÁVRHY ŘEŠENÍ

Na základě analýzy současného stavu, která byla provedena podle normy ISO/IEC 27002, budou v této části diplomové práce popsány nálezy a následně navržena řešení. Taková řešení by nadále neměla být v rozporu s již zmíněnou normou. Forma řazení nálezu je nastavena stejně jako u analýzy, tedy řídí se od nejnižších kapitol normy.

4.1 Bezpečnost lidských zdrojů

Úroveň bezpečnosti lidských zdrojů je ve společnosti velmi kvalitní. Nálezy vztahující se k této oblasti se netýkají samotné společnosti. Nález souvisí s činností třetí strany, ovšem její počínání může mít následný dopad na samotnou společnost ABC.

4.1.1 Prověřování

Prověřování spadá podle normy pod kapitolu bezpečnost lidských zdrojů. Samotné prověřování se týká oblasti před vznikem pracovního poměru.

Nález: Společnost ABC před vznikem pracovního poměru provádí prověřování kandidátů, zda informace uvedené v jejich životopisech jsou pravdivé. Ovšem tato společnost využívá i služeb náborářských agentur, neboť sama není schopna efektivně nabírat tolik kvalifikovaných specialistů. Náborářské agentury jsou následně odměňovány za každého specialistu, kterého ony doporučí a uplyne jeho zkušební doba. Podle dostupných informací ovšem prověřování ze strany agentur není dostatečně kvalitní.

Návrh: Upravit smluvní podmínky mezi společnostní ABC a náborářskou agenturou tak, že k dokumentům, které o uchazeči obvykle předává, by přidala ještě výsledek prověření uchazeče.

4.2 Řízení aktiv

Řízení aktiv probíhá ve společnosti přehledně. Každé aktivum má svého vlastníka, a i při velkém množství aktiv je téměř vždy jasné, kdo za co odpovídá.

4.2.1 Vlastnictví aktiv

Každé aktivum, které se ve společnosti nachází, má svého vlastníka aktiv (tzv. Service Owner) případně odpovědnou osobu. Proto při prvotní analýze se jeví řízení aktiv jako bezchybné. Až po podrobnější analýze a konzultaci se specialisty byl objeven mírný nedostatek.

Nález: V případě, že chce zaměstnanec, se kterým byla společnost spokojena, opustit společnost ABC, je mu nabídnuta možnost odkupu počítače, který používal. Do této chvíle je vše naprosto v pořádku a neodporuje to žádným pravidlům. Počítač je následně přeinstalován, aby na disku nezůstala žádná firemní data. Ovšem pro účel reinstalace se používá připravený obraz disku (tzv. image, pozn. autora), který je používán pro firemní účely. V důsledku toho jsou na nainstalovaném operačním systému předinstalovány programy, které by odcházející zaměstnanec již neměl mít k dispozici. Jedním z takových programů je Endpoint security neboli antivirová ochrana na koncovém zařízení. Nejen, že tato ochrana čerpá licenční klíče, ale také zůstává zobrazena bezpečnostním specialistům v systému pro správu antivirové ochrany. Vzhledem ke způsobu reinstalace se rovněž čerpá interní licence na operační systém. Přitom všechny používané počítače jsou nakupovány s tzv. OEM licencí. Mezi další předinstalované programy lze zařadit například kancelářských balík Microsoft Office nebo jiné specifické programy, které uživatel potřeboval k výkonu své práce. I zde dochází ke zbytečnému čerpání licencí a tedy plýtvání finančními prostředky organizace.

Návrh: Pro tento účel by bylo plně dostačující stáhnout „čistý“ ISO soubor s poslední verzí operačního systému Windows přímo z oficiálních stránek společnosti Microsoft (stažení je zdarma, pozn. autora) a následně provést instalaci na počítač, který bude odprodán končícímu zaměstnanci. Tato akce by měla vyřešit všechny výše zmíněné nálezy. Čistý operační systém nebude obsahovat žádné programy společnosti, a rovněž bude využívat OEM licenci pro operační systém, která se již na zařízení nachází.

4.3 Řízení přístupu

Řízení přístupu je jednou z problematičtějších oblastí. Na základě analýzy zde bylo učiněno několik nálezů. Tyto nálezy nejsou nijak kritické, ale společnost by měla některé nálezy ošetřit.

4.3.1 Zřízení přístupu uživatele

Nález: V případě, že se organizaci chystá opustit některý ze zaměstnanců, je spuštěn proces, při kterém jsou odebrána veškerá práva a vrácena všechna aktiva. Tento proces funguje dobře a správně a za každou část procesu někdo odpovídá. Pro tento proces využívá společnost nástroj nazvaný E-Management. Problém nastává ve chvíli, kdy zaměstnanec v rámci organizace změní pracovní pozici. Obvyklý proces probíhá tak, že po přijetí zaměstnance do nového týmu, mu přidělí nová práva (většinou v adresáři Active Directory) jeho nový manažer. Opomíjí se ovšem odebrání přístupových práv, kterými zaměstnanec disponoval v předchozím týmu. V případě dlouhodobé ignorace akumulace těchto oprávnění může mít přímý dopad na Access Management (neboli řízení přístupu).

Návrh: Pro účel změny pracovní pozice v rámci organizace se jeví jako nejvhodnější řešení vytvoření nového procesu pomocí nástroje E-Management. Takový nástroj je v rámci organizace zavedený. Jednalo by se o zjednodušený proces odchozího zaměstnance, kde jediným předmětem procesu by byla úprava přístupů a práv.

Alternativním řešením tohoto nálezu může být vytvoření tiketu zaměstnancem v systému Hellshare. Odpovědná osoba pak přístupy upraví. Je potřeba, aby se daný tiket rozdělil na dva další podúkoly, kdy jeden úkol zaměstnanci práva a přístupy odebere a další úkol přidá. Zpravidla tento krok nemůže provézt jedna osoba.

Rozšíření návrhu: Zavedení pravidelných přístupů inicializovaných z pozice vlastníka aktiv. Díky tomu bude dosaženo přehlednějšího stavu přístupů.

4.3.2 Řízení privilegovaných přístupových práv

Nález: V mnoha týmech lze nalézt několik nástrojů, pro které existuje pouze jeden účet. Z toho důvodu pak nelze přesně dohledat, který z uživatelů provedl určité změny. V důsledku toto nastává problém s vedením logů o změnách v systémech.

Návrh: V případě, že to technologie neumožňuje, mělo by být řešeno pomocí Priviledge Access Managementu tak, aby byla zajištěna nepopiratelnost.

4.3.3 Omezení přístupu k informacím

Nález: Omezení přístupu k informacím je ve společnosti řešeno velmi dobře, až na jeden případ. V rámci celé organizace s pobočkami po celém světě byl před téměř jedním rokem implementován nový tiketovací systém. Tento systém slouží pro účel ITSM neboli Information Technology Service Management. Oproti předchozímu řešení je vidět pokrok v mnoha směrech. Nový nástroj poskytuje přehledný dashboard, který si každý může upravovat podle svých potřeb. Existuje zde spousta možností pro optimalizaci procesů. V rámci nástroje lze procházet i interní dokumentaci. Společnost do současné chvíle používala svojí interní znalostní databázi, kterou nazývá KB (Knowledge Base), a v současné době se pracuje na migraci této databáze právě do nástroje Hellshare. V novém nástroji jsou rovněž přehledně vidět veškeré logy. Ovšem při zadávání projektu na nový nástroj ITSM bylo mezi požadavky uvedeno převzetí přístupových práv ze starého nástroje. A právě zde tkví jádro problému, neboť starý nástroj žádné řízení práv neměl. Nový nástroj řízení práv sice umožňuje, ale v současnou chvíli není nijak řízen a platí tedy, že každý, kdo má do systému přístup, vidí na veškeré tikety. A to je ten největší problém. Protože do systému mají přístup nejen všichni zaměstnanci v rámci celé organizace, která čítá téměř 60 tisíc zaměstnanců, ale i externí strany typu poskytovatelé připojení na internet, externí specialisté pracující s nástroji typu SAP apod. Možná v tuto chvíli může vyvstat otázka, proč právě v této podkapitole je popisován tento problém, který spíše souvisí s řízením přístupu. Ovšem jedná se o problematiku, která spadá podle ISO/IEC 27002 pod stejnou kapitolu (kapitola č. 9 Řízení přístupu) a autor nevidí největší problém, že všichni klíčoví uživatelé tohoto nástroje vidí všude v rámci nástroje, ale že mají přístup k informacím, které lze naleznout v obsahu všech tiketů. Takové zneužití

informací může mít přímý dopad na organizaci. Příklad takové modelové situace je popsán v následující kapitole.

Uživatel je zaměstnancem společnosti na pozici marketingový specialista. Potřebuje rozšířit velikost e-mailové schránky a založí si tiket. Vzhledem k tomu, že od následujícího dne jede na týdenní dovolenou, do tiketu uvede žádost o zvětšení velikosti mailboxu, a aby to měl vyřízené, než se vrátí z dovolené, uvede i informace, jako je uživatelské jméno, název počítače a samozřejmě jeho přihlašovací heslo. Takový jev se stává a nikdy tomu nelze 100 % zabránit. Lidi můžou být na takové věci školeni pořád, ale vždy se někdo takový najde. Tiket je vytvořen a čeká na zpracování ve frontě lokální podpory (lokální Service Desk). Mezitím se připojí externí strana. Vzhledem k tomu, že externích stran je v rámci celé nadnárodní organizace opravdu velké množství, může se stát, že právě jedna z externích stran může být napadena, a díky přístupu má tedy přístup i do ITSM nástroje. Útočník, který má přístup do ITSM nástroje, si už velmi snadno vyfiltruje všechny tikety, které například obsahují klíčové slovo „password“. V tuto chvíli se mu naskytuje mnoho možností, jak takové situace využít. Pokud je záškodník jen trochu strategicky založený, pak bude například dlouhodobě tahat data, která posléze může například prodat konkurenci. V případě krátkozrakosti útočníka provede tzv. Inside attack, který může provést na více místech zároveň. Takových vnitřních útoků už se pak nabízí celá řada, počínaje phishingovou kampaní (která může být díky ověřenému odesílateli v rámci organizace velmi úspěšná) a konče například ransomwarem.

Návrh: Úkolem každého bezpečnostního manažera by mělo být zavedení takových opatření, která sníží rizika pod úroveň přijatelného rizika. Jedná se o stav, kde se protíná křivka nákladů na opatření a křivka dopadu rizik. Takový bod je nazýván přiměřená bezpečnost (viz obrázek č. 8).

V případě tohoto nálezu můžeme však ošetřit velké riziko, a to s pouze minimálními náklady vzhledem k tomu, že ITSM nástroj podporuje řízení přístupu. Řízení přístupu by tedy mohlo být v rámci nástroje děleno do několika kategorií tak, aby externí strany neviděly nikam jinam než do tiketů, kam mají mít přístup. Tímto drobným opatřením lze předejít velkým škodám, které by jinak mohly být způsobeny.

4.3.4 Bezpečné postupy přihlášení

Nález: Ve společnosti jsou vysoké požadavky na komplexitu hesel. Takové silné heslo pak ovšem daný uživatel opakuje i v jiných systémech, kde je vyžadováno další heslo. To může vést k situaci, kdy odhalení hesla v jednom systému může mít dopad na všechny systémy, ve kterých bylo použito stejné heslo daného uživatele.

Návrh: Pro tento účel může být využito přístupových karet (tzv. badge), které zaměstnanci používají pro vchod do budovy. Vzhledem k tomu, že většina zaměstnanců používá laptopy od společnosti Dell, disponuje část zaměstnanců i čtečkou karet, která je právě integrována v některých laptopech zmíněné značky. Díky kartě by se zaměstnanec mohl snadno autentizovat do operačního systému, ale i do dalších nástrojů. Alternativou tohoto řešení by pak byly jiné kryptografické prostředky či tokeny, pomocí kterých by se uživatelé přihlašovali. Ovšem z pohledu nákladů se jeví využití vstupových karet jako nejvhodnější.

Nález č. 2: Některé jednoduší nástroje, které se v organizaci používají a zároveň nejsou napojeny na Active Directory, nepožadují komplexitu hesla. Příkladem takového nástroje je docházkový systém. Ten jako defaultní nastavení pro každého uživatele nastaví uživatelské identifikační číslo (ID) nejen jako přihlašovací jméno, ale i jako heslo. Uživatelské ID lze snadno dohledat v Active Directory. Takový stav by nepředstavoval takové riziko v případě, kdy by docházkový systém po prvním přihlášení vynucoval změnu hesla (ostatně jak je tomu u přihlášení ve většině jiných systémů), ovšem v tomto případě taková změna není vynucena. Pokud si tedy uživatel heslo nezmění, záškodník se může jeho přihlašovacími údaji přihlásit do docházkového systému a upravit docházku. Tento jev už má přímý finanční dopad na poškozeného uživatele. Ovšem i organizace by mohla utrpět. Byť ne z finančního pohledu, nýbrž z pohledu renomé. Protože pokud není společnost schopna zabezpečit přihlašovací údaje vlastních zaměstnanců, tak proč by měla být schopna zabezpečit přihlašovací údaje celé organizace čítající desítky tisíc zaměstnanců.

Návrh: V kombinaci s předchozím nálezem v této podkapitole by měla být provedena hlubší analýza z pohledu bezpečnosti. Na základě provedené analýzy by měly být

zavedeny lepší autentizační metody pro všechny nástroje. Způsoby vyhovujících autentizačních metod byly popsány v předchozím návrhu.

4.3.5 Systém správy hesel

Nález: Každé oddělení společnosti je úzce specializované. Každé oddělení tedy i využívá specifické nástroje, které jsou často velmi nákladné. I to je jeden z důvodů, proč zaměstnanci mají do těchto nástrojů pouze jedny přihlašovací údaje. Tento nedostatek z pohledu vedení logů o změnách byl již popsán výše a není předmětem tohoto nálezu. Problém tkví ve způsobu uchovávání a správy hesel. Každé oddělení používá nástroj, kde jsou nahrána všechna hesla. Jinak řečeno: potřebují znát jedno silné heslo do nástroje, který spravuje ostatní hesla do různých systémů. Tento nástroj je velmi dobře zašifrovaný pomocí šifrovací metody AES-256. Ovšem největší problém je ve způsobu řízení správy hesel pomocí tohoto nástroje. Přesněji žádné řízení není. Všechna hesla jsou zašifrována a uložena v souboru, který si každý načte ze sdíleného disku při spuštění aplikace. Ovšem chybí zde centrální dohled a správa nad tímto nástrojem, neboť v současnou chvíli ani není jasné, kam má které oddělení přístup. V kombinaci s nedostatečným vedením logů v této oblasti může bezpečnostní incident spojený s tímto problémem vyústit až do zastavení některé služby.

Návrh: Vzhledem k tomu, že používaný nástroj KeyPass neumožňuje LDAP integraci (používá Active Directory), nejvhodnějším řešením se jeví implementace nového nástroje, který dokáže komunikovat s AD. Tím by mělo být dosaženo snadnějšího řízení. V případě nové nastupujícího zaměstnance by pouze stačilo přidat uživatele do správné AD skupiny, podle které by měl daný uživatel práva číst povolená hesla.

4.4 Fyzická bezpečnost a bezpečnost prostředí

4.4.1 Zásada prázdného stolu a prázdné obrazovky monitoru

Nález: Zásada prázdné obrazovky v případě nečinnosti je ve společnosti ABC dodržena řádně díky automatickému zamykání obrazovky. V případě dodržování prázdného stolu na konci pracovního dne to je ovšem jiné. Často se stává, že zaměstnanci zapomenou na svém pracovním stole dokumenty, které lze někdy označit za citlivé. Mezi takové

dokumenty by mohly patřit například pracovní výkazy, změny pracovních smluv apod. V případě ignorace tohoto nálezu může dojít k neoprávněnému přístupu, ztrátě a poškození informací, a to během pracovní doby i mimo ni.

Návrh: Kontrola pracovních stolů na konci pracovního dne. Tato kontrola by měla být nařízena nejen zaměstnanci, ale rovněž by měla být zavedena kontrola stolů odpovědným nadřízeným. Kontrola ze strany nadřízeného stačí pouze zběžná a sloužila by k ujištění, zda jsou dodržena všechna pravidla.

4.5 Bezpečnost provozu

4.5.1 Dokumentace provozních postupů

Nález: Jak již bylo zmíněno výše, společnost ABC má zavedenou interní dokumentaci známou jako KB. V této dokumentaci jsou popsány mimo jiné i provozní postupy. Ovšem mnoho z postupů není aktualizováno a některé chybí úplně. Společnost neustále inovuje nástroje, a proto dokumentace, která byla platná včera, již není platná dnes. Navíc v některých případech neexistuje vůbec. To se děje zejména u týmů na 3. úrovni, tedy u nejvíce specializovaných odborníků. Mnoho z těchto týmů je přetíženo prací a na aktualizaci dokumentace není prostor. V případě, že takový tým nabírá nového člena, naučení se všech systémů a postupů je pak pro něj velmi nesnadný úkol. Navíc se zde naráží i na fakt, že dokumentaci nikdo nechce dělat.

Návrh: Navrhované řešení tohoto problému koreluje s úkolem, který byl popsán výše v souvislosti s ITSM nástrojem. Interní dokumentace bude totiž v blízké době přesunuta do nástroje Hellshare. V souvislosti s tím by se měly zavést pravidelné kontroly interní dokumentace odpovědnými vlastníky služeb. Takové kontroly lze vyvolat automatizovaně, neboť nástroj ITSM dovoluje generovat tikety v pravidelných intervalech. Díky tomu by mohla být interní dokumentace vždy aktualizovaná.

4.5.2 Opatření na ochranu proti malwaru

Nález: Opatření pro detekci, prevenci a zotavení pro účel ochrany před malwarem jsou řešena pomocí více systémů. V případě koncových zařízení se používá řešení od

společnosti McAfee a pro operativní bezpečnost je v rámci organizace vyčleněný celý bezpečnostní tým. Tento tým nastavuje pravidla pro detekci malwaru a udržuje ochranné prvky aktualizované, aby bylo zabráněno vniknutí. Ochrana proti malwaru je tedy v rámci organizace velmi kvalitní. Problém nastává přímo uvnitř organizace, neboť v rámci ABC není zakázáno ani kontrolováno připojení externího média na koncovou stanici. Interní zaměstnanec tak může připojit USB disk a zkopírovat interní dokumenty. To může mít velký dopad na organizaci.

Návrh: S přihlédnutím k již používanému nástroji od McAfee lze rozšířit tento nástroj o detekci zapojení USB. Taková detekce je součástí produktu McAfee Complete Data Protection, který firma již vlastní a který umožňuje zobrazovat pouze data z ověřených zdrojů.

Nález č. 2: Další nález patřící do stejné kategorie se týká schválených aplikací. Společnost má seznam schválených aplikací, které uživatelé mohou používat. Uživatelé ovšem mají administrátorská práva na svých počítačích a mohou si tak instalovat další aplikace, včetně těch neschválených. To je způsobeno tím, že v rámci organizace není implementováno opatření, které zabraňuje nebo detekuje použití neautorizovaného softwaru. Podle standardu ISO/IEC 27002 tento nález úzce souvisí s dalšími oblastmi, a to se Zaznamenáváním událostí formou logů a také s Instalací softwaru na provozních systémech.

Návrh: Implementace opatření, které bude omezovat uživatele k instalaci pouze schváleného softwaru. Tím bude zamezeno instalaci neověřených aplikací. Pro tento účel lze použít nástroje, které jsou již hojně využívány v organizaci. Mezi takové nástroje patří například App Blocker, který je součástí Active Directory. V tomto nástroji lze velmi specificky nastavit, který uživatel či skupina uživatelů mohou instalovat vybrané programy.

4.5.3 Zaznamenávání událostí formou logů

Nález: jak již bylo popsáno, v nálezu č. 2 v podkapitole 4.5.2 uživatelé si mohou instalovat na svá zařízení, co chtějí. Ovšem bezpečnostní tým není schopen provádět dostatečný monitoring, protože k tomu nemá dostatečné prostředky.

Návrh: Implementace monitorovacího nástroje, který bude informovat bezpečnostní tým o snaze instalovat neschválený software.

4.5.4 Správa a řízení technických zranitelností

Nález: Při analýze síťové infrastruktury byla nalezena procesní chyba související s pravidly vytvořenými na firewallech. Pokud chce mít vlastník některého virtuálního serveru přístup k některé službě, musí vytvořit tiket s žádostí o vytvoření pravidla na firewallu. Tým síťových specialistů následně vytvoří příslušné pravidlo a zavře se tiket. Takovýto proces lze nazvat řízením technické zranitelnosti, protože síťový specialista vytvoří „díru“ na firewallu, aby byla možná komunikace. Chybí zde ovšem proces pro zrušení takového pravidla ve chvíli, kdy pravidlo již nemá opodstatnění. Vzhledem k tomu, že tímto způsobem to ve společnosti už funguje delší dobu, dochází ke kumulaci nepotřebných výjimek. Následkem může být interní síť náchylná k útokům cíleným na tyto bezpečnostní mezery.

Návrh: Zavedení periodických auditů pravidel nastavených na síťových prvcích a především pak firewallech. Pro tento účel může být využito nástroje Tuffin, kterým organizace již disponuje. Nástroj detekuje aktivitu pravidel a vytváří reporty neaktivních pravidel.

4.6 Bezpečnost komunikací

4.6.1 Opatření v sítích

Nález: V návaznosti na předchozí podkapitolu týkající se správy a řízení technických zranitelností je nutno zmínit chyby v kontrolách síťových zařízení. Síťoví specialisté sice mají dostupné nástroje pro kontrolu pravidel na firewallech, ale kontroly neprovádějí.

Návrh: Zavedení pravidelných kontrol síťových prvků. Takové kontroly by měly být prováděny periodicky, např. každý rok. Předmětem kontroly by měla být všechna nastavená pravidla na zařízení a následná kontrola pravidel, zda jsou stále validní.

Nález č. 2: Pro vytváření pravidel na ochranných zařízeních sítě typu firewall je určen proces, který začíná vytvořením tiketu v ITSM nástroji. Poté, co žadatel vytvoří tiket, je

vytvořeno pravidlo na firewallu a až v dalším kroku se žádá o schválení tzv. „Service Ownera“. Následně je provedena validace. Pravidlo se pravděpodobně vytváří dříve, než je změna schválena z důvodu pomalé odezvy vlastníka aktiva, přičemž změnu je potřeba provést co nejdříve.

Návrh: Úprava procesního postupu je v tomto případně nutná, aby nedošlo k problémům s nastavenými pravidly, která mohou způsobit bezpečnostní incident, neboť například vytvořené pravidlo může být v rozporu s jiným existujícím pravidlem. Z toho důvodu se jako nejlepší řešení jeví upravit proces tak, že bez schválení nebude možné pravidlo vytvořit (například tak, že tým síťových specialistů obdrží tiket až po schválení). Dále je třeba v procesu zavést úroveň priorit. Pokud bude například nutno vytvořit dané pravidlo do 24 hodin, bude obsahovat prioritu 1, přičemž vlastník aktiva bude muset schválení provést například do 4 hodin od podání žádosti. Díky segmentaci úkolů podle priorit (které ITSM nástroj umožňuje) bude vlastník vědět, které úkoly musí vyřešit přednostně.

4.6.2 Politiky a postupy při přenosu informací

Nález: Každý uživatel disponuje služebním telefonem s operačním systémem iOS nebo Android. Tyto telefony jsou následně řízeny pomocí MDM, čímž je dosaženo vysokého zabezpečení. Jednou z funkcionalit MDM je oddělení pracovní části od osobní na mobilním zařízení, proto například nelze překopírovat text ze služebního e-mailu do jiných aplikací. Toto pravidlo zaměstnanci obchází tak, že si přepošlou zprávu na svůj osobní e-mail, který následně otevřou ve služebním telefonu (ať už pomocí prohlížeče nebo aplikace) a potřebný text zkopírují.

Návrh: Provedení analýzy, zda některá oddělení musí komunikovat pomocí e-mailu mimo organizaci, a případně omezit možnost komunikace pouze na určité domény, jako jsou například ověření dodavatelé. Díky tomu bude navýšena bezpečnost nejen z pohledu politik a postupů při přenosu informací, ale rovněž například při phishingových kampaních, kdy uživatelé ani nebudou schopni podlehnout phishingovému útoku, protože nebudou mít práva na e-mail odpovědět. To platí pouze v případě, že by se uživatel pokusil odpovědět na takový podvodný e-mail. V případě, že by útočník odkazoval na podvodnou webovou stránku, tam by aplikace zabezpečení již nefungovala. Společně s výše uvedenou restrikcí by se měly provádět kontroly, zda se takové kopírování či

přenášení firemních dat neděje jiným způsobem. Tím se sníží riziko úniku dat z organizace.

4.7 Akvizice, vývoj a údržba systému

4.7.1 Analýza a specifikace požadavků bezpečnosti informací

Nález: Při analýze ITSM nástroje, který se hojně ve společnosti používá, byla objevena absence řízení práv a přístupů. Do tohoto nástroje mají přístup i externí strany a v podstatě vidí vše, co se v tomto nástroji nachází. Tato problematika již byla popsána výše. V tomto případě se ovšem jedná o chybu při stanovení požadavků na nový informační systém. V rámci požadavků na nový informační systém bylo z pohledu politik a přístupů požadováno převzetí ze staršího nástroje zvaného Service Desk Express. Tento požadavek je v rozporu s bezpečnostními politikami, protože starší nástroj žádné řízení politik a práv neobsahoval. Jedná se tedy o procesní chybu.

Návrh: Pokud se při stanovení požadavků na nový projekt budou přebírat některé dílčí části, je potřeba provést bezpečnostní analýzu i těchto částí. Je třeba analyzovat již implementované nástroje, zda vyhovují bezpečnosti informací dle doporučené normy ISO/IEC 27002. Následně by se bezpečnostní kontroly měly provádět při každé změně informačního systému. Pokud společnost bude chtít zavést řízení přístupů v ITSM nástroji, bude to pro ni mnohem nákladnější, protože se jedná již o produkční nástroj. Pokud by tento aspekt zvážila již při stanovení požadavků, mohlo být dosaženo nižších celkových nákladů.

4.8 Doporučená opatření

Pro všechny nálezy byla navržena řešení, která by měla zajistit vyšší bezpečnost informací. Všechna tato opatření se vztahovala ke standardu ISO/IEC 27002. Z analýzy ovšem vyplývá, že společnost nemá rovněž zavedený SIEM (Security Information and Event Management). Tento systém by dle Vyhlášky č. 316/2014 o kybernetické bezpečnosti měla mít zavedena každá společnost, které se dotýká Kybernetický zákon

podle § 28 odst. 2 zákona č. 181/2014. Ten obsahuje bezpečnostní opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů a další náležitosti, které musí tyto společnosti splňovat. Společnost ABC se sice na území ČR nestará o tak velké informační systémy, aby do této vyhlášky spadala, ovšem podpora, kterou poskytuje pro celý svět, je tak velká a významná, že do této kategorie z pohledu autora spadá. Jako příklad postačí, že společnost řídí 8 000 virtuálních serverů umístěných v několika datacentrech nebo zajišťuje chod SAPových serverů, které také vykazují určitou významnost. Z těchto důvodů autor doporučuje společnosti ABC zavést SIEM, který jí zajistí monitoring, ukládání a správu bezpečnostních událostí. Nutno říci, že společnost je na to skvěle připravena, neboť vede kvalitní logovací záznamy, a proto poslední krok – zavedení SIEMu – by již neměl představovat příliš velký problém.

Seznam dalších vybraných doporučených opatření, která autor práce považuje za ta nejdůležitější, bude již jen heslovitě popsán níže, neboť zevrubný popis byl proveden výše v návrhu vlastních opatření.

- Úprava ITSM nástroje
  - Jedno z největších nalezených rizik, které může mít větší dopad na organizaci.
- Vytváření, kontrola a mazání pravidel na síťových zařízeních typu firewall
  - Procesní chyba
- Úprava politik a postupů při přenosu informací
  - Vytvořit politiky, které zabrání zaměstnancům přeposílat si e-maily na své osobní účty.
- Revalidace interní dokumentace
  - Pro některé procesy není dokumentace aktuální.
- Používání sdílených účtů
  - Není vždy možné přiřadit osobu k provedené změně.

4.9 Ekonomické zhodnocení

Investování peněžních prostředků do informační bezpečnosti se zprvu může obhajovat před nezainteresovanými osobami velmi obtížně. Ovšem názor takových osob

se rychle mění po prvním incidentu, který způsobil opravdový dopad na chod podnikání, a tedy i finanční ztráty. Ignoraci informační bezpečnosti ve firemním prostředí lze chápat jako výrobní linku, které neposkytujeme žádný servis. Ovšem v případě bezpečnosti může být dopad daleko větší, neboť v případě útoku, který je schopen paralyzovat informační a komunikační infrastrukturu ve společnosti, se může zastavit vše. Nejen jedna výrobní linka, ale všechny výrobní linky, všechna oddělení, vše, co je zapojeno do firemní sítě. A právě z těchto důvodů jsou investice do informační bezpečnosti tak důležité.

Analyzovaná společnost do informační bezpečnosti investuje nemalé sumy. Navzdory tomu bylo nalezeno několik bezpečnostních nesrovnalostí, které by v krajním případě mohly mít přímý dopad nejen na samotnou společnost ABC, s.r.o., ale rovněž na jejího výhradního zákazníka čítajícího téměř 60 tisíc zaměstnanců. Pokud tedy chceme spočítat, jaké ztráty mohou bezpečnostní mezery způsobit, je třeba uvažovat nejhorší scénář, tedy úplné zastavení výroby celého holdingu. Samozřejmě se taková situace může jevit jako absurdní, ale ve společnosti lze nalézt informační technologie téměř ve všech strojích, zařízeních a kancelářích a každé takové zařízení tedy představuje z pohledu informační bezpečnosti riziko. Proto uvažujme, že by neprovedení navržených opatření vyústilo v paralyzaci počítačových sítí v celém holdingu. Tento holding dle veřejně dostupných dat (data za rok 2018) utrží 18,08 miliard EUR. To představuje průměrný denní příjem 49,53 milionů EUR. Pokud by tedy došlo jen k částečnému narušení bezpečnosti infrastruktury na několik hodin, škody by mohly být i několik milionů EUR. Podíváme-li se tedy na navržená opatření v této diplomové práci, zjistíme, že jsou téměř všechna řešitelná úpravou procesů či politik, a představují tedy jen velmi nízké náklady ve formě práce specialistů (kteří jsou již ve společnosti zaměstnáni) ve výši několika desítek člověkohodin. Náklady tedy mohou dosahovat maximálně několik jednotek tisíc EUR. Případná customizace ze strany dodavatele ITSM nástroje je pak odhadnuta na částku 20 tisíc EUR. Jak lze vidět, stále se jedná o minimální náklady. V porovnání s tím, jaké škody mohou být způsobeny, tedy zdravý rozum velí provést návrhy, neboť návratnost investice je již v okamžiku prvního odražení útoku.

Bezpečnostní riziko je dnes již jedna z položek, které jsou zohledňovány v pojištění. Znamená to tedy, že proti takovému riziku se dá pojistit. V případě takového připojištění,

se musí posuzovat, kolik stojí opatření a o kolik by se snížilo bezpečnostní riziko, a tedy i potřebný balík peněz vynaložený na pojištění. Tedy před implementací každého navrhnutého opatření je nutno posoudit snížení rizika a jeho dopad na snížení ceny pojištění.

ZÁVĚR

V teoretické části práce byly popsány základní pojmy a terminologie vztahující se k zaměřené problematice informační bezpečnosti. Následně byly podrobněji rozebrány ty oblasti, o kterých bylo pojednáno v dalších částech práce, nebo mají úzkou souvislost s probíranou problematikou. V teoretické části lze tedy nalézt rozdělení normalizačních institucí, norem, rámců a metodik, které se zabývají nejen informační bezpečností.

Analýza současného stavu byla úzce zaměřena na problematiku bezpečnosti informací a její možné mezery ve vybraném firemním prostředí. Z toho důvodu byla nejdříve analyzována společnost z pohledu organizační struktury, účelu podnikání a vnitropodnikové infrastruktury. Následně byla provedena podrobná analýza podle normy ISO/IEC 27002:2013 se zaměřením na bezpečnostní mezery.

Oblast navrhovaných řešení byla provedena na základě analýzy současného stavu, kdy každý jednotlivý nález byl popsán, a následně bylo pro tento nález navrženo řešení. Posloupnost navrhovaných řešení je stejná jako v případě analytické části, tedy kopíruje strukturu podle výše zmíněné normy.

Tato diplomová práce byla vypracována v době, kdy autor vidí informační bezpečnost jako značně podceňovanou oblast ve většině organizací. Příkladem současného stavu může být počet útoků na velké nemocnice, kdy jen za poslední rok bylo provedeno mnoho útoků a z toho 2 útoky proběhly úspěšně ve prospěch útočníka (informace získány z oficiálních stránek NÚKIB a ČTK). Pokud by takové organizace byly certifikovány podle norem řady ISO/IEC 27000, šance na jakékoliv narušení informačních aktiv by byly značně minimalizovány. Z toho důvodu se autor zaměřil téma diplomové práce právě směrem k informační bezpečnosti, neboť zde vidí velký potenciál pro možný rozvoj. Z výše zmíněných důvodů se autor rozhodl vypracovat diplomovou práci ve společnosti ABC, s.r.o., kde čelil nesnadnému úkolu. Musel nalézt bezpečnostní nesrovnalosti ve společnosti, která patří mezi minoritu organizací, které nepodceňují informační bezpečnost. Důkazem tohoto stavu jsou celá dvě oddělení zaměřená na informační bezpečnost, která jsou plná vysoce kvalifikovaných specialistů. Určitého výsledku, který je předmětem této práce, bylo dosaženo snad i díky autorově pohledu nezainteresované osoby, kdy měl určitý nadhled. Výsledkem této diplomové práce je pak

několik pozitivních i negativních přínosů. Hlavním pozitivním přínosem by měl být výstup této práce, který analyzované organizaci pomůže zvýšit úroveň informační bezpečnosti. Další kladné přínosy pro autora jsou nejen ve splnění školních povinností, ale především pak ve zlepšení znalostí a získání lepšího povědomí v oblasti informační bezpečnosti. Negativum snažení je pak značné snížení autorovi důvěry vůči všem organizacím, které nejeví snahu o získání certifikací v oblasti informační bezpečnosti nebo alespoň o implementaci metodik či rámců podle nejlepších zkušeností z praxe.

SEZNAM POUŽITÝCH ZDROJŮ

[1] SEDLÁK, Petr. *Management informační bezpečnosti: Úvod a základní pojmy* [online]. Brno, 22. září 2014 [cit. 2020-04-10].

[2] ICT (Information and Communication Technologies). In: ManagementMania.com [online]. Wilmington (DE) 2011-2020, 20.08.2017 [cit. 10.04.2020]. Dostupné z: https://managementmania.com/cs/informacni-a-komunikacni-technologie

[3] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[4] SEDLÁK, Petr. *Management informační bezpečnosti: Přehled norem* [online]. In: . 20. října 2013 [cit. 2020-04-10].

[5] History of ITIL. *ITIL central* [online]. [cit. 2020-04-11]. Dostupné z: https://itsm.fwtk.org/History.htm

[6] SKÁLA, Jiří. Best Practise řízení ICT služeb: ITSM a ITIL [online]. [cit. 2020-04-11]. Dostupné z: http://home.zcu.cz/~steiner/KOPO/Prednasky/9_Prednaska%209_ITSM.pdf

[7] *Hlavní oblasti ITSM dle ITIL* [online]. [cit. 2020-04-11]. Dostupné z: http://www.itil.cz/index.php?id=989

[8] SEDLÁK, Petr. *ISMS: Zavádění a provozování ISMS* [online]. In: . 20. října 2013 [cit. 2020-04-10].

[9] The ISO story. *International Organization for Standardization* [online]. [cit. 2020-04-13]. Dostupné z: https://www.iso.org/about-us.html

[10] NIST: Computer Security Division. *National Institute of Standards and Technology* [online]. [cit. 2020-04-13]. Dostupné z: https://www.nist.gov/itl/csd

[11] NOVÁK, Luděk a Josef POŽÁR. *Systém řízení informační bezpečnosti*. 2011. ISBN 978-80-7251-356-7.

[12] IT Service Management. *Managementmania* [online]. 04.11.2016 [cit. 2020-04-14]. Dostupné z: https://managementmania.com/cs/it-service-management

[13] ISO/IEC 27002:2013. In: *RiskAnalysisCOnsultants* [online]. [cit. 2020-04-15]. Dostupné z: https://www.rac.cz/rac/homepage.nsf/CZ/27002

[14] About ENISA. In: *Https://www.enisa.europa.eu/* [online]. [cit. 2020-04-15]. Dostupné z: https://www.enisa.europa.eu/about-enisa

[15] SLA (Service Level Agreement). In: ManagementMania.com [online]. Wilmington (DE) 2011-2020, 14.02.2018 [cit. 22.04.2020]. Dostupné z: https://managementmania.com/cs/service-level-agreement

[16] Matice odpovědnosti RACI (RACI Responsibility Matrix). *Managementmania* [online]. 17.03.2016 [cit. 2020-04-14]. Dostupné z: https://managementmania.com/cs/matice-odpovednosti-raci

[17] *RACI (RASCI) model / metoda / tabulka* [online]. [cit. 2020-05-11]. Dostupné z: http://www.finance-management.cz/080vypisPojmu.php?X=RACI+RASCI+model&IdPojPass=55

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

IT	Information Technology
ICT	Information and Communication Technology
ISMS	Information Security Management System
ITSM	Information Technology Service Management
SLA	Service Level Agreement
ITIL	Information Technology Infrastructure Library
ISO	International Organization for Standardization

SEZNAM GRAFŮ

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH