VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZMĚN IDENTITY MANAGEMENTU V PODNIKU
COMPANY IDENTITY MANAGMENT CHANGES PROPOSAL

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. David Hruška

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

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. David Hruška**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2017/18

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

Návrh změn identity managementu v podniku

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Navrhnout změny IM ve společnosti.

Základní literární prameny:

BERTINO, E. a K. TAKAHASI. Identity Management: Concepts, Technologies and Systems. Boston: Artech House, 2011. ISBN 978-1-608807-039-8.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací. Praha: Český normalizační institut, 2013.

DOUCEK P. a kol. Řízení bezpečnosti informací. 2. rozšířené vydání. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. 1. vyd. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

POŽÁR J. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005. ISBN 80-86898-38-5.

YIP D., G. WILLIAMSON, I. SHARONI a K. SPAULDING. Identity Management: A Primer. Lewisville: MC Press, 2009. ISBN 978-1583470930.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

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

ABSTRAKT

Tato diplomová práce je zaměřena na návrh implementace změn identity managementu do konkrétní společnosti. V teoretické části jsou uvedeny základní pojmy a také podrobný popis identity managementu. Dále je zde popsána analýza současného stavu bezpečnosti informací v dané společnosti, provedena analýza rizik a výběr opatření pro minimalizaci nalezených rizik. Na závěr této práce jsou navrženy změny, jejich postup a časový plán zavedení vybraných opatření.

ABSTRACT

This diploma thesis focuses on the proposal to implement changes of identity management into a particular company. In the theoretical part are the basic concepts and a detailed description of the identity management. There is also described an analysis of the current state of information security in the company, risk analysis and selection of measures to minimize the risks found. At the end of this thesis are proposed changes, their procedure and timetable for implementation of selected measures.

KLÍČOVÁ SLOVA

Identity management, ISMS, bezpečnost, proces, společnost, architektura, přístup, heslo, analýza rizik, PDCA model, informační systém, normy řady ISO/IEC 27000

KEYWORDS

Identity Management, ISMS, Security, Process, Company, Architecture, access, password, risk analysis, PDCA model, information system, ISO / IEC 27000 series standards

BIBLIOGRAFICKÁ CITACE

HRUŠKA, D. *NÁVRH ZMĚN IDENTITY MANAGEMENTU V PODNIKU*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. Počet stran 73 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

ČESTNÉ PROHLÁŠENÍ

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

V Brně dne 16. 5. 2018 .....

podpis

PODĚKOVÁNÍ

Chtěl bych tímto poděkovat vedoucímu práce panu Ing. Viktoru Ondrákovi, Ph.D. za vedení práce, ochotu, profesionální přístup a odbornou pomoc pří psaní diplomové práce a také panu Ing. Tomáši Hanykovi za cenné rady a oponenturu.

OBSAH

ÚVOD

Informace, zejména ty důvěrné, mají v dnešní době velkou cenu a pro společnost je tedy velice důležité chránit takové informace před vnějším zneužitím, poškozením či dokonce ztrátou. Společnost se snaží takovým hrozbám předejít tím, že investuje značnou část finančních prostředků do patřičných opatření, kde samozřejmě platí, že čím větší je informační bezpečnost požadována, tím vyšší náklady jsou potřeba na zavedení změn. Jedním z opatření, které významně přispívá k vyšší bezpečnosti, je systém řízení identit. I přes použití těch nejmodernějších technologií je však nemožné zajistit stoprocentní bezpečnost, protože nejrizikovější faktor jsou právě lidé respektive zaměstnanci společnosti. Je nutné dbát na školení všech zaměstnanců ohledně možných hrozeb a nastavit také případné postihy, aby měla dotyčná osoba potřebu dodržovat všechna bezpečnostní pravidla.

V této diplomové práci se budu zabývat integrací změn identity managementu ve společnosti Cleverlance Enterprise Solutions a.s. Téma diplomové práce jsem si vybral na základě zkušeností z odvětví bezpečnosti ze současného zaměstnání, kde pracuji jako CyberArk administrátor a spravuji přístupy na servery významných klientů z Francie a Nizozemska. Společnost Cleverlance jsem si vybral, jelikož jsem zde byl na praxi jak na střední škole, tak na bakalářském studiu. Nejdříve popíši teoretická východiska a na základě analýzy stavu společnosti navrhnu řešení v podobě změn Identity managementu za dodržení všech požadavků.

CÍLE PRÁCE A METODIKA

Cílem této práce je vypracovat, na základě analýzy současného stavu ve společnosti, návrh na změnu systému řízení identit tak, aby vyhovoval požadavkům moderních bezpečnostních technologií a ve firmě se bezpečnost informací maximálně posílila.
Systém musí dodržovat normu ISO/IEC 27001. K dosažení cíle použiji doporučení z rodiny norem rámec systému pro řízení identit. Samozřejmostí je také analýza současného stavu a další prvky teoretických východisek.

V první části této práce jsou zpracována teoretická východiska jako základní pojmy a podrobnosti týkající se systému řízení bezpečnosti informací (ISMS). Také je zde shrnuta metodika COBIT, knihovna ITIL, normy řady ISO/IEC 2700 a zejména Identity management jako takový. V další části jsou uvedeny základní informace o dané společnosti a je provedena analýza současného stavu bezpečnosti informací ve společnosti. V závěrečné části této práce je provedena analýza rizik a navržena bezpečnostní opatření i s postupem zavedení daných opatření pro minimalizaci zjištěných rizik. Nedílnou součástí je také ekonomické zhodnocené zavedených změn a shrnutí celé práce.

1 TEORETICKÁ VÝCHODISKA

V následující části diplomové práce se budu věnovat problematice identity managementu a ISMS, včetně norem, zákonu a institucí které se danou problematikou také zabývají [1, 2, 7].

1.1 Základní pojmy

Aktivum (Asset)
Mezi aktiva patří vše co má pro podnik nějakou hodnotu (hmotný i nehmotný majetek).

Bezpečnost (Security)
Určuje nám míru ochrany proti hrozbám, které můžou nastat.

Data
Data můžeme získat výpočtem, měřením atd. Pokud jím ale nepřiřadíme význam, jsou to pro nás pouze bezvýznamná čísla nebo text.

Informace (Information)
Pro vytvoření informace jsou nám potřebná data, které následně upravíme do čitelné a užitečné podoby.

Hrozba (Threat)
Událost, která může jakýmkoliv způsobem ohrozit bezpečnost našich aktiv. Rozděluje se na subjektivní a objektivní. Subjektivní jsou hrozby, které plynou z lidského faktoru. Naopak objektivní jsou přírodního původu (požár, povodeň, atd.).

Riziko (Risk)
Určuje nám míru, jak moc je naše aktivum ohroženo (pravděpodobnost ohrožení našeho aktiva).

Zranitelnost (Vulnerability)
Jedná se o slabinu v systému, která může mít za následek poškození nebo zničení aktiv.

Bezpečnostní incident (Security Incident)
Bezpečnostní incident je jakýkoli útok neboli využití zranitelného místa s cílem krádeže nebo poškození určitého aktiva.

Informační bezpečnost (Information security)
Řeší ochranu informací jako celek, zaměřuje se na zachování dostupnosti, důvěrnosti a integrity.

Dostupnost (Availability)
Zajišťuje nám, že daná informace je uživateli přístupná v požadovaný čas.

Důvěrnost (Confidentiality)
Zajišťuje nám, že daná informace je přístupná pouze oprávněnému uživateli.

Integrita (Integrity)
Zajišťuje nám, že daná informace je celkově správná a úplná.

Identifikace (Identification)
Proces určení identity v dané databázi.

Autentizace (Authentication)
Proces ověření skutečné identity, například pomocí hesla nebo pin.

Autorizace (Authorize)
Proces, který povoluje uživateli určité akce, neboli dává mu nějaké oprávnění.

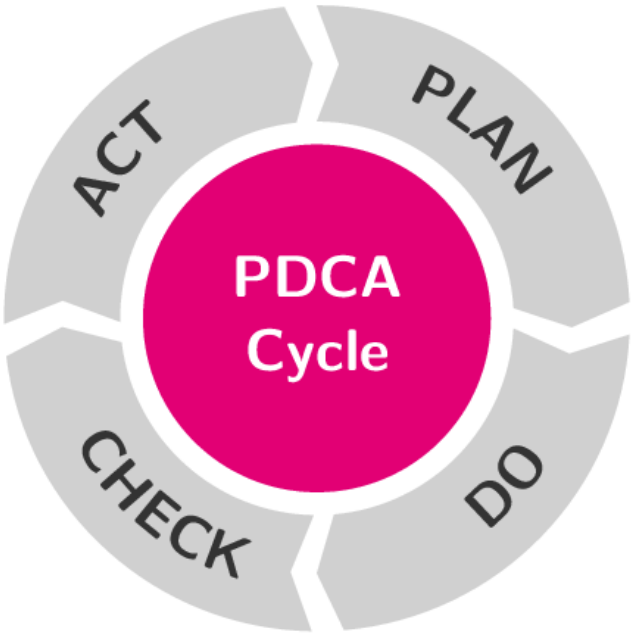
ACL (Access Control List)
Seznam oprávnění uživatelů v dané databázi.

1.2 Systém řízení bezpečnosti informací

ISMS (Information Security Management System) je základem pro účelné a účinné řízení bezpečnosti informací. Představuje část celkového systému řízení organizace, založenou na přístupu organizace k rizikům činnosti, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací [3].

1.2.1 Model PDCA

Tvůrcem modelu PDCA je W. E. Deming, který tento model použil ve svých pracích o sčítání lidu v Japonsku po druhé světové válce. Deming v tomto modelu formuloval zásady vymezení určitého systému řízení, také jeho realizaci a cyklickou snahu o neustálé zlepšování daného systému. Koncept PDCA modelu se dříve používal v průmyslu pro inovaci a nasazování systému řízení. Dnes je tento přístup základem nejen pro oblast řízení informační bezpečnosti, ale také pro mezinárodní standardy v oblasti integrovaných systémů řízení [3].



Obrázek 1: Model PDCA [16]

Model je tedy snahou postupného zlepšování pomocí neustálého opakování čtyř hlavních činností:

- **Plan (Plánuj)**
  Stanovení ISMS - prvním krokem je stanovení politiky ISMS, její cíle, procesy a postupy, které souvisí se zlepšováním bezpečností informací.
- **Do (Dělej)**
  Implementace ISMS - zde již zavádíme stanovenou politiku ISMS a také všechna opatření, procesy i postupy.
- **Check (Kontroluj)**
  Monitorování a přezkoumání ISMS - provádíme posouzení, případně i měření výkonu procesu vůči stanovené politice ISMS a cílům. Výsledky následně předáváme vedení organizace.
- **Act (Jednej)**
  Udržování a zlepšování ISMS - provedení opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS. [6]

1.2.2 Ustanovení ISMS

V rámci ustanovení musí společnost provést následující kroky:

- stanovit hranice a rozsah ISMS na základě činnosti společnosti a jejich cílů
- určit metodu pro analýzu a hodnocení rizik
- identifikovat rizika, hrozby a jejich dopad na aktiva společnosti
- určit pravděpodobnost výskytu rizika
- návrh možností na eliminaci rizik případně jejich akceptaci
- výběr určitých opatření a nákladů na provedení
- schválení od vedení společnosti a udělení souhlasu k zavedení změny

1.2.3 Zavádění a provoz ISMS

Cílem v druhé etapě cyklu PDCA je hlavně prosazení daného bezpečnostního opatření, které bylo ustanoveno v první etapě. Je velice důležité vysvětlit všem uživatelům a také

manažerům bezpečnostní hrozby a principy, proto je nutné vše pečlivě naplánovat včetně termínů, pověřených osob apod. Veškerá bezpečnostní opatření by měla být součástí Příručky bezpečnosti informací.

Pro druhou etapu jsou důležité tyto činnosti [5]:

- Je potřeba vytvořit plán eliminace rizik a následně ho aplikovat v praxi.
- Jasně stanovit pravidla a postupy u daných opatření
- Zapsat pravidla do Příručky bezpečnosti informací
- Zavést potřebná bezpečnostní opatření z předchozí etapy
- Zaškolení uživatelů, manažerů a všech pracovníků z oblasti řízení bezpečnosti.
- Zasadit se o způsob měření a sledování účinnosti opatření
- Vytvořit postup pro řešení incidentů a detekci vzniku
- Zdroje, informace a dokumenty se záznamy ISMS musí podléhat procesu řízení.

1.2.4 Monitorování a přezkoumání ISMS

Následuje třetí etapa cyklu PDCA, kde je hlavní cíl prověřit veškerá zavedená bezpečnostní opatření včetně důsledků na ISMS, abychom dostali účinnou zpětnou vazbu. Ze zpětné vazby může vedení podniku získat představu o skutečném stavu a fungování ISMS. Je zde potřeba provést interní audity ISMS alespoň jednou za rok. Management podniku prozkoumá na jejich základě, zda je ISMS v souladu s obecnými potřebami organizace, a vytvoří závěrečnou zprávu o celkovém stavu, pokud jsou nalezeny chyby, nebo nedostatky, jsou následně eliminovány v následující fázi [5].

1.2.5 Údržba a zlepšování

Tato etapa údržba a zlepšování je poslední v celém cyklu, hlavní cíl je, jak už název napovídá, vylepšovat, kontrolovat a zavádět změny. Na základě předchozí etapy, kde ze závěrečné zprávy lze zjistit, zda je ISMS v souladu s obecnými potřebami podniku či nikoliv. Je zde tedy nutné provést činnosti jako zlepšení ISMS, zavést nápravné nebo preventivní opatření pro nápravu chyb. Tato etapa tedy slouží pro odstranění nedostatků systému a určitými opatřeními také předejít budoucímu návratu těchto chyb [5].

1.3 Systém řízení bezpečnosti informací

V této kapitole budou stručné popsány metodika COBIT a knihovna ITIL, které se využívají v oblasti řízení bezpečnosti.

1.3.1 ITIL

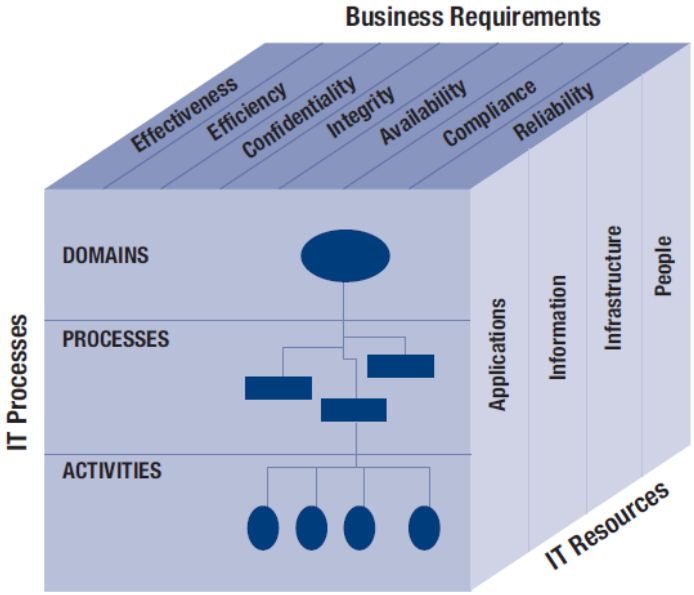
Information Technology Infrastructure Library (ITIL) můžeme považovat za mezinárodní standard pro správu IT služeb. Je to v podstatě sada publikací s praktickými zkušenostmi, které řeší jak dodávat kvalitní IT služby, procesy nebo funkce. Jsou zde popsány typy procesního řízení infrastruktury a služeb. ITIL je takový rámec, který je založen na celoživotním cyklu tzn. Strategie, návrh a přechod služeb, jejich provoz a neustálé zlepšování. To co ovšem knihovna ITIL neřeší, jsou konkrétní pracovní role, architektura organizační struktury a pracovní postupy či jejich obsah. [2]. Knihovnu ITIL spravuje organizace Office of Government Commerce (OGC), která v roce 2007 vydala již třetí verzi této knihovny [2, 5].

Obrázek 2: Cyklus ITIL [17]

1.3.2 COBIT

Mezinárodně uznávaná metodika COBIT (Control Objectives for Information and related Technology) se snaží strukturovat systém řízení informačních a komunikačních technologií tak, aby mu rozuměli jak řídící pracovníci, tak uživatelé s nižšími znalostmi IT. Cílem je, aby využití informací a nasazení ICT podporovalo dlouhodobý rozvoj organizace, naplňovalo cíle podniku a snižovalo případné rizika [2].

Pěkně lze metodiku také popsat pomocí COBIT kostky, která na svých osách *x* (Informační kritéria), ose *y* (IT procesy) a ose *z* (IT zdroje) znázorňuje prolínání těchto kritérií. Mezi požadavky na informační kritéria patří účelnost, účinnosti, důvěryhodnost, integrita, dostupnost a spolehlivost. Mezi zdroje IT patří aplikace, informace, infrastruktura a lidi. Poslední IT procesy rozdělujeme na úrovni domény, procesů a cílů aktivit [5].



Obrázek 3: COBIT kostka [18]

1.3.3 Normy řady ISO/IEC 27000

V kapitole níže budou popsány některé normy řady ISO/IEC 27000. Tyto normy obsahují doporučení pro zavedení systému řízení bezpečnosti informací. Řada norem ISMS má souhrnný název Informační technologie - Bezpečnostní techniky a jejím úkolem je pomoct organizacím všech typů a velikostí zavést a provozovat ISMS. Obsahuje především následující normy [2, 7]:

ČSN ISO/IEC 27000 Systémy řízení bezpečnosti informací - Přehled a slovník

Tato norma nabízí přehled systému řízení bezpečnosti informací. Je zde vysvětleno co znamení ISMS, k čemu a proč se využívá. Jsou zde uvedeny pojmy a terminologie pro ostatní normy v ISMS. V současnosti je platná verze této české normy z roku 2014, která byla přeložena z mezinárodní normy [2, 7].

ČSN ISO/IEC 27001 Systémy řízení bezpečnosti informací - Požadavky

Tato norma specifikuje požadavky na ustavení, zavedení, udržování, neustálé zlepšování a případnou certifikaci ISMS v rámci organizace. Jsou zde stanoveny požadavky na posuzování a ošetření rizik, tedy na výběr a zavedení bezpečnostních opatření. Nejnovější vydání normy 27001 je z roku 2014, resp. její mezinárodní předlohy z roku 2013. Pro dosažení shody s touto normou, musí být splněny všechny požadavky [8, 10].

ČSN ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací

Norma nabízí přes několik tisíc bezpečnostních opatření a doporučení pro řízení systému bezpečnosti informací v podniku, ty jsou rozděleny do strukturovaných oblastí a kapitol. Díky těmto doporučením může podnik snáze dosáhnout svých strategických cílů. Na základě této normy lze rychle a účinně zmapovat stav bezpečnosti. Norma v současnosti používá nejnovější vydání z roku 2013 [2, 9].

ČSN ISO/IEC 27003 Směrnice pro implementaci systému řízení bezpečnosti informací

Tato norma od jejího vydání v roce 2011 popisuje proces plánování pro implementaci systému řízení bezpečnosti informací, který se dále dělí na pět následujících etap:

- Získání souhlasu managementu podniku se zahájením
- Určení rozsahu a krajních bodů
- Analýza požadavků
- Hodnocení a eliminace rizik
- Návrh ISMS

Výsledkem těchto fází je plán projektu ISMS, který musí být v souladu s normou ISO/IEC 27001 [2].

ČSN ISO/IEC 27004 Řízení bezpečnosti informací - Měření

Tato norma z roku 2011 obsahuje doporučení pro užívání a vývoj metrik, které jsou potřeba pro měření účinnosti zavedení systému ISMS a jeho bezpečnostních opatření. Implementace těchto doporučení je předmětem programu měření bezpečnosti informací. Tento program zahrnuje procesy rozvoje metrik a měření, provádění měření, analýzu dat a hlášení výsledků měření a dále proces vyhodnocení a zlepšování programu měření bezpečnosti informací [2].

ČSN ISO/IEC 27005 Řízení rizik bezpečnosti informací

Tato norma z roku 2011 vychází z konceptu normy ISO/IEC 27001 a poskytuje řídícím pracovníkům doporučení pro řízení rizik bezpečnosti informací. Každá organizace si následně určí svůj postup individuálně [2].

ČSN ISO/IEC 27006 Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

V následující normě, jak již název napovídá, jde o požadavky a doporučení v oblasti auditů pro orgány, které provádí audit nebo certifikaci ISMS. Současná norma je z roku 2011 [2].

ČSN ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací

Poslední popisovanou normou, které je také z roku 2011, je směrnice pro audit ISMS. Jsou zde také doporučení pro řízení auditu jako v přechozí normě s rozdílem, že tato norma vychází zejména z normy ČSN EN ISO/IEC 19011 neboli směrnice pro audit systému managementu jakosti nebo systému environmentálního managementu [2].

Obrázek 4: Přehled řady norem ISO/IEC 27000 [Upraveno dle [13]]

1.4 Identity management

„Správa identit (Identity management) je široká administrativní oblast, která se zabývá identifikace jednotlivce v systému (np. země, sítě nebo podniku) a kontrola jejich přístupů ke zdrojům v rámci tohoto systému tím, že sdruží uživatelské práva a omezení se zavedenými identitami.“ [1].

1.4.1 Účastnici identity managementu

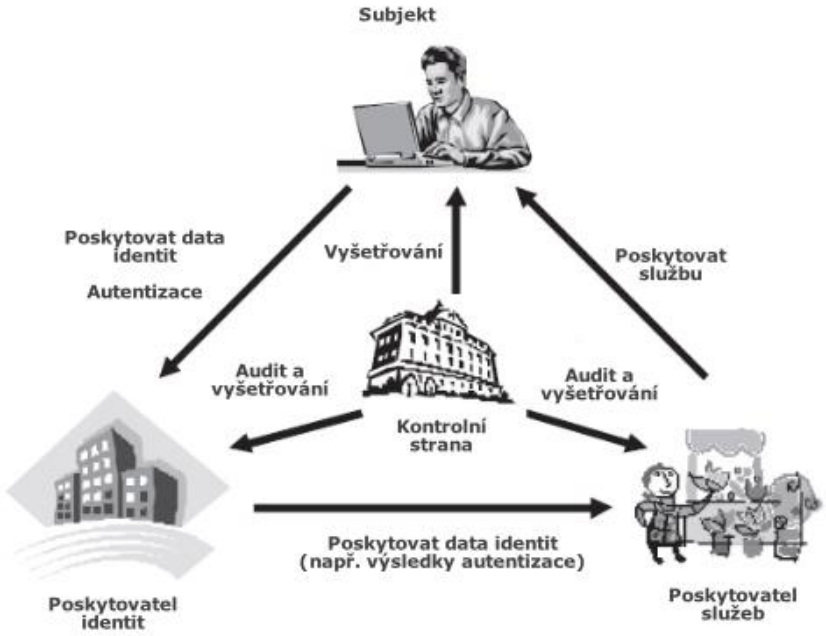
Identity management (IdM)má za úkol poskytovat identity v rámci služeb. Je tedy jasné, že se nejedná o uzavřený systém, ale naopak systém otevřený, ve kterých je zainteresováno více stran rozdělených do rolí [1].

- **Subjekty**
  Je to nejzákladnější skupina účastníků identity managementu, tedy sami uživatelé. Jsou to entity s identitami. Ty obsahují identifikátory, oprávnění a atributy.
- **Poskytovatelé identit**
  Základními úkolu teto skupiny je vytváření a přiřazovaní specifických atributů pro subjekty, provazování atributů a přiřazování oprávnění.

- **Poskytovatelé služeb**

  Skupina, která funguje v IDM jako role, která poskytuje služby a prostředky které si subjekt zažádá. Subjekt musí prokázat svým oprávněním, že má na služby právo.
- **Kontrolní strany**

  Poslední skupina má za úkol především kontrolu a regulaci. Používá se hlavně v auditu.



Obrázek 5: Účastnici identity managementu [Upraveno dle [1]]

Identity management významně souvisí s bezpečností a přispívá k ochraně digitálního majetku společnosti. Nasazení takového systému je komplexní záležitost a otázkou několika měsíců. Společnost může díky IdM používat centrální správu IT a výrazně zjednodušit veškeré procesy [1, 12].

1.4.2 Architektura

Typická architektura by měla být centrálně orientovaná za předpokladu, že koncové systémy jsou propojeny s centrálním prvkem pomocí agentů. Když se řekne koncový systém, je to například systém nebo aplikace, kde jsou uloženy uživatelské účty. Pod pojmem agent neboli konektor můžeme chápat způsob ke komunikaci mezi IdM a

koncovým uzlem. Pro komunikaci se používají standartní protokoly, nejvyužívanější je například LDAP. Identity management funguje za předpokladu, že správně pracují další produkty, ze kterých je IdM složený. Existují tři základní technologie, které se navzájem doplňují, a je velice důležité žádnou nevynechat. Tyto technologie budou podrobněji popsány v dalších kapitolách [1, 12].

- Systém řízení přístupů
- Adresářová služba
- Provisioning

1.4.3 Výhody

Správa identit může společnosti velice prospět zejména zvýšenou bezpečností, snížením nákladů a efektivitou procesů. Výhody, proč je IdM prospěšný, jsou shrnuty níže [1].

- Monitorování přístupu do aplikací a jasně stanovená bezpečností pravidla
- Produktivita zaměstnanců a zjednodušení procesů
- Absence zbytečného papírovaní, menší vytížení help-desku
- Snazší implementace nových služeb a změn
- Potenciální zisk nových zákazníků

1.4.4 Nevýhody

Každá změna má i své nevýhody, níže jsou některé uvedeny:

- Počáteční požadavky na zaměstnance a náklady na implementaci IdM
- Úprava firemní politiky a procesů
- Náklady na průběžné školení pracovníků

1.4.5 Životní cyklus identit

Koloběh v rámci identit je možné rozdělit na čtyři základní části: [1]

- Vytvoření
- Používání
- Úprava
- Řízení
- Zánik

Vytvoření

První část cyklu je vznik, neboli vytvoření identity. Tato část se následně rozděluje na několik menších částí: [1]

1. Dokazování atributů – testování atributů autoritami (podmínka)
2. Vydání oprávnění – autorita/subjekt vydává oprávnění (heslo)
3. Formování identity – shromáždění všech části identity (identifikátor, oprávnění a atributy) a následné vytvoření identity

Používaní

Hned po vytvoření identity, se musí ustanovit pravidla, jak s ní nakládat. Nejdůležitější vlastností pro práci s identitou je bezpečnost a nenarušování soukromí, které nám zajišťují tři způsoby: [1]

1. Důvěryhodná komunikace – Základem důvěryhodné komunikace jsou důvěryhodné identity. Hlavním úkolem je aby obě strany komunikace byly schopny rozlišit a ověřit identitu na druhém konci komunikačního uzlu.
2. SSO (Single Sign-On) – Připojení jednoho subjektu k více službám.
3. Sdílení atributů – Služba, která snižuje redundanci a nekonzistenci atributů mezi poskytovateli identit a služeb.

Úprava

Důležitým krokem v rámci životního cyklu identit je upravování. Identity můžou nebo obsahují data, která se za celý cyklus nezmění, ale i data které své hodnoty mění. Z oblasti oprávnění to může být vypršení platnosti hesla nebo certifikátu. V oblasti atributů np. rodné číslo, bydliště, atd. Při upravování musí byt zachována integrita. [1]

Řízení

Veškeré operace v IdM je třeba zaznamenávat. V řízení životního cyklu můžeme řízení rozdělit na dvě skupiny [1].

- Politiky – ty můžeme dále rozdělit na autentizační, které nám definují úroveň zabezpečení jako například autentizace pomocí hesla či otisku prstů, a autorizační, které nám určují podmínky, za kterých se může jeden subjekt přistupovat k určitým datům či službě.
- Audit – Díky auditu může společnost zkontrolovat, zda je veškerá činnost v souladu s bezpečnostní politikou. Tím, že jsou data ukládána na centrální úložiště a následně analyzována, zvyšuje se celková bezpečnost.

Zánik

Konečnou fází životního cyklu je zánik. Zánik může být částečný nebo úplný, a také přirozený nebo vynucený. Částečný zánik je spíše vypršení než zánik, tedy například vypršení hesla. Úplný zánik je ukončením platnosti celé identity, například odchodem do důchodu, nebo v horším případě úmrtím. Za přirozený zánik lze považovat situaci, kdy člověk ukončí pracovní poměr v dané společnosti. Vynuceným zánikem můžeme chápat jako odcizení identity, tedy například kreditní karty [1].

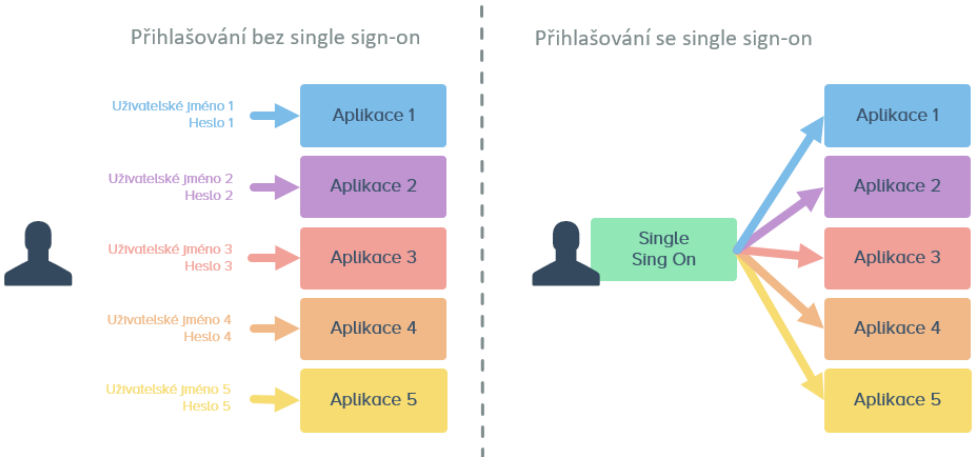
1.4.6 Řízení přístupu

U řízení přístupu se používá několik technologií jako například SSO, RBAC, Provisioning, apod., které jsou popsaný níže. Uživatel se s nimi každodenně setkává, proto je důležité nezanedbat tuto kapitolu při změně IdM. Společnost přiradí svým zaměstnancům práva na základě provedené analýzy a také by měla pravidelně ověřovat, zda je uživatelé stále potřebuje [4].

Single sign-on (SSO)

Pod pojmem SSO si můžeme představit autentizační proces neboli jednotné přihlášení v rámci společnosti, díky kterému uživatel získá přístup k více službám informačního systému. Proces autentizace je proveden na začátku celé relace a poté se již uživatel nemusí znovu autentizovat. Je zde jasná výhoda a to ta, že uživatelé si nemusí pamatovat zbytečně více přihlašovacích údajů do různých aplikací a služeb a postačí mu pouze jedno

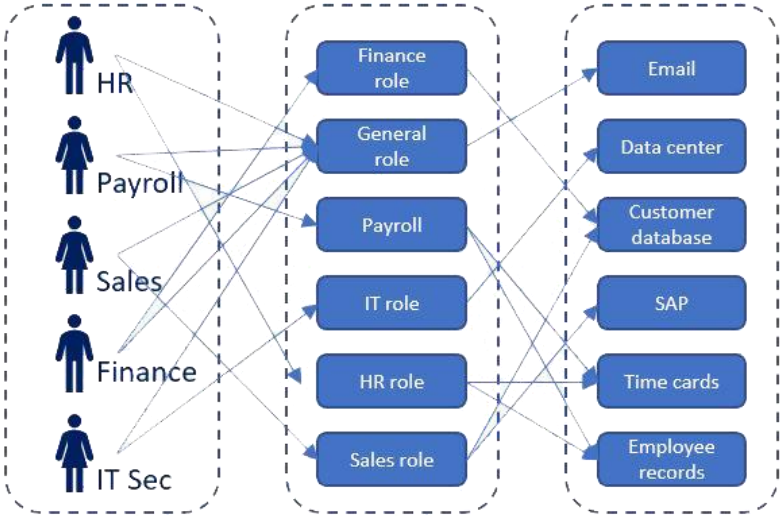
silné heslo. Z toho nám plyne také nevýhoda, která přináší bezpečnostní riziko ztráty přihlašovacích údajů a získání přístupu pro útočníka do všech aplikací. Technologie Single sign-on se nejčastěji používá ve větších podnicích, kde uživatel potřebuje přístup do více aplikací [1, 4].



Obrázek 6: Princip SSO [Upraveno dle [14]]

Role Based Access Control (RBAC)

Princip tohoto modelu je v přidělování oprávnění do rolí a ta jsou přidělována uživatelům, kteří mají přístup k jen k určitému druhu aplikace či systému. Role jsou v podniku vytvářeny na základě pozic a pracovní funkce či povinností. Tím, že se uživateli přiřadí role, tak zdědí veškerá práva přiřazená k této roli a zjednoduší se tak správa oprávnění a to se uplatní zejména ve větších firmách, kde je mnoho aplikací a systémů. Role se dají uživatelům snadno měnit a do rolí se dají přidávat či odebírat další oprávnění. Uživatel může mít více rolí podle toho, jakou pozici ve firmě zastává. Typické role jsou například IT specialista, HR koordinátor, Payroll koordinátor, apod. [4].



Obrázek 7: Model RBAC [19]

1.4.7 Provisioning

Tento systém neboli proces můžeme považovat za jeden ze stavebních kamenů IdM. Vytváří se zde uživatelské účty, přidělují role a oprávnění nebo také provádějí automatizované změny v systému. Dá se říci, že provisioningový systém spravuje veškeré účty a jejich práva v systémech a je vytvářen tzv. globální pohled na identitu pracovníka. Výhoda je ta, že společnosti snižuje náklady a administrátoři mají jednodušší práci při vytváření a udržování účtů díky tomu, že při zrušení či vytvoření přístupu pracovníka se tato akce propíše do všech dalších systémů. Nevýhoda je ovšem ta, že díky manuálním zásahům může dojít k chybám, jelikož účet zaměstnance, který dal výpověď a jeho účet nebyl včas smazán, může napáchat značné problémy. Fungování provisioningu tedy spočívá v tom, že při vytvoření identity proběhne synchronizace účtů do dalších systémů včetně přidělení přístupových práv na základě rolí. Opakem je de-provisioning, kde se v celém systému smaže identita uživatele [4, 5].

- **Workflow**

  Tento systém je součástí provisioningu a stará se o žádosti, které přesměrovává na určité osoby a ty následně žádost schválí nebo zamítnou a předají informaci provisioningu. Workflow má vlastní uživatelské rozhraní, díky kterému mohou uživatelé vytvářet požadavky a přijímat potvrzení o udělení přístupu [4, 5].

1.4.8 Trezory hesel

Uživatel je v dnešní době nucen pamatovat si spoustu hesel a ta musí zpravidla splňovat přísná pravidla a uživatel to řeší tím, že si hesla zapíše v papírové nebo elektronické podobě a proto se zvyšuje riziko zneužití těchto informací. Tento problém se dá řešit zmíněnými trezory hesel neboli aplikace na úschovu hesel, které rozdělujeme na online a offline trezory. První zmíněný je tedy trezor respektive aplikace, která je uložena na vzdáleném serveru a uživatel k ní může přistupovat odkudkoli, ale potřebuje připojení k internetu, připadá zde v úvahu také zneužití dat. Další varianta je offline trezor hesel, který má podobu aplikace na osobním disku, kde si uživatel může ukládat své přihlašovací údaje a má je tak vždy k dispozici, pokud ale uživatel nemá svůj osobní počítač k dispozici, musí si trezor vzít na přenosné médium. Jakou variantu uživatel zvolí, se musí řídit směrnicí a vnitropodnikovou politikou, kdy se například nesmějí používat přenosné disky, aby se do vnitřní sítě společnosti nedostal nežádoucí narušitel. Aplikace je chráněná silným heslem, případně otiskem prstu či přenosným tokenem, po zadání hesla již uživatel vidí veškeré svoje přihlašovací údaje a může s nimi pracovat. Hesla jsou zpravidla chráněna pomocí šifrovacích algoritmů jako RC4 či AES s délkou klíče až 256 bitů. V aplikacích je možné také vygenerovat nové heslo podle zadaných parametrů a složitosti nebo také zapnout upozornění před expirací hesla. Užitečnou výhodou je také komfortní kopírování z trezoru přímo do pole pro přihlášení například do emailu [20].

1.4.9 Adresářový systém

Poslední technologií, kterou si popíšeme je adresářový systém, který je také velice důležitou součástí IdM. Díky němu se dají efektivně ukládat údaje o identitách a ty pak slouží pro další aplikace. Tento systém je charakteristický svou hierarchickou strukturou, vysokou dostupností a škálovatelností, má vysokou rychlost při čtení, ale bohužel pomalý zápis. Nejčastěji se používá Active Directory, které je blíže popsáno níže. Jako protokol se používá již standardně LDAP, který se dá použít jako autentizační server, nicméně je vhodný pouze do menších společností, protože adresářové systémy neudržují informace o uživatelské relaci, proto zde není možné použít SSO [1].

- **Active Directory**

  Tato služba je standardně součástí operačního systému Windows Server. Centrálně spravuje síťové prostředky a administrátor zde může přidávat, odebírat a přesouvat uživatele nebo skupiny či jiné prvky. Active directory umí spolupracovat s dalšími adresářovými službami standardně přes protokol LDAP [1].

1.5 Kryptografie

Kryptografie se používá, pokud je potřeba data zašifrovat a zamezit tak, aby si je nepověřená osoba přečetla. Slouží také při zajištění integrity, tedy hlavně pokud chceme data bezpečně přesouvat [11].

Kryptografii rozdělujeme:

- Symetrickou
- Asymetrickou
- Bez klíčů

Symetrická kryptografie

- šifrování a dešifrování probíhá stejně (zrcadlení) -
- je potřebný tajný klíč
- A a B sdílejí společný klíč, který E nezná
- délka se odvíjí od algoritmu a odolnosti proti útoku
- Velikost klíčů: 512b. je považováno za bezpečné (standard)
- Problém s distribucí klíčů – telefon, kurýr, skřínka

Asymetrická kryptografie

- A a B mají vlastní veřejný klíč (pro šifrování a ověření podpisu) a soukromý klíč (dešifrování a vytvoření podpisu)
- Vyměňuji se pouze veřejné klíče
- Velikost klíčů: 2048 až 4096b.
- Algebraická záležitost, problém je jak si uživatelé klíče vymění

Kryptografie bez klíčů

- Hashovací funkce

1.6 Kerberos

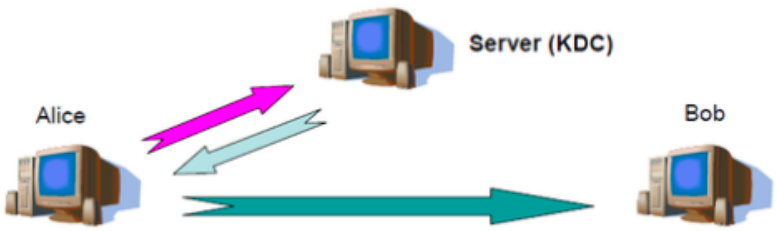
Kerberos je možné obecně popsat jako autentizační protokol, který provádí autentizaci pro systémy typu klient-server za pomocí symetrického šifrování. Princip jeho autentizace je takový, že na základě autentizace subjekt dostane lístek, díky kterému dále prokazuje právo na určité služby. V tomto procesu vystupuje také důvěryhodná třetí strana, která se nazývá Key-Distribution Center. TU je možné dále rozdělit na autentizační server a Ticket-Granting Server [11].

Postup:

1. Klient se autentizuje na Autentizačním serveru pomocí hesla
2. Po úspěšné autentizaci dostane lístek, který mu dává práva ke komunikaci s řídicím serverem
3. Pošle Ticket-Granting Serveru svůj lístek od Autentizačního serveru
4. Od Ticket-Granting serveru dostane další lístek, který ho opravňuje komunikovat se serverem, na kterém je služba kterou vyžaduje

V tomto procesu se vyskytují dva typy lístků. Výhodou je, že server, který poskytuje služby, nemá žádný přístup ke klientovým autentizačním údajům, jako je třeba heslo.
Lístky se tedy dělí: [11]

- Lístek, který je generovaný pouze jednou a dává uživateli právo žádat o služby na různých serverech
- Lístek, který je generované pro každý server zvlášť a dává klientovi právo žádat o služby pouze na konkrétním serveru



Obrázek 8: Zjednodušený systém Kerberos [11]

1.7 CyberArk

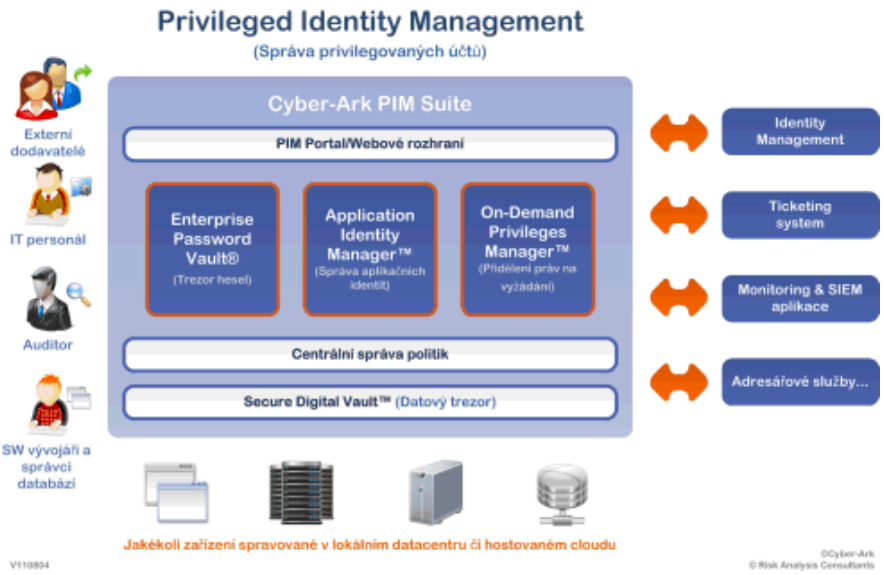
Cyberark je světově známá aplikace zaměřená na informační bezpečnost, zejména na správu privilegovaných identit jako například uživatelů, aplikací, souborů či dalších důvěrných informací. Software se snaží zvyšovat produktivitu administrátorů, chránit společnost před nebezpečím ze strany zaměstnanců a také naplňovat požadavky na úspěšný audit. Toto řešení je ovšem finančně velice náročné a proto ho používají zejména větší společnosti jako například největší světové banky [21].

Obrázek 9: Logo společnosti CyberArk (Zdroj: [22])

- Privileged Identity Management Suite (PIM)

  Tento nástroj pro správu privilegovaných identit nabízí společnostem unikátní řešení přístupu a monitoringu uživatelských aktivit spojených se správou účtů lokálních i cloudových řešení. Díky řešení PIM může společnost monitorovat, spravovat a auditovat privilegované identity a zabránit tak neoprávněným přístupům ze strany zaměstnanců a nedojde tak k možným únikům citlivých informací. Správa privilegovaných účtů nabízí: [21].

- Sprava jmen a hesel pro aplikace či služby
- Kontrola přístupu k privilegoévaným účtům
- Splnění požadavků pro adudit
- Snadná integrace do firemního přostředí
- Definování oprávnění pro uživatele
- Správu politik



2 ANALÝZA SOUČASNÉHO STAVU

V této části se zabývám analýzou současného stavu společnosti, jako jsou základní informace, údaje o zaměstnancích, HW a SW, v neposlední řadě také současný stav bezpečnosti informací. Informace byly poskytnuty od vedení a zaměstnanců společnosti. Budu se řídit doporučeními normy ISO/IEC 27001. Prošetří se tak aktuální stav IdM ve společnosti. Dále provedu analýzu procesů, které souvisí s životním cyklem identit.

2.1 Základní údaje o společnosti

Obchodní jméno: *Cleverlance Enterprise Solutions a.s*

Sídlo: *Na Zámecké 8/410, 140 00 Praha 4*
Pobočka Brno: *Purkyňova 101, 612 00 Brno*

Den zápisu do OR: *28.12.2005*
Právní forma: *Akciová společnost*
IČ: *27408787*
Základní kapitál: *5 000 000,- Kč*
Webová stránka: http://www.cleverlance.com/cz

Obrázek 11: Logo společnosti Cleverlance Enterprise Solutions a.s [15]

2.2 Podnikání společnosti

Firma Cleverlance Enterprise Solutions a.s (Dále jen Cleverlance) vznikla v roce 2000 jako ryze česká IT firma, která se specializovala na technologii J2EE a již v roce 2003 se etablovala jako největší dodavatel řešení na této platformě v ČR a SR. Tak jak firma reagovala na technologické změny i obchodní trendy, přidávala do svého portfolia průběžně nové technologie, řešení, kompetence a specifické know-how. Díky tomu se několikrát po sobě Cleverlance stala nejúspěšnějším českým poskytovatelem softwaru podle žebříčku „Technology Fast 50“ v regionu střední Evropy. Prestižním magazínem Inside byla vyhodnocena jako nejrychleji rostoucí česká vývojářská společnost.

Cleverlance patří do Cleverlance Group, což je skupina českých IT společností s mezinárodní působností poskytující konzultace, řešení a služby zejména v oblastech financí, telekomunikací, utilit a veřejné správy. Do skupiny patří společnosti Cleverlance Enterpise Solutions, AEC, TrustPort, CTS TRADE IT a Cleverlance H2B.

Firma Cleverlance se zabývá poskytováním služeb v oboru IT se zaměřením na využití vícevrstvých technologií:

- Návrh a vývoj systémů na zakázku
- Návrh a implementace portálových řešení
- Redesign architektury a optimalizace stávajících aplikací
- Převod aplikací z technologií J2EE na .NET
- Integrace mezi technologiemi .NET a J2EE
- Převod aplikací z dvou do třívrstvé architektury
- Návrh a vývoj mobilních řešení
- Project management
- Testování dodávaných i stávajících aplikací
- Post-implementační podpora dodávaných i stávajících systémů
- Outsourcing konzultačních služeb a dodávaných řešení

2.3 Analýza trhu

Firma Cleverlance se pohybuje na trhu IT, vývoje software, kde se pohybuje v dnešní době hodně firem, nicméně pro mě je Cleverlance zajímavá a výjimečná v tom, že vytváří konkrétní řešení na míru a to pomocí multi-kanálových aplikací. Vyvíjí je pro: internet, mobilní a telefonní bankovnictví, samoobslužné systémy pro objednávání a zřizování služeb, systémy řízení a podpory mobilních pracovníků servisních služeb nebo systémy optimalizace a řízení procesů mezi prodejními kanály (front office) a back office.
Firma spolupracuje s firmami AEC a Trustport, které jsou pod záštitou Cleverlance Group. Konkurenti v oblasti vývoje SW na zakázku například Vivian Software (www.vivian.cz) nebo Arbes (www.arbes.com). Hlavním zdrojem financování je samotná činnost podniku – podniku se daří dosahovat stálého zisku.

2.4 Ekologické, etické, legislativní a jiné aspekty podnikání

Ekologická stránka podniku se nedá uvažovat, jelikož firma podniká v oblasti vývoje software. Z etického hlediska se zaměstnavatel chová velmi dobře k zaměstnancům, zákazníkům a vytváří příjemné pracovní prostředí. Z legislativního pohledu nakládá firma v souladu se všemi zákony.

2.5 Analýza obecného okolí SLEPT

Sociální faktory

Vzhledem k tomu, že společnost se primárně zaměřuje na poskytování služeb právnickým osobám, tak se dá říci, že demografický faktor nepředstavuje pro společnost rizikovou kategorii. Společnost by i v případě nepříznivého demografického vývoje měla mít dostatek zakázek, jelikož poptávka po zabezpečovacích systémech s rozmachem informačních technologií bude nadále růst.

Vzhledem k tomu, že nové technologie jsou využívány zejména mladší generací, tak je nutné, aby se společnost zaměřila na nejnovější technologie, neboť v budoucnu bude tato mladá generace tyto technologie vyžadovat.

Legislativní faktory

Dá se říci, že na činnost společnosti se nevztahují nikterak specifické zákony, či jiné právní předpisy. Nejrelevantnějšími předpisy tak zůstávají následující předpisy:

- zákon č. 89/2012 Sb., občanský zákoník, v platném znění,
- zákon č. 586/1992 Sb., o daních z příjmu, ve znění pozdějších předpisů,
- zákon č. 235/2004 Sb. o dani z připadané hodnoty, ve znění pozdějších předpisů.

Dále je dobré zmínit, že na společnost se nově bude vztahovat i zákon č. 112/2006 Sb., o evidenci tržeb, a proto se na účinnost tohoto zákona musí připravit. Za další významné legislativní faktory lze označit příslušná nařízení Rady a nařízení Evropského parlamentu, které se zabývají mezinárodním obchodem, a to jak v rámci Evropské unie, tak rovněž v rámci obchodu mimo Evropskou unii.

Ekonomické faktory

V současné době se dá říci, že v České republice, jakožto i v Evropské unii, panuje příznivá ekonomická situace. Hrubý domácí produkt České republiky v roce 2017 vzrostl na 4,5 %. V roce 2018 se dá očekávat, že ekonomická situace bude nadále pozitivní. Míra nezaměstnanosti v ČR dosahuje v současné době rekordně nízké úrovně a rovněž inflace je velmi nízká.

Co se týče daňového zatížení, tak v současné době je situace ustálená, přičemž se v blízké době neočekává změna daňového systému, přestože určité politické strany již představily svůj předvolební program, avšak výsledek voleb dosud není jistý.

Přestože předchozí odstavce vyznívají pro společnost pozitivně, tak je rovněž vzít v potaz situaci, že Česká národní banka plánuje ukončit intervence vůči euru a rovněž skutečnost, že Evropská centrální banka může v krátkém časovém horizontu ukončit kvantitativní uvolňování, kterým se snaží podpořit ekonomiku celé eurozóny. Přestože Česká republika není členem tohoto uskupení, tak vliv tohoto uvolňování lze pozorovat i v rámci ČR. Z tohoto důvodu je možné, že údaje v přechozím odstavci se mohou díky těmto skutečnostem změnit k horšímu.

Politické faktory

Politická situace v rámci České republiky se dá označit za stabilní. Jak již bylo zmíněno, tak činnost společnosti může ovlivnit elektronická evidence tržeb a případné změny daňového systému, avšak tato změna by případně nastala v řádu let, vzhledem k blížícím se volbám. Zde je rovněž dobré zmínit, že společnost podléhá dohledu několika orgánů, příkladem lze uvést Českou obchodní inspekci.

Vzhledem k tomu, že společnost má dodavatele zejména ze zemí Evropské unie, tak je nutné říci, že činnost společnost může rovněž ovlivnit politika EU, avšak v současné době se to neočekává.

Technologické faktory

Tento faktor je nutné, s ohledem na předmět podnikání společnosti, považovat za velmi důležitý. Společnost by tak měla sledovat technologický vývoj a nabízet svým zákazníkům produkty, které v sobě mají integrovány nové technologie.

V současné době lze pozorovat velký rozmach zabezpečovacích prvků, které jsou propojeny s dalšími zařízeními, přičemž přenos informací je zde nejčastěji realizován pomocí TCP/IP protokolu. Některé tyto produkty již dokáží například spolehlivě rozpoznat dle obličeje. Další produkty zase disponují hlasovou asistentkou, která může odpovídat na dotazy uživatele. Do budoucna lze očekávat, že společnost se bude muset vypořádat se systémovou integraci těchto produktů.

2.6 Situační analýza

Firma se nachází v blízkosti centra Brna, konkrétně v městské části Královo Pole. Sídlí v budově společností Česká pojišťovna a.s., kde je v podnájmu. Vstup do budovy je možný pouze přes hlavní dveře, kde se nachází recepce, na které je neustále někdo přítomný. Venkovní obvod budovy je chráněn kamerovým systémem a obraz je přenášen na recepci. Firma se nachází v pravém křídle budovy ve třech nadzemních podlažích. Chodby jsou vybaveny alarmem, který reaguje na pohyb. Alarmový systém se aktivuje po odchodu posledního zaměstnance. Není zde žádná fyzická ostraha ani žádný čipový systém pro identifikaci osob. Z hlediska přírodních katastrof firma nemusí mít strach o zaplavení,

jelikož se nenachází v záplavové oblasti a na požár jsou na chodbách budovy připravené hasicí přístrojem včetně požárních čidel.

2.7 Analýza interních faktorů – 7S

Strategie

Cílem společnosti je nadále svým zákazníkům poskytovat kvalitní služby v oblasti zabezpečení a vývoje softwarových řešení. Společnost plánuje navýšit objem realizovaných zakázek, čímž chce navýšit tržby o 10 %. Z tohoto důvodu společnost rovněž plánuje nábor nových pracovníků. Tito pracovníci budou taktéž využiti v rámci servisních služeb, které společnost plánuje více rozvíjet. Společnost má rovněž v plánu rozšířit propagaci, a to zejména formou služby Google Ad Sense a pomocí cílených reklam na sociální síti Facebook.

Struktura

Vzhledem k tomu, že na pobočce v současné době pracuje 25 pracovníků, tak se tato společnost dá zařadit do kategorie menších společností, a proto i organizační struktura společnost je jednoduchého charakteru. Nejvyšší postavení v rámci této struktury mají jednatelé společnosti, přičemž každý z nich má primárně na starost jedno ze dvou dalších oddělení. Těmito odděleními jsou obchodní a technické oddělení. Organizační struktura má tak liniovou podobu.

Obchodní oddělení má na starost zejména oslovování potencionálních zákazníků, komunikaci se stávajícími zákazníky, ale i marketing, nákup zboží, fakturaci, příjem a vyřizování objednávek.

Oproti tomu technické oddělení je primárně zaměřeno na samotnou realizaci zakázky, má tak na starost instalaci bezpečnostních systémů, pravidelnou údržbu a rovněž zajišťuje následný pozáruční servis a správu IT vybavení společnosti.
Ostatní služby jsou společnosti poskytovány od specializovaných subjektů, přičemž se zejména jedná o právní služby.

Spolupracovníci

Společnost, s ohledem na předmět podnikání, vyžaduje u svých pracovníků minimálně středoškolské vzdělání v oboru IT. Dalšími požadavky jsou zejména komunikativnost, spolehlivost a schopnost týmové spolupráce.

Co se týče skladby současných pracovníků, tak se jedná o kvalifikované a zkušené pracovníky ve středním věku. Společnost však zaměstnává i brigádníky, kteří pro ni představují levnou pracovní silou, přičemž tito brigádníci naopak získají cenné zkušenosti přímo z praxe.

Společnost se snaží budovat přátelské pracovní prostředí a nechce, aby zkušení pracovníci odcházeli ke konkurenci. Z tohoto důvodu se společnost snaží nabízet vyšší mzdové ohodnocení, přičemž k proaktivnímu přístupu jsou pracovníci motivování bonusy, které mohou získat nad rámec sjednané mzdy.

Schopnosti

Za základní schopnosti, které společnost vyžaduje, se dají zejména označit znalosti v IT oboru, které pracovníci získají v rámci středoškolského nebo vysokoškolského studia. Tyto znalosti jsou následně zdokonalovány jak dlouholetou praxí, tak školením, které společnost svým pracovníkům pravidelně financuje. Zde je dále dobré zmínit, že společnost disponuje rozsáhlým know-how, které získala během své podnikatelské činnosti.

Sdílené hodnoty

Celková kultura společnosti se dá hodnotit velmi pozitivně. Ve společnosti panuje dobrá nálada a pracovníci sdílejí hodnoty společnosti. K tomu jsou mimo jiné vedeni již zmíněným motivačním programem. Vzhledem k přátelskému pracovnímu prostředí a dobrému finančnímu ohodnocení se dá říci, že loajalita pracovníků ke společnosti je na vysoké úrovni. Někteří pracovníci zde pracují téměř od založení společnosti.

Systémy

Veškerá komunikace ve společnosti probíhá primárně pomocí telefonů, e-mailů a pravidelných porad s vedením. Rozhodovací procesy jsou realizovány primárně na základě letitých zkušeností v oboru. Slabé místo společnosti lze označit v absenci informačního systému, který by poskytoval společnosti zpětnou vazbu a přehledně zobrazoval dřívější realizované zakázky, jakožto i veškerou komunikaci se zákazníky. Společnost dále využívá zejména kancelářskou sadu Microsoft Office, přičemž nejvíce používanou aplikaci je Microsoft Excel. Pomocí tohoto programu si společnost například vede seznam zákazníků a plánuje zde nákup potřebného materiálu a zboží.

Styl řízení

Vzhledem k tomu, že ve společnosti je dobrá kultura a přátelské prostředí, tak rovněž i řízení společnosti je realizováno v podobném duchu. Styl řízení se dá tedy označit za velmi benevolentní a demokratickým. Na pravidelných poradách se tak může vyjádřit jakýkoliv pracovník. Je však nutné zmínit, že rozhodující slovo mají vždy jednatelé společnosti.

2.8 SWOT analýza

Na základě dříve provedených analýz je dále zpracována SWOT analýza společnosti, která zachycuje jak její slabé a silné stránky, které byly získány na základě analýz vnitřního prostředí, tak její příležitosti a hrozby, které byly odvozeny na základě analýz vnějšího prostředí společnosti.

Silné stránky	Slabé stránky
• Kvalifikovaní pracovníci • Vysoká kvalita dodávaných služeb • Stabilní pracovní kolektiv • Rozsáhle know-how • Dobré vztahy se zákazníky a pracovníky • Dobré jméno	• Nedostatečná propagace • Neefektivní komunikace • Zastaralé webové stránky • Absence informačního systému
Příležitosti	**Hrozby**
• Nové technologie – biometrie, propojení s dalšími zařízeními • Nárůst poptávky po zabezpečení a vývoje software • Systémová integrace bezpečnostních prvků od více výrobců • Příznivá ekonomická situace	• Nízké bariéry vstupu – konkurence • Ukončení intervencí ČNB a kvant. uvolňování ECB • Rozmach firem zabývající se bezpečností • Ukončení spolupráce ze strany některého z dodavatelů • Zvýšení daňového zatížení • Elektronická evidence tržeb

2.8.1 Silné stránky

Firma Cleverlance umí bezkonkurenčně sloučit vývoj softwaru na zakázku a vysoké bezpečnostní standardy. Druhým pilířem specifického přístupu je důraz na uživatelskou zkušenost. Investice do kvalitní ergonomie jsou investicemi do použitelnosti softwaru. Další předností je široké využívání vývoje řízeného modelem (Model-Based Development, MBD). Jeho hlavními přínosy jsou 1) ochrana investic do analýzy a vývoje obchodních procesů, 2) nezávislost na technologiích a v neposlední řadě 3) významné prodloužení životnosti IS, který nezastarává a nevyžaduje pravidelný re-engineering. Mezi silné stránky také patří portfolio zákazníků, mezi které se řadí velcí hráči v oborech finančnictví (banky, pojišťovny, leasingové a úvěrové instituce), telekomunikací, obchodu a služeb.

2.8.2 Slabé stránky

Slabé stránky firmy jsou hlavně nedostatečná propagace a reklama. Co by však mohlo stát za zmínku je, že firma Cleverlance by mohla více využívat mladých studentů z VUT v Brně během jejich studia například na testování aplikací nebo výpomoc při

programování nového softwaru, dále pak zvyšující se nároky na servery, počítače a počítačovou síť, které musí firma obměňovat, to se však týká obecně všech IT firem.

2.8.3 Možnosti a příležitosti

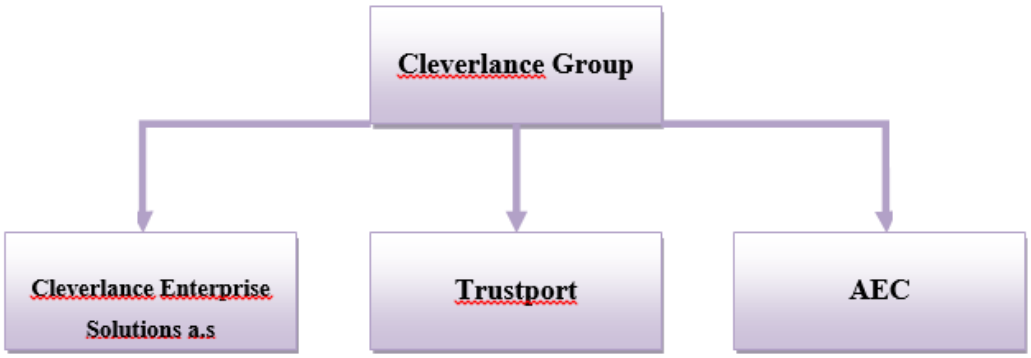
Mezi příležitosti bych zařadil stálou možnost růstu firmy, nabírání nových klientů hlavně v oblasti finančnictví. Pobočka v Brně má velké ambice na další nově vznikající Brněnské firmy. Poptávka po zabezpečení

2.8.4 Hrozby

Mezi hlavní hrozby patří konkurence, kterou je zapotřebí neustále sledovat, pro společnost je také důležité udržet si významné kontrakty s bankami na kterých je závislá.

2.9 Organizační struktura společnosti

Jedná se o podnik, který je součástí skupiny Cleverlance Group, ta má pod sebou další jednotky jako jsou firmy AEC a Trustport.



Obrázek 12: Organizační struktura podniku [Zdroj: Vlastní]

Představenstvo firmy Cleverlance se skládá ze tří členů:

- Ing. Jiří Bíba
- MUDR. Vít Urbanec
- Ing. Petr Štros

Za společnost jedná každý člen představenstva samostatně.
Dozorčí rada:

- Ing. Martin Vít
- Jiří Dosoudil
- Ing. Petr Brňák

2.1 Informační situace v podniku

Každý z pracovníků má svůj stůl, kde se nachází stolní pracovní stanice, na kterém běží operační systém Windows 7, do nějž se přihlašuje pomocí svého ID a hesla. Na každém takovém počítači je nainstalována antivirová ochrana společnosti eset NOD32, kde je pravidelně aktualizována antivirová databáze. Zaměstnanci nejsou nijak kontrolování. Všichni zaměstnanci mají přístup na datový server, kde by měly pracovat s podklady a dokumenty k zakázkám. Překopírování těchto souborů na vlastní počítač či flash disk není nijak kontrolováno. Každá pracovní stanice má své vlastní UPS, které po výpadku elektrického proudu je schopno napájet pracovní stanici ještě 15 minut a tím je umožněno řádné ukončení všech rozpracovaných věcí. Firma využívá zabudované síťové připojení, které má napojené na svůj router. Všechny stolní pracovní stanice jsou připojeny do sítě přes kabel. Kabely jsou vedené ve zdi a ukončeny zásuvkou na zdi. Programátoři používají jeden wifi router pro multiplikaci LAN portů a pro testování zařízení s WIFI. V případě výpadku energie je v budově napojen zdroj nepřerušovaného napájení (UPS) pro síťové prvky. Server se skládá ze stanice, která běží pod operačním systémem Windows server 2008 a skládá se z disku o kapacitě 200GB zapojeného v RAID 1. Email a web je řešen externě přes poskytovatele internetového připojení Poda. Dále firma disponuje dvěma síťovými úložišti NAS o velikosti 2TB zapojeného v RAID 1. Jeden se nachází spolu se serverem v serverové místnosti a druhý na stole v kanceláři. Tyto NAS úložiště slouží pouze pro zálohu serveru. Server je používán pouze pro práci s daty nic jiného se na něm nenachází. Firma používá i účetní systém a to od společnosti Money, jehož součástí je přehled zakázek, pohledávek nebo správa zákazníků. Bezpečnost provozu a komunikací. Informace, které společnost zpracovává, jsou chráněny před malwerem a to dostatečně bezpečným antivirovým softwarem AVG Internet Security, který blokuje viry, spyware a jiný malware, obsahuje navíc i firewall a kontroluje jak data v počítači, tak příchozí soubory z e-mailu či z webu.

Pro vyšší bezpečnost je zavedena politika, která zakazuje instalovat neautorizovaný software a přistupovat na neznámé a nebezpečné webové stránky.
Pro ochranu informací v sítích je fyzické připojení do vnitřní sítě chráněno umístěním routeru na bezpečném místě, kam nemá veřejnost přístup. Bezdrátové Wi-Fi připojení do sítě je chráněno zabezpečením WPA2 a je nastaveno silné heslo, které brání připojení neoprávněných osob k dané síti. Samozřejmě k bezpečnosti komunikací přispívá i zabezpečení každého připojeného počítače pomocí antiviru a firewallu.

2.2 Analýza ICT

Společnost využívá dva typy serverů pro zabezpečení bezproblémové činnosti informačních technologií. Jedná se o hlavní server a záložní server. Hlavní server a záložní server byly zakoupeny od firmy IBM s operačním systémem Windows server 2008 R2. Na hlavním serveru je umístěn SQL server, který slouží jako databáze pro systém ASAP, dále Exchange server, DNS server, DHCP server, Print server a File server.

Konfigurace hlavního serveru
Výrobce: IBM
CPU: 2x Intel Xeon E5-2620 v2
RAM: 32 GB ECC
RAID Controller: Řadič M5110 (RAID 0/1/10/5/50)
Operační systém: Windows server 2008 R2

Záložní server
Výrobce: IBM
CPU: Intel Xeon E5-2620 v2
RAM: 16 GB ECC
RAID Controller: Řadič M5110 (RAID 0/1/10/5/50)
Operační systém: Windows server 2008 R2

Firemní síť je postavena na 100 Mbps rychlosti a skládá z desktopových počítačů a notebooků. Ty jsou zapojeny do 16-ti portového switche síťovými kabely kategorie 5e,

spolu se síťovou tiskárnou. Pro bezdrátovou konektivitu slouží Wi-Fi router se standardem IEEE 802.11 b/g/n, chráněný šifrovacím algoritmem WPA2. Pracovníci jako projektový manažer, manažer IT atd. vlastní pracovní notebook. Připojení notebooků a jiných chytrých zařízení jako tablety a mobily je realizováno WiFi routerem 802.11a/b/g/n.

2.3 Bezpečnost lidských zdrojů

Společnost má definovaná pravidla pro sepisování pracovních smluv s novými zaměstnanci. Tedy postupy podle, kterých mají být zaměstnanci seznámeni s podmínkami pracovního vztahu, se svými právy a povinnostmi, které zahrnují mimo jiné i dohodu o mlčenlivosti, která řeší únik informací mimo organizaci. Při nástupu do pracovního poměru tedy podepisují všichni zaměstnanci dohodu o zachování mlčenlivosti, což je velice důležité, protože mohou při práci přijít do styku s citlivými a důvěrnými informacemi, které se týkají společnosti, nebo i samotných klientů.
Stejně tak má společnost definovaná pravidla pro ukončení pracovního vztahu, která v sobě zahrnují povinnost navrátit všechny prostředky, odebrání přístupových práv apod. Samozřejmostí je i to, že dohodou o mlčenlivost jsou zaměstnanci vázáni také po skončení pracovního poměru. Stejně tak jsou stále platné i některé další odpovědnosti a povinnosti již bývalých zaměstnanců.

2.4 Řízení přístupu a ochrana osobních údajů

Pro zabránění neoprávněného přístupu k informacím jsou všechny počítače chráněny heslem. Každý zaměstnanec tak má přístup pouze ke svému účtu. Také jsou zavedeny postupy pro vytvoření nového uživatelského účtu pro nového zaměstnance a odstranění uživatelského účtu při zrušení pracovního poměru.
Osobní údaje všech zaměstnanců společnost bezpečně uchovává a zajišťuje tak jejich ochranu v souladu se zákonem o ochraně osobních údajů. Má také vypracovanou politiku pro ochranu osobních údajů, se kterou je každý zaměstnanec seznámen při nástupu do zaměstnání.

2.5 Analýza rizik

Prvním krokem analýzy je identifikace hodnocení aktiv. Tento seznam byl sestaven na základě komunikace s vedením společnosti. Další krok je ohodnocení aktiv podle dopadu na organizaci v důsledku porušení důvěrnosti, integrity a dostupnosti daného aktiva. Nejvíce pravděpodobná rizika jsou zachycena v tabulce č. 4 na další stránce, přičemž v níže uvedených tabulkách jsou zachycena kritéria, na jejichž základě byla tato rizika ohodnocena.

2.5.1 Identifikace a hodnocení rizik

Tabulka 1: Hodnoty pravděpodobnosti [Zdroj: Vlastní]

Hodnota	Pravděpodobnost
0-20	velmi nepravděpodobné
20-40	nepravděpodobné
40-60	přípustné
60-80	téměř jisté
80-100	hraničí s jistotou

Tabulka 2: Hodnocení dopadu [Zdroj: Vlastní]

Hodnota	Dopad
0,1-1	nulový
1,1-2	mírný
2,1-3	ohrožující
3,1-4	hrozivý
4,1-5	zničující

Tabulka 3: Hodnocení závažnosti rizik [Zdroj: Vlastní]

Riziko	Hodnota rizika
Běžné	1-2
Závažné	2-3
Kritické	3-4

V následující tabulce je zachyceno 15 hrozeb z pěti oblastí, které společnost ohrožují při realizaci plánované změny, přičemž ke každé hrozbě je uveden možný scénář, jejich pravděpodobnost (sloupec PRS) a dopad (sloupec D). Vynásobením posledně zmíněných charakteristik bylo dospěno k hodnotě rizika, která je zachycena u jednotlivých hrozeb ve sloupci H.

Tabulka 4: Identifikace rizik [Zdroj: Vlastní]

č.	Hrozba	Scénář	PRS [%]	D	H
Technologická rizika					
1	Výpadek internetu	Nedostupnost informačního systému	10	5	0,5
2	Nedostupnost služby	Výpadek informačního systému	45	5	2,3
3	Migrace dat	Chybějící data	15	2,5	0,4
4	Zálohování	Ztráta dat	35	2	0,7
5	Napadení sítě	Únik cenných informací a dat	55	4,5	2,5
6	Porucha hardwaru	Nefungující PC	25	4,5	1,1
Personální rizika					
7	Nedostatečné proškolení pracovníků	Neznalost ovládání systému	60	5	3
8	Neúmyslný incident	Únik či poškození cenných dat a informací	10	2,5	0,3
9	Nepřizpůsobení se změně	Nízká produktivita	35	3	1,1
Finanční rizika					
10	Nesprávné vyčíslení přínosů	Delší doba návratnosti investice	20	2	0,4
11	Překročení stanoveného rozpočtu	Dodatečné náklady	25	2,5	0,6
Bezpečnostní rizika					
12	Nedostatečné zabezpečení systému	Únik cenných informací a dat	15	4	0,6
13	Nedostatečné zabezpečení klientských stanic	Únik cenných informací a dat	20	5	1
Organizační rizika					
14	Špatně sjednaná smlouva	Neposkytnutí potřebných služeb	50	4,5	2,3
15	Nedodržení stanoveného termínu	Prodloužení implementace	30	3	0,9

2.6 Požadavky investora

Vedení společnosti potřebuje navrhnout informační systém pro rozvíjející se Brněnskou pobočku, aby se usnadnila práce zaměstnanců a mohla probíhat lepší kontrola probíhajících procesů.

- **Požadavky na IS**
  - Cena systému – Cena systému pro malý podnik by měla být rozumná, neměla by přesáhnout 150 000 Kč.
  - Dostupnost – Systém by měl být dostupný a dodací lhůty krátké.
  - Jazykové verze – Systém musí být primárně v českém jazyce.
  - Finance a účetnictví – Účtování, kontrolovaní faktur a dokladů, k sestavování účetních výkazů a pro správu financí.
  - Prodej a vystavení faktur – Pro podporu celého obchodního procesu (objednávky, dodávky, fakturace, apod.).
  - Analýzy - Možnost tvorby jednoduchých i rozsáhlejších pohledů na chod firmy. Tvorba analýz, statistických studií apod.
  - Import a export dat - Možnost exportu a importu dat. Pro zálohování nebo práci s kompatibilními systémy.
  - Rozšíření ERP modulů – Systém musí být rozšířitelný o další funkční moduly, které může firma v budoucnu využít.
  - Intuitivní ovládání – Ovládání systému musí být uživatelsky přívětivé a jednoduché, výhodou je i vlastní rozvržení nebo organizace domovské stránky.

Dále chce společnost revitalizovat politiku hesel a řízení přístupu. V poslední řade navrhnout řešení pro eliminaci rizik. Náklady na změnu by neměly přesáhnout částku 200 000,- Kč.

2.7 Zhodnocení analýzy

V analýze současného stavu bylo nejdříve pojednáno o obecném prostředí a informací o firmě, byla provedena analýza rizik, SWOT analýza, analýza obecného prostředí SLEPT, analýza interních faktorů 7S a v poslední řadě také analýza ICT.

Z analýzy vyplynulo, že jsou zde bezpečností rizika, která je potřeba eliminovat. Mezi hlavní nedostatky patří absence informačního systému, špatně nastavená politika a ukládání hesel, nedostatečné školení uživatelů a řízení přístupu. Řešením těchto nedostatků se bude zabývat další část diplomové práce.

3 NÁVRH ŘEŠENÍ

V závěrečné části diplomové práce budu vycházet z výsledků analýzy současného stavu a teoretických poznatků. Je třeba zde navrhnout správné uložení hesel a jeho politiku, navrhnout řízení odpovědnosti za činnosti a procesy, řízení uživatelských rolí, přidávání a odebíraní práv uživatelů.

3.1 Uložení a politika hesel

Zaměstnanci často potřebují znát mnoho hesel pro přihlášení do různých aplikací a je samozřejmostí jejich obměna nejpozději každých 90 dní. Uživatelé tak v některých případech ukládají svá hesla do nešifrovaných poznámek v počítači. Proto navrhuji zavést program na ukládání hesel KeyPass. Uživatel si pamatuje pouze jedno heslo, které slouží k přihlášení do trezoru hesel, kde má k dispozici všechna další hesla a může je tak jednoduše vykopírovat i s uživatelským jménem. O aplikace uvedu více informací níže.

3.1.1 Politika hesel

Z bezpečnostního hlediska by měla být politika nastavena tak, aby nebylo možné heslo uhodnout a bylo odolné vůči slovníkovému útoku. Zaměstnanci proto musí projít školením jak vytvářet kvalitní hesla, kde je kladen důraz na délku, složitost a obsah. Navrhuji doplnit do směrnice následující body:

- Minimální délka hesla je 8 znaků
- Heslo musí obsahovat 2 velká a 2 malá písmena.
- Heslo musí obsahovat 2 číslice
- Heslo musí obsahovat 1 speciální znak

- Upravit životnost hesla ze 180 dní a jeho opakování
- Životnost hesla je 90 dní
- Opakovat se nesmí poslední 3 hesla

Pro implementaci pak je nutné schválení změn od managementu společnosti, nastavit změny v systému IT oddělením a informovat uživatele o změně.

3.1.2 Implementace KeyPass

Navrhuji implementovat program KeyPass, který slouží jako lokální trezor hesel, uživatel si pamatuje pouze jedno heslo, které slouží k přihlášení do trezoru hesel, kde má k dispozici všechna další hesla a může je tak jednoduše vykopírovat i s uživatelským jménem. Vidí zde také poslední změnu hesla, aplikace ho upozorní na blížící se expiraci. Program je podporován všemi operačními systémy a podporuje také mobilní zařízení. Počet hesel, která uživatel může uložit je neomezený a je možné si heslo na základě vstupních parametrů vygenerovat. Aplikace je jednoduchá a přehledná.

Implementace by měla probíhat následovně:

- Žádost o zařazení mezí programy, které jsou součástí tzv. zelených stránek. Uživatelé si mohou stáhnout takový software třetích stran pro pracovní účely.
- Program musí být schválen managementem a IT oddělením
- Musí být vytvořena příručka pro uživatele a rozšířena mezi všechny zaměstnance
- V poslední řadě je třeba doplnit směrnici

3.2 Řízení přístupu

Ve společnosti Cleverlance je řízení přístupu zajišťováno pomocí Active Directory. Nejsou ovšem vytvořeny skupiny pro určitou sortu pracovníků, proto navrhuji pomocí Group Policy, rozdělit pracovníky podle jejich postavení ve firmě a to na skupiny:

- IT administrátoři
- Management společnosti
- HR administrátoři
- Technické dokumenty

3.2.1 Schvalování rolí a odebíraní práv

Pro nového zaměstnance je třeba přiřadit jeho roli ve společnosti podle Group Policy, vedoucí pracovník takového oddělení pak tuto změnu musí schválit. Jakmile zaměstnanec změní svoji pozici, nebo ukončí pracovní poměr, je důležité, aby mu byla odebrána přístupová práva a učet deaktivován či mu byla přidělena jiná skupina s jiným

oprávněním. Toto bude mít na zodpovědnost vedoucí pracovník IT oddělení. Jednou za tři měsíce bude probíhat revalidace neboli kontrola všech zaměstnanců, zda mají správně přiřazená práva.

3.2.2 Přístup k síťovým službám

Uživatelé mají přístup do sítě internet, mají možnost také přistupovat na hlavní server společnosti, včetně print a file serveru. Ve firemní síti jsou zakázány stránky citlivého obsahu nebo některé weby nesouvisející s náplní práce jako například Facebook.

3.3 Sdílení uživatelského účtu

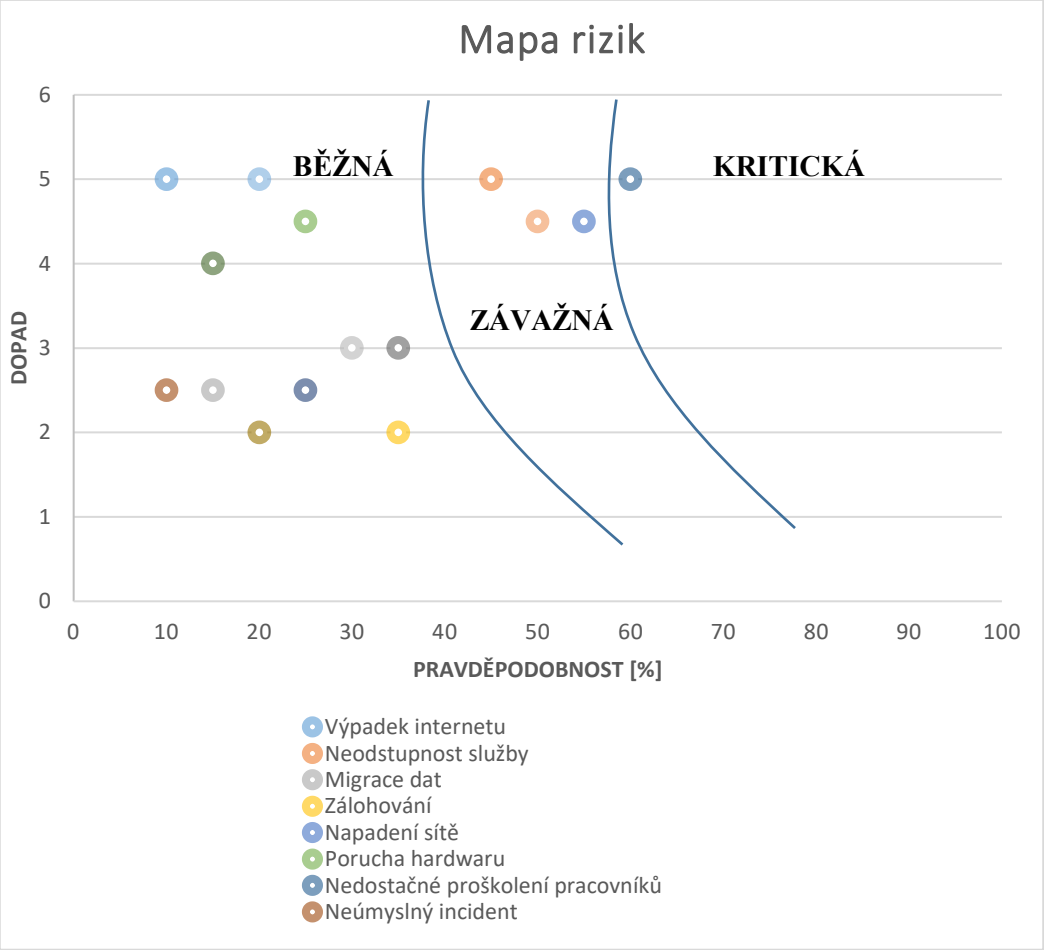
Přestupek jako sdílení uživatelského účtu je závažné porušení bezpečnostní politiky podniku. Uživatel v dobré víře, že pomohl kolegovi, může způsobit závažné škody tím, že sdílí svůj účet. Není možné technicky zamezit takovému postupu, proto navrhuji zavést vetší informovanost uživatelů o nebezpečí a také důsledcích, které by měli být razantní jako například snížení ohodnocení nebo pokuta, v horších případech i propuštění. Zaměstnancům je třeba důrazně dát najevo, že budou potrestáni v případě takového porušení bezpečnostní politiky. Navrhuji, aby IT oddělení zavedlo vhodný program pro sledování podezřelé aktivity, a bude ji integrovat se systémem IdM. Program může například vyhodnocovat pomocí auditních záznamů přihlášení z neobvyklých míst, či více míst zároveň a v neobvyklém čase.

3.4 Systém vzdělávání zaměstnanců

Na základě analýzy současného stavu navrhuji zavést systém vzdělávání zaměstnanců v oblasti informační bezpečnosti, jelikož nyní jsou zaměstnanci školení pouze při nástupu do společnosti. Navrhuji, aby se takové školení opakovalo jednou ročně ať už sezením a prezentací IT oddělení nebo online prezentace se zpětnou vazbou a kontrolním testem.
Je třeba, aby byl každý zaměstnanec seznámen se směrnicemi společnosti, novinkami z oblasti IdM jako například politiku hesel. Školení bude provádět přidělený pracovník IT oddělení.

3.5 Mapa rizik

Na základě získaných hodnot rizik, která jsou zachycena v tabulce č. 4, byla vytvořena mapa rizik, která je uvedena níže. Z tohoto grafu plyne, že kritickým rizikem může být nedostatečné proškolení pracovníků. Dále do skupin závažných rizik spadají celkem tři rizika a do kategorie běžná rizika patří zbývajících 11 rizik. Doporučení, jak jednotlivé hodnoty rizik snížit, jsou následně uvedena v tabulce č. 5 níže.



Graf 1:Mapa rizik [Zdroj: Vlastní]

3.6 Návrhy na snížení rizik

Tabulka 5: Návrhy na opatření a snížení rizik [Zdroj: Vlastní]

č.	Hrozba	Návrh na opatření	Nová PRS [%]	D	Nová hodnota	Náklady	R
Technologická rizika							
1	Výpadek internetu	Pořízení spolehlivého internetu, smluvní ošetření u dodavatele, sankce	5	5	0,25	0	jednatel
2	Nedostupnost služby	Smluvní ošetření u dodavatele, sankce	20	5	1	0	jednatel
3	Migrace dat	Kontrola při provádění operace, kontrola integrity a konzistence dat	5	2,5	0,125	0	technické oddělení
4	Zálohování	Častější zálohy na více místech	20	2	0,4	0	technické oddělení
5	Napadení sítě	Pravidelná aktualizace systémů, využívání antivirových programů, zabezpečení bezdrátové sítě, fyzický firewall	30	4,5	1,35	15495	technické oddělení
6	Porucha hardwaru	Pravidelný servis, obměňování HW, nákup určitého HW na sklad	10	4,5	0,45	0	technické oddělení
Personální rizika							
7	Nedostatečné proškolení pracovníků	Důsledné školení zaměstnanců, prostor pro otázky a návrhy	25	5	1,25	9600	jednatel
8	Neúmyslný incident	Pravidelné školení pracovníků	10	2,5	0,25	0	jednatel
9	Nepřizpůsobení se změně	Zvýšení motivace pracovníků	15	3	0,45	0	jednatel
Finanční rizika							
10	Nesprávné vyčíslení přínosů	Realizace detailní analýzy a kalkulace	10	2	0,2	0	obchodní oddělení
11	Překročení stanoveného rozpočtu	Striktní dodržování finančního plánu, vytvoření finanční rezervy	15	2,5	0,375	0	obchodní oddělení
Bezpečnostní rizika							

12	Nedostatečné zabezpečení systému	Vytvořit a striktně hlídat striktní dodržování firemních zásad a politiky hesel, u dodavatele ošetřit zabezpečení přímo ve smlouvě a definovat sankce	10	4	0,4	0	technické oddělení
13	Nedostatečné zabezpečení klientských stanic	Vytvořit a hlídat dodržování firemních zásad a politiky hesel	15	5	0,75	0	technické oddělení
Organizační rizika							
14	Špatně sjednaná smlouva	Detailní analýza smlouvy a konzultace s AK	25	4,5	1,125	5000	jednatel
15	Nedodržení stanoveného termínu	Kontrola milníků projektu a hlídat časové rezervy	15	3	0,45	0	jednatel

3.7 Pavučinový graf rizik

Následující pavučinový graf zachycuje hodnoty jednotlivých rizik před a po provedení doporučených opatřeních. Z tohoto grafu je patrné, že doporučená opatření lze hodnotit jako účinná.

Graf 2: Pavučinový graf rizik [Zdroj: Vlastní]

3.8 Návrh informačního systému

Na základě výše provedených analýz bylo vyhodnoceno, že jednou z možných změn je pořízení informačního systému, který doposud společnost na pobočce nevlastní. V současné době se dobře zvolený a implementovaný informační systém dá považovat za jeden z dílčích kroků k úspěšnému podnikání. Takový systém by měl společnosti přinést mnohem efektivnější řízení jejich procesů, zjednodušit komunikaci mezi pracovníky, jakožto i sdílení potřebných dat. Od pořízení informační systému lze tedy očekávat, že pracovníkům přinesu úsporu času a společnosti z dlouhodobějšího hlediska rovněž i úsporu nákladů a zvýšení efektivity a bezpečnosti práce. Dalším důvodem pro pořízení je konkurence společnosti, která vyvíjí tlak na neustálé zlepšování a zefektivňování procesů. Informační systém by tak společnosti měl přinést rovněž zvýšení konkurenceschopnosti.

3.9 Lewinův model

3.9.1 Rozmrazení

a) Síly inicializující proces změny

Za primární sílu inicializující proces změny se dá označit nespokojenost vedení společnosti a rovněž pracovníků se současným stavem. Jak bylo na základě dříve provedených analýz zjištěno, tak komunikace mezi pracovníky není efektivní, přičemž tato skutečnost je mimo jiné způsobena tím, že ve společnosti není komplexně řešeno sdílení potřebných dat pro rozhodování a realizaci zakázek. Vzhledem k tomu, že společnost v současné době primárně využívá pro sdílení tabulky v programu Microsoft Excel, tak samotná správa těchto dat je velice časově náročná, nepřehledná a neefektivní. Doby trvání jednotlivých procesů ve společnosti se tak prodlužují. Společnost rovněž zvažuje, že otevře nové pobočky, a proto je nutné, aby tyto pobočky byly vzájemně propojeny. Mimo jiné z těchto důvodů bylo rozhodnuto o pořízení informačního systému do společnosti.

b) Sponzor změny

Sponzorem změny bude samotná společnost, která bude zavedení této změny financovat. Jednatelé společnosti tak budou rovněž poskytovat agentovi změny potřebnou součinnost.

c) Agent změny

Jako agent či nositel změny byl zvolen zástupce vedoucího technického oddělení, neboť má s výběrem informační systému zkušenosti z předchozího zaměstnání, zná velmi dobře současné procesy ve společnosti a je schopen tuto změnu koordinovat v rámci celé společnosti. Tento pracovník bude mít na starost rovněž komunikaci se zvoleným dodavatelem informačního systému, se kterým vypracuje potřebnou detailní projektovou dokumentaci.

d) Intervenční oblasti

Vzhledem k tomu, že zavedení informačního systému se dá považovat za komplexní záležitost, tak tato změna ovlivní chod celé společnosti a všech pracovníků. Z tohoto důvodu bude nutné následně všechny pracovníky společnosti řádně proškolit.

Očekává se tedy, že tato změna se dotkne obou oddělení společnosti. Příkladem lze uvést, že se tato změna dotkne jednotlivých oddělení následovně:

- Obchodní oddělení – tvorba nabídek, administrativní činnost, fakturace, finanční plánování, marketing, nákup zboží aj.
- Technické oddělení – evidence technické dokumentace, řízení projektů

Nový informační systém bude disponovat těmito moduly:

- Vedení docházky pracovníků
- Řízení kontaktů
- Projektový management
- Řízení vztahu se zákazníky
- Business Intelligence
- Účetnictví

3.9.2 Změnový proces

Samotná realizace změny bude provedena pomocí nástrojů projektového managementu, přičemž vedoucím tohoto projektu bude agent změny, tedy zástupce vedoucího technického oddělení.

V tomto projektu budou nejprve na základě požadované specifikace osloveni dodavatelé informačních systémů. Následně bude provedeno vyhodnocení získaných nabídek, ze kterých bude zvolen vhodný kandidát. V dalším kroku bude společně se zvoleným dodavatelem provedena analýza procesů ve společnosti, budou stanoveny nutné předpoklady pro zavedení informačního systému a následně bude již realizována implementace zvoleného systému. Po řádném otestování funkčnosti a stability tohoto systému bude realizována migrace dat ze stávajících tabulek, přičemž tyto data budou připravena již před samotnou implementací, a bude provedeno proškolení pracovníků. Po proškolení bude informační systém předán společnosti a tento systém bude nasazen do ostrého chodu.

Zhodnocení

Po provedené implementaci informačního systému bude možné provést zhodnocení předmětné změny. Toto zhodnocení bude realizováno tak, že bude porovnána efektivita práce na jednotlivých pozicích před a po jeho zavedení.

3.9.3 Zamražení

Jak vedení společnosti, tak jednotliví pracovníci s touto změnou souhlasí, a proto by tato změna měla být přijata bez komplikací, neboť pracovníkům přinese zvýšení efektivnosti jejich práce a usnadnit jim tak jejich pracovní náplň.

3.10 Časový harmonogram změny

Vzhledem k tomu, že společnost není schopna přesně odhadnout doby trvání jednotlivých dílčích činností, tak pro určení doby trvání bude využita metoda PERT. Tato metoda vychází z tří bodového odhadu, přičemž tyto údaje byly získány na základě předchozích

zkušeností. Pomocí této metody je následně možné naleznout kritickou cestu projektu, která představuje posloupnost navazujících činností, které mají nulovou časovou rezervu. Počátek projektu byl stanoven na měsíc srpen tohoto roku, a to zejména z důvodu toho, že v tomto období bývá pravidelně činnost společnosti částečně omezena z důvodů čerpání dovolené. Dále je dobré uvést, že níže uvedený časový harmonogram byl sestaven tak, aby během realizace projektu nedošlo k omezení činností společnosti nebo jeho pracovníků.

Za účelem zpracování časové a pravděpodobnostní analýzy bylo nutné nejdříve vypočítat některé číselné charakteristiky. Tyto výpočty byly realizovány za pomocí těchto vzorců:

$$y_{ij} = \frac{a_{ij} + 4m_{ij} + b_{ij}}{6}$$

$$\sigma^2 y_{ij} = \frac{\left(b_{ij} - a_{ij}\right)^2}{36}$$

$$\sigma y_{ij} = \frac{b_{ij} - a_{ij}}{6}$$

Jednotlivé činnosti projektu jsou zachyceny v tabulce níže, přičemž z provedené časové analýzy rovněž plyne, že:

- Celková doba trvání projektu představuje 40 dní.
- Kritická cesta vede přes uzly: 1-2-5-11-14-15.
- Z celkových 21 činností je 6 kritických, a proto je procento kritičnosti rovno 28 %.

Na základě vypočtených charakteristik a síťového grafu lze nyní přistoupit rovněž k pravděpodobnostní analýze.

Jaká je pravděpodobnost, že se projekt prodlouží o 1 den?

$$P(T \leq 41) = F\left(\frac{PT - TM_n}{\sigma_{TM_n}}\right) = F\left(\frac{41 - 40}{\sqrt{4{,}45}}\right) = F(0{,}47) = F(u) = 68{,}08\ \%$$

Doba trvání projektu se prodlouží o 1 den s pravděpodobností 0,6808, přičemž v procentuálním vyjádření se jedná o 68,08 %.

Jaká je pravděpodobnost, že se projekt zkrátí o 2 dny?

$$P(T \leq 38) = F\left(\frac{PT - TM_n}{\sigma_{TM_n}}\right) = F\left(\frac{38 - 40}{\sqrt{4{,}45}}\right) = F(-0{,}97) = 1 - F(0{,}97)$$
$$= 1 - \ 0{,}8289 = 0{,}1711 = 17{,}11\ \%$$

Pravděpodobnost, že se doba trvání projektu zkrátí o 2 dny, je 0,1711, v procentuálním vyjádření se jedná o 17,11 %.

Tabulka 6: Jednotlivé činnosti projektu [Zdroj: Vlastní]

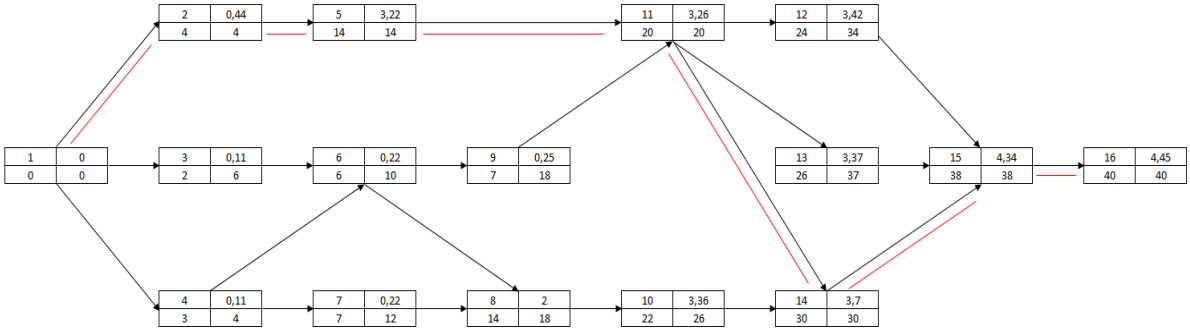
Označení	Popis činnosti	t_{ij} [dny]
A	Příprava interních dat pro následnou migraci	4
B	Schůzka s dodavatelem informačního systému	2
C	Výběr vhodné konfigurace serveru	3
D	Migrace dat	10
E	Návrh od dodavatele	4
F	Schválení konfigurace serveru	2
G	Doprava serveru	4
H	Montáž serveru	6
I	Implementace datového skladu	8
J	Uzavření smluvního vztahu s dodavatelem	1
K	Příprava serveru	8
L	Poskytnutí licencí	2
M	Příprava klientských stanic	6
N	Instalace informačního systému	4
O	Konfigurace informačního systému	6
P	Školení pracovníků	10
Q	Integrace dat	4
R	Testování stability systému	8
S	Přidělení práv jednotlivým pracovníkům	1
T	Testování funkčnosti a stability informačního systému	4
U	Ostrý provoz informačního systému	2

Tabulka 7: Vypočtené charakteristiky činností [Zdroj: Vlastní]

Ozn.	i	j	a_{ij}	m_{ij}	b_{ij}	y_{ij}	σ^2	σ	ZM	KM	ZP	KP	RC
A	1	2	2	4	6	4	0,44	0,67	0	4	0	4	0
B	1	3	1	2	3	2	0,11	0,33	0	2	4	6	4
C	1	4	2	3	4	3	0,11	0,33	0	3	5	8	5
D	2	5	5	10	15	10	2,78	1,67	4	14	4	14	0
E	3	6	3	4	5	4	0,11	0,33	2	6	6	10	4
F	4	6	1	2	3	2	0,11	0,33	3	5	8	10	5
G	4	7	3	4	5	4	0,11	0,33	3	7	8	12	5
H	7	8	2	6	10	6	1,78	1,33	7	13	12	18	5
I	6	8	4	8	12	8	1,78	1,33	6	14	10	18	4
J	6	9	0,5	1	1,5	1	0,03	0,17	6	7	17	18	11
K	8	10	2,5	8	13,5	8	3,36	1,83	14	22	18	26	4
L	9	11	1,8	2	2,2	2	0,00	0,07	7	9	18	20	11
M	5	11	5,4	6	6,6	6	0,04	0,20	14	20	14	20	0
N	11	12	2,8	4	5,2	4	0,16	0,40	20	24	30	34	10
O	11	13	5	6	7	6	0,11	0,33	20	26	31	37	11
P	11	14	8	10	12	10	0,44	0,67	20	30	20	30	0
Q	10	14	3,5	4	4,5	4	0,03	0,17	22	26	26	30	4
R	14	15	5,6	8	10,4	8	0,64	0,80	30	38	30	38	0
S	13	15	0,5	1	1,5	1	0,03	0,17	26	27	37	38	11
T	12	15	2	4	6	4	0,44	0,67	24	28	34	38	10
U	15	16	1	2	3	2	0,11	0,33	38	40	38	40	0

3.11 Síťová analýza

Podrobný obrázek je uveden v příloze.



Graf 3: Síťový graf [Zdroj: Vlastní]

3.12 Proces objednávky

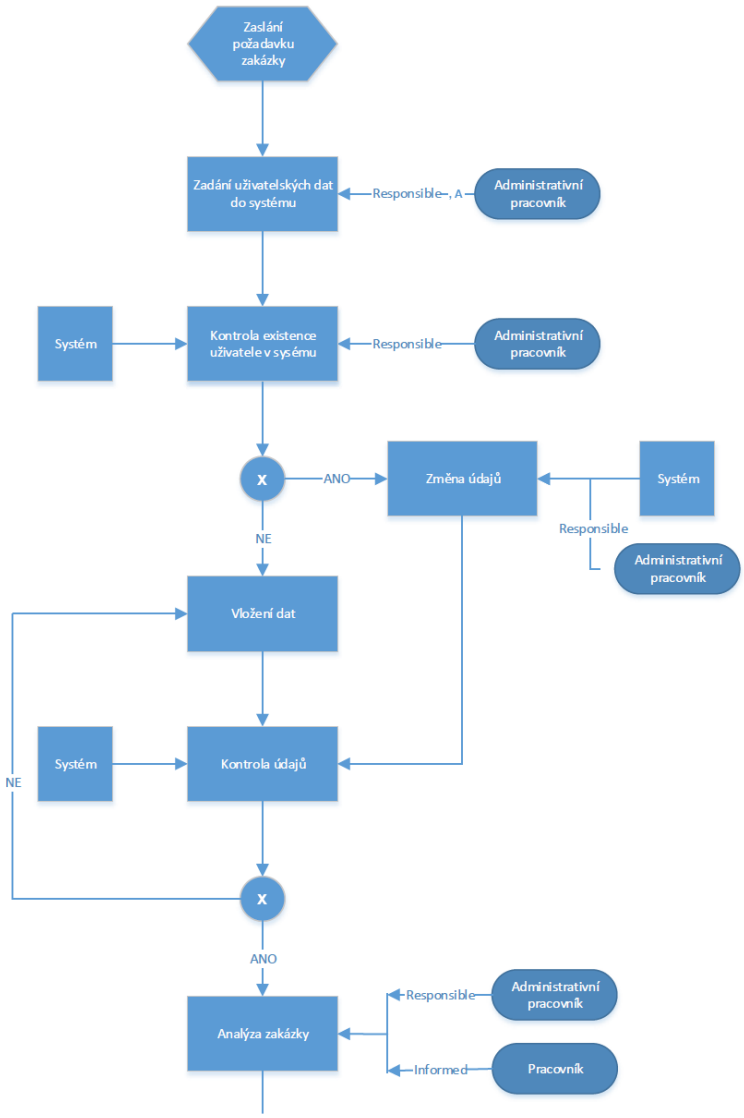
3.12.1 RACI matice

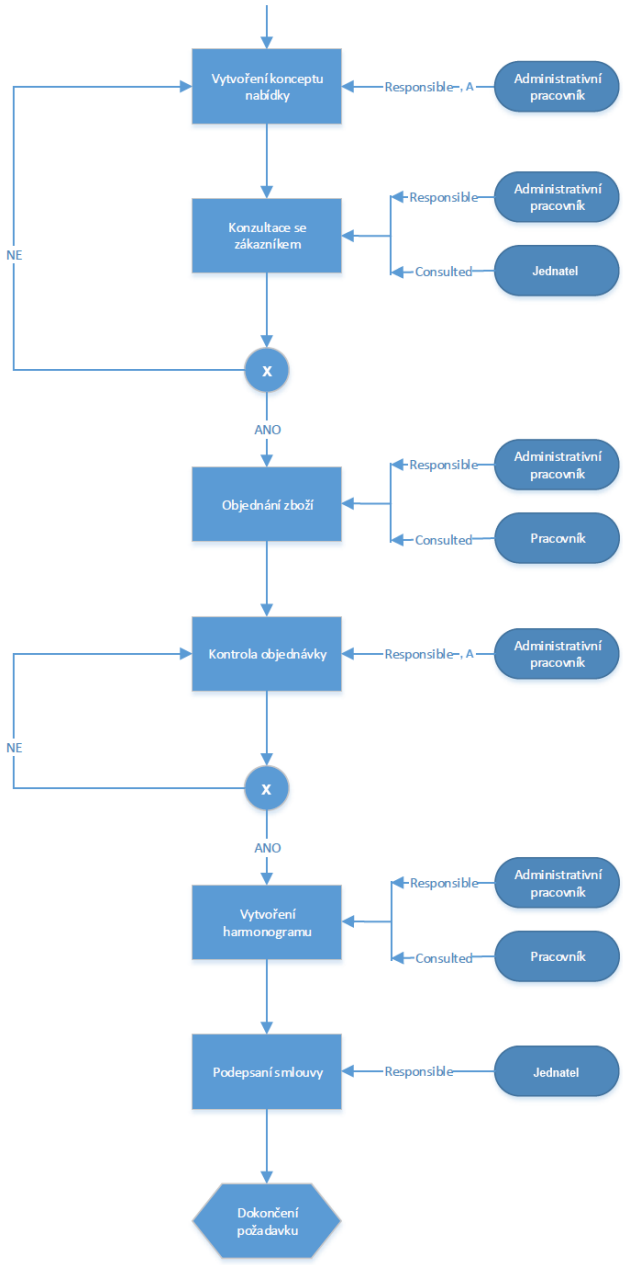
Zde je uvedená RACI matice procesu vytvoření objednávky ve společnosti s pomocí informačního systému.

Tabulka 8: RACI matice [Zdroj: Vlastní]

RACI matice	Procesní role		
	Administrativa	Technické oddělení	Vedení společnosti
Zadání uživatelských dat do systému	R, A		
Kontrola Existence uživatele v systému	R		
Změna údajů	R		
Vložení dat	R		
Kontrola dat	R		
Analýza zakázky	R	I	
Vytvoření konceptu nabídky	R, A		
Konzultace se zákazníkem	R		C
Objednání zboží	R	C	I
Kontrola zboží	R, A		
Vytvoření harmonogramu	R	C	
Podepsání smlouvy			R

3.12.2 EPC diagram – vyřízení objednávky





Obrázek 13: EPC diagram [Zdroj: Vlastní]

3.13 SLA – Service Level Agreement

SMLUVNÍ STRANY: Cleverlance Enterprise Solutions a.s a Asseco Solutions

DEFINICE SLUŽBY: Firma Cleverlance Enterprise Solutions a.s požaduje správu a údržbu informačního systému, dále servis nebo případný upgrade systému/modulů.

ZODPOVĚDNOST: Za poskytnutý servis a údržbu je zodpovědná definovaná osoba firmou Asseco Solutions. Společnost Cleverlance Enterprise Solutions a.s se zavazuje k

poskytnutí zodpovědné osoby, která umožní vstup do prostor nájemce pro potřeby plnění servisních úkonů.

ČASY A TERMÍNY: Správa a údržba systému bude prováděna každé pondělí v 6:00, po dohodě nebo v případě havárie i v jiném termínu schválený vedením firmy. Firma Asseco Solutions se zavazuje k odstranění závad do 8 hodin od nahlášení poruchy.

KVANTITA A KVALITA ZPRACOVÁNÍ: Správu a údržbu má na starosti pověřený zaměstnanec dodavatele. Uživatelé Cleverlance Enterprise Solutions a.s požadují funkční systém s podporou všech firemním procesů. Kvalita je v souladu s technickými parametry uvedené poskytovatelem

METRIKY: Kontrola následujících metrik na začátku užívání a vždy jednou týdně, nebo po nápravě poruchy technikem. Měření je prováděno zaměstnanci pomocí každodenního užívání systému.

HLÁŠENÍ O NEDODRŽENÍ SMLOUVY: Probíhá okamžitě po zjištění, nejpozději však do 1 pracovního dne.

ODPOVĚDNOST ZA ŠKODU: V případě způsobené havárie dodavatelem, je povinen škodu uhradit/spravit bez nároku na kompenzaci jeho zdrojů. Společnost Asseco Solutions nezodpovídá za interní škody například ušlého ekonomického zisku způsobené neznalostí uživatelů

CENY: První dva roky zdarma poté měsíční platba za servis a údržbu je 3000 Kč.

POKUTY A PENÁLE: V případě nedodržení stanoveného termínu, nebude se dodavateli účtovat týdenní poplatek 500Kč. Pokud kvůli nedodržení termínu nastane havárie informačního systému, musí dodavatel uhradit ztrátu ušlého zisku v plné výši.

3.14 Ekonomické zhodnocení

Pořízení informačního systému a jeho implementace představuje pro společnost náklady, které musí vynaložit. Tyto náklady zejména spočívají v nákupu potřebného HW, licencí a dále ve službách spojených s implementací a údržbou tohoto systému. Tyto náklady jsou shrnuty v následující tabulce.

Tabulka 9: Náklady na informační systém [Zdroj: Vlastní]

Položka	Náklady	Počet	Náklady celkem
Licence informačního systému	7140 Kč/rok	5	35 700 Kč
Migrace dat	400 Kč/hod	20	8 000 Kč
Implementace systému	600 Kč/hod	25	15 000 Kč
Servisní služby	první dva roky zdarma	3	0 Kč
Nákup serveru	40000 Kč	1	40 000 Kč
		∑	**98 700 Kč**

Tabulka níže zachycuje náklady společnosti spojené s opatřeními, která byla v předchozí části společnosti doporučena k tomu, aby snížila hodnoty identifikovaných rizik. Zde je nutné zmínit, že pouze některá doporučení představují pro společnost dodatečné náklady, neboť většina z těchto doporučení spočívají zejména v důsledné kontrole prováděných činností, popřípadě v přenesení odpovědnosti na dodavatelský subjekt.

Tabulka 10: Náklady na eliminaci rizik [Zdroj. Vlastní]

Položka	Náklady	Počet	Náklady celkem
Právní služby	2500 Kč/hod	2	5 000 Kč
Extra školení zaměstnanců	1200 Kč/hod	8	9 600 Kč
Licence antivirového programu	2 149 Kč	5	10 745 Kč
HW firewall	4 750 Kč	1	4 750 Kč
		∑	**30 095 Kč**

Celkové náklady tedy nepřekročili částku 200 000,- Kč a požadavky investora byly splněny.

ZÁVĚR

Cílem této diplomové práce bylo navrhnout inovaci a změny v systému řízení identit ve společnosti Cleverlance.

V první části této diplomové práce byla uvedena teoretická východiska týkající se identity managementu. Následně byla zpracována analýza podniku, kde byla nejprve společnost analyzována z pohledu vnějšího okolí. Byla zpracována analýza SLEPT a rovněž Porterův model pěti sil, dále z pohledu vnitřního pohledu, kde byla provedena analýza 7S. Na základě těchto výsledků byla následně zpracována SWOT analýza společnosti. V poslední řadě také analýza řízení přístupů a analýza rizik. Po provedení výše zmíněných analýz bylo přistoupeno již k samotnému návrhu změny. Vzhledem k tomu, že bylo zjištěno, že společnost dosud nedisponuje informačním systémem, který by pokrýval procesy ve společnosti, tak bylo rozhodnuto, že tato změna bude spočívat v pořízení a zavedení takového systému. Předmětná změna byla v práci popsána pomocí Lewinova modelu, přičemž byl rovněž navržen časový harmonogram a ekonomické náklady. Zmíněná doporučovaná změna byla následně podrobena analýze rizik. Identifikovaná rizika byla následně ohodnocena a byla navržena patřičná opatření vedoucí ke snížení hodnot těchto rizik, přičemž jejich účinnost byla ilustrována pomocí pavučinového grafu. V závěru práce bylo krátce pojednáno o nákladech, které bude muset společnost na zvolenou změnu vynaložit.

Cíle této diplomové práce byly tímto splněny.

SEZNAM POUŽITÉ LITERATURY

1. BERTINO, E. A K. TAKAHASI. Identity Management: Concepts, Technologies and Systems. Bostno: Artech House, 2011. ISBN 978-1-608807-039-8.
2. ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4.
3. POŽÁR J. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005. ISBN 80-86898-38-5.
4. YIP D., G. WILLIAMSON, I. SHARONI a K. SPAULDING. Identity Management: A Primer. Lewisville: MC Press, 2009. ISBN 978-1583470930.
5. DOUCEK P. et al. Řízení bezpečnosti informací. 2. Rozšířené vydání o BCM. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
6. DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.
7. ČSN ISO/IEC 27000. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnostní informací - Přehled a slovník. Praha: Úřad pro technickou normalizaci, 2014.
8. ČSN ISO/IEC 27001.. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnostní informací - Přehled a slovník. Praha: Úřad pro technickou normalizaci, 2005.
9. ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací. Praha: Český normalizační institut, 2013.
10. ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.
11. MALINKA, K. Kryptografie (Přednášky). Brno: VUT v Brně, Fakulta podnikatelská, 2013.
12. IDENTITY MANAGEMENT. Identity management. Techtarget.com [online]. [cit. 2018-5-2]. Dostupné z: http://searchsecurity.techtarget.com/definition/identity-management-ID-management

13. Přehled norem ISO/IEC 27000. Identity management. Slideplayer.cz [online]. [cit. 2018-5-4]. Dostupné z: http://slideplayer.cz/slide/2589937/9/images/7/P%C5%99ehled+%C5%99ady+norem+ISO/IEC+27000.jpg
14. SINGLE SIGN ON (SSO). SSO. Managementmania.com [online]. [cit. 2018-5-6]. Dostupné z: https://managementmania.com/cs/single-sign-on
15. CLEVERANCE. Logo společnosti. Rmol.cz [online]. [cit. 2018-4-3]. Dostupné z: https://www.rmol.cz/sites/default/files/main-images/cleverlance_logo.jpg
16. CYKLUS PDCA. PDCA. Texample.net [online]. [cit. 2018-4-18]. Dostupné z: http://www.texample.net/media/tikz/examples/PNG/pdca-cycle.png
17. ITIL. Knihovna ITIL. leansixsigmaexperts.com [online]. [cit. 2018-4-18]. Dostupné z: https://www.leansixsigmaexperts.com/sites/default/files/images/ITIL-258317-edited.png
18. COBIT. Kostka COBIT. ocplayer.cz [online]. [cit. 2018-4-11]. Dostupné z: http://docplayer.cz/docs-images/26/4469938/images/15-0.png
19. RBAC. Model RBAC. thorteaches.com [online]. [cit. 2018-4-13]. Dostupné z: https://thorteaches.com/wp-content/uploads/2017/09/RBAC.png
20. RUBENKING NEIL. The Best Free Password Managers for 2016. www.pcmag.com [online]. [cit. 2018-4-20]. Dostupné z: http://www.pcmag.com/article2/0,2817,2475964,00.asp
21. CYBERARK. CyberArk software. cyberark.com [online]. [cit. 2018-4-26]. Dostupné z: https://www.cyberark.com/solutions/security-risk-management/
22. CYBERARK. Logo CyberArk. venafi.com [online]. [cit. 2018-4-27]. Dostupné z: https://www.venafi.com/techpartner/cyberark
23. CYBERARK PIM. CyberArk Privileged Identity Management Suite. rac.cz [online]. [cit. 2018-4-27]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/Cyber-ArkPIM

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM OBRÁZKŮ