VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ŘÍZENÍ PŘÍSTUPU K DATŮM SPOLEČNOSTI
DESIGN OF ACCESS CONTROL TO COMPANY DATA

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Matej Havlas**
AUTHOR

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

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Matej Havlas**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2020/21

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

Návrh řízení přístupu k datům společnosti

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Navrhnout řízení přístupu k firemním datům.

Základní literární prameny:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

BUNKER G. a G. FRASER-KING. Data Leaks For Dummies. Canada: Wiley Publishing, Inc., 2009. ISBN 978-0-470-38843-3.

GAWRONSKI M. Guide to the GDPR. Nizozemsko: Kluwer Law International B.V., 2019. ISBN 978-94-035-1414-7.

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

OSMANOGLU E. Identity and Access Management: Business Performance Through Connected Intelligence. Newnes, 2013. ISBN 9780124104334.

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

V Brně dne 28.2.2021

L. S.

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

Abstrakt

Obsahom bakalárskej práce je návrh systému prístupu zamestnancov ku firemným dátam na základe dostupnej literatúry a znalostí nadobudnutých počas štúdia na VUT Fakulte Podnikatelskej. Prvá časť sa bude venovať teoretickým východiskám práce. Druhá časť sa bude venovať analýze súčasného stavu a tretia časť sa bude venovať návrhu riešenia, ktoré bude vychádzať z analýzy súčasného stavu a teoretických východísk práce.

Abstract

The content of my bachelor thesis consists of a proposal for a system of data access management to company data, based on available literature and acquired knowledge through my studies on BUT Faculty of Management. First part will be theoretical background. Second part will be analysis of current state and third part will contain proposed solution, based on analysis of current state and theoretical background.

Kľúčové slová

Dáta, Prístup, Analýza, Bezpečnosť, Autentifikácia, Autorizácia

Key words

Data, Access, Analysis, Security, Autentication, Authorization

Bibliografická citácia

HAVLAS, Matej. Návrh řízení přístupu k datům společnosti [online]. Brno, 2021 [cit. 2021-05-12]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133315. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prehlásenie

Prehlasujem, že predložená bakalárska práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brne dňa 16. mája 2021 .....

podpis autora

Poďakovanie

Ďakujem vedúcemu bakalárskej práce, Ing. Viktorovi Ondrákovi, Ph.D., za odborné vedenie a cenné rady pri písaní tejto práce. Rovnako sa chcem poďakovať svojim rodičom za ich podporu pri štúdiu, Ing. Báčikovi, Ing. Kostkovi a Ing. Volkovi za konzultácie, ktoré mi pomohli pri tvorbe tejto práce.

Obsah

Úvod

V dnešnej dobe sú dáta veľmi cenné. Je potrebné ich patrične chrániť. Dáta sú spracovávané v rôznych systémoch, pričom do každého systému potrebuje užívateľ heslo, ktoré musí spĺňať stále vyššie bezpečnostné štandardy. To stavia zamestnancov a zamestnávateľov do situácie, kedy zamestnanci dookola používajú tie isté typy hesiel a zamestnávatelia prideľujú prístupy bez riadnej evidencie. Pri viacerých systémoch je potrebné vytvárať samostatné identity, čo ďalej komplikuje autorizáciu užívateľov.

V mojej bakalárskej práci sa budem zaoberať návrhom prístupu k dátam spoločnosti. Budem sa zameriavať hlavne na oblasť autentifikácie, autorizácie a zdieľania dát na vnútrofiremnej úrovni.

1 Cieľ práce a metódy spracovania

1.1 Cieľ práce

Cieľom bakalárskej práce je navrhnúť systém prístupu dát v stredne veľkej firme. Práca sa bude zameriavať na interné prístupy a na zdieľané dokumenty s klientami. V návrhoch riešenia bude braný ohľad na preferencie firmy a jej klientov v oblasti autorizácie a autentifikácie.

1.2 Čo práca nerieši

Práca nerieši detaily konkrétnych nastavení Mobile Device Managementu, Politiky predchádzaniu straty dát a ani konkrétnu detailnú konfiguráciu Microsoft Azure Active Directory a SharePointu. Práca ďalej nerieši ani kompletnú implementáciu navrhovaných riešení.

1.3 Metódy spracovania

Pri spracovávaní návrhov som vychádzal z vlastnej praxe, praxe odborníkov v danej oblasti a predpokladaným vývojom informačných technológií. Pre jednotný vzhľad práce som použil výhradne nástroj draw.io. Väčšinu obrazového materiálu som vytváral sám. Svoje návrhy som počas svojej praxe postupne implementoval aj napriek tomu, že to samotná práca neriešila. Z tohto dôvodu som na základe jedného užívateľa do návrhov riešenia pridal aj časový odhad jednotlivých činností.

2 Teoretické východiská práce

2.1 Údaj

Údaj pozostáva z faktov alebo čísel, ktoré nemajú bez vonkajšieho kontextu zmysel. Za údaj môžeme považovať všetko bez ohľadu na to, či obsahuje informačnú hodnotu. (24, 23)

2.2 Informácia

Informáciu tvorí viacero údajov vložených do kontextu. Štruktúrovaná a organizovaná informácia môže byť premenená na znalosť, na základe ktorej vie človek alebo počítač urobiť rozhodnutie. (24)

2.3 Dáta

Dáta vieme definovať tromi spôsobmi a to nasledovne:

- Dáta sú akékoľvek informácie spracovávané v informačných systémoch.
- Údaje v širšom zmysle, vyjadrujú základné charakteristiky informačného systému.
- Informácie v štandardnom tvare, vhodné pre strojové spracovanie. (25)

2.4 Spracovávanie dát

Podnikové informačné systémy slúžia na jednoduchšie spracovanie skupín dát, ktoré by človek nedokázal spracovať ručne. Väčšina dnes používaných riešení spracovania dát funguje cez Cloud, pričom sa o bezpečnosť stará poskytovateľ služby. (2, 4)

Dva najčastejšie používané systémy na spracovanie dát sú:

2.4.1 ERP – enterprise resource planning

Slúži na plánovanie podnikových zdrojov. Existujú dva varianty. All-in-one riešenie, ktoré integruje všetky procesy v podniku a zastrešuje veľké množstvo

funkcionalít. Problémom All-in-one riešenia je nemožnosť úpravy systému. (4)

On Demand varianta je softvér vyvíjaný na zákazku, ktorý je upravený podľa presnej špecifikácie klienta. Nevýhodou softvéru na zákazku je jeho vyššia cena a nutnosť detailnej špecifikácie na začiatku vývoja. (4)

2.4.2 CRM – customer relationship management

Umožňuje Business to business podnikom poskytovanie lepšej zákazníckej podpory a správu dôležitých informácií o klientoch. CRM sa najčastejšie používa v spojení s telefónnymi ústredňami, ktoré ponúkajú CRM ako súčasť balenia. CRM umožňuje nahrávanie hovorov, zaznamenávať často riešené problémy a merať čas za koľko sa problém vyrieši. Systém si udržuje internú databázu volaných čísel, mien zákazníkov a emailov, čím vyžaduje vyššiu mieru zabezpečenia. (1, 4)

2.5 Ukladanie dát

Ukladanie dát je schopnosť uchovania všetkých dôležitých dát v organizovanej štruktúre, pre zaistenie okamžitej dostupnosti, s garanciou dôveryhodnosti a integrity. To je docielené ukladaním dát na záznamové médium, pripojené k počítaču alebo inému druhu výpočtovej techniky. (26, 27)

2.5.1 Lokálne ukladanie dát

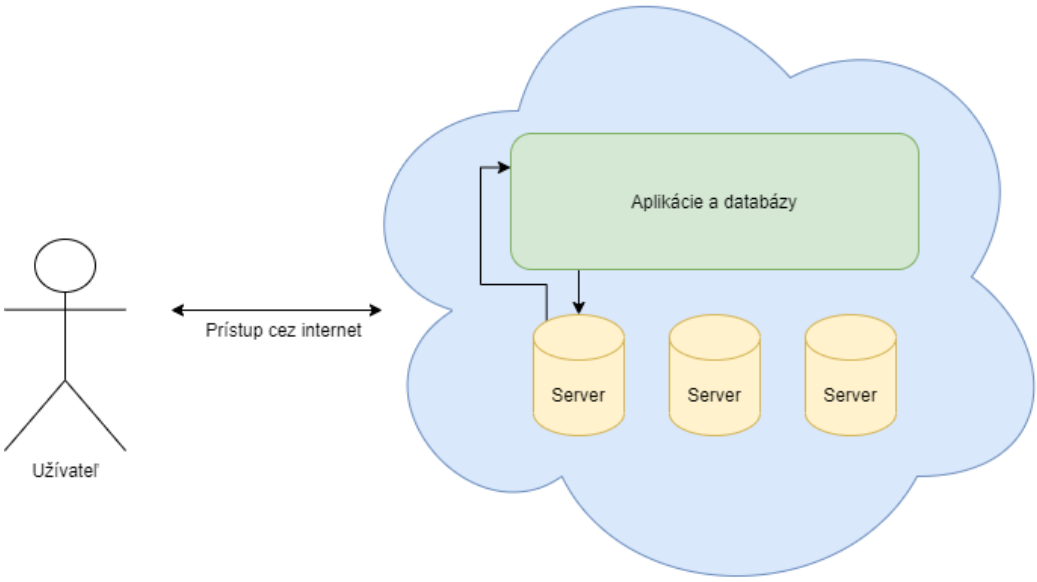
Dáta sú uchovávané lokálne na záznamové médium, ktoré je fyzicky pripojené k počítaču užívateľa a to buď interne, alebo externe. Užívateľ zodpovedá za obsah média a taktiež za jeho dôveryhodnosť, dostupnosť a integritu uložených dát. Výhodou lokálneho úložiska je kapacita, nevýhodou je zálohovanie dát, o ktoré sa musí starať užívateľ. Príkladom lokálnych médií sú USB kľúče, CD alebo HDD. (28, 29)

2.5.2 Centralizovaná databáza

Centralizovaná databáza je databáza uložená na jednom mieste z ktorého je spravovaná a upravovaná. Databáza sa nachádza na centrálnom počítači a pre prístup k dátam je potrebné internetové pripojenie. Nevýhodou centralizovanej databázy je zvýšený prenos dát pri väčšom počte aktívnych užívateľov. (30, 31)

2.5.3 Cloud

Pojem cloud označuje akýkoľvek server alebo zhluk serverov dostupných z internetu, na ktorom sú skladované dáta, alebo na ktorom bežia aplikácie. Cloudové servre sa nachádzajú v dátových centrách po celom svete. Používaním cloudových serverov užívateľom odpadá potreba spravovať fyzické serveri v budovách a nutnosť chodu aplikácií na vlastných strojoch. Užívatelia majú dáta a aplikácie prístupné na ktoromkoľvek autorizovanom zariadení s prístupom na internet. (7)



Obrázok 1 Cloud [Zdroj: vlastné spracovanie]

Typy rozdelenia Cloudu :

- Súkromný - vyhradený pre 1 konkrétnu organizáciu, dáta nie sú zdieľané medzi viacero dátových centier.
- Verejný - poskytovaný treťou stranou, poskytovateľ môže zastrešovať viacero organizácií a rozložiť dáta do viacerých dátových centier.
- Hybridný – Kombinácia súkromného a verejného Cloudu. Umožňuje organizácii využívať verejný cloud na dáta a súkromný cloud ako archív.(7)

2.6 Virtualizácia

Virtualizácia umožňuje chod viacerých virtuálnych počítačov na jednom fyzickom stroji v jednom momente. Výhodou virtualizácie je, že v prípade zlyhania jedného z virtuálnych počítačov , sú dáta zálohované na ďalších. Táto technológia umožňuje poskytovateľom rozložiť dáta organizácií medzi viaceré fyzické dátové centrá po celom svete. Okrem toho umožňuje komplexnejšie poskytovanie služieb podľa potrieb užívateľov. (5, 7)

2.6.1 Software as a Service (SaaS)

Poskytovanie softvéru bez perpetuálnej licencie. Tento spôsob využitia cloudu umožňuje používanie softvéru bez nutnosti inštalácie na zariadenie. Aplikácia je hosťovaná na serveri a užívateľ má prístup ku aplikácii cez webové rozhranie. Medzi SaaS sa radí aj CRM program salesforce. (5, 7, 8)

2.6.2 Platform as a Service (PaaS)

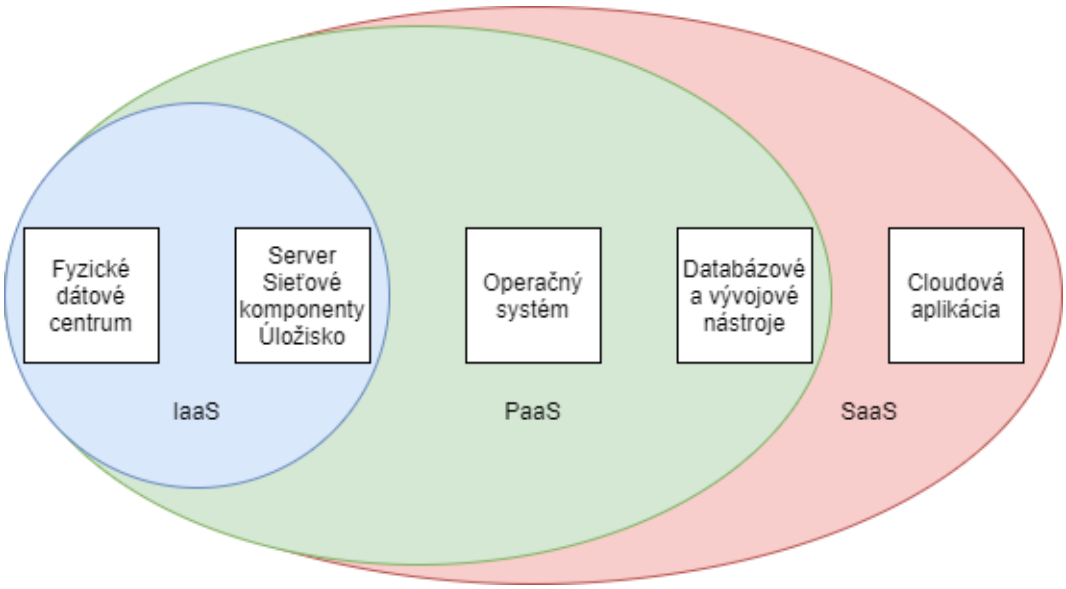
Užívateľ platí za platformu, na ktorej si vyskladá aplikácie. Poskytovatelia PaaS štandardne dodávajú sady komponentov a softvérových podsystémov obsahujúcich operačný systém alebo databázové komponenty a vývojové nástroje. Príkladom PaaS riešenia je Microsoft Azure. (5, 7)

2.6.3 Infrastructure as a Service (IaaS)

Užívateľ si prenajíma hardvér z dátového centra. Jedná sa predovšetkým o dátové úložiská, servery alebo iné hardvérové komponenty. (5, 7)

