VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

POSOUZENÍ INFORMAČNÍHO SYSTÉMU FIRMY A NÁVRH ZMĚN
INFORMATION SYSTEM ASSESSMENT AND PROPOSAL OF ICT MODIFICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Lukáš Barnet**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Miloš Koch, CSc.**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Lukáš Barnet**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**doc. Ing. Miloš Koch, CSc.**
Akademický rok:	2018/19

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

Posouzení informačního systému firmy a návrh změn

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnosti, posoudit tento stav a navrhnout změny, směřující ke zlepšení stávajícího stavu a eliminaci nalezených rizik.

Základní literární prameny:

BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3. aktualiz. a dopl. vyd. Praha: Grada, 2012. 323 s. ISBN 978-80-247-4307-3.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2. přeprac. a aktualiz. vyd. Praha: Grada, 2009. 496 s. ISBN 978-80-247-2615-1.

MOLNÁR, Zdeněk. Efektivnost informačních systémů. 2. rozš. vyd. Praha: Ikar, 2000. 178 s. ISBN 80-247-0087-5.

SCHWALBE, Kathy. Řízení projektů v IT. Brno: Computer Press, 2007. 720 s. ISBN 978-80-251-1-26-8.

SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2. aktualiz. a rozš. vyd. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

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

V Brně dne 28.2.2019

L. S.

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

Abstrakt

Tato diplomová práce se zabývá posouzením informačního systému firmy a návrhem změn. Práce je rozdělena do tří částí. První, teoretická část, je zaměřena na vysvětlení základních pojmů, které jsou v diplomové práci použity. Druhá, analytická část, obsahuje představení společnosti, její analýzu a rovněž analýzu informačního systému. Na základě těchto informací je sestavena poslední, návrhová část, jejímž obsahem je zvýšení zabezpečení informačního systému společnosti Tereos TTD, a.s.

Klíčová slova

informační systém, IS, hodnotící metodika ZEFIS, Lewinův model, bezpečnostní strategie, FortiGate, LOGmanager

Abstract

This diploma thesis deals with the assessment of the company information system and the proposal of changes. The thesis is divided into three parts. The first, theoretical part, is focused on the explanation of the basic terms used in the thesis. The second, analytical part contains the introduction of the company, its analysis and also the analysis of the information system. Based on this information, the last, design part is compiled, the content of which is to increase the security of the information system of Tereos TTD, a.s. company.

Key words

information system, IS, ZEFIS evaluation methodology, Lewin's model, security strategy, FortiGate, LOGmanager

Bibliografická citace

BARNET, Lukáš. *Posouzení informačního systému firmy a návrh změn* [online]. Brno, 2019 [cit. 2019-05-06]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/116577. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Miloš Koch.

Čestné prohlášení

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

V Brně dne 6. května 2019

_____

podpis studenta

Poděkování

Touto cestou bych rád poděkoval panu doc. Ing. Miloši Kochovi, CSc. za odborné vedení, výpomoc a poskytnutí cenných rad a připomínek v průběhu vypracovávání diplomové práce.

OBSAH

ÚVOD

V dnešní době přicházíme do styku s informačními systémy téměř neustále, aniž bychom si to mnohdy uvědomovali. Při neustálém rozvíjení a zlepšování informačních technologií je důležité tyto informační systémy rovněž neustále zdokonalovat. Je totiž naprosto nezbytné, aby informační systém (IS) byl efektivní a práci ulehčoval, mnohdy se však v praxi totiž stává, že je tomu přesně naopak, což rozhodně není správné řešení. Dobře fungující informační systém může společnosti v dnešním silném konkurenčním prostředí získat výhodu a výrazně pomoci.

Velmi podceňovaná je bohužel bezpečnost informačních systémů, což je v dnešní době, kdy čím dál častěji dochází k útokům hackerů / crackerů, velmi rizikové počínání. Tato problematika je tedy nedílnou součástí této diplomové práce, která je zaměřena na posouzení informačního systému a návrh změn a jejím hlavním cílem je zvýšení zabezpečení informačního systému společnosti Tereos TTD, a.s.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této diplomové práce je analýza stávajícího stavu informačního systému společnosti Tereos TTD, a.s., vyhodnocení jeho efektivnosti a bezpečnosti a následný návrh změn směřující ke zlepšení aktuálního stavu systému a především jeho bezpečnosti.

V první, teoretické části, jsou vysvětleny základní pojmy, které slouží pro objasnění a pochopení souvislostí v celé diplomové práci. Druhá, analytická část, je zaměřena na představení společnosti, které zahrnuje její popis a historii, nabízené produkty a organizační strukturu, na což navazuje analýza vnějšího prostředí firmy (PEST a Porterova analýza) a také SWOT analýza a rovněž analýza informačního systému pomocí hodnotící metodiky ZEFIS. Na základě získaných informací je sepsána poslední, návrhová část práce, jejímž výstupem je zvýšení zabezpečení informačního systému společnosti. Pro tento návrh je vytvořen časový a obsahový plán, Lewinův model, identifikace, analýza a vyhodnocení rizik a na závěr je uvedeno ekonomické zhodnocení a shrnutí přínosů těchto změn.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretické části práce jsou objasněny základní pojmy a výrazy, které budou později využity v praktické části práce. Je zde charakterizován především informační systém, technologie a metody pro analýzu společnosti.

1.1 Data

Slovo „data“ je převzato od množného čísla latinského slova „datum“, které bylo odvozeno od „dare“, což znamená „dát“ a data tak lze chápat jako „něco daného“. V oblasti IT byl pojem „data“ vždy používán jako označení pro čísla, text, zvuk a obraz (1).

Data je možno rozlišovat do dvou kategorií:

- **Strukturovaná data** – data jsou zde ukládána pomocí relačních databázových systémů. Díky tomuto strukturovanému uložení je práce s daty efektivnější a lze jednoduše vybírat jen konkrétní data, která jsou zapotřebí pro řešení nějakého problému;
- **Nestrukturovaná data** – tato data jsou popisována jako tzv. „tok bytů“ bez dalšího rozlišení. Jedná se např. o obrázky, zvukové nahrávky a video záznamy, ale také textové dokumenty (1).

V oblasti podnikových informačních systémů data představují významné údaje a jsou rozdělena do tří skupin:

- **Data o společenských podmínkách** – data týkající se rozvoje služeb, technologií a produktů včetně faktorů ovlivňujících jejich výrobu. Spadají zde také data spojená s náklady a produktivitou výroby;
- **Data o trhu** – do této skupiny patří data o konkurenci, nabídce a poptávce a o komoditním trhu;

- **Interní data o podniku** – data o podnikových zdrojích a fungování společnosti, spadají sem také prognózy pro prodej nebo finanční plán. Výstupy těchto dat jsou podkladem, který slouží k rychlé reakci na změnu svého okolí (3).

1.2 Informace

Informace lze chápat jako zprávy nebo vjemy splňující tři požadavky. Tím prvním je syntaktická relevance – subjekt, který přijímá zprávu, ji musí být schopen detekovat a porozumět jí. Dalším požadavkem je sémantická relevance – subjekt musí vědět, co daná zpráva znamená a co vypovídá o něm a okolí. Posledním požadavkem je pragmatická relevance – zpráva musí pro příjemce mít nějaký význam (2).

Informace lze členit dle mnoha hledisek, na informace operativní, strategické a taktické dle stupně řazení, krátkodobé a dlouhodobé, aktuální a prognostické, historické a mnoho dalších (2).

Informace jsou popisovány jako tzv. „data v kontextu“ – tedy data srozumitelná a použitelná. Hodnota informace je součástí procesu transformace dat na informace, má tedy subjektivní charakter (1).

1.3 Znalosti

Znalosti lze charakterizovat jako informace o tom, jak využít jiná data a informace v různých situacích. Podle Roberta M. Hayese jsou znalosti výsledkem porozumění právě sdělené informace a její integrace s dřívějšími informacemi (2).

Znalosti je také možno definovat jako vzájemně provázané struktury souvisejících poznatků, které jsou měnitelé a rozšířitelné. Znalost něčeho znamená jejich reprezentaci včetně schopnosti provádět s nimi různé kognitivní operace, na jejichž základě lze částečně předvídat, co se může v reálném světě stát (1).

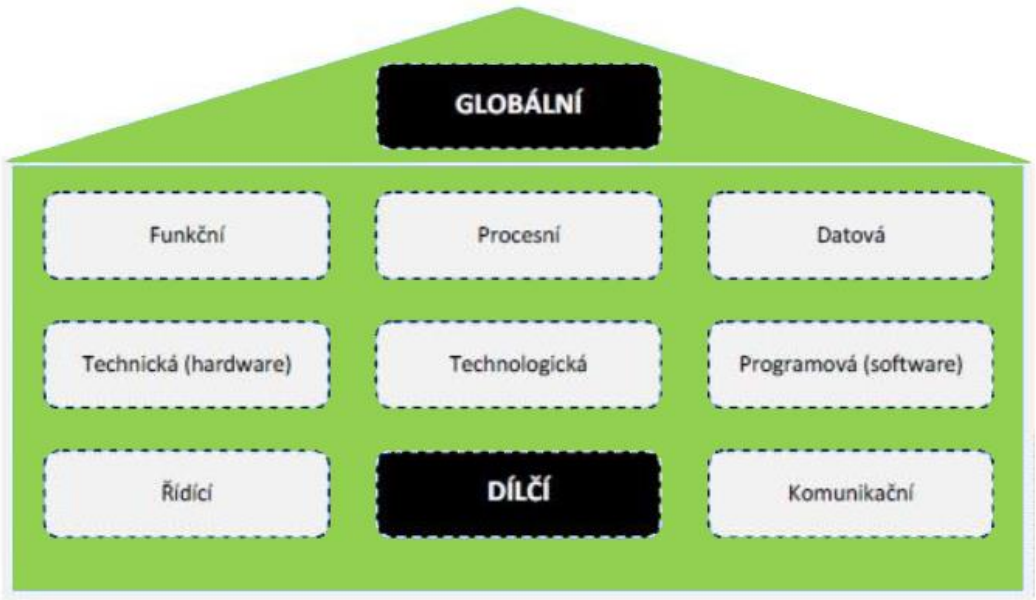
Vzájemnou provázanost dat, informací a znalostí dobře vyjádřili Checkland a Scholes: „*Technologie pracují s daty, lidé je interpretují jako informace nesoucí význam, které se stávají podnětem pro další jednání. Proces interpretace je kognitivní záležitost, ve kterém stěžejní roli hrají znalosti.*“ (1, s. 4).

1.4 Informační systém

Informační systém lze definovat jako množinu prvků, jejich vzájemných vazeb a určitého chování – z pohledu informačních technologií jsou těmito prvky pouze hardware a software. Doc. Koch s nadsázkou dodává, že IS je pro společnost v podstatě to samé, co jsou šaty pro člověk, tedy může je mít vlastní nebo půjčené (outsourcing), ale musí je mít (2).

1.4.1 IS z pohledu architektur

Architekturu informačního systému lze popsat jako návrh struktury systému, který splňuje dané funkční, informační, kvalitativní a ekonomické požadavky (4).



Obr. 1: Informační systém z pohledu architektur. (4, vlastní zpracování)

Globální architektura je základním schématem, ideou informačního systému, kterou tvoří jednotlivé stavební bloky, jež představují skupiny aplikací včetně jejich datových základen a technického vybavení. Dílčí architektury se zaměřují na podrobnější návrhy IS dle různých hledisek, mezi které spadá např. analogie s plány rozvodu vody, elektřiny a plynu v plánu domu (4).

Funkční architektura rozděluje informační systém na subsystémy a skupiny funkcí postupnou dekompozicí globální architektury, přičemž tato dekompozice probíhá až k dílčím elementárním funkcím (4).

Procesní architektura se zaměřuje na popis budoucích stavů procesů ve společnosti se zaměřením na neautomatizované činnosti a funkce IS, které jsou plánovanými reakcemi na události, k jímž bude docházet. Smyslem této architektury tedy je připravit co nejefektivnější reakce společnosti na externí události (4).

Technická (hardwarová) architektura určuje typy a rozmístění prostředků výpočetní a komunikační techniky. Je znázorňována schématem a specifikací počítačových sítí, serverů, počtem koncových uživatelských počítačů a dalších zařízení (4).

Technologická architektura určuje způsob zpracování jednotlivých aplikací v těsné návaznosti na definovanou technickou, datovou a programovou architekturu (4).

Datová architektura představuje návrh datové základny společnosti. Při návrhu se vychází z definice jednotlivých objektů, jejich položek a vzájemných vazeb mezi nimi. Zvolí se vhodný datový model (v současnosti jednoznačně patří k nejrozšířenějším relační model) a výsledkem datové architektury je schéma všech databází a jejich vět, např. v podobě entito-relačního diagramu společně s tabulkami struktur vět (4).

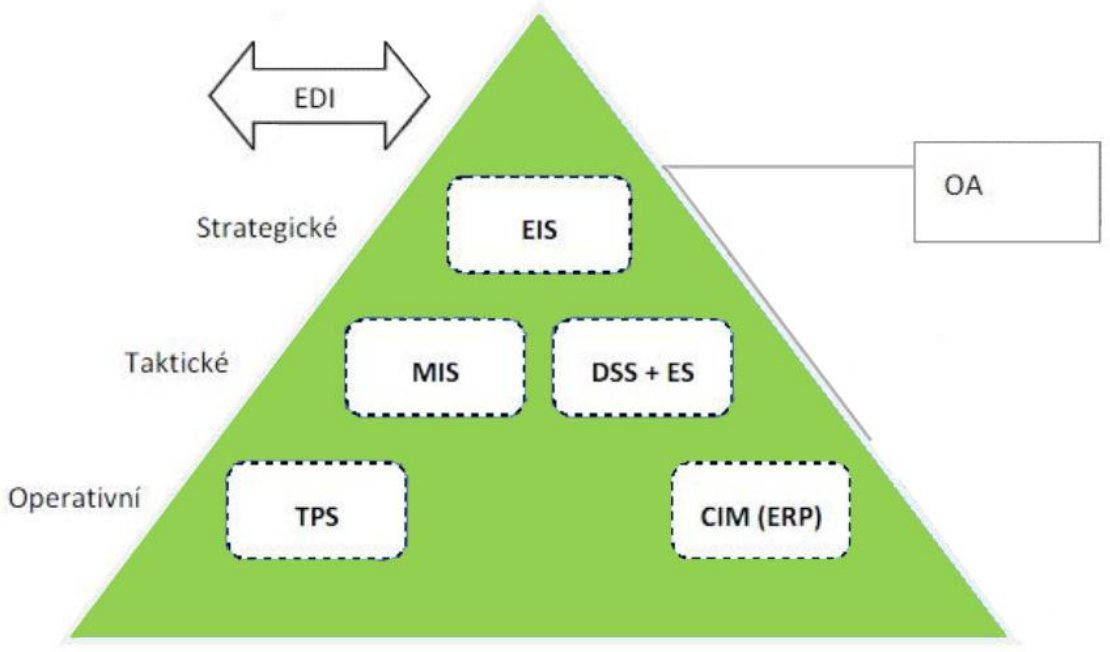
Programová architektura určuje, z jakých programů a programových komponent se bude skládat výsledný informační systém a jaké mezi nimi budou existovat vazby (4).

Komunikační architektura vymezuje vnější rozhraní systému a jeho komunikace s okolím (4).

Řídící architektura definuje pravidla fungování systému, standardy a organizaci služeb uživatelů. Lze zde také zahrnout organizační strukturu a pravidla fungování systému (4).

1.4.2 IS z pohledu úrovně řízení

Při řízení společnosti platí, že pro jednotlivé řídící vrstvy jsou zapotřebí různé informace, přičemž dle klasické řídící pyramidy je třeba největší množství informací pro nejnižší úroveň řízení, zatímco nejvyšší (strategické) řízení značně využívá zvláště externích informací z okolí společnosti a vysoce agregovaných informací zevnitř společnosti (4).



Obr. 2: Informační systémy z pohledu úrovně řízení. (4, vlastní zpracování)

CIM (Computer Integrated Manufacturing) – počítačem integrovaná výroba, jež zahrnuje přímé řízení technologických procesů. Jedná se o předchůdce ERP (5).

ERP (Enterprise Resource Planning) – nástupci CIM, pokrývající celou problematiku procesů společnosti, jako jsou např. plánování, finance, výroba nebo řízení zdrojů (5).

TPS (Transaction Processing System) – zástupci klasických dávkových systémů, kteří jsou umístěni přímo u pracovníka. Jejich funkce jsou prováděny opakovaně a je požadována vysoká rychlost odezvy a spolehlivost. Jsou používány výhradně pro účely operativního řízení (5).

MIS (Management Information System) – podporují taktické řízení společnosti, mají kořeny v účetních a ekonomických systémech. Jsou určeny pro sumarizace a agregace dat za určité období (5).

DSS (Decision Support System) – systémy sloužící pro podporu rozhodování. Většinou se zaměřují na analýzy dat z MIS, určené pro taktické i strategické řízení a poskytují velmi přehledné nástroje pro vizualizaci nebo pro distribuci informací (5).

EIS (Executive Information System) – systémy pro vrcholové vedení, které umožňují přístup k datům z nižších vrstev a externích zdrojů a agregují informace do nejvyšší úrovně (5).

EDI (Electronic Data Interchange) – část IS, zaměřující se na komunikaci společnosti s jejím okolím, dodavateli, odběrateli, bankami či státními institucemi (5).

1.4.3 IS z pohledu výroby a odbytu

Tento model představuje řešení, která jsou v současnosti nejobvyklejší. Systémy SCM a CRM jsou nasazovány pouze u firem, které mají velmi vysoké množství dodavatelů nebo odběratelů. Jádrem je ERP systém, který je doplněný o systémy MIS (4).

Obr. 3: Informační systémy z pohledu výroby a odbytu. (4, vlastní zpracování)

MIS (Management Information System) – manažerská nadstavba, sloužící k dokonalejšímu rozhodování na základě přesnějších informací (6).

SCM (Supply Chain Management) – řízení dodavatelského řetězce, které významně zlepšuje schopnost reagovat na požadavky zákazníků a umožňuje propojení jednotlivých článků dodavatelského řetězce (dodavatel – výrobce – distributor – prodejce – odběratel) (6).

ERP (Enterprise Resource Planning) – jádro IS společnosti, zahrnuje plánování a řízení všech klíčových procesů na všech úrovních (výroba, logistika, finance, lidské zdroje) (6).

CRM (Customer Relationshim Management) – řízení vztahu se zákazníky, které řeší, jakým způsobem získat informace o stávajících i budoucích zákaznících, jak vytvářet služby a produkty, které budou zákazníkům vyhovovat apod. (6).

1.4.4 Klasifikace IS

Každá společnost a každá její organizační část požaduje specifický způsob zpracovávání informací, se kterými dále pracuje. Tyto pohledy jsou rozděleny na následující čtyři základní úrovně (7).

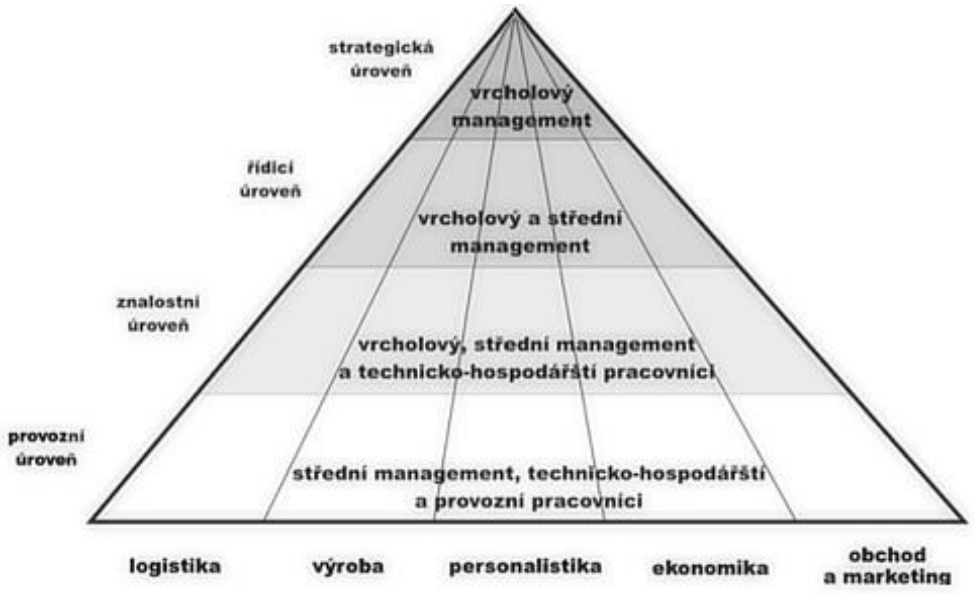
Provozní úroveň – V této úrovní se nachází systémy, které zpracovávají každodenní podnikovou agendu, mezi které patří např. realizace zakázek nebo potřeby nákupu a prodeje. Hlavním požadavkem je aktuálnost a přesnost. Tato úroveň je také často nazývána transakční (7).

Znalostní úroveň – Do této úrovně jsou zařazeny klientské aplikace informačního systému jako ERP či CRM, ale také kancelářské aplikace (Microsoft Office), které jsou označovány jako tzv. „groupware“. Tyto aplikace se zabývají tokem dokumentů a podporují znalosti zaměstnanců (7).

Řídící úroveň – Zde jsou zpracovávány hlavně informace nezbytné ke splnění administrativních úkolů. Pohled na tuto úroveň lze rovněž brát jako otázku, zda „vše funguje, jak má“, na niž jsou v pravidelných intervalech získávány odpovědi

prostřednictvím reportů o výsledcích. V případě, že se management rozhodne zvýšit produkci, se tato úroveň rovněž zabývá možnými výhledy do budoucna a následnou návratností vynaložených nákladů (7).

Strategická úroveň – Tato úroveň je využívána výhradně vrcholovým managementem, protože jsou zde zahrnuty dlouhodobé strategické cíle společnosti. Úroveň slouží k identifikaci dlouhodobých trendů napříč celou společností. Cílem je odhalení případné změny chování trhu a připravení vhodné změny, zdali je možná (7).



Obr. 4: Informační pyramida podle organizačních úrovní. (7)

1.4.5 Životní cyklus IS

Implementace IS, od samého zadání tvorby až po ukončení provozu, zahrnuje sled činností, které jsou popsány níže (8).

Plánování – Jedná se o jednu z nejdůležitějších fází. Klíčová je zde komunikace s uživatelem (zákazníkem), při které dochází k získávání informací o něm a zjišťování potřeb. Špatně získané informace mohou jednak snížit kvalitu výsledného produktu, a také zvýšit celkové náklady. Po dokončení této fáze vznikne dokument, jež definuje hlavní problémy a jejich řešení (8).

Analýza – V této fázi dochází k detailní analýze požadavků a vzniká základ návrhu informačního systému. Jsou zde také navrhovány moduly, které budou následně použity ve výsledném produktu. Tento návrh by měl obsahovat řešení možných problémů a být co nejvíce konkrétní (8).

Návrh – Zde se řeší volba vhodného softwaru, hardwaru, designu a dalších jednotlivých částí IS, výsledkem jsou pak specifikace programů a jejich zdrojové kódy (8).

Implementace – V této fázi je již IS nainstalován na požadované stanice a probíhá školení zaměstnanců, vytváření dokumentace a případné řešení posledních problémů (8).

Provoz – Většinou se začíná nejprve zkušebním provozem, při kterém se provádí se kontrola přijímá zpětná vazba od uživatelů (8).

1.4.6 ERP (Enterprise Resource Planning)

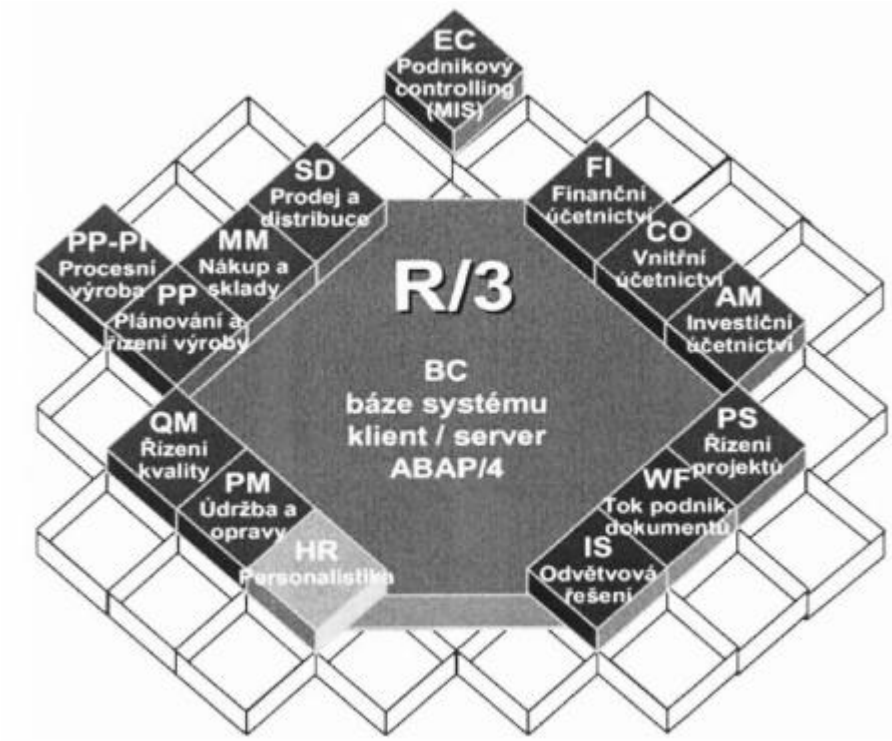
Definic pro ERP existuje velké množství, obecně z nich však vyplývá, že za Enterprise Resource Planning jsou považovány aplikace představující softwarové řešení, která jsou užívaná k řízení podnikových dat a pomáhají plánovat celý logistický řetězec od nákupu, přes sklady, po výdej materiálu a řízení obchodních zakázek od jejich přijetí až po expedici, a to včetně plánování výroby, finančního a nákladového účetnictví i řízení lidských zdrojů (6).

ERP může být také chápán jako hotový software, který společnosti umožňuje automatizování a integrování jejich hlavních procesů, sdílení společných dat a poskytování jejich dostupnosti v reálném čase. Systém ERP také představuje podnikovou databázi, do které jsou zapisovány všechny významné transakce a jsou zde data zpracovávána, monitorována a na jejím základě reportována (6).

Funkční moduly ERP

Zde spadají hlavní činnosti, které jsou vzájemně propojeny a společně tak tvoří celek ERP. Příkladem základních funkčních modulů může být dnes již sice historické, ale pro

objasnění schematicky přehledné řešení od SAP (produkt SAP R/3), které je znázorněno na následujícím obrázku (6).



Obr. 5: Základní funkční moduly ERP na příkladu produktu SAP R/3. (6)

ERP pokrývají obzvláště dvě hlavní funkční oblasti, kterými jsou:

- **Logistika** – v ERP zahrnují celou podnikovou logistiku – nákup, skladování, výrobu, distribuci (prodej) a obzvláště plánování zdrojů;
- **Finance** – zahrnují finanční, nákladové a investiční účetnictví a podnikový controlling (6).

Dělení na dvě hlavní funkční oblasti se projevuje rovněž ve struktuře jednotlivých ERP modulů, ale detailnější členění je u jednotlivých dodavatelů ERP natolik specifické, že při porovnávání nabídek uváděných na webových stránkách si je sice jejich struktura popisů s ohledem na nabízenou funkčnost do značné míry velmi podobná, ale zároveň těžce srovnatelná. Hlavní rozdíly je možné nalézt v počtu modulů a jejich uspořádání a zejména v zaměření konkrétního ERP na určitou aplikační oblast a typy procesů (6).

1.4.7 Trendy ve vývoji trhu s ERP systémy

Podnikové informační systémy jsou vyvíjeny již několik desítek let. Dnešní společnosti si mohou vybírat z nepřeberného počtu možností, jakým způsobem zabezpečit zpracování podnikových informací. Mohou se rozhodnout mezi systémem na míru, standardním ERP řešením nebo outsourcingem aplikace, či celými podnikovými procesy (7).

Na počátku minulého století tomu ale bylo zcela jinak. O digitální ekonomice se mohlo tehdejším firmám jen zdát. K automatizované a standardizovanému zpracovávání dat vedla společnosti snaha o dosažení vyšší konkurenceschopnosti, rozšíření vlastní působnosti a efektivnější fungování zaběhnutých procesů (7).

Za prehistorické předchůdce ERP je možné označit systémy, které byly využívány již ve 20. až 40. letech minulého století u společností Baťa a Philips. Tyto řídící systémy vykazovaly silnou motivaci a vedly pracovníky k dodržování podnikových standardů. Díky jednotnému konceptu řízení se společnost Baťa mohla odlišit od konkurence a sjednotit interní procesy, díky čemuž minimalizovala náklady na výrobu, distribuci a řízení. Úroveň automatizace byla pochopitelně omezená možnostmi technologií dané doby, přestože tedy nelze hovořit o automatizovaném IS dnešního pojetí, nikterak to nesnižuje jeho význam (7).

Vznik ERP systémů jako takových se datuje od počátku 60. let 20. století. Toto období zahájily požadavky výrobních společností na automatizované plánování spotřeby materiálů – MRP (Material Requirements Planning). První systém tohoto typu vzniknul díky spolupráci IBM a Case Corporation. Od té chvíle začaly implementace neustále rozsáhlejších MRP systémů, které ke svému provozu a správě vyžadovaly servisní týmy a dostatečně výkonný hardware (7).

Počátkem 70. let začaly vznikat první softwarové společnosti, jako např. SAP (1972) nebo Lawson Software (1975), které si kladly za cíl nabízet standardní podnikové aplikace integrující klíčové procesy. Koncem 70. let se kvůli požadavkům průmyslových firem MRP koncept rozrůstá na plánování všech výrobních zdrojů – MRP II (Manufacturing Resource Planning) (7).

Koncem 80. let přichází na trh další významná IT korporace, PeopleSoft, která se zaměřuje na vývoj softwaru pro řízení lidských zdrojů. Tento průlom v oblasti plánování a řízení výroby a chápání smyslu integrace a komunikace byl dovršen zakomponováním procesů řízení lidských a kapitálových zdrojů. Vývoj těchto řešení je pochopitelně doprovázen i technologickým pokrokem, který začíná prosazovat model klient/server, což uzavřelo druhou fázi vývoje podnikových IS, ze kterých vychází současná ERP řešení (7).

V průběhu 90. let se společnosti začaly stále více orientovat na pořizování standardních softwarových produktů, jež integrují oblast plánování a řízení celého logistického toku. Na začátku 90. let se stále více začal prosazovat samotný termín Enterprise Resource Plannig, a to hlavně v souvislosti s rozšiřováním funkcionality na řízení lidských zdrojů a financí a pokrýváním specifických oblastí průmyslových firem, jako např. řízení projektů a výroba investičních celků. Důležitým milníkem se pak stal rok 1995, kdy Oracle představil sadu podnikového softwaru Oracle Applications 10 – prapůvodce dnešního moderního řešení Oracle E-business Suite (7).

Na konci 90. let, kdy začala expanze internetových služeb do firem, dodavatelé plně do svých rukou převzali aktivitu ve vývoji, díky čemuž se výrazně zkrátily časové intervaly mezi zásadními změnami v nabídce podnikových IT řešení. Přelom nového tisíciletí by z hlediska vývoje ERP systémů bylo možné rozdělit do tří po obě rychle následujících fází. Tou první, která je dodnes dominantní, představuje tradiční způsob implementace ERP systémů spočívající v budování podnikových aplikací dle individuálních potřeb zákazníků. Druhá fáze doplňuje tu první nabídkou přednastavených ERP řešení, která představuje snahu uspořit vysoké náklady na úpravy softwaru. Tato metoda kromě úspor rovněž přináší prvek standardizace a nabídku nejlepších praktik. Poslední fázi představuje pronájem ERP systémů po internetu – ASP (Application Service Providing). Tato podoba outsourcingu nabídla nový způsob, jak menším společnostem, zpřístupnit špičková softwarová řešení. Tento trend však počátkem 21. století začal upadat, jelikož pro spoustu společností bylo důvěryhodnější pořízení ERP formou klasického implementačního projektu a provoz tzv. „pod vlastní střechou“. Od roku 2005 se však na českém trhu objevuje „druhá vlna“ dodavatelů zavádějících progresivnější modely ERP a CRM systémů, kterou charakterizují pojmy outsourcing a cloud computing (7).

Outsourcing

Pro pojem „outsourcing“ dosud nebyl nalezen vhodný překlad, lze jej však volně přeložit jako vyčleňování nebo externí využívání cizích zdrojů. Ve skutečnosti jde o vyčlenění služeb, procesů nebo činností mimo společnosti pomocí formy dlouhodobého smluvního vztahu. Tyto outsourcované služby, procesy a činnosti jsou pak zajišťovány externím dodavatelem a jsou řízeny na základě SLA (Service Level Agreement – dohoda o úrovni poskytovaných služeb) (9).

Význam outsourcingu spočívá ve dvou hlavních aspektech – v rozhodnutí, které činnosti outsourcovat a ve způsobu realizace. Jestliže je rozhodnuto o vyčlenění určitých činností, je nutné velice pečlivě všechny uvolněné zdroje (např. převedení nebo propuštění zaměstnanců či prodej a likvidace zařízení) přesunout jinam. Při vyčlenění kterékoli činnosti je nezbytné, aby si společnost zachovala znalost o celkovém konceptu výsledného produktu a o rozmezích mezi vlastní a nakupovanou činností. Outsourcing pro každou společnost představuje zvýšené riziko, že nakupovaná služba nebude disponovat požadovanými parametry, velmi důležitý je tak výběr dodavatele, smluvní ošetření a způsob řešení rizik (10).

Projekt outsourcingu má obyčejně následující fáze:

- Stanovení cílů (např. reakce na vývoj v odvětví nebo zvýšení návratnosti kapitálu);
- Výběr vhodných činností (vícekriteriální hodnocení, např. porovnávání nákladů, nabídka na relevantním trhu, možnosti ošetření rizik);
- Rozhodnutí o způsobu vyčlenění (nákup od dodavatele nebo spojenectví s vhodným partnerem);
- Definování parametrů dodávané činnosti;
- Výběr dodavatele nebo partnera;
- Uzavření smlouvy (10).

Pomocí outsourcingu lze zajistit cokoliv, co je pro společnost výhodné, je možné smluvně dohodnout a kde lze určit KPI k ohodnocení práce poskytovatele. Příklady oborů, kde je outsourcing v praxi využíván, jsou:

- Finanční řízení a ekonomika firmy (vedení účetnictví);
- Informatika a řízení ICT (provoz ICT infrastruktury nebo aplikací);
- Facility management (správa budov a infrastruktury);
- Logistika a doprava (spediční služby) (11).

Z využití outsourcingu v praxi lze např. uvést příklad, kdy společnost nemá dostatečné vědomosti či hardware k provozování fungující sítě, tak si zajistí outsourcingovou firmu, která se za smluvní poplatek o provoz sítě postará. Síť tak bude plně v režii dodavatele, který nese zodpovědnost za její funkčnost. V případě, že dojde k poruše jakéhokoliv hardwaru nebo softwaru, zaměstnanec podá hlášení outsourcingové společnosti a ta jej musí dle smluvních podmínek do určitého času vyměnit či opravit, dle podmínek SLA (9).

K využívání outsourcingu mohou vést různé důvody, které je možné kombinovat, jako např.:

- Nižší náklady, které dokáže garantovat pouze poskytovatel služby;
- Vyšší kvalita nabízených služeb ze strany poskytovatele;
- Přenesení rizik na poskytovatele;
- Nedostatek vlastních zkušeností;
- Nedostatek vlastních lidských zdrojů;
- Nedostatek investičních prostředků;
- Větší zkušenosti dodavatele v konkrétní oblasti nebo s technologií;
- Potřeba specializovaných technologií, pro které společnost nemá dostatek zkušených zaměstnanců (11).

Cloud computing

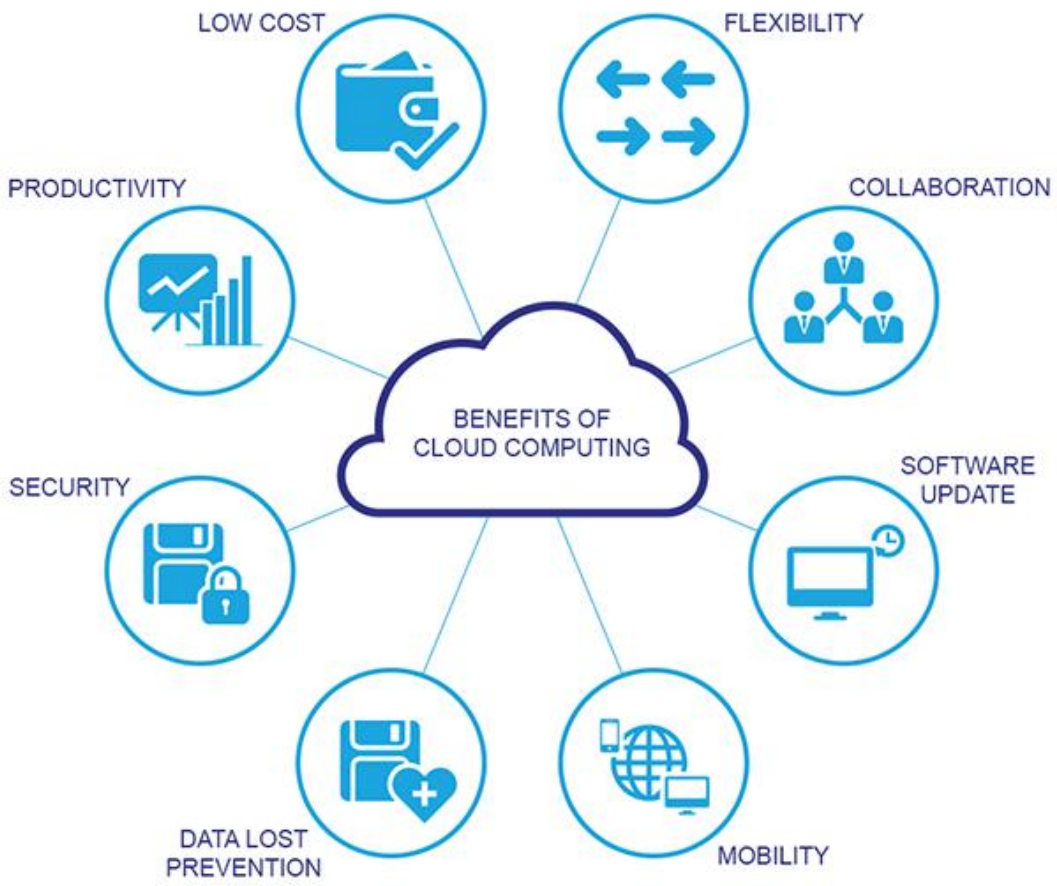
Slovo „cloud“ v překladu znamená mrak a s nabízením IS si lze toto slovní spojení představit ve smyslu, že jsou data uložena „někde, kde na ně fyzicky není vidět“. Cloud computing lze jednoduše popsat jako doručování výpočetních služeb (servery, úložiště, sítě, software, analytické nástroje, inteligentní funkce apod.) přes internet. Toto řešení nabízí rychlejší inovace, flexibilitu prostředků a úspory. Uživatel obvykle platí jen za cloudové služby, které skutečně využije, což pomáhá snižovat provozní náklady, efektivněji provozovat infrastrukturu a přizpůsobovat se měnícím se obchodním potřebám (12).

Cloud computing poskytuje mnoho výhod, mezi které patří zejména:

- **Náklady** – eliminace nákladů spojených s nákupem hardwaru a softwaru a provozem datových center, kam spadají servery, zdroje nepřetržitého napájení, chlazení anebo IT pracovníci;
- **Rychlost** – služby jsou většinou poskytovány jako samoobslužné a na vyžádání, takže i ohromná množství výpočetních prostředků lze v případě rychlého internetového připojení zajistit takřka okamžitě;
- **Výkon** – největší poskytovatelé cloudu běží v celosvětové síti zabezpečených datových center, která jsou pravidelně upgradována tím nejmodernějším hardwarem, což oproti jednomu podnikovému datovému centru přináší řadu výhod;
- **Zabezpečení** – velké množství poskytovatelů cloud computingu nabízí širokou škálu zásad a technologií, které posilují stav zabezpečení, čímž napomáhají k ochraně dat, aplikací a infrastruktury před potenciálními hrozbami;
- **Produktivita** – odstranění potřeby řady nezbytných činností spojených se správou datového centra (nastavení hardwaru, záplatování softwaru a další časově náročné úkoly), díky čemuž lze ušetřený čas využít smysluplněji;
- **Globální rozměr** – neboli schopnost elastické škálovatelnosti, znamená dodání vhodného množství IT prostředků dle potřeby, např. méně nebo více výpočetního výkonu nebo úložiště z vhodné geografické polohy (12).

Většina služeb cloud computingu spadá do tří hlavních kategorií, kterým se taktéž říká stack cloud computingu, jelikož jsou postaveny jedna na druhé:

- **IaaS** – Infrastruktura jako služba – základní kategorie služeb cloud computingu, ve které dochází k pronájmu výpočetního výkonu, IT infrastruktury, sítí, úložiště atd. za průběžný poplatek;
- **PaaS** – Platforma jako služba – dodávání prostředí pro vývoj, testování a správu softwarových aplikací. Tento typ je určen především pro vývojáře, kterým poskytuje důležitý výkon k vývoji aplikací, bez starostí o nastavování a správu IT;
- **SaaS** – Software jako služba – dodávání softwarových aplikací pomocí internetu, na vyžádání a na základě předplatného (12).



Obr. 6: Princip cloud computingu. (13)

1.5 Analytické nástroje

V této části budou popsány základní principy analytických nástrojů, mezi které patří např. SWOT analýza, PEST analýza, Porterova analýza nebo hodnotící metodika ZEFIS.

1.5.1 SWOT analýza

Tato analýza je určena ke zjištění klíčových silných (Strengths) a slabých (Weakness) stránek, příležitostí (Opportunities) a hrozeb (Threats) společnosti. Jsou zde zpracovávány a zdůrazňovány klíčové položky vyplývající z interního a externího auditu – silné a slabé stránky vyplývající z vnitřního prostředí společnosti a příležitosti a hrozby z vnějšího okolí (14).

SWOT analýzu je možné použít k hodnocení celé společnosti, pro jednotlivé oblasti, produkty nebo jiné účely. Její podstatou je identifikování klíčových silných a slabých stránek uvnitř společnosti – v čem je společnost dobrá a v čem naopak slabá. Je také důležité znát významné příležitosti a hrozby, které se nacházejí ve vnějším prostředí. Cílem této analýzy je identifikování a následné zredukování slabých stránek, podporování silných stránek, hledání příležitosti a znalost hrozeb (15).

Obr. 7: SWOT analýza. (15)

Analýza externího prostředí (příležitosti a hrozby)

Vedení společnosti musí rozpoznat hlavní příležitosti a hrozby, kterým čelí. Účelem této analýzy je donutit manažera předvídat důležité trendy, které mohou mít na společnost dopad (14).

Analýza interního prostředí (silné a slabé stránky)

Silné a slabé stránky nezahrnují všechny charakteristické rysy společnosti, ale pouze ty, které mají souvislost s kritickými faktory úspěchu. Příliš dlouhý seznam ukazuje na nedostatečnou koncentraci a neschopnost rozlišit, co je podstatné. Z tohoto důvodu jsou silné a slabé stránky relativní, nikoli absolutní (14).

1.5.2 PEST analýza

PEST analýza rozebírá klíčové makroekonomické faktory ovlivňující společnost. Tato analýza rozděluje vlivy do čtyř skupin:

- **P** – politické – vliv politických stran, zákony, stabilita a vývoj politické situace, nadnárodní politika;
- **E** – ekonomické – rychlost růstu ekonomiky, inflace, nezaměstnanosti, vývoj HDP, úrokové sazby, daně;
- **S** – sociální – skladba společnosti, kultura, náboženství, etika (úroveň korupce, dodržování zákonů atd.), zvyklosti;
- **T** – technologické – úroveň průmyslu, dopravy, dopady nových technologií, inovační potenciál a tempo jeho růstu (16).

Analýza se snaží sledovat vliv makrookolí na fungování společnosti. Přestože toto makrookolí téměř není možné ovlivňovat, správné sledování této oblasti může firmě pomoci ke zjištění, v jakém prostředí se nachází a jaké jsou nejpodstatnější faktory, které podnikání v této oblasti ovlivňují. Společnost má také díky PEST analýze možnost se připravit dopředu na rizikové oblasti a trendy, které je možné z této analýzy vyčíst (16).

PEST analýza je nejčastěji používána při rozhodování nad dlouhodobým strategickým cílem společnosti nebo plánování realizace velkého projektu. Dalším důvodem pro

provedení této analýzy jsou i akvizice nebo investice. Na rozdíl od SWOT analýzy tedy není aplikována příliš často (17).

1.5.3 Porterova analýza

Porterova analýza slouží ke zjištění externího prostředí ovlivňující společnost. Podstatou této analýzy je předpověď vývoje konkurenční situace v analyzovaném odvětví, získána na základě odhadu možného chování následujících pěti subjektů působících na trhu a rizik, která představují:

- **Stávající konkurence** – její schopnost ovlivňovat cenu a množství produktu / služby;
- **Nová konkurence** – možnost, že vstoupí na trh nový subjekt, který ovlivní cenu a množství produktu / služby;
- **Dodavatelé** – jejich vyjednávací schopnosti k ovlivnění ceny a nabízeného množství potřebných surovin a nákladů na jejich pořízení;
- **Odběratelé** – jejich schopnosti k ovlivnění ceny a poptávaného množství produktu / služby;
- **Substituty** – možnost vzniku náhražek produktů dané společnosti jinými produkty (18).

Působení těchto sil rozhoduje o schopnosti společnosti získat ze svých investic určitý zisk. Síly ovlivňují nejen ziskovost odvětví trhu, ale také výši cen a nákladů a jsou základním faktorem pro návratnost investic. Cílem každé společnosti je správné porozumění vlivu těchto faktorů a jeho využití k dosazení co nejvyšších zisků (19).

Obr. 8: Porterova analýza. (18)

1.5.4 Hodnotící metodika ZEFIS

ZEFIS je elektronický konzultant, který umožňuje najít nedostatky v oblasti IS a jejich zabezpečení. Poskytuje nejen doporučení, jaké věci by bylo vhodné vylepšit, ale také ukazuje, zda a v jaké míře trpí těmito nedostatky ostatní podobné společnosti (20).

V systému se nejprve pomocí dotazníků popíše společnost, její informační systémy a procesy. Systém ZEFIS na základě těchto odpovědí a souvislostí mezi nimi vytvoří přehled základních nedostatků, které následně zobrazí podle možného dopadu na společnost ve třech pásem rizika: červené – vysoké riziko, oranžové – střední riziko, zelené – nízké riziko. Systém rovněž poskytuje doporučení, jak je možné nedostatky obecně odstranit a ukazuje u každého nedostatku srovnání, jak vypadá situace u srovnatelných společností, aby bylo možné si udělat představu, zda jde o nedostatek běžný, nebo ne (20).

Hodnotící metodika ZEFIS dělí rizika do následujících sedmi oblastí:

- **Technika (Hardware)** – správný hardware umožňuje, aby na něm bylo možné realizovat systémy a programy a aby byl dostatečně rychlý a spolehlivý;
- **Programy (Software)** – zaměřuje se na informační systémy a programy, které jsou ve společnosti používány. Prvním úkolem IS je doručovat správnou informaci na správné místo a ve správný čas, a druhým (možná ještě důležitějším) je pomáhat zaměstnancům v jejich práci;
- **Pravidla (Orgware)** – pravidla, směrnice a pracovní postupy určující, jak mají být činnosti správně prováděny a zjišťují, zda existují a zda jsou dodržována a kontrolována;
- **Pracovníci** – schopnost zaměstnanců pracovat podle pravidel, bez zbytečných chyb;
- **Data** – zkoumá se, zda jsou bezpečně uložena, dostatečně chráněná a kompletní;
- **Zákazníci** – tato oblast zkoumá, zda systémy, které se jich týkají, nebo s nimi pracují, vyhovují jejich potřebám a zájmům a zda jsou osobní data chráněna dle požadavků GDPR;
- **Provoz** – ověřuje, zda mají pracovníci zajištěnou podporu, jestli dodržují pravidla a na jaké problémy při své práci narážejí (20).

1.5.5 Lewinův model

Lewinův třífázový model změn patří mezi nejstarší a nejznámější modely změn ve společnosti. Tyto změny mají dle Kurta Lewina probíhat ve třech fázích:

- **Rozmrazení** – současné úrovně (příprava změny);
- **Změna** – přechod na novou úroveň (intervence v systému);
- **Zamrazení** – nové úrovně (fixace dosažených výsledků) (21).

Model odpovídá na následující otázky: Jaký vliv bude mít změna? Co všechno tato změna ovlivní? Jakého stavu chceme díky změně dosáhnout? Jaké síly působí pro realizace změny a jaké proti? Které úseky společnosti tato změna zasáhne? Jakým způsobem se změna provede? Jak celý proces dopadl? (21).

1.5.6 FMEA (Analýza možných vad a jejich následků)

FMEA je používána pro preventivní odstranění možných závad a chyb. Pomáhá identifikovat nejkritičtější a nejpravděpodobnější chyby u výrobků nebo procesů a umožňuje rozeznat možnosti vzniku poruch, určit jejich možné následky, ohodnotit rizika a bezpečně jim předejít. Hlavní myšlenka vychází z toho, že pro každý projev poruchy na nejnižší úrovni se analyzují možné lokální nebo systémové následky (22).

Cílem FMEA je vypracování podrobného rozboru celého výrobku z hlediska jeho poruchovosti a případných nápravných opatření již v předvýrobních etapách, aby se dosáhlo produkce výrobků dle předem stanovených požadavků a s minimálními ztrátami (22).

Výhody

- Systémový přístup k prevenci nekvality;
- Zkrácení doby řešení vývojových prací;
- Snížení ztrát vyvolaných nízkou kvalitou systému;
- Optimalizace návrhů a snížení počtu změn ve fázi realizace;
- Podpora účelného využívání zdrojů;
- Ohodnocení rizika možných chyb a na jeho základě stanovení priority a opatření vedoucí ke zlepšení kvality návrhu;
- Zlepšení značky (jméno a konkurenceschopnost firmy);
- Poskytování podkladů pro zpracování nebo zlepšení plánu jakosti;
- Zvýšení spokojenosti zákazníků (22).

2 ANALÝZA SOUČASNÉHO STAVU

Tato část diplomové práce se zabývá popisem a analýzou současné situace ve společnosti Tereos TTD, a.s., díky jejímž pokladům budou následně realizovány návrhy změn informačního systému.

2.1 Představení společnosti

Obchodní název:	Tereos TTD, a.s.
Sídlo:	Dobrovice, Palackého náměstí 1, PSČ 29441
Právní forma:	Akciová společnost
Identifikační číslo:	161 93 741
Základní kapitál:	1 321 011 386 Kč
Datum vzniku a zápisu:	28. března 1991
Předmět podnikání:	výroba cukru a jeho modifikací
	výroba a úprava kvasného lihu
	výroba chemických a biochemických výrobků na bázi cukru a zpracování vedlejších produktů, vznikajících při výrobě cukru
	nákup zemědělských výrobků a surovin pro výrobu cukru a jeho modifikací
	agrochemická, technologická a technická služba pro pěstitele cukrovky

2.1.1 Popis a historie

Obr. 9: Logo společnosti Tereos TTD, a.s. (23)

Společnost Tereos TTD, a.s., se sídlem v Dobrovici, je největším producentem cukru a lihu v České republice a jedna z deseti největších českých potravinářských společností. Ročně je v jejich cukrovarech vyrobeno až 350 tisíc tun cukru a 120 milionů litrů lihu (z toho 60 milionů lihu pitného). Kromě cukrovaru a lihovaru v Dobrovici je součástí společnosti také cukrovar v Českém Meziříčí, lihovar v Chrudimi, Kojetíně a Kolíně a Balicí centrum v Mělníce.

Jedinou základní surovinou pro produkci společnosti je cukrová řepa. Pěstuje ji více než 500 pěstitelů na celkové ploše přesahující 40 000 hektarů. Průměrný výnos řepy z jednoho hektaru dosahuje 80 tun při 16 % cukernatosti, což tyto pěstitele řadí na úroveň těch nejvyspělejších cukrovarnických zemí. Díky dlouhodobé spolupráci s TTD mají pěstitelé zajištěný stabilní odbyt až pro 3 miliony tun řepy.

Historie společnosti sahá až do roku 1831, kdy Karel Anselm Thurn-Taxis, někdejší vlastník dobrovického panství a člen německého knížecího rodu Thurn-Taxisů, nechal přebudovat zámek v Dobrovici na cukrovar. Od té doby je cukrovar nepřetržitě v provozu na tomtéž místě, díky čemuž se stal jedním z nejstarších dosud fungujících řepných cukrovarů na světě a vůbec nejstarším, který využívá původní výrobní budovy.

Po zlatých časech 19. století a skomírání po většinu 20. století, kdy byly cukrovary postupně uzavírány, vstoupil v roce 1992 do Dobrovice francouzský kapitál (dnešní

společnost Tereos), který podpořil rozvoj a opět navázal na to nejlepší z české cukrovarnické tradice. V únoru roku 2012 společnost Tereos TTD dále přikoupila lihovar v Kojetíně a v roce 2019 taktéž lihovar v Kolíně.

2.1.2 Nabízené produkty

Jak již bylo zmíněno, společnost prodává cukr a líh. Cukr nabízí na B2B a B2C trhu, líh pak výhradně na trhu B2B. Co se týče cukru, společnost nabízí různé typy produktů:

- Cukr bílý krystal
- Cukr bílý krupice
- Cukr moučka
- Cukr kostky
- Cukr Camping / Hygienicky balený cukr

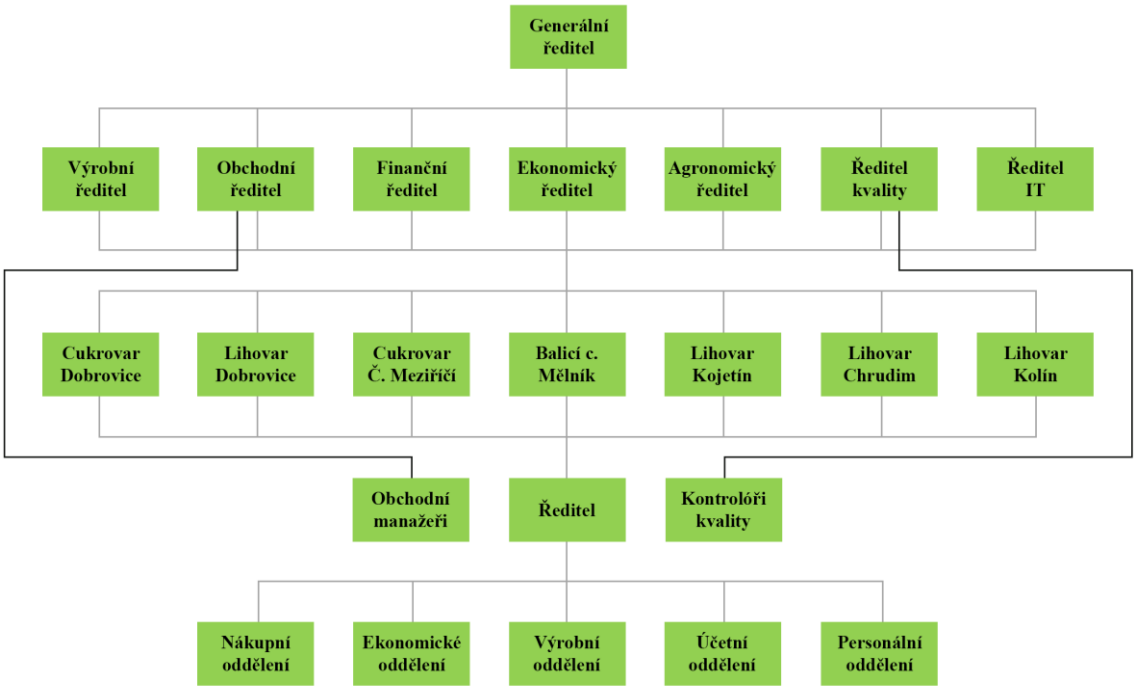
Tereos TTD vyrábí mnoho druhů lihu ve špičkové kvalitě:

- Líh rafinovaný velejemný neutrální
- Líh rafinovaný velejemný
- Líh rafinovaný jemný
- Líh technický
- Líh bezvodý
- Líh bezvodý medicinální
- Líh v kvalitě pro UV
- Líh obecně denaturovaný
- Líh zvláště denaturovaný

Společnost dále nabízí nemrznoucí směsi, E85 nebo další produkty spojené s výrobou cukru a lihu, jako např. úkap, dokap, melasové výpalky a přiboudlina.

2.1.3 Organizační struktura

Na následujícím obrázku je zobrazena organizační struktura celé společnosti, která je funkcionálního charakteru.



Obr. 10: Organizační struktura společnosti Tereos TTD, a.s. (Vlastní zpracování)

2.2 Analýza společnosti

Tato kapitola obsahuje analýzu společnosti, pro kterou byly provedena PEST, Porterova a SWOT analýza, a také analýzu informačního systému pomocí hodnotící metodiky ZEFIS a SWOT analýzy.

2.2.1 PEST analýza

Metoda PEST je součástí analýzy vnějšího prostředí, které působí na společnost, tzv. makroprostředí. Přestože společnost nemůže nijak výrazně tyto faktory ovlivnit, je nezbytné je sledovat, aby na ně bylo možné reagovat.

Politická oblast

Pro společnost jsou politické a legislativní vlivy ohromnou zátěží. Na firmu je kladem veliký důraz na dodržování přísných norem a zákonů, čímž např. vzniká permanentní hrozba doměřování spotřební daně a s tím spojené pokutování.

Od roku 2012, kdy Českou republiku postihla metanolová aféra, navíc společnost čelí dramatickému zvýšení rozličných opatření, která představují ohromnou byrokratickou a administrativní zátěž a nepřetržitou kontrolu ze strany celní správy.

Mezi další významný politický vliv, který ovlivňuje příjmy společnosti, patří povinné přidávání paliva z obnovitelných zdrojů do benzínu. Jeho omezení nebo zrušení by pro společnost znamenalo omezení výroby ethanolu s významnými ekonomickými důsledky.

Všechna tato omezení ze strany státu mají alespoň jeden „pozitivní“ vliv, a to je svým způsobem ochrana před konkurencí. Kvůli velmi přísným zákonům a omezením se v tomto odvětví trhu de facto neobjevuje nová konkurence.

Ekonomická oblast

Výrazným ekonomickým faktorem je kromě kurzu měny také výše spotřební daně. Ta v současnosti činí 285 Kč / litr 100 % lihu a její zvýšení, které vláda plánuje pro rok 2020 (ve výši 13 %), bude pro společnost znamenat komplikace ve výrobě, protože obchodní řetězce budou chtít naplnit sklady ještě levnými lihovinami, takže TTD nejspíš nebude stíhat výrobu a následně, několik měsíců po zdražení, bude mít mnohem nižší prodeje.

Společnost je rovněž velmi ovlivňována propojeným evropským trhem, kvůli čemuž musí čelit silné konkurenci, která, zvláště v případě cukru, velmi sráží cenu a mnohým cukrovarům nezbývá jiné řešení než ukončení činnosti. Paradoxně, další úbytek konkurence způsobený neustálým snižováním ceny, může časem pomoci k opětovnému zvýšení ceny cukru.

Rovněž automobilový průmysl ve Středočeském kraji, především Škoda Auto a s ní spojených mnoho dodavatelských společností, velmi ovlivňuje zaměstnanost v regionu. Nabízí nadprůměrně vysoké mzdy a nutí tak ostatní společnosti (včetně Tereos TTD) výrazně zvedat mzdy a benefity, jinak je zaměstnanci opustí.

Sociální oblast

Ačkoli Češi mají ke konzumaci alkoholu velmi kladný vztah, v poslední době jsou stále častěji k vidění kampaně, které je odrazují od pití. Mezi tyto vlivy lze zařadit např. rady lékařů, různé průzkumy a pořady v televizi, které zdůrazňují, že konzumace alkoholu je velmi nezdravá. Dále je v přípravě zákon, který bude přikazovat označení etiket lahví s lihovinami nálepkami ve stylu „konzumace alkoholu škodí zdraví“, podobně jako je tomu u tabákových výrobků.

Společenský tlak je také vyvíjen na snižování obsahu cukru ve všech potravinách. S kampaní „cukr = bílý jed“ se setkal snad každý z nás. Toto tvrzení je samozřejmě přehnané a nepravdivé, ale neustále nabývá na intenzitě, což do budoucna pro firmu rovněž znamená možný úbytek tržeb.

Technologická oblast

Co se týče zvýšení automatizace výroby, tento trend zde není na místě, jelikož výroba se nachází ve fázi, kterou již není třeba více automatizovat, a naopak je tu nezbytný lidský faktor. Navíc, případné automatizační procesy by byly natolik nákladné, že jejich realizace by byla ekonomicky nevýhodná.

Společnost se neustále potýká se zpřísňováním emisních limitů a s tím spojených kontrol čistoty ovzduší, které obzvláště zkoumají množství uvolňování dusíku a síry, které je způsobeno spalováním uhlí. Firma je nucena instalovat drahé zařízení, jež do síry přidává vápno, které s ní zreaguje a způsobuje snížení obsahu vypouštěné síry. Do budoucna však pravděpodobně dojde k nahrazení uhelného kotle plynovým, který tyto problémy zcela eliminuje.

Požadavky na kontrolu životního prostředí se týkají i vody. Společnost musí používat vlastní čističku odpadních vod, jelikož k výrobě používá vodu z řeky, kam ji následně vrací, čímž je také nucena splňovat velmi přísné limity a normy.

Tab. 1: Shrnutí PEST analýzy. (Vlastní zpracování)

Politická oblast	**Ekonomická oblast**
• Nutnost dodržování neustále se zpřísňujících norem a zákonů • Narůstající byrokratická a administrativní zátěž	• Kurz měny • Výše spotřební daně • Konkurence na propojeném evropském trhu
Sociální oblast	**Technologická oblast**
• Kampaně proti pití alkoholu • Společenský tlak na snižování obsahu cukru v potravinách	• Neustálé zpřísňování emisních limitů • Povinnost používání vlastní čističky odpadních vod

2.2.2 Porterova analýza

Porterův model pěti sil slouží ke zjištění externího prostředí, které ovlivňuje společnost. Mezi tyto faktory patří: stávající konkurence, potencionální nová konkurence, substituční vliv a vliv dodavatelů a odběratelů.

Stávající konkurence

Společnost Tereos TTD má v České republice v produkci a prodeji cukru dominantní postavení na trhu, není tak konkurenčními firmami, kam patří Cukrovar Vrbátky, Moravskoslezské Cukrovary, Cukrovar Litovel a Cukrovar Prosenice, příliš ohrožena. V rámci Evropy je konkurence mnohem silnější, mezi nejvýznamnější hráče na poli patří Francie, Španělsko, Německo, Itálie a Polsko.

Na trhu s lihem má společnost v České republice ještě dominantnější postavení a konkurence zda v podstatě není. Na evropském trhu je však konkurence mnohem nejsilnější, nejvíce v Německu, Francii, Polsku, Slovensku a Maďarsku.

Nová konkurence

V České republice je kvůli byrokratické zátěži vznik nové konkurenční společnosti velmi nepravděpodobný. V rámci Evropy však nová konkurence vzniká. Nejvíce na vzestupu je Maďarsko, kde se z ohromného množství kukuřice vyrábí škrob, tekuté cukry a líh. Tyto komodity začínají společnosti Tereos TTD konkurovat nejen na evropském trhu, ale začínají se pomalu dostávat i do Česka.

Substituty

Možnost vzniku substitutů na trhu s cukrem a lihem je značně omezená, ne však nemožná. A tak se v polední době stává substitutem dovoz cukru získaného z cukrové třtiny vypěstované v Jižní Americe a Asii. Ten díky své značně nižší ceně a obrovskému vyprodukovanému množství začíná na evropském trhu konkurovat stávajícím cukrovarům, které se mu cenou nemohou rovnat.

Dodavatelé

Dodavateli jsou zemědělci, kteří pěstují cukrovou řepu. Toto pěstování je však dotováno státem a ministerstvo zemědělství údajně zvažuje snížení těchto dotací. V případě, že se tak stane, zemědělci značně omezí pěstování cukrové řepy, kterou nahradí plodinou s vyšší výnosností (např. řepkou olejkou) a společnost Tereos TTD nebude mít z čeho vyrábět, což by pro společnost mělo nedozírné následky, jelikož řepu kvůli vysoké ceně dopravy není možné dovážet ze zahraničí.

Odběratelé

Značný vliv mají velcí odběratelé, kteří tvoří většinu příjmů společnosti. Cirka 20 % z nich odebírá 80 % zboží (klasické Paretovo pravidlo). Mezi tyto odběratele patří nadnárodní výrobní společnosti, které díky svému velkému odebíranému množství tlačí na co nejnižší nákupní cenu a společnost Tereos TTD se jim pochopitelně snaží vyjít vstříc, jelikož si je vědoma skutečnosti, že by mohla být snadno nahrazena zahraničními konkurenty, čímž by přišla o většinu svých příjmů. TTD je však velkou a nadnárodní společností, díky čemuž je schopna pokrýt požadavky těchto odběratelů nejen na českém trhu, ale v rámci celé Evropy, čímž se pro ně stává velmi silným partnerem.

Tab. 2: Shrnutí Porterovy analýzy. (Vlastní zpracování)

Faktor	Hrozby	Příležitosti
Stávající konkurence	• Posílení konkurence na evropském trhu	• Zvýšení podílu na evropském trhu
Nová konkurence	• Posílení maďarské konkurence	• Nízká pravděpodobnost vzniku nové konkurence na tuzemském trhu
Substituty	• Zvýšení dovozu cukru z cukrové třtiny	/
Dodavatelé	• Snížení dotací pro pěstování cukrové řepy	• Udržení stávající produkce cukrové řepy
Odběratelé	• Odchod velkých odběratelů ke konkurenci	• Silné partnerské vztahy s odběrateli v rámci celoevropského trhu

2.2.3 SWOT analýza

Tato analýza slouží ke zjištění silných a slabých stránek, příležitostí a hrozeb společnosti. V následující tabulce jsou sepsány údaje, které byly získány zejména z předchozích analýz.

Tab. 3: SWOT analýza společnosti. (Vlastní zpracování)

Silné stránky	**Slabé stránky**
• Dobré jméno společnosti • Vysoká kvalita výrobků • Silná pozice na tuzemském trhu • Výhodné geografické umístění • Silné dodavatelské a odběratelské vztahy • Vyspělé technologie ve výrobě	• Neustálá omezení ze strany státu • Omezení výrobní technologie na pouze jednu vstupní surovinu
Příležitosti	**Hrozby**
• Zvýšení prodejů nemrznoucí směsi • Zvýšení procentuálního podílu obnovitelných paliv (ethanolu)	• Kurz měny • Legislativní změny • Potencionální nedostatek vstupní suroviny • Sílící tlak na omezování spotřeby cukru a alkoholu

Silné stránky

Mezi silné stránky společnosti patří dobré jméno, vysoká kvalita výrobků, silná pozice na tuzemském trhu, výhodné geografické umístění v rámci Evropy, silné dodavatelské a odběratelské vztahy a vyspělé technologie používané ve výrobě. Další silnou stránkou je fakt, že se jedná o silnou a stabilní společnost, díky čemuž se nemusí obávat náhlých změn na trhu.

Slabé stránky

Do slabých stránek společnosti jednoznačně spadají neustálá omezení ze strany státu spojená s legislativní kontrolou, která velmi znepříjemňují a komplikují podnikání. Jedná se tedy o vnější faktory, které firma není schopna ovlivnit, ale může se jim pouze přizpůsobit. Jako další slabou stránkou společnosti by bylo možné zmínit omezení výrobní technologie na zpracování pouze jedné vstupní suroviny – cukrové řepy. Jak je známo, líh je možné vyrobit např. také z obilí, brambor a kukuřice, ale technologie TTD jsou přizpůsobeny pouze na zpracování cukrové řepy.

Příležitosti

Společnost moc nových příležitostí k růstu nemá. Lze sem zařadit např. zvýšení prodejů nemrznoucí směsi a zvýšení procentuálního podílu obnovitelných paliv (ethanolu).

Hrozby

Neustálou hrozbou jsou legislativní změny a kurz měny. V případě výrazného posílení koruny vůči euru by pro společnost bylo velmi složité prodávat cukr na evropském trhu. Dalšími hrozbami jsou potencionální nedostatek vstupní suroviny anebo čím dál silnější společenský tlak na omezování spotřeby cukru a alkoholu.

2.3 Analýza informačního systému

Tato kapitola obsahuje hodnotící metodiku ZEFIS a SWOT analýzu informačního systému společnosti.

2.3.1 Hodnotící metodika ZEFIS

Hodnotící metodika ZEFIS zahrnuje analýzu sedmi klíčových oblastí. K získání výsledků bylo zapotřebí na portálu ZEFIS.cz odpovědět na 170 otázek týkajících se informačního systému a společnosti samotné.

Nedostatky informačního systému

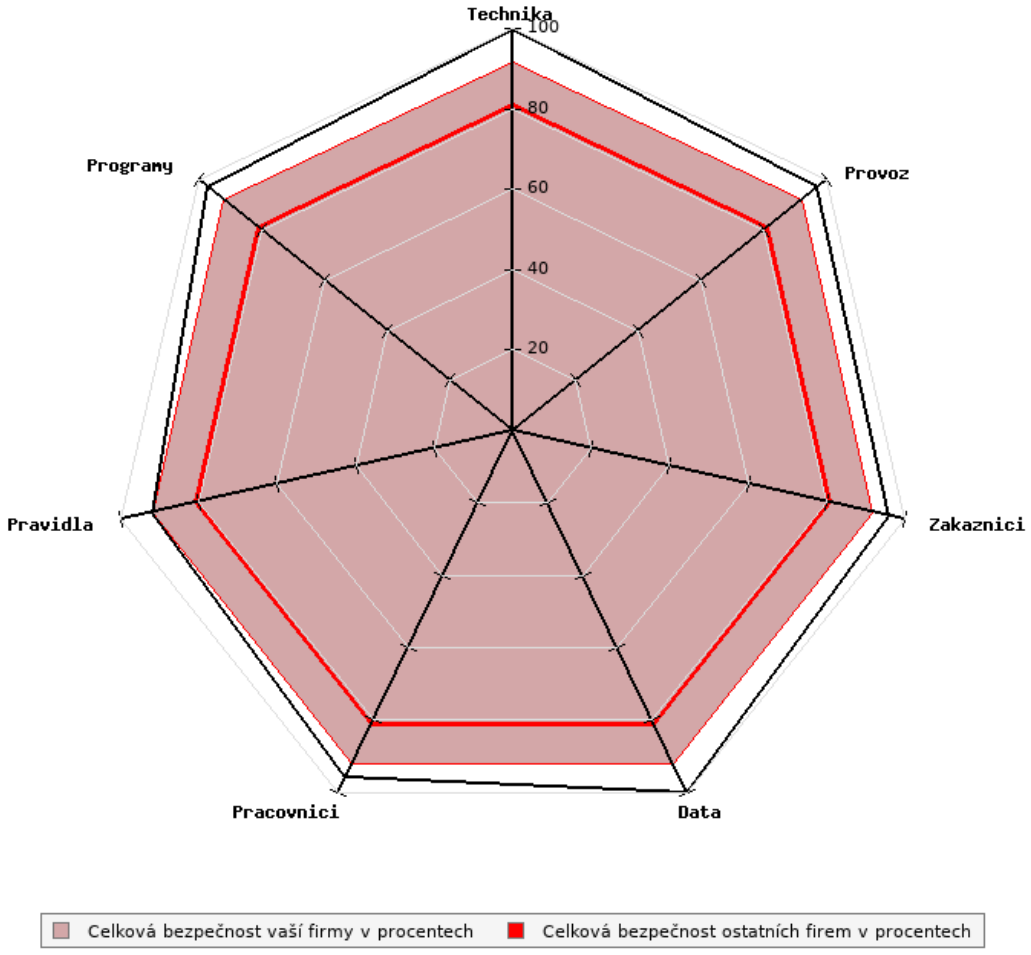
Společnost Tereos TTD používá informační systém Helios Green, který byl zakoupen jako hotový produkt a následně vylepšen o požadované prvky navíc. Jak je možné vidět na následujícím obrázku, společnost má tento systém dobře nastavený, protože pouze dva nedostatky byly ohodnoceny rizikem s vysokou významností, které je nejdůležitějším faktorem, jelikož celková úroveň systému je dána jeho nejslabším článkem.

Oblast	Významnost	Bezpečnost	Typ	Název
Pravidla	Vysoká	Ne	Neshoda	Chybí informační strategie
Pravidla	Vysoká	Ano	Neshoda	Chybí strategie bezpečnosti
Pracovníci	Střední	Ano	Neshoda	Neprobíhají periodická bezpečnostní školení uživatelů IS
Pracovníci	Střední	Ano	Neshoda	Bezpečnostní hrozba z přístupu na internet
Data	Střední	Ano	Neshoda	Riziko zneužití dat, virového útoku
Pravidla	Nízká	Ano	Neshoda	Špatně nastavené pracovní postupy
Programy	Nízká	Ne	Neshoda	Nejednotné ovládání systému
Programy	Nízká	Ne	Neshoda	Pracovníkům chybí některá data nebo funkce
Provoz	Nízká	Ne	Neshoda	Pomalá doba odezvy technické podpory
Provoz	Nízká	Ne	Neshoda	Není známo, jak jsou příjemci spokojeni s výstupy procesu

Obr. 11: Výpis nedostatků informačního systému. (24)

Bezpečnost informačního systému

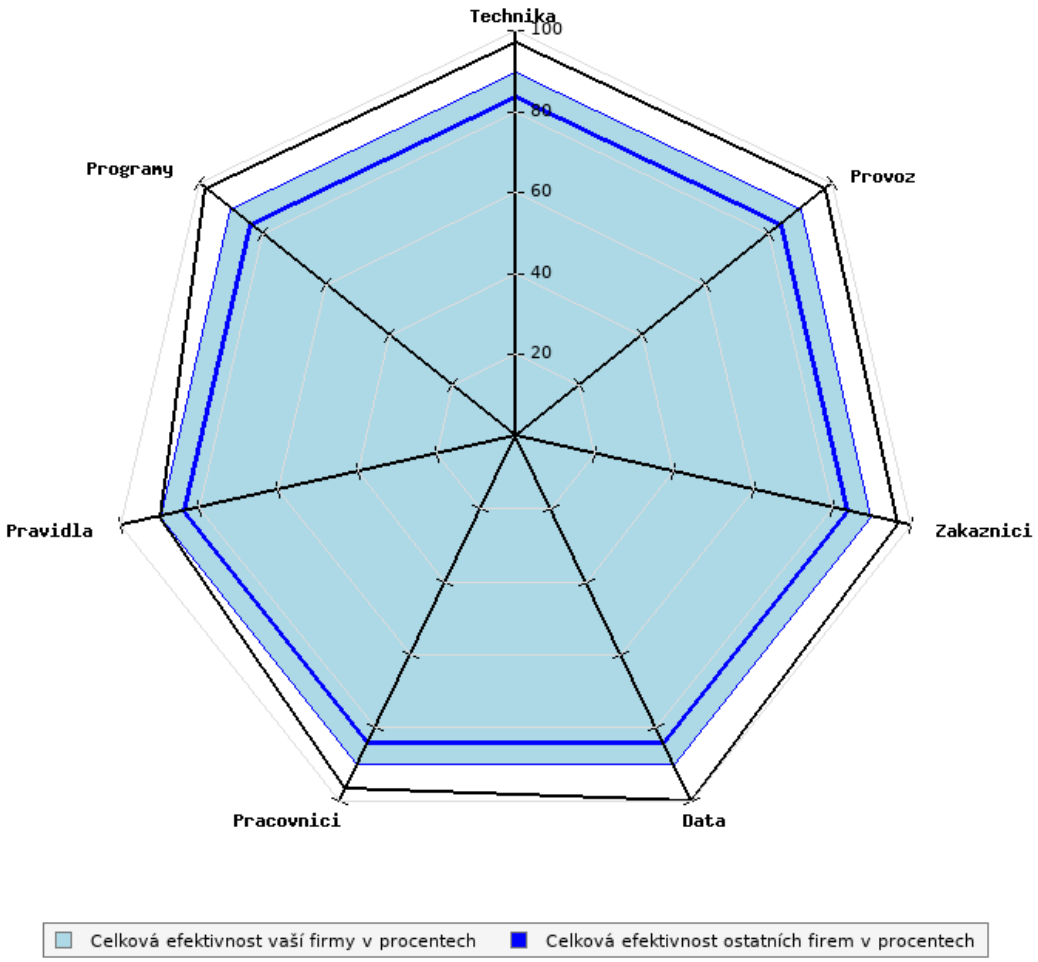
Celková úroveň bezpečnosti IS byla na základě průzkumu ohodnocena výsledkem 92 %. V porovnání se zabezpečením u jiných společností, viz. legenda na obrázku 12, se tedy jedná o dobrý výsledek, z čehož je možné usoudit, že bezpečnost je poměrně kvalitně zajištěna, nicméně i přes tento fakt má (relativně závažné) nedostatky.



Obr. 12: Bezpečnost informačního systému. (24)

Efektivnost informačního systému

Efektivnost představuje stupeň dosažení stanoveného cíle, kterým jsou správně vybrané, nastavené a provozované informační systémy a procesy společnosti. Na grafu na obrázku 13 je možné vidět odhad efektivnosti jednotlivých oblastí, který dosáhl hodnocení 90 %, což je nadprůměrný výsledek. Cílem u efektivnosti IS je usilování o vyvážené řešení, kdy by všech sedm oblastí mělo dosahovat přibližně stejných hodnot, jelikož takové řešení má nejnižší náklady a nejvyšší účinnost.



Obr. 13: Efektivnost informačního systému. (24)

V následujících odstavcích jsou popsány nejvýznamnější nedostatky (ty, které jsou na obrázku 11 zvýrazněny červenou a oranžovou barvou) informačního systému a doplněny o doporučení jejich eliminace. Podklady k těmto nedostatkům byly převzaty z portálu ZEFIS.

Chybí informační strategie

Strategie je způsob, jakým se dostat k určenému cíli, který si předsevzalo vedení společnosti a podle toho stanovuje své cíle, kam chce směřovat, a vytváří podnikovou strategii, jak těchto cílů dosáhnout. Součástí podnikové strategie je rovněž strategie informační, ve které se stanovuje, jaké informační systémy a technika jsou zapotřebí pro dosažení podnikových cílů.

- **Vytvořit informační strategii** – Nejdříve je třeba mít cíle, kterých má společnost dosáhnout. U těchto cílů se stanoví, jaké nástroje z oblasti informačních systémů jsou nezbytné, aby bylo cílů dosaženo. Informační strategie tedy obsahuje postupy, co je zapotřebí koupit, kde, kdy a jak implementovat a vše potřebné, včetně zaškolení zaměstnanců.

Chybí strategie bezpečnosti

Strategie bezpečnosti je postup, který stanovuje, co vše se musí udělat, aby ve výsledku byly zabezpečeny informační systémy a technika a také, aby zaměstnanci nedělali žádné rizikové činnosti, které by mohly vést ke zničení nebo zneužití dat. Chybějící strategie bezpečnosti je velmi riskantní, jelikož počítačoví útočníci mohou kdykoli odcizit velmi citlivá data, proto je nezbytné se jí věnovat.

- **Vytvořit bezpečnostní strategii** – Při sestavování bezpečnostní strategie je nejprve nutné vymezit, která aktiva je zapotřebí chránit a stanovit technická a organizační opatření, jak tyto hrozby eliminovat. Míra rizika je dána dopadem a pravděpodobností vzniku. Je tedy zřejmé, že velké nebezpečí nehrozí tam, kde je malý dopad na společnost. Taková rizika lze pominout. Velmi nebezpečná jsou ale rizika, kde dopad na společnost je velký a pravděpodobnost vzniku je vysoká. Zde jako častý příklad z praxe lze uvést ponechání firemního notebooku na

sedadle automobilu nebo umístění serverovny do místnosti v suterénu, s okny bez mříží.

Neprobíhají periodická bezpečnostní školení uživatelů IS

Jestliže informační systém shromažďuje citlivá osobní data, je nezbytné provádět pravidelná bezpečnostní školení zaměstnanců, kde jsou jim připomínány hlavní bezpečnostní opatření, kterými jsou povinni se řídit.

- **Zajistit periodická bezpečnostní školení zaměstnanců** – Tato školení musí zaměstnancům připomínat, jaká pravidla a zásady musí dodržovat, aby nedocházelo k únikům dat. Protože vzhledem k tomu, že informační systém společnosti obsahuje citlivá osobní data, která je třeba v případě, že dojde k bezpečnostnímu incidentu, chránit, je nutné dokázat, že k ochraně dat bylo vyvinuto maximální možné úsilí.

Bezpečnostní hrozba z přístupu na internet

Přístup na internet je dnes považován za samozřejmost, ale z webu je možné bez vědomí uživatele stáhnout počítačové viry, které dokáží ohrozit chod celé společnosti.

- **Posoudit nezbytnost přístupu na internet** – Je důležité dobře zvážit, zdali zaměstnanci ke své práci potřebují plný přístup k internetu, anebo si vystačí s omezeným přístupem na vybrané webové stránky, čímž se riziko napadení viry značně snižuje. Řešení v podobě úplného odříznutí zaměstnance od internetu jednak není dobře přijímáno, ale hlavně je v podstatě nemožné, protože všichni nevýrobní pracovníci společnosti bez přístupu na internet de facto nemohou svou práci vykonávat.

Riziko zneužití dat, virového útoku

V případě, že je zaměstnanci dovoleno připojit ke svému počítači externí média (flash disky, externí HDD apod.), může z počítače nebo do počítače cokoli zkopírovat nebo nainstalovat neschválené programy a mohl by tedy, v případě že nejsou nastavena omezení, nakazit počítač virem, což zvyšuje riziko úniku dat.

- **Omezit připojování externích médií k počítačům pracovníků** – Vesměs není důvod, proč by měl zaměstnanec ke svému pracovnímu počítači připojovat externí média, je tedy třeba zvážit, zda je nezbytné tuto možnost technicky (přímo v nastavení počítače, nikoli pouze „ústní dohodou“) zakázat, či nikoli. Společnost Tereos TTD na svých počítačích nemá technicky zakázáno připojování externích médií, pouze není možné instalovat nechválené programy.

2.3.2 SWOT analýza

V následující tabulce je stručně shrnuta SWOT analýza informačního systému, která hodnotí jeho silné a slabé stránky, příležitosti a hrozby.

Tab. 4: SWOT analýza informačního systému. (Vlastní zpracování)

Silné stránky	**Slabé stránky**
• Poměrně kvalitní zabezpečení • Vysoká efektivnost • IS je sám o sobě kvalitní produkt od renomované společnosti	• Chybějící informační a bezpečnostní strategie • Neperiodická bezpečnostní školení zaměstnanců
Příležitosti	**Hrozby**
• Vytvoření informační a bezpečnostní strategie • Zajištění periodických bezpečnostních školení zaměstnanců • Omezení připojování externích médií k firemním PC • Omezení přístupu na internet	• Možný únik dat a napadení systému kvůli neomezenému přístupu na internet a možnosti připojování externích médií k firemním PC

3 VLASTNÍ NÁVRHY ŘEŠENÍ

Z předešlých analýz byly zjištěny hlavní nedostatky informačního systému, které slouží jako podklad pro vlastní návrhy řešení. V této části diplomové práce bude pracováno výhradně s výsledky hodnotící metodiky ZEFIS. Primárním cílem je zvýšení zabezpečení informačního systému společnosti.

3.1 Zvýšení zabezpečení informačního systému společnosti

Ačkoli v hodnotící metodice ZEFIS dosáhla celková úroveň bezpečnosti informačního systému hodnocení 92 %, bezpečnostní strategie společnosti stále obsahuje kritické chyby, které je třeba eliminovat. Vyřešení těchto nedostatků přinese mnohem vyšší zabezpečení IS, což je v dnešní době, kdy čím dál častěji dochází k útokům hackerů / crackerů, naprosto nezbytné. Navíc je třeba tato citlivá data chránit i kvůli GDPR, jinak firmě hrozí vysoké pokuty.

3.1.1 Bezpečnostní školení zaměstnanců

Z hodnotící metodiky ZEFIS vyplynulo, že ve firmě neprobíhají periodická bezpečnostní školení uživatelů IS. V návaznosti na toto zjištění navrhuji zavedení pravidelných (dvakrát za rok) interních bezpečnostních školení, kde budou zaměstnanci seznámeni s novými změnami a zásadami, které je třeba dodržovat, aby nedocházelo k únikům dat.

Školení budou probíhat dvěma způsoby. Nevýrobní zaměstnanci, kteří pracují s počítači a přichází do styku s informačním systémem denně, se zúčastní kurzu, kde jim nové informace bude předávat pracovník IT oddělení. Těchto zaměstnanců je přibližně 200. Zbylým pracovníkům (více jak 300) budou potřebné materiály rozeslány e-mailem. Všichni zaměstnanci následně budou muset své nově nabyté znalosti prokázat v on-line testu. Ti, kteří neuspějí, budou test muset absolvovat znovu, dokud nedosáhnou požadovaného výsledku.

3.1.2 Šifrování disků firemních PC

Počítače společnosti jsou chráněny pouze uživatelským jménem a heslem. Pevné disky však šifrovány nejsou a v případě odcizení notebooku tak stačí pouze vyjmout disk, připojit jej do počítače a všechna data budou zpřístupněna. Toto je velmi riskantní počínání a je třeba jej napravit.

Opatřením proti ztrátě dat je zašifrování celých disků počítačů (FDE – Full Disk Encryption), na které zaměstnanci data ukládají. Při FDE je zašifrován celý disk včetně prázdných míst a nešifrovaná je pouze malá část určená pro start počítače. Veškeré informace na disku jsou tak chráněny a uživatel nijak neovlivňuje, zda soubor uloží šifrovaně či nikoli, protože celý prostor je šifrován automaticky.

Jako všechno, i šifrování disků má svá pro a proti. Mezi nevýhody patří např. požadavky na výkonnější hardware počítačů, a to kvůli šifrování a dešifrování velkého objemu dat. Rovněž fakt, že je šifrován celý disk, může způsobit, že počáteční šifrování může trvat i několik hodin. Doba šifrování je pochopitelně závislá na velikosti disku, u prvotního šifrování je však třeba počítat většími časovými nároky.

FDE by mělo splňovat následující požadavky:

- Silná správa klíčů
- Ukládání šifrovacích klíčů odděleně od šifrovaných dat
- Malá zátěž výpočetního výkonu
- Obnovení klíčů (lokálně, mimo lokalitu a obnovení po havárii)
- Odolnost proti poruchám (aby výpadky napájení nebo vypnutí počítače uživatelem neovlivnily proces šifrování)
- Schopnost šifrování na pozadí
- Podpora úsporného režimu a hibernace

Pro FDE navrhuji program Bitdefender, jehož hlavní výhodou je (mimo jiné) integrace do Active Directory, čímž je ošetřena ztráta klíčů.

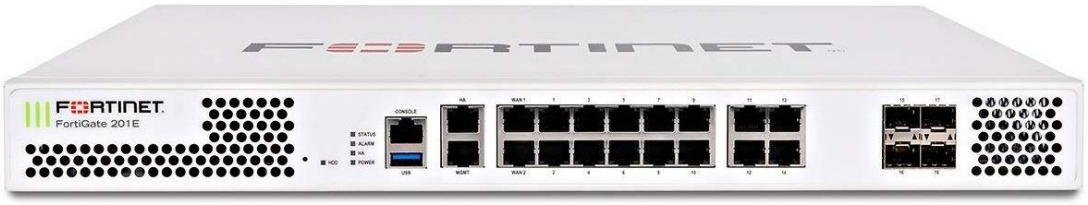
3.1.3 Omezení přístupu na internet

Přístup zaměstnanců na internet je dnes jedním z klíčových faktorů, které ovlivňují chod a výkonnost společnosti. Ale je třeba brát na vědomí rizika, která jsou s neomezeným používáním internetu spjatá. Tato rizika mohou mít velký dopad na byznys společnosti a způsobit např. přímou finanční ztrátu, ztrátu konkurenční výhody nebo diskreditaci společnosti samotné. Řešení v podobě úplného zákazu připojení k internetu však vůbec není na místě, protože všichni nevýrobní pracovníci společnosti Tereos TTD bez internetu nemohou svou práci vykonávat.

Omezení přístupu na internet lze řešit vícero metodami. Jako první se nabízí omezení ve stylu „kdo, kam a kdy“. V tomto případě se vytvoří různé skupiny uživatelů, které budou mít vymezený přístup na konkrétní weby dle časového rámce. Toto řešení si lze např. představit tak, že účetním bude umožněn přístup výhradně na adresy bank a úřadů a to pouze v pracovní době.

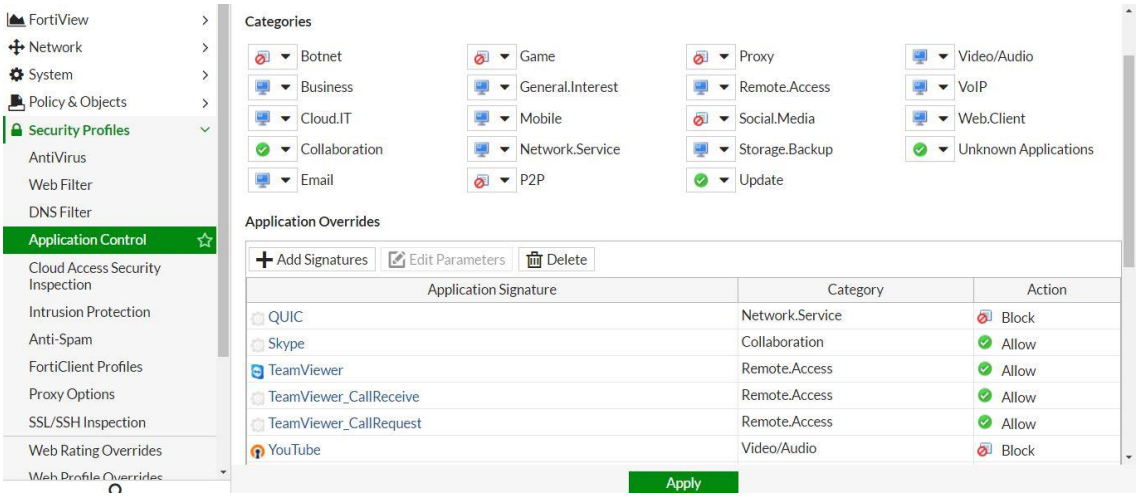
FortiGate

Mnohem efektivnější je však komplexní řešení od společností, které se problematikou bezpečnosti zabývají. Jednou z předních firem je Fortinet. Tato společnost nabízí velmi sofistikované zařízení FortiGate, které nabízí ochranu na základě bezpečnostní analýzy webů.



Obr. 14: Zařízení FortiGate. (25)

Fortinet u webů např. zkoumá, zda se na nich nenacházejí boti, jestli nebyly napadeny nebo zda nejsou jinak zranitelné. Weby, které jsou vyhodnoceny jako nebezpečné, jsou následně uloženy do databází. Tyto pravidelně aktualizované databáze jsou pak za poplatek poskytovány firmám, které díky tomu mají zaručenou mnohem vyšší bezpečnost při používání internetu. Databáze lze následně filtrovat také na základě zájmových oborů – když správce sítě nechce, aby uživatelé navštěvovali např. sociální sítě nebo weby pro dospělé, tak vše může jednoduše zakázat a o nic víc se nestará. Tato nastavení se provádí v sekci Security Profiles. Tyto bezpečnostní profily jsou postaveny z několika základních pravidel, např. že celý datový tok, který jimi prochází, musí podléhat standardní antivirové analýze a DNS filtrování – zachycení neznámých adresací, které by chtěl přeložit jiný jmenný server. Pro zvýšení bezpečnosti by ke správě tohoto zařízení měl být umožněn pouze fyzický přístup vybraným osobám.



Obr. 15: Ukázka prostředí programu FortiGate. (26)

Společnost Fortinet rovněž nabízí komplexní formu zabezpečení, kterou nazývá Security Fabric. V tomto řešení se do brány (FortiGate) zaimplementují koncová zařízení a switche, které jsou následně zobrazovány ve formě „stromu“, kde jsou sledovány toky informací a nabízeny analýzy chyb – zdali jsou na switchi nebo na koncovém zařízení apod. Implementace tohoto řešení je však velmi nákladná a není nezbytně zapotřebí, proto navrhuji zvýšení zabezpečení „pouze“ v podobě výše zmiňovaného zařízení FortiGate.

3.1.4 Omezení připojování externích médií k firemním PC

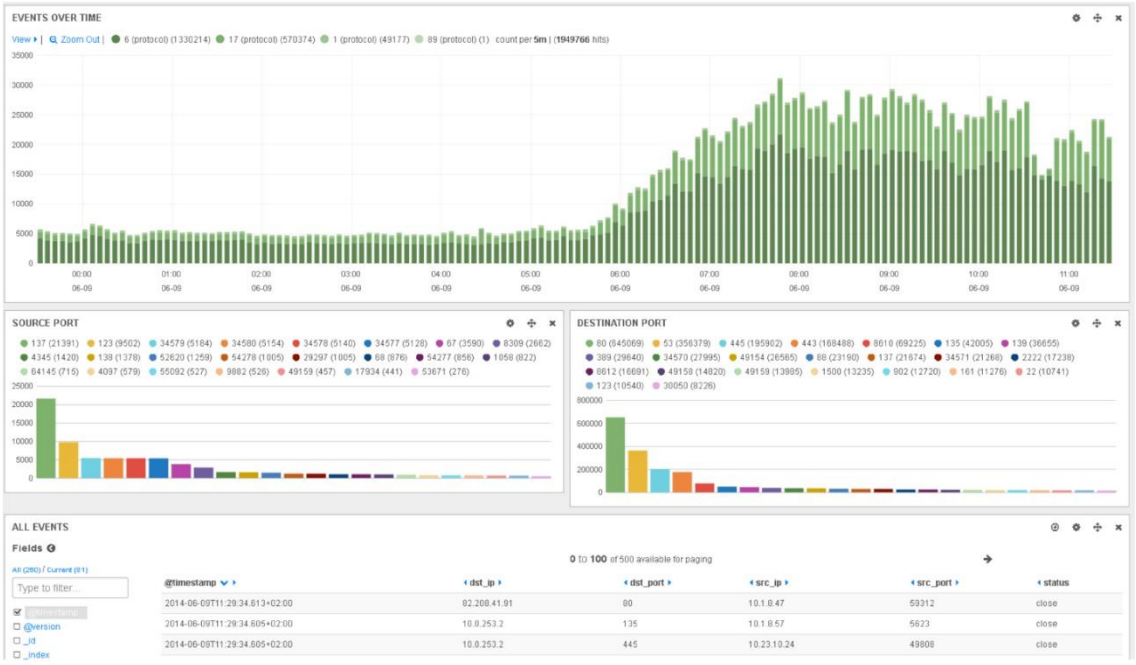
Na počítačích společnosti TTD není zakázáno připojování externích médií, pouze není umožněno instalovat firmou nechválené programy. To je však nedostatečné řešení, jelikož právě klasický „fyzický“ útok pomocí přístupných portů počítačů je jedno z největších rizik úniku dat a to kvůli infikovaným médiím, která po připojení spustí např. ransomware nebo jiný škodlivý kód, který se může do počítače dostat bez jakékoli interakce uživatele a skrytě se nainstalovat ihned po připojení disku do USB konektoru.

Navrhuji tak omezení připojování externích médií k firemním PC. Externí média lze blokovat více způsoby. První možností je plošný zákaz přes Active Directory, v Group Policy. Zde je možné vymezit okruh zařízení, na která by bylo možné externí média připojovat a na která ne. Výjimky by mohly být uděleny pro interní počítače, které slouží především pro prezentace v přednáškových místnostech. Tyto počítače ale nebudou mít umožněn přístup do vnitřní sítě firmy a bude pro ně vytvořen charakteristický adresář, z kterého poté bude možné dokumenty a prezentační materiály převzít, aby nebyla ohrožena vnitřní síť. Dalším způsobem je blokování pomocí antivirového programu, který společnost využívá. Zde lze počítače rozdělit do skupin, u kterých se nastaví, zda se k zařízením v nich mohou externí média připojovat či nikoli. Počítače, které toto připojování budou mít povoleno, nebudou mít po připojení k síti ihned umožněný přístup, ale nejprve u nich proběhnou hlubší analýzy v podobě testů veškerých archivů a neznámých souborů. Oba zmíněné způsoby rovněž dokáží připojovaná zařízení rozlišit dle velkého množství kritérií, např. pomocí typu (flash disk, tiskárna atd.), hardwarového čísla nebo sériového čísla. Je tedy rovněž možné nastavit, že do počítačů lze připojit pouze např. síťovou tiskárnu a žádné jiné zařízení.

Díky tomuto omezení se sníží riziko útoku z vnitřní sítě a případné krádeže dat. Zaměstnanci by jako náhradu sdílení dat přes flash disky více využívali aplikace pro synchronizaci a sdílení dat v informačním systému společnosti, jako např. Microsoft One Drive.

LOGmanager

Pro ještě vyšší zabezpečení doporučuji implementaci LOGmanageru. Jedná se o velmi výkonné zařízení, které analyzuje, kdo vytvořil, upravil, přesunul nebo smazal soubory nebo adresáře, komu posílal e-maily, jaké navštěvoval webové stránky atd., zkrátka analyzuje veškerá kliknutí (logy) všech uživatelů IS. Tato data jsou následně ukládána po dobu několika měsíců. Kvůli velkému objemu, který tato data tvoří, je velmi složité vše sledovat. LOGmanager však nabízí velmi dobré řešení v podobě sledování anomálií pomocí triggerů. Zde je možné nastavit upozornění např. pro víc jak 20 naráz překopírovaných souborů nebo víc jak 3 nepovedená přihlášení a program následně vše přehledně vizuálně zobrazuje pomocí tzv. peeků. Díky tomu lze podezřelé anomálie (např. útoky na hesla uživatelů) jednoduše odhalit a případně eliminovat. Toto zařízení navíc disponuje velmi důležitou certifikaci pro GDPR. Ta garantuje, že veškeré uložené záznamy jsou neměnné po celou dobu životnosti zařízení. Pro zvýšení bezpečnosti by ke správě tohoto zařízení měl rovněž být umožněn pouze fyzický přístup vybraným osobám a datový tok by měl být pouze jednosměrný – do zařízení.



Obr. 16: Ukázka prostředí programu LOGmanager. (27)

3.2 Popis implementace zařízení FortiGate a LOGmanager

Tato část práce navazuje na předchozí sekci a detailněji popisuje implementaci zařízení FortiGate, které slouží pro omezení přístupu na internet a také zařízení LOGmanager, jež poskytuje analýzu chování uživatelů informačního systému. Díky implementaci těchto zařízení se velmi významně zvýší informační bezpečnost společnosti Tereos TTD.

3.2.1 Časový a obsahový plán

Tento plán zahrnuje popis jednotlivých činností navrhované změny a orientační odhad doby trvání. Tyto návrhy, které byly vytvořeny pomocí programů MS Office Excel a Project, zahrnují všechny činnosti, které je třeba zohlednit při realizaci změny.

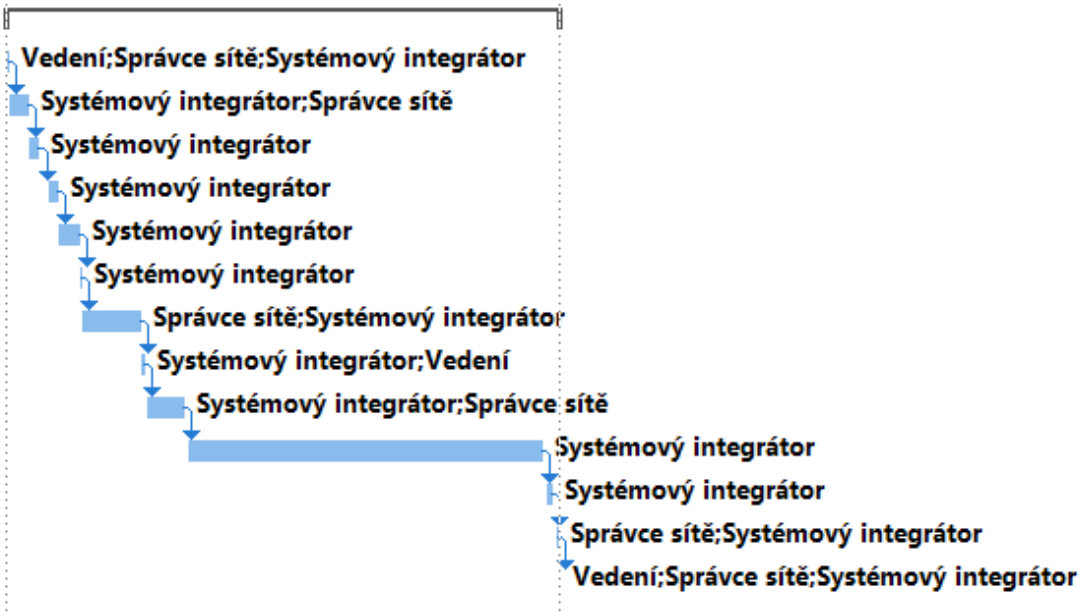
Ačkoli se jedná o zavádění dvou zařízení, postup jejich implementace obsahuje stejné činnosti, dobu trvání i osoby zodpovědné za celý průběh změny. Jedná se totiž o typově stejnou změnu – koupě hotového zařízení, které si bude firma napojovat do vlastní sítě. Z tohoto důvodu byla pro implementaci obou zařízení vytvořena pouze jedna tabulka a jeden Ganttův diagram.

Tab. 5: Návrh činností při implementaci změny. (Vlastní zpracování)

	Název činnosti	Doba trvání (dny)	Předchůdce
	Omezení přístupu na internet	**273**	
1	Meeting	1	
2	Výběrové řízení	10	1
3	Analýza a porovnání nabídek	5	2
4	Předvedení nabídek samotnými výrobci	5	3
5	Ověření nabídek pomocí referencí	10	4
6	Výběr nejlepšího kandidáta	2	5
7	Testovací provoz	30	6
8	Nákup zařízení	2	7
9	Implementace zařízení	20	8
10	Testování a analýzy výstupů	180	9
11	Zavedení do ostrého provozu	5	10
12	Potvrzení úspěšné implementace změny	2	11
13	Dokončení projektu	1	12

Jak je patrné z tabulky výše, navrhovaná implementace každého zařízení spočívá ve 13 krocích, z nichž každý má přímou návaznost na předchůdce. Zahájení probíhá formou meetingu, kde systémový integrátor a správce sítě navrhnou vedení společnosti požadavek na zvýšení zabezpečení IS. Poté proběhne výběrové řízení kandidátů a následná analýza a porovnání jejich nabídek. V následujícím kroku si společnost TTD nechá všechny nabídky odprezentovat samotnými výrobci, načež proběhne ověření jejich tvrzení za pomocí referencí. Po absolvování všech předchozích kroků bude vybraný nejlepší kandidát – v tomto případě zařízení FortiGate a LOGmanager. Toto řešení pak bude zařazeno do testovacího provozu a když bude vyhovovat všem požadavkům, uskuteční se jeho nákup. Po zakoupení zařízení následuje jeho implementace, testování a analýzy, které budou probíhat více než půl roku. Po potvrzení, že je zařízení dostatečně odladěné pro chod společnosti, bude zavedeno do ostrého provozu, čímž je v podstatě tato implementace dokončena.

Odhadovaná doba trvání změny u jednoho zařízení je 273 dnů. Implementace obou zařízení by však neměly probíhat simultánně – z důvodu vyšší priority, kterou má omezení přístupu na internet, nejprve doporučuji instalaci zařízení FortiGate a až následně LOGmanager. V součtu tak plánovaná změna bude trvat nejméně rok a půl. Tato doba se však může lišit v souvislosti s výskytem předem neplánovaných problémů a celková doba tak pravděpodobně bude delší.



Obr. 17: Ganttův diagram implementace změny. (Vlastní zpracování)

3.2.2 Lewinův model

Před započetím implementací navrhovaných změn je vhodné odpovědět na několik otázek, které spočívají např. v určení, jaké jsou síly působící pro změnu a naopak, které síly působí proti změně.

Síly působící pro změnu

- Zájem společnosti o změnu
- Zvýšení zabezpečení informačního systému
- Zvýšení produktivity práce zaměstnanců
- Snížení objemu datového toku

- Předcházení ztrátě kritických dat

Síly působící proti změně

- Možné zpomalení sítě
- Špatně provedená analýza zařízení
- Poměrně vysoké finanční náklady

Agent změny

Agentem změny bude systémový integrátor a správce sítě. Jejich hlavním úkolem bude výběr nejlepšího kandidáta a následná implementace zařízení do informačního systému firmy. Budou tak mí na starosti celou změnu od samého počátku až do konce. Rozhodnutí k uskutečnění navrhované změny bude v kompetencích vedení společnosti, které rovněž bude schvalovat samotné nákupy zařízení, nicméně není považováno za přímého agenta změny.

Intervenční oblasti

Implementace zařízení FortiGate a LOGmanager zasáhne všechny uživatele informačního systému společnosti. Ti se o této intervenci však za normálních okolností vůbec nedozví. Tyto změny je zasáhnou jen u zařízení FortiGate a to pouze v případě, když budou chtít vstoupit na nepovolené webové stránky, které byly vyhodnoceny jako nebezpečné. Zaměstnance tak kvůli těmto změnám není třeba zvlášť školit, protože budou pouze jejími pasivními uživateli a bude stačit je o novinkách jen informovat pomocí e-mailu. Nejvýznamnější intervenční oblastí, která se bude o tuto problematiku aktivně zajímat, je správa sítě.

Fáze intervence

Tato fáze probíhá dle stanoveného harmonogramu tak, aby na sebe jednotlivé činnosti postupně navazovaly. Samotný harmonogram je zpracován pomocí Ganttova diagramu, který se nachází v sekci 3.2.1.

- **Fáze rozmrazení** – Cílem této fáze je provedení různých analýz současné situace a jsou zde shromažďovány veškeré podklady a informace pro další fázi. Výstupem je

zjištění nedostatečné informační bezpečnosti a návrh na její zvýšení v podobě omezení přístupu na internet a analýzy chování uživatelů IS.

- **Fáze změny** – Jedná se o fázi, ve které bude zahájena implementace zařízení FortiGate / LOGmanager, která zahrnuje meeting, výběrové řízení, ověření pomocí referencí, půl roku trvající testování a analyzování a následně zavedení do ostrého provozu.
- **Fáze zmrazení** – Tato fáze je konečnou etapou implementace změny. Dochází zde k plnému využívání nových zařízení a rovněž k prověření, zdali jsou naplněna všechna očekávání a jestli vynaložené náklady byly vhodně investované.

Verifikace dosažených výsledků

U zařízení FortiGate bude kontrola dosažených výsledků prováděna zejména sledováním zablokovaných prokliků na zařízením zablokované webové stránky a rovněž pomocí srovnání hlášení antivirového programu o útocích na síť v době před a po implementaci zařízení.

V případě LOGmanageru bude verifikace probíhat sledováním a vyhodnocováním podezřelých anomálií chování pomocí tzv. peeků, čímž lze např. odhalit útoky na hesla uživatelů.

3.2.3 Identifikace a analýza rizik

Během plánované změny je důležité, aby společnost počítala s možností vzniku rizik, která jsou spjata de facto s každým projektem. Rizika mohou ovlivnit průběh celé změny, je tedy nutné je správně analyzovat.

Pro většinu projektů je jedním z největších rizik čas a s ním spjaté nedokončení v požadovaném termínu. Zde však čas nehraje významnou roli, jelikož implementace bezpečnostních zařízení nemá vliv na chod společnosti jako takové a případné zpoždění projektu má tedy pouze malou závažnost. Mezi nejzávažnější rizika zde patří nedostatečné zabezpečení zařízení a špatně provedená analýza výstupů a je třeba jim tedy věnovat největší pozornost.

FMEA (Analýza možných vad a jejich následků)

Tato analýza byla použita pro nalezení a vyhodnocení možných rizik, která by měla negativní dopad na realizaci změn. Jelikož návrh popisuje implementaci zařízení pro omezení přístupu na internet a analýzu chování uživatelů informačního systému, analyzovány byly pouze aspekty související s touto problematikou.

Z důvodu, že implementace obou zařízení má téměř totožný průběh, u kterého hrozí stejná rizika, byla rovněž vytvořena „pouze“ jedna tabulka FMEA.

Pro rizika byla zvolena stupnice 1 – 10, jejíž význam je uveden v následující tabulce.

Tab. 6: FMEA – stupnice závažnosti. (Vlastní zpracování)

Parametr	Číselné hodnocení	Popis parametru
Žádné	1 – 2	Riziko nepředstavuje žádnou anebo téměř žádnou hrozbu nebo škodu.
Malé	3 – 4	Následky rizika mohou způsobit ztráty, které však nejsou příliš významné.
Střední	5 – 6	Realizace rizika přináší znatelnou újmu.
Velké	7 – 8	Následky rizika jsou významné a mohou způsobit značné ztráty.
Velmi vážné	9 – 10	Následky rizika by byly velmi nákladné jak finančně, tak i časově a představují velký problém.

Tabulka 7 popisuje stupnici pravděpodobnosti výskytu rizikové události.

Tab. 7: FMEA – stupnice pravděpodobnosti výskytu. (Vlastní zpracování)

Parametr	Číselné hodnocení	Popis parametru
Nepravděpodobné	1 – 2	Realizace rizika je možná pouze teoreticky.
Výjimečné	3 – 4	Rizikový aspekt se skoro nevyskytuje a jeho výskyt je málo pravděpodobný.
Malé	5 – 6	K výskytu rizikového aspektu nedochází příliš často, ale jeho výskyt není překvapující.
Velké	7 – 8	Výskyt rizikového aspektu je možný a lze ho předpokládat s vysokou pravděpodobností.
Trvalé	9 – 10	Je téměř jisté, že se rizikový aspekt vyskytne.

V následující tabulce je stanovena stupnice s hodnotami pravděpodobnosti odhalení rizikové události a možnosti prevence.

Tab. 8: FMEA – stupnice pravděpodobnosti odhalení, možnost prevence. (Vlastní zpracování)

Parametr	Číselné hodnocení	Popis parametru
Snadné	1 – 2	Výskyt je snadno předvídatelný, opatření k předcházení jsou známá a snadno použitelná.
Náhodné	3 – 4	Výskyt je předvídatelný, opatření k omezení jsou známá a většinou používána.
Možné	5 – 6	Výskyt aspektu je těžko předvídatelný a opatření k zamezení jsou spíše známá, ale nejsou příliš použitelná.
Omezené	7 – 8	Výskyt aspektu je těžko předvídatelný a opatření k zamezení jsou známá, ale jsou těžko použitelná.
Nemožné	9 – 10	Výskyt aspektu je nepředvídatelný, opatření k zamezení jsou pouze na úrovni havarijní připravenosti a reakce.

V následující tabulce je již FMEA přímo aplikována na návrhy řešení. Rizika, která mají hodnotu RPN přesahující 200, představují vyšší riziko. Opatření jsou navrhnuta pro všechna rizika, protože je zapotřebí snížit pravděpodobnost výskytu všech rizik, a ne pouze těch největších.

Tab. 9: FMEA. (Vlastní zpracování)

	Riziko 1	**Riziko 2**	**Riziko 3**	**Riziko 4**	
Popis rizika, aspektu, vady	Špatně provedená analýza výstupů	Komplikované napojení na IS	Absence klíčové osoby	Nedostatečné zabezpečení	
Možné příčiny	Nedostatek času	Chybějící potřebný modul	Špatná organizace času / komunikační šum	Neznalost všech bezpečnostních rizik zařízení	
Důsledky	Nedostatečná optimalizace zařízení a softwaru	Komplikované programování chybějících částí	Výrazné zpoždění dokončení projektu	Možný únik dat	
Stupeň závažnosti	9	7	8	10	
Pravděpodobnost výskytu	6	4	5	6	
Pravděpodobnost odhalení, možnost prevence	4	2	3	5	
RPN	216	56	120	300	**692**
Navrhovaná opatření, nástroje prevence	Věnovat dostatek času důkladné analýze	Včasné řešení problematiky s dodavatelem IS	Důraz na dodržování termínů a dostatečnou komunikaci	Patřičná znalost všech možných rizik	
Stupeň závažnosti	9	7	8	10	
Pravděpodobnost výskytu	3	2	2	4	
Pravděpodobnost odhalení, možnost prevence	2	1	2	3	
RPN	54	14	32	120	**220**

3.2.4 Vyhodnocení rizik

Celkově byla identifikována 4 (n = 4) rizika, z nichž 2 byla vyhodnocena s vyšším rizikovým číslem RPN (200). Opatření byla ale navržena i ke všem zbylým rizikům, aby byla pravděpodobnost jejich vzniku co nejmenší.

Mezi nejzávažnější rizika patří nedostatečné zabezpečení, které má hodnotu RPN 300. Takto vysoké hodnocení získalo především kvůli vysokému stupni závažnosti a poměrně nízké pravděpodobnosti odhalení a možnosti prevence. Dalším rizikem s RPN vyšším než 200 je špatně provedená analýza výstupů. Zbylá rizika nepředstavují pro projekt významnou závažnost, protože jsou předem snadno odhalitelná.

Pro porovnání stavu před a po zavedení opatření stavu, jsou pro oba tyto stavy vypočítána průměrná riziková čísla – ØRPN, kde n = celkový počet rizik.

- ØRPN před zavedením opatření = $\sum$ RPN / n = 692 / 4 ≅ 173
- ØRPN po zavedení opatření = $\sum$ RPN / n = 220 / 4 ≅ 55

Po srovnání těchto stavů vyplývá, že se správně zavedenými opatřeními je možné celkovou míru rizika výrazně snížit.

3.3 Ekonomické zhodnocení

Tato kapitola je poslední částí návrhu změny a zabývá se zhodnocením nákladů potřebných na implementaci doporučených zařízení pro zvýšení informační bezpečnosti společnosti. Do těchto nákladů nebudou uvedeny mzdy zaměstnanců, kteří budou mít tuto změnu na starosti, ale „pouze“ částky potřebné pro pořízení daných zařízení.

V obou případech (jak FortiGate, tak LOGmanager) se jedná o koupi již hotových řešení, která budou zaměstnanci společnosti Tereos TTD napojena a spravována ve vlastní síti a nebude se tedy jednat o formu cloud computingu. U zařízení FortiGate je navíc k pořizovací třeba počítat s pravidelným ročním poplatkem za aktualizované databáze nebezpečných webů.

V následující tabulce je uveden cenový odhad pořízení těchto zařízení. Z této tabulky lze např. vyčíst, že v případě FortiGate jsou pořizovací náklady v porovnání se zařízením LOGmanager téměř poloviční, nicméně je zde hrazen pravidelný roční poplatek, který bude při používání tohoto zařízení tím nejvyšším nákladem. Celková cena implementace obou zařízení a roční poplatek za první rok tak vyjde odhadem na 1 750 000 Kč.

Tab. 10: Ekonomické zhodnocení. (Vlastní zpracování)

Zařízení	Pořizovací náklady	Další náklady	Celkem
FortiGate	550 000 Kč	250 000 Kč / rok	800 000 Kč
LOGmanager	950 000 Kč		950 000 Kč
			1 750 000 Kč

3.3.1 Přínosy

Po implementaci navrhovaných změn společnost velmi výrazně zvýší zabezpečení svého informačního systému, což je tím nejdůležitějším přínosem. Konkrétní přínosy implementace jednotlivých zařízení jsou popsány v následujících odstavcích.

FortiGate

Zde jsou hlavním přínosem pravidelně aktualizované databáze nebezpečných webů, díky kterým společnost Tereos TTD může efektivně omezit přístup na internet. Součástí této placené služby je rovněž nepřetržitá profesionální podpora a servis ze strany výrobce a pravidelná školení o aktuálních hrozbách. Díky tomu, že společnost Tereos TTD bude tuto formu zabezpečení outsourcovat, nemusí zaměstnávat bezpečnostní experty a naplno si tak vystačí se stávajícími správci sítě, kteří občas provedou pouze kontroly funkčnosti a opravy aktuálních nastavení pro potřeby firmy. Tímto řešením společnost rovněž ušetří nemalé náklady na mzdy bezpečnostních expertů, jejichž odhad je sepsán v následující tabulce.

Tab. 11: Roční odhad snížení mzdových nákladů na bezpečnost. (Vlastní zpracování)

Pracovní pozice	Počet zaměstnanců	Měsíční mzda	Celkové roční náklady
Bezpečnostní expert	2	70 000 Kč	1 680 000 Kč

Díky omezení přístupu na internet je předpokládáno zvýšení produktivity práce zaměstnanců, jelikož jim nebude mimo jiné umožněno navštěvovat např. sociální sítě nebo zájmové weby typu YouTube apod. Ekonomické výhody, které tato změna přinese, lze však jen velmi těžce odhadnout, protože zaměstnancům by byla vyplácena stejná mzda, i kdyby zmíněné weby navštěvovali. Nicméně jejich zvýšená produktivita byť jen o půl hodiny denně (kterou průměrně stráví na těchto webech) při odhadovaném počtu 150 zaměstnanců tvoří necelé 4,5 milionu korun ročně, které pro společnost nejsou zbytečně vynaloženými náklady a mohou jí přinést např. vyšší příjmy. Tento odhad mzdových nákladů je pro větší přehled sepsán v tabulce 12.

Tab. 12: Roční odhad zbytečně vynaložených mzdových nákladů. (Vlastní zpracování)

Počet zaměstnanců	Prům. doba denně	Prům. hod. mzda	Celk. roční náklady
150	0,5 h	240 Kč / h	4 320 000 Kč

Spolu se zmíněným zákazem navštěvování webů typu YouTube apod., souvisí také snížení datového toku, což zajistí zvýšení dostupnosti ostatních služeb v síti.

Hlavní přínosy lze sepsat do následujícího seznamu:

- Zvýšení zabezpečení IS
- Nepřetržitá profesionální podpora a servis od výrobce
- Nižší náklady na bezpečnost díky outsourcingu
- Vyšší produktivita práce zaměstnanců
- Snížení datového toku

LOGmanager

Implementace tohoto zařízení má rovněž velké mnoho přínosů, které lze shrnout následovně:

- Předcházení ztrátě kritických dat
- Sběr logů pro řešení provozních problémů a bezpečnostních incidentů
- Centrální přehled s grafickou prezentací
- Splnění požadavků Zákona o kybernetické bezpečnosti a GDPR

ZÁVĚR

Cílem této diplomové práce je analýza stávajícího stavu informačního systému společnosti Tereos TTD, a.s., vyhodnocení jeho efektivnosti a bezpečnosti a následný návrh změn směřující ke zlepšení aktuálního stavu systému a především jeho bezpečnosti.

V teoretické části práce jsou vysvětleny základní pojmy z oblasti informačních systémů, od architektur IS, jejich klasifikace, až po trendy v ERP. Dále jsou zde popsány analytické nástroje, do kterých spadá SWOT, PEST a Porterova analýza, ale také hodnotící metodika ZEFIS, Lewinův model nebo FMEA, které jsou nedílnou součástí dalších částí práce.

Analytická část se zaměřuje na představení společnosti Tereos TTD, a.s., které zahrnuje její popis a historii, nabízené produkty a organizační strukturu. Po těchto informacích následuje analýza vnějšího prostředí (PEST a Porterova analýza) a také SWOT analýza, která přehledně shrnuje silné a slabé stránky, příležitosti a hrozby společnosti. Další sekcí je analýza informačního systému, která je provedena hodnotící metodikou ZEFIS a následně shrnuta SWOT analýzou.

Na analytickou část práce navazuje poslední, návrhová část, jejímž hlavním cílem je zvýšení zabezpečení informačního systému firmy. Díky podkladům získaných z předchozích analýz jsou navrhnuta čtyři opatření, která mají potenciál výrazně zvýšit bezpečnostní strategii společnosti. Mezi tato opatření patří bezpečnostní školení zaměstnanců, šifrování disků firemních PC, omezení přístupu na internet a omezení připojování externích médií k firemním PC. Poslední dvě řešení jsou navíc detailněji popsána – omezení přístupu na internet je řešeno v podobě implementace zařízení FortiGate a opatření k omezení připojování externích médií k firemním PC je provedeno pomocí zařízení LOGmanager. Pro tento návrh je vytvořen časový a obsahový plán, Lewinův model a identifikace, analýza a vyhodnocení rizik. Závěrem je uvedeno ekonomické zhodnocení a shrnutí přínosů těchto změn.

SEZNAM POUŽITÝCH ZDROJŮ

(1) SKLENÁK, Vilém. *Data, informace, znalosti a Internet*. Vyd. 1. Praha: C.H. Beck, 2001, 507 s. ISBN 80-7179-409-0.

(2) KOCH, M. a V. ONDRÁK. *Informační systémy a technologie*. Vyd. 3. Brno: Akademické nakladatelství CERM, 2008, 166 s. ISBN 978-80-214-3732-6.

(3) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2., přeprac. a aktualiz. vyd. Praha: Grada, 2009. Expert (Grada). ISBN 978-80-247-2615-1.

(4) KOCH, Miloš. *Management informačních systémů*. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. ISBN 978-80-214-4157-6.

(5) HRONEK, Jiří. *Informační systémy* [online]. Přírodovědecká fakulta Univerzita Palackého, Katedra informatiky: 2007 [cit. 2019-01-05]. Dostupné z: https://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

(6) BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy: podnik v informační společnosti.* 3. aktualiz. a dopl. vyd. Praha: Grada, 2012. 323 s. ISBN 978-80-247-4307-3.

(7) SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi.* 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.

(8) WOJTOWICZ, E. *Výběr informačního systému*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2011. 83 s. Vedoucí diplomové práce doc. Ing. Miloš Koch, CSc.

(9) MOLNÁR, Zdeněk. *Efektivnost informačních systémů.* 2. rozš. vyd. Praha: Grada, 2001. Management v informační společnosti. ISBN 80-247-0087-5.

(10) Outsourcing. *Management-Consulting.cz* [online]. [cit. 2019-01-14]. Dostupné z: http://www.management-consulting.cz/cz/outsourcing

(11) Outsourcing. *ManagementMania.com* [online]. [cit. 2019-01-14]. Dostupné z: https://managementmania.com/cs/outsourcing

(12) Co je cloud computing? Průvodce pro začátečníky. *Microsoft.com* [online]. [cit. 2019-01-14]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/

(13) Cloud computing. *VisiontechMe.com* [online]. [cit. 2019-01-15]. Dostupné z: http://www.visiontechme.com/cloud-computing.php

(14) KOTLER, Philip. *Moderní marketing: 4. evropské vydání.* Praha: Grada, 2007. ISBN 978-80-247-1545-2.

(15) SWOT analýza. *ManagementMania.com* [online]. [cit. 2019-01-20]. Dostupné z: https://managementmania.com/cs/swot-analyza

(16) SRPOVÁ, Jitka a Václav ŘEHOŘ. *Základy podnikání: teoretické poznatky, příklady a zkušenosti českých podnikatelů.* Praha: Grada, 2010. ISBN 978-80-247-3339-5.

(17) Kde se vzala a k čemu je PEST analýza. *BusinessVize.cz* [online]. [cit. 2019-01-24]. Dostupné z: http://www.businessvize.cz/planovani/kde-se-vzala-a-k-cemu-je-pest-analyza

(18) Analýza pěti sil 5F. *ManagementMania.com* [online]. [cit. 2019-01-24]. Dostupné z: https://managementmania.com/cs/analyza-5f

(19) PORTER, Michael E. *Konkurenční výhoda: (Jak vytvořit a udržet si nadprůměrný výkon).* Praha: Victoria Publishing, 1993. ISBN 80-856-0512-0.

(20) Co je portál ZEFIS. *ZEFIS.cz* [online]. [cit. 2019-01-26]. Dostupné z: https://www.zefis.cz/index.php?p=21

(21) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích.* 2., aktualiz. a rozš. vyd. Praha: Grada, 2006, 296 s. : il. ISBN 80-247-1667-4.

(22) FMEA Analýza příčin a důsledků. *SvetProduktivity.cz* [online]. [cit. 2019-02-18]. Dostupné z: http://www.svetproduktivity.cz/slovnik/FMEA-Analyza-pricin-a-dusledku.htm

(23) O společnosti. *CukrovaryTTD.cz* [online]. [cit. 2019-02-21]. Dostupné z: http://www.cukrovaryttd.cz/o-spolecnosti/profil/

(24) Výsledky. *ZEFIS.cz* [online]. [cit. 2019-02-26]. Dostupné z: https://www.zefis.cz/index.php?p=55&sp=0

(25) Products. *Fortinet.com* [online]. [cit. 2019-04-02]. Dostupné z: https://www.fortinet.com/products.html

(26) Forum. *Fortinet.com* [online]. [cit. 2019-04-02]. Dostupné z: https://forum.fortinet.com/download.axd?file=0;143116

(27) LOGmanager – logmanagement system and SIEM. *LOGmanager.cz* [online]. [cit. 2019-04-06]. Dostupné z: https://www.logmanager.cz/

SEZNAM OBRÁZKŮ

SEZNAM TABULEK