2.6.4 Function as a service (FaaS)

Užívateľ platí len za časť aplikácie, ktorú momentálne využíva. Kontajnerizácia aplikácií umožnila nový spôsob využívania cloud riešenia nazývaný aj bez serverový. Aplikácia nebeží na konkrétne vyhradenom serveri, ale spúšťa sa len v prípade, že ju užívateľ práve používa. Podľa počtu užívateľov potom dynamicky mení svoju veľkosť. (7)



Obrázok 2 Rozdelenie druhu Cloud služieb [Zdroj: vlastné spracovanie]

2.7 Mobile Device Management (MDM)

Mobilná správa zariadení umožňuje administrátorovi správu koncových firemných zariadení užívateľov. Funguje na princípe klient – server architektúry, kde koncové zariadenie preberá rolu klienta. Zariadenie o sebe na server posiela dáta v reálnom čase. (14, 15, 32)

- International Mobile Equipment Identity (IMEI). GUID zariadenia, pomocou ktorého MDM server jednoducho identifikuje zariadenie.
- Roaming. Poskytuje serveru informácie o aktuálne využívanej mobilnej sieti.
- Stav batérie. Odosiela na server stav batérie. Ten dokáže spätne z dát vyhodnotiť potencionálne pokazenú batériu

- GPS lokalizácia. Zariadenie odosiela informácie o svojej aktuálnej polohe na server.
- Informácie o firmvéri. Zariadenie odosiela na server aktuálnu verziu operačného systému, čo MDM umožňuje zoskupovať zariadenia podľa typov a verzií operačných systémov
- Výrobca zariadenia. Umožňuje hromadné pridávanie zariadení do MDM.
- Aktuálny nastavený jazyk.
- Nainštalovaný softvér. Odosiela verziu nainštalovaného softvéru a nastavenia. Umožňuje administrátorom vyžadovať konkrétne nastavenia aplikácií.
- Aktivita. Odosiela na server záznam aktivity z jednotlivých užívateľských profilov.
- Stav siete. Poskytuje serveru aktuálny stav siete, na ktorej je užívateľ pripojený.
- Dátum pridania. Označuje dátum, od ktorého sa zariadenie nachádza pod správou MDM.
- Posledný MDM – klient. Ukladá na server predošlé konfigurácie MDM klientov na zariadení. (32)

2.8 IAM Identity and Access Management

Riadenie prístupu a identity je o definovaní a spravovaní rolí individuálnych sieťových entít, ktoré tvoria užívatelia alebo zariadenia v Cloudoch a lokálnych aplikáciách. Jedným objektom je jedna digitálna identita na jedného užívateľa alebo na jedno zariadenie. V momente, keď je zariadeniu alebo užívateľovi priradená jeho digitálna identita, je s ním spojená počas celého životného cyklu v organizácií.

Na začiatku cyklu je vytvorená identita. Tej je následne pridelená rola, s ktorou vie užívateľ požiadať o prístup. Po schválení prístupov nasleduje autentifikácia a autorizácia účtu. (9, 12, 13, 34)

2.8.1 BYOID Bring Your Own Identity

BYOID je spôsob, kde sa užívateľ hlási do systému identitou poskytnutou treťou stranou. BYOID je často spojovaná s funkcionalitou single sign-on a v tejto kombinácií umožňuje prihlasovanie do viacerých portálov cez jednu identitu. (9)

2.9 Autentifikácia

Autentifikácia je overenie, že daná identita skutočne patrí danému užívateľovi. Pre overenie užívateľov sa používa jednoduché alebo viac faktorové overovanie. Pri jednoduchom overovaní stačí užívateľovi (alebo útočníkovi) poznať heslo. Viac faktorové overovanie zahŕňa v prihlasovacom procese niečo, k čomu má prístup len užívateľ. Viac faktorové overovanie vyžaduje minimálne 2 z nasledujúcich metód autentifikácie:

- Niečo, čo užívateľ vie – Typicky heslo alebo odpoveď na bezpečnostnú otázku.
- Niečo, čo užívateľ vlastní – Typicky dôveryhodné zariadenie, ktoré nie je možné duplikovať (Karta, USB, mobilný telefón, kľúč).
- Niečo, čím užívateľ je – Typicky otlačok prsta alebo biometrický scan sietnice alebo tváre. (9, 10, 11)

2.9.1 RBA – Risk Based Autentication

Risk Based Autentication (RBA) je spôsob autentifikácie, ktorý na základe kontextu prihlasovania vyhodnocuje potrebné kroky pre autentifikáciu užívateľa. Systém zisťuje typ pripojenia, zariadenie z ktorého sa užívateľ prihlasuje, IP z ktorej sa zariadenie prihlasuje a kedy sa užívateľ pokúša k dátam pristupovať. Na základe týchto faktorov systém vyhodnotí, čo všetko je pre autentifikáciu užívateľa potrebné.(9, 12)

2.9.2 SSO Single Sign-on

Princíp jednotného prihlásenia umožňuje prihlásenie sa do viacerých aplikácií pomocou jedného autentifikačného procesu. Užívateľ je tak po prihlásení automaticky prihlásený na všetky služby spojené s poskytovateľom SSO. Microsoft, Facebook či Google poskytujú taktiež Single Sign-off, ktorý znamená, že užívateľ je po odhlásení z jednej aplikácie následne odhlásený zo všetkých (9, 13)

2.10 Autorizácia

Po autentifikácií, ktorá overuje prístup užívateľov nasleduje autorizácia, ktorá určuje, či má daný užívateľ prístup k dátam alebo službe o ktorú žiada. Pokiaľ je užívateľ autorizovaný, je mu následne prístup povolený. Autorizácia môže byť viazaná na kontext z RBA, čo napríklad umožní prístup ku pracovným dátam len počas pracovných hodín. (9)

2.11 Prideľovanie prístupu

Prístup je možné prideliť identite troma spôsobmi.

2.11.1 IBAC - Identity Based Access Control.

Prideľovanie priameho prístupu sa viaže priamo na identitu. Zaniká až so zánikom identity, pričom je stále možné získavať nové prístupy. Tie sa na identite hromadia a časom sa môže stať, že identita má prístupy na miesta, ku ktorým by ich mať už nemala. (19)

2.11.2 RBAC - Role Based Access Control.

Identite je priradená rola, s ktorou sú následne spojené prístupy. Prístupy sa entite nehromadia vzhľadom na ich viazanosť na rolu, dochádza však k riziku duality rolí, poprípade k ich klonom s len drobnými rozdielmi. Tento spôsob prideľovania rolí je momentálne najpoužívanejší.(19, 20)

2.11.3 ABAC - Atribute Based Access Control.

Identite je priradený atribút, na ktorý sa viaže oprávnenie. Tento spôsob je z hľadiska bezpečnosti dát najefektívnejší, nakoľko umožňuje administrátorom pridať časové obmedzenie trvania atribútov. (19)

2.12 Active Directory

Active Directory je hierarchická štruktúra operujúca na princípe klient-server, ktorá uchováva informácie o objektech v sieti. Active Directory obsahuje :

- Schémy, ktoré definujú objekty. Určujú formát mien a maximálne veľkosti objektov
- Globálny katalóg, ktorý obsahuje všetky objekty v databáze
- Indexovací mechanizmus, ktorý umožňuje užívateľom nájsť objekty
- Replikovacie služby, ktoré umožňujú kopírovanie informácií do všetkých doménových kontrolérov na sieti. (16)

2.12.1 Active Directory Domain Service (AD DS)

Uchováva informácie o užívateľských identitách ako sú meno, priezvisko a užívateľské meno. Na základe toho potom páruje identitu s autorizáciou k dátam. Pod AD DS spadajú nasledujúce služby:

- Doménové služby – správa komunikácie medzi užívateľmi a službami
- Certifikačné služby – vytváranie, distribúcia a správa certifikátov
- LDAP – Protokol pre prístup k dátam
- SSO – Single Sign-on / Single Sign-off
- Správa právomocí – ochrana súborov pred neautorizovanými užívateľmi. (16, 17)

2.12.2 Štruktúra Active Directory

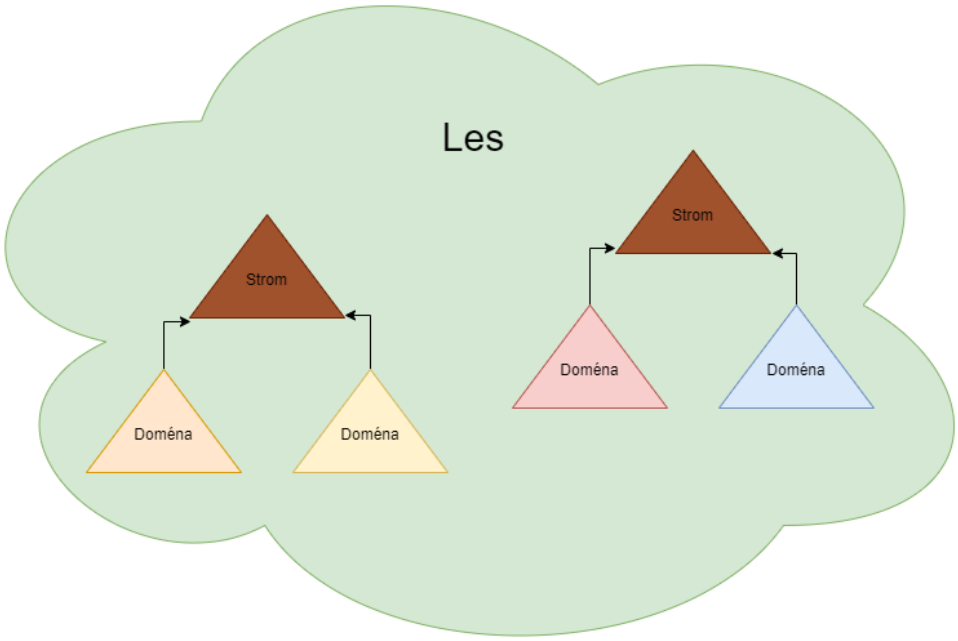
Active Directory je rozdelený na tri úrovne. Úroveň domén, stromov a les.

Doména: Združuje užívateľov využívajúcich rovnaký (spoločný) menný priestor. Doména umožňuje systému duplikovať dáta na miesta, kde sú potrebné. Tento spôsob umožňuje využívanie Active Directory aj na sieťach s obmedzeným prenosovým pásmom.(17, 18)

Organization Unit: Organizačná jednotka je kontajner, ktorý na úrovni domén zoskupuje objekty pre účely administrácie. (17)

Strom: Spojenie domén do hierarchickej, logickej štruktúry v ktorej sú zdieľané informácie o dôveryhodnosti a bezpečnosti pripojenia. (33)

Les: Zoskupenie domén s rovnakou schémou, globálnym katalógom, indexovacím mechanizmom a replikačnými službami. V prípade, že sú domény súčasťou rovnakého lesa, platí pre ne obojsmerné tranzitívne pravidlo o dôveryhodnosti a bezpečnosti pripojenia, tak ako v strome.(33)



Obrázok 3 Logická schéma Active Directory [Zdroj: vlastné spracovanie]

2.13 GDPR

GDPR je právny rámec Európskej únie, ktorý má za úlohu chrániť osobné údaje obyvateľov Európskej únie.

2.13.1 GDPR údaje

Česká legislatíva definuje osobné údaje spadajúce pod GDPR smernicu ako akýkoľvek osobný údaj umožňujúci identifikovať konkrétnu fyzickú osobu. Medzi tieto údaje patria napríklad meno a priezvisko, pohlavie, dátum narodenia, ale aj IP adresa. (21,22)

- Všeobecné údaje – údaje o rasovej alebo etnickej príslušnosti, politických názoroch, vierovyznaní, sexuálnej orientácií alebo zdravotnom stave
- Genetické údaje – medzi tieto údaje spadajú jedinečné genetické znaky fyzických osôb, na základe ktorých je možné danú osobu identifikovať
- Biometrické údaje – údaje vyplývajúce z konkrétneho spracovania fyzických alebo fyziologických údajov o fyzickej osobe, na základe ktorých je danú osobu možné identifikovať. (22)

2.13.2 Čo garantuje GDPR

Európska únia garantuje zaobchádzanie s dátami na základe 6 princípov:

- Princíp zákonnosti, transparentnosti a férovosti
- Princíp spracovania dát obmedzuje, do akej miery môžu byť dáta spracované
- Princíp minimalizácie dát
- Princíp korektnosti
- Princíp časového obmedzenia limituje, ako dlho smie spracovávateľ dáta uchovávať
- Princíp bezpečnosti zaručuje dôveryhodnosť dostupnosť a integritu dát. (3)

3 Analýza

3.1 Popis spoločnosti

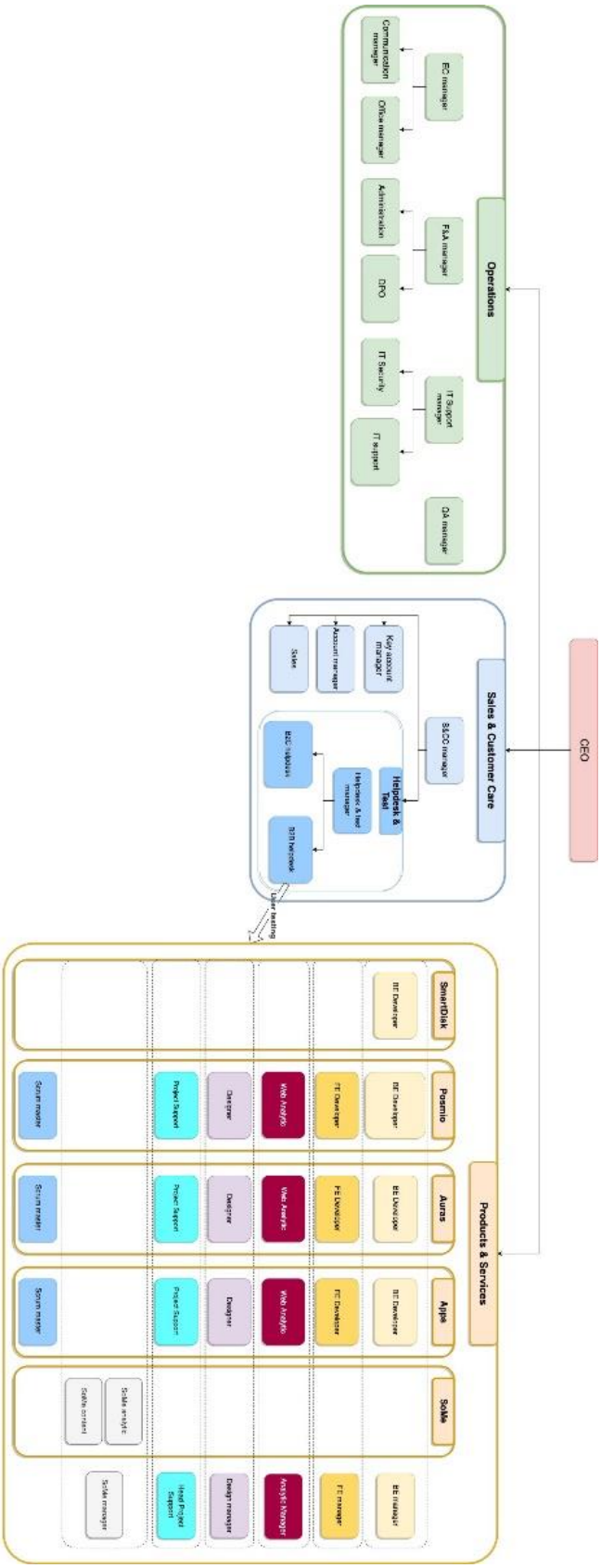
3.1.1 Základné údaje

Firma bola založená v roku 2006 ako marketingová agentúra. Postupne sa pretransformovala z fyzickej reklamy na online a neskôr prešla na vývoj webov. Misia firmy a s ňou spojený hlavný proces je „Spoločne s klientami realizovať ich predstavy v digitálnom svete efektívne, zrozumiteľne a s dlhodobou starostlivosťou.“

3.1.2 Činnosti

Dnes firma vyvíja rôzne webové aplikácie pre klientov ako sú Philip Morris International, Kooperativa alebo McDonald´s. Spravuje web stánky a databázy a zároveň vyvíja vlastný softvér určený na licenčný predaj.

3.1.3 Organizačná štruktúra



Obrázok 4 Organizačná štruktúra [Zdroj: Matěj Kostka]

3.1.3.1 Oddelenia:

- Analytic

Analyzujú firmou spravované weby klientov pomocou Google nástrojov. Jedná sa o proces, ktorý má firma v rámci customer care programu.

- Back End Developer

Vývoj Softvéru podľa inštrukcií projektových manažérov. Upravovanie Softvéru podľa požiadaviek klienta sprostredkovaných projektovým manažérom a oprava chýb na základe podnetov z Helpdesku.

- Designer

Tvorba náročnejšej grafiky pre klientov. Úprava fotiek, tvorba animácií a design reklamných materiálov.

- Front End Developer

Vývoj vizuálnej stránky Softvéru. Tvorba jednoduchej grafiky pre webový front end a G.U.I. Všetko podľa presnej špecifikácie projektového manažéra.

- Helpdesk

Riešenie telefonických a emailových podnetov klientov a ich koncových zákazníkov. Problémy buď riešia priamo oni. V prípade závažnejších problémov sa spíše incident, ktorý preberá konkrétny programátor buď z Front endu alebo z Backendu.

- IT Support

Správa interných serverov, zodpovednosť za dostupnosť intranetu. Správa sieťovej infraštruktúry a zabezpečovanie hladkého chodu firemných zariadení. Vyvíjanie aplikácií pre zlepšenie výkonu oddelenia (evidenčné systémy, mobile device management) .

- Operations

CEO, ekonomické oddelenie, personálne oddelenie, office manažér. Rozhoduje o celkovom smerovaní firmy, prioritizuje požiadavky klientov a má na starosti finančnú stránku firmy.

- Project Manager

Oddelenie sa skladá z projektových manažérov a projekt executives. Manažéri komunikujú s klientom o požiadavkách a predstavách. Starajú sa o deadliny v projektoch a nastavujú priority svojim teamom. Executives plnia priamo drobné požiadavky klientov, ktoré nevyžadujú úpravy od programátorov.

- Sales

Sales sa venuje predovšetkým prieskumu trhu, na základe ktorého s vedením rozhoduje, koho s akým produktom osloviť.

- Customer Care

Zaisťovanie sprostredkovania popredajných služieb klientov. Ak je niečo treba doladiť alebo upraviť na hotovom produkte, klient sa obráti na toto oddelenie.

- Social Media

Tvorenie obsahu a správa profilov na sociálnych sieťach klientov. Všetky druhy blogov a sociálnych médií.

3.2 Spracovávané dáta

3.2.1 Rozdelenie do skupín podľa procesov

Procesy som rozdelil na 4 základné kategórie:

- Hlavné procesy: napĺňajú základné strategické smerovanie organizácie a ich výstupy sú určené externým zákazníkom
- Vedľajšie procesy: sú tiež určené externému zákazníkovi, ale z hľadiska strategického smerovania ich výsledky možno definovať ako vedľajší produkt
- Riadiace procesy: procesy obsahujúce činnosti a aktivity, organizácia reguluje a riadi všetky vnútorné procesy tak, aby ich činnosti zodpovedali strategickým cieľom
- Podporné procesy: vnútorné procesy, ktoré predstavujú jednotlivé funkčné procesy, ktoré sú nevyhnutné pre uskutočňovanie hlavných procesov

Z toho vyplýva nasledovné delenie:

- Hlavné procesy: tvorba reklamných materiálov, vyvíjanie softwaru
- Vedľajšie procesy: updatovanie softwaru, komunikácia so zákazníkom, správa sociálnych sietí, helpdesk, analýza webov, organizovanie stretnutí s klientami, prijímanie podnetov od klientov.
- Riadiace procesy: najímanie zamestnancov, prioritizácia procesov, schvaľovanie projektov, riadenie projektov, personalistika, rozpočet, schvaľovanie financií
- Podporné procesy: Správa interných serverov, udržovanie sieťovej infraštruktúry, revízia zariadení, teamové meetingy, prieskum trhu, výber klientov, správa databázy

3.2.2 Rozdelenie do skupín podľa typu dát

Dáta z hľadiska ich obsahu delíme na tieto kategórie:

- strategické dokumenty firmy: Plány do budúcnosti, obchodné stratégie, kontakty
- vnútorné dokumenty: Smernice, know-how, poznámky z meetingov, návody, audity, zálohy
- obchodné dáta: Požiadavky klientov, ceny, prieskum trhu, riešené tickety, hovory, spracované GDPR dáta od klientov
- vyvíjaný Softvér: Kód, grafika, dokumentácia
- Databázy: Interné evidenčné systémy
- Účtovníctvo: Faktúry za nákupy, výplaty zamestnancov, rozpočet,
- Personalistika: Dáta zamestnancov spadajúce pod GDPR
- Logy

Pre všetky dáta je určená kritickosť. Tá je rozdelená na 5 stupňov, pričom pre každý ďalší stupeň platia predošlé.

1. Strata alebo zverejnenie nie je pre firmu problém
2. Strata alebo zverejnenie môže viesť k sankciám pre firmu
3. Strata alebo zverejnenie môže znamenať ukončenie pracovného pomeru
4. Strata alebo zverejnenie je nahlásené ako bezpečnostný incident na NUKIB
5. Strata alebo zverejnenie sú pre firmu likvidačné

Kritickosť dát je určená v tabuľke číslo 1 až 3 v poslednom stĺpci.

Tabuľka 1 Tabuľka dát Strategické a Vnútorné dokumenty [Zdroj: vlastné spracovanie]

	Typ Dát	Data Creator	Data User	Data owner	Data Supervisor	Data Spectator	K
Strategické dokumenty firmy:	Plány do budúcnosti	CEO + Customer care	Sales, Operations, Customer Care	CEO	CEO	Managers	4
	Obchodné stratégie	Sales + customer care	Operations, sales , project managers	Operations	CEO		4
	Kontakty	CEO	Managers	Operations	CEO		5
Vnútorné dokumenty:	Smernice	IT Support	Operations	IT-Support	IT-Support	Všetci	1
	Know-how	Všetci	Všetci	Managers	Managers		2
	Poznámky z meetingov	Project managers	Všetci	Project managers	Project managers	Teamy	2
	návody	IT-Support	IT-Support	IT-Support	IT-Support	Operations	2
	audity	IT-Support	Operations	Operations	IT-Support	Operations	4
	zálohy	Všetci		IT-Support	IT-Support	IT-Support	5

Tabuľka 2 Tabuľka dát Účtovníctvo, Personál a Logy [Zdroj: vlastné spracovanie]

	Typ Dát	Data Creator	Data User	Data owner	Data Supervisor	Data Spectator	K
Účtovníctvo:	Faktúry za nákupy		Ekonomické	CEO	IT-Support	Externá firma	4
	Výplaty zamestnancov	Ekonomické	Ekonomické	Ekonomické	CEO	Personálne oddelenie	5
	Rozpočet	Operations	Managers	Operations	Operations		4
Personál:	Dáta zamestnancov	Personálne oddelenie	Operations	Operations	IT-Support	Managers	5
Logy:	Celofiremné logy	IT-Support	IT-Support	IT-Support	IT-Support	IT-Support	4

Tabuľka 3 Tabuľka dát Obchodné dáta, Vyvíjaný softvér a Databázy [Zdroj: vlastné spracovanie]

	Typ Dát	Data Creator	Data User	Data owner	Data Supervisor	Data Spectator	K
Obchodné dáta:	Požiadavky klientov		Project Managers	Operations	Project Managers	Teamy	4
	Ceny	Operations + Customer care		Operations			3
	Prieskum trhu	Sales	Project Managers	CEO	Sales	Managers	2
	Riešené tickety	Helpdesk	Back end + Front end developers	Helpdesk	Customer care	Všetci	4
	Spracované GDPR dáta od klientov	Klient	Helpdesk, Project Managers	Klient	Helpdesk, Project Managers		5
	Hovory	Helpdesk	Customer care	Customer care	Helpdesk	Operations, Customer care	4
Vyvíjaný Softvér:	Návody	Back End	Front End developers	CEO	Project Managers	Teamy	3
	Audity	Designer	Everyone	CEO		Všetci	3
	Zálohy	Back End + Front End developers	Project Managers			Všetci	3
Databázy	Interné evidenčné systémy	IT-Support	IT-Support	IT-Support	IT-Support	Operations + Managers	5

3.2.3 Systém pre spracovanie a ukladanie dát pre skupiny

Na spracovávanie a ukladanie dát z procesov sa používajú ERP, CRM, MySQL, centralizované intranetové databázy a aj samostatné ukladanie súborov na lokálnom úložisku alebo cloude. Často sa pri tom stáva, že procesy putujú cez viaceré úložiská počas ich spracovania a nechávajú po sebe redundantné dáta.

Dáta v rámci hlavných procesov začínajú spracovaním v ERP, kde klient definuje požiadavky. Odtiaľ je rozdelená práca, ktorá sa ďalej zapisuje do intranetovej databázy. Medzikroky sa ukladajú vo forme samostatných súborov na počítače vlastníkov súborov. Tu pri zálohách vznikajú duplicity. Dokončené produkty končia na serveroch klientov.

Vedľajšie procesy sa od hlavných líšia tým, že väčšina dát z procesov vzniká a končí na tom istom type úložiska. Ak proces začne v CRM, po celý čas sú medzikroky uložené len v ňom. Pre ERP a Cloud platí, že medzikroky sa ukladajú lokálne na počítačoch zamestnancov ale výsledok samotného procesu je ako celok uložený na ERP alebo Cloude.

Dáta z riadiacich procesov vznikajú na počítačoch zamestnancov, a cez distribučné kanály končia buď v ERP alebo cloudoch. Dáta sú extrémne citlivé a vzniknuté duplicity počas spracovania sú potencionálne nebezpečné.

Podporné procesy za sebou zanechávajú logy, ktoré sú roztrúsene naprieč úložiskami.

3.3 Fyzické uloženie dát

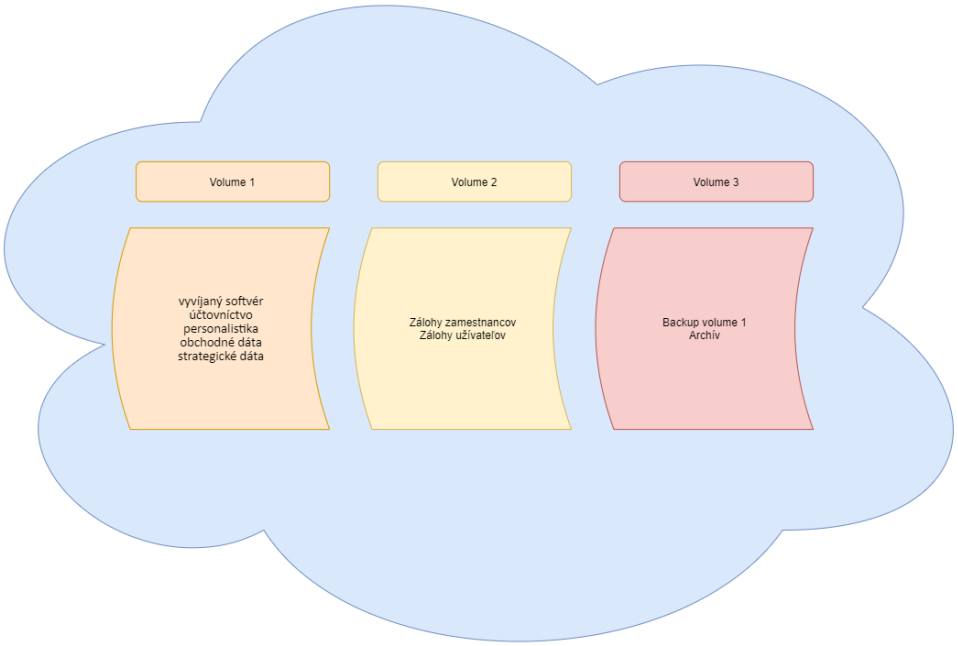
Systém samotného ukladania je chaotický, nakoľko sa dáta nachádzajú duplicitne na viacerých miestach. Nejedná sa však o zálohy, ale len o neporiadok v súboroch, ktoré vznikli verziovaním. Firma používa kombináciu ERP, CRM, SQL, intranetové databázy a aj samostatné ukladanie súborov na úložisku.

Ako ERP sa používa Targetprocess, ktorý má funkciu vkladania poznámok, do ktorých užívatelia často vkladajú dôležité informácie taktiež umožňuje spracovanie dát. Využívajú ho všetky štyri skupiny procesov. Ukladajú sa sem strategické dokumenty, obchodné dáta a vnútorné dokumenty.

CRM Salesforce je nástroj v ktorom sa dáta spracovávajú a zároveň aj ukladajú. Tento spôsob je využívaný len pri vedľajších procesoch a ukladajú sa sem obchodné dáta.

SQL spracováva a ukladá databázy pri podporných procesoch.

Intranetová databáza slúži pre riadiace a podporné procesy v organizácií a funguje na LDAP protokole. Je rozdelená na 3 časti.



Obrázok 5 Rozdelenie partícií na NAS [Zdroj: vlastné spracovanie]

Prvá časť je určená na dáta z riadiacich a podporných procesov. V druhej sú zálohy počítačov zamestnancov vo firme a zálohy bývalých zamestnancov (Užívateľov) . V tých sa nachádzajú všetky druhy dát z procesov. Záloha je inkrementálna, preto nevzniká až toľko redundantných dát. Nevýhodou je nutnosť častej kontroly pre náchylnosť na nekonzistentnosť dát. V tretej časti sú zálohy celej prvej časti (Backup) a Archív.

Samostatné ukladanie súborov na úložiská bez logickej hierarchie je časté a platí pre dáta zo všetkých štyroch skupín procesov a taktiež pre všetky typy dát. Používajú sa pri tom lokálne úložiská firemných počítačov ale aj cloudové riešenia od firmy Microsoft, Apple a Google. Týmto spôsobom končia dáta aj v centrálnej intranetovej databáze. Dáta uložené u týchto subdodávateľov sa nachádzajú na serveroch Európskeho hospodárskeho spoločenstva ktoré spĺňajú GDPR regulácie.

Jediné, čo sa udržuje v papierovej forme sú zmluvy, účtovné doklady a GDPR regulované dokumenty od zamestnancov. Tieto sú po doručení naskenované a uložené do centrálnej intranetovej databázy, ale odkladá sa aj fyzická kópia pre prípadné kontroly. Firma nemá jasne definovanú skartovaciu politiku. Keďže firma používa elektronický podpis, netreba tlačiť faktúry.

3.4 Užívatelia

3.4.1 Rozdelenie na skupiny

Vo firme sú ľudia rozdelení do teamov, kde každý team robí na inom projekte. Túto skupinu budeme definovať ako Team. Toto rozdelenie je chaotické, lebo ľudia môžu byť aj vo viacerých teamoch naraz. Preto pridáme rozdelenie na oddelenia z úvodu analýzy. Existujú skupiny súborov, kde sú zahrnuté všetky oddelenia, a preto sa v analýze nachádza atribút Everyone. Ďalej si pre každý typ dát musíme prideliť rolu.

- Data Creator: vytvára dáta pri procesoch, ale nenesie za ne zodpovednosť.
- Data User: ďalej spracováva originálne dáta v iných procesoch.
- Data Owner: vlastní dáta vytvorené procesmi a zodpovedá za prideľovanie práv.
- Data Supervisor: nesie zodpovednosť za integritu a dostupnosť dát pre ownerom oprávnených užívateľov.
- Data Spectator: dáta vie zobraziť, ale nemá povolené úpravy.

3.4.2 K akým skupinám dát majú užívatelia prístup

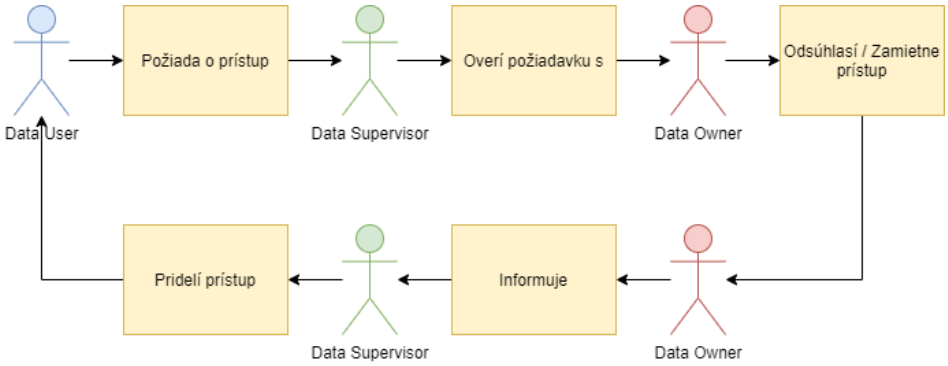
Procesy vytvárajú dáta, zameriavame sa na typ dát. Delenie sa nachádza v kapitole 3.2.2, kde platí, že ak nie je políčko vyplnené nevieme jednoznačne dohľadať ani vymedziť skupinu užívateľov. Tento problém nastáva pohybom ľudí medzi oddeleniami a teamami, pričom pri zmene teamu alebo oddelenia nie vždy data owner kontroluje prístupy.

3.4.3 Prideľovanie prístupov k dátam

Prideľovanie prístupu k dátam je znázornené na nasledujúcich grafoch. Rola Data User a Data Spectator je v tomto prípade rovnaká z pohľadu žiadosti o prístup k dátam, pričom rozdiel je len druhu prístupu (Data User = Read/Write, Data Spectator = Read Only). Prístupy zanikajú až po ukončení pracovného pomeru so zamestnancom, alebo po pridelení zdieľaného účtu inému zamestnancovi.

Pridelenie prístupu	Procesné kroky				
R - Responsible A - Accountable C - Consulted I - Informed	Požiadanie	Kontaktovanie Data Ownera	Rozhodnutie o pridelení prístupov	Zabezpečenie prístupov	Aktualizovanie prístupov
Data Creator					
Data User / Data Spectator	A/R			I	
Data Supervisor	C	A/R	I	A/R	C
Data Owner		I	A/R	C	A/R
Výstup procesu	User/ Spectator požiada Supervisora o prístup	Data Owner je informovaný o požiadavke	Data Owner rozhodne, či treba prístup prideliť	Userovi/ Spectatorovi boli udelené prístupy	Data Owner má prehľad, kto má k dátam aktuálne prístup

Obrázok 6 RACI prideľovania prístupu k dátam [Zdroj: vlastné spracovanie]



Obrázok 7 Cyklus požiadavky medzi ľuďmi [Zdroj: vlastné spracovanie]

3.4.4 Spôsob autentifikácie užívateľov

Užívatelia sa do systému prihlasujú pomocou protokolu LDAP, ktorý beží na internom serveri. Na prihlásenie sa používa iba užívateľské meno a heslo (jednofaktorové overovanie). Vďaka tomuto protokolu majú užívatelia garantovaný prístup do intranetu a na NAS úložisko cez hlavnú internú sieť. LDAP umožňuje front end a back end developerom prístup do GitHubu a SQL. Užívateľom je pri zakladaní zložiek na internom NAS úložisku nastavený prístup a to buď read/write, read only alebo zložku vôbec nevidia.

Ďalší spôsob autentifikácie je prístup cez Office 365. Klienti firmy používajú Guest funkcie nastavenia Microsoft účtov na prideľovanie prístupov do ich interných programov. Každý zamestnanec má svoje vlastné Office 365 konto a k nemu priradenú licenciu a to „Business Basic“ alebo „Business Standard“. Základná licencia slúži na prístup do Cloudu a do mailovej schránky spravovanej cez Exchange server na strane Microsoftu. Štandardná licencia je prideľovaná zamestnancom, ktorí na dennej báze používajú okrem nástrojov Outlook a Teams aj prémiový balík Office 365. Pre zdieľané / dočasné prístupy sa využíva možnosť vytvorenia zdieľanej emailovej schránky, takzvaného shared – mailboxu, ktorý sa napáruje na originálny účet zamestnancov.

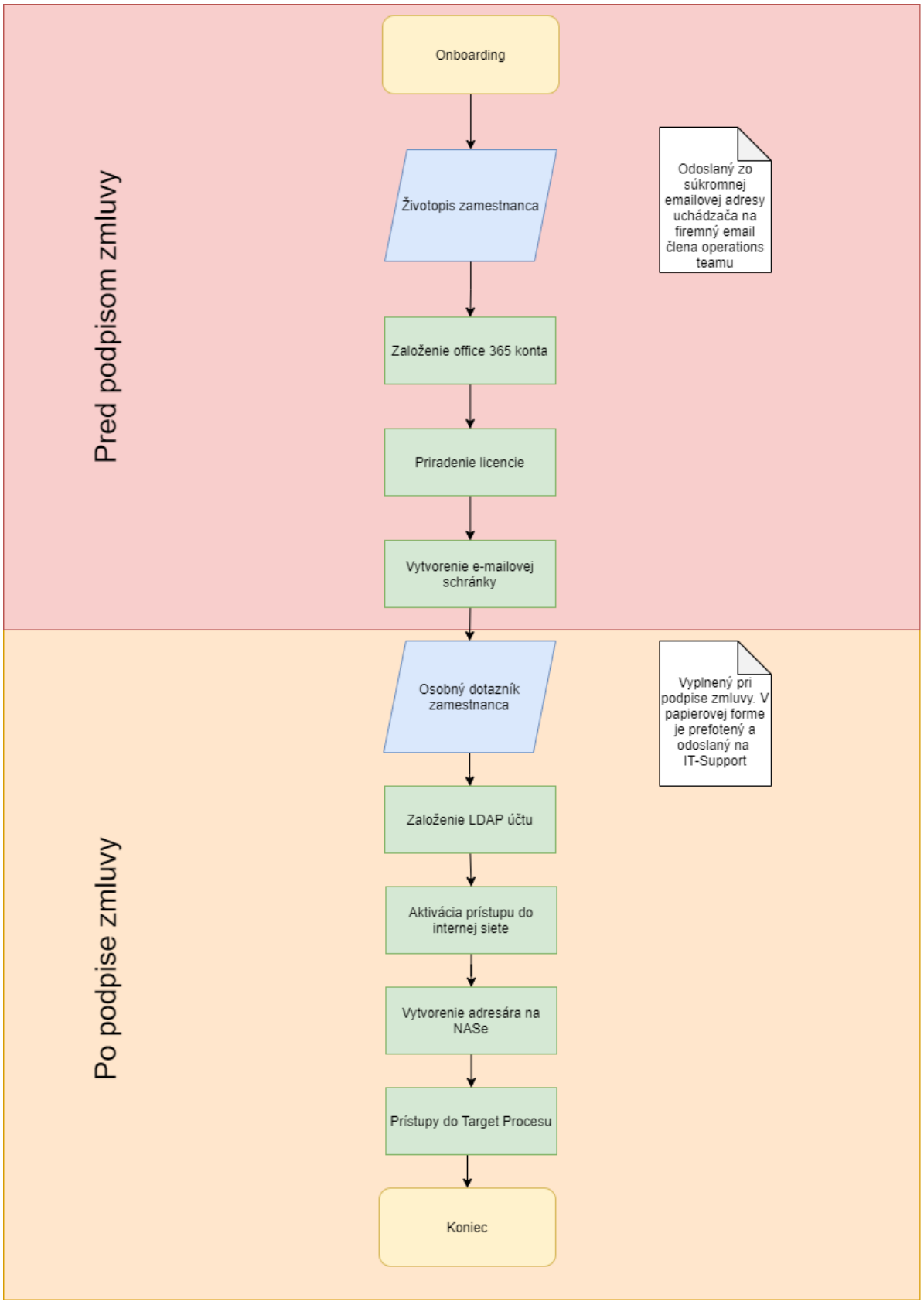
ERP má samostatnú autentifikáciu. CRM má samostatnú autentifikáciu spravovanú treťou stranou.

3.4.5 Onboarding

Proces, pri ktorom sa z uchádzača stáva zamestnanec a vytvára sa mu identita a základné prístupy potrebné na prácu. Tieto prístupy má každý zamestnanec bez ohľadu na jeho pozíciu vo firme. Cieľom je, aby mal zamestnanec v deň nástupu všetko nachystané, a od pracovníka IT-Supportu len prebral notebook.

OnBoarding	Procesné kroky								
R - Responsible A - Accountable C - Consulted I - Informed	Odoslanie životopisu	Založenie Office 365 Konta	Pridelenie licencie	Vytvorenie e-mailovej schránky	Odoslanie osobného dotazníku zamestnanca	Založenie LDAP účtu	Aktivácia prístupu do internej siete	Vytvorenie adresára na NASe	Prístupy do Target Procesu
Operations	R		I		A/R	C			C
Manažér uchádzača	A	I	C	I		I	I	C	I
IT-Support	I	A/R	A/R	A/R	I	A/R	A/R	A/R	A/R
Uchádzač	C				C			I	
Výstup procesu	Pracovník IT-Supportu dostane životopis uchádzača	Uchádzač má Office 365 autentifikáciu	Pridelenie licencie na základe pracovnej náplne	Uchádzačovi môžu byť odoslané prihlasovacie údaje	IT pracovník dostane údaje pod ochranou GDPR	Zamestnanec získa LDAP autentifikáciu	Zamestnanec sa dostane na intranet	Zamestnanec získava vlastný adresár	Zamestnanec môže dostávať pracovné úlohy

Obrázok 8 RACI Onboarding [Zdroj: vlastné spracovanie]



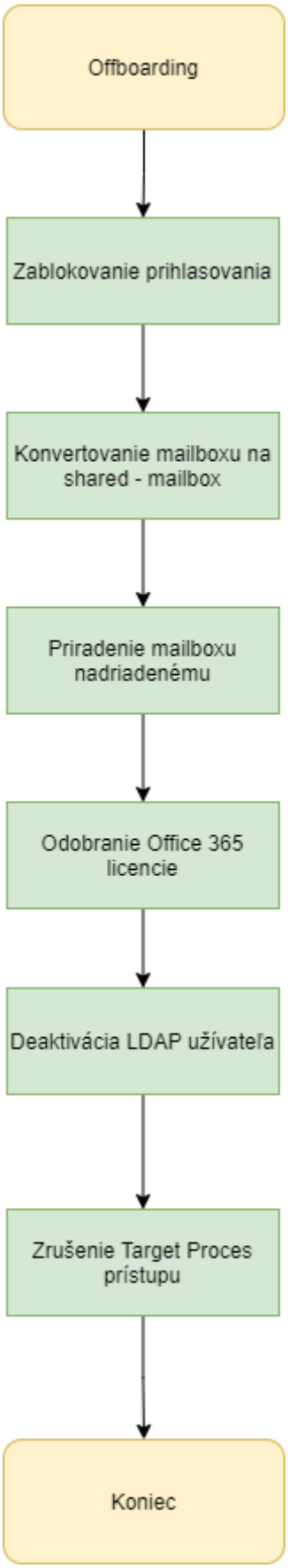
Obrázok 9 Postup Onboardingu [Zdroj: vlastné spracovanie]

3.4.6 Offboarding

Proces ktorý nastáva po ukončení pracovného pomeru so zamestnancom. Pri odovzdaní pracovného notebooku sa ešte stále zamestnancovi odoberú prístupy, ktoré mu boli onboardingom pridelené. Výstupom tohto procesu je zablokovanie prístupov zamestnanca a ponechanie jeho identity. Offboarding je vykonávaný pracovníkmi IT- Supportu vždy v posledný deň výpovednej lehoty zamestnanca.

OffBoarding	Procesné kroky					
R - Responsible A - Accountable C - Consulted I - Informed	Oznámenie ukončenia pracovného pomeru	Zablokovanie prihlasovania do Office 365 Konta	Konvertovanie mailboxu na shared-mailbox	Odobratie licencie	Zablokovanie užívateľa v LDAP	Zrušenie prístupu do Target procesu
Operations	R		I			I
Manažér zamestnanca	A		C		I	
IT-Support	I	A/R	A/R	A/R	A/R	A/R
Zamestnanec	C					
Výstup procesu	Pracovník IT-Supportu je informovaný o offboardingu	Zamestnanec nemôže používať Office konto na autentifikáciu	Emailová schránka je priradená nadriadenému zamestnanca	Zo zamestnanca sa stáva nelicencovaný užívateľ	Užívateľ je zablokovaný, ale naďalej zostáva v systéme	Užívateľ sa nevie prihlásiť a jeho profil zostáva archivovaný

Obrázok 10 RACI Offboarding [Zdroj: vlastné spracovanie]



Obrázok 11 Postup Offboardingu [Zdroj: vlastné spracovanie]

3.5 Požiadavky vedenia

Vedenie chce mať väčší prehľad o tom, kto má prístup k dátam, kto mu ho udelil a kto dáta reálne upravoval. Od kedy do kedy sú dáta u danej osoby a ak dáta uniknú či už v rámci firmy alebo von, dohľadať pôvodcu úniku.

Možnosť vymazať firemné dáta na diaľku z počítačov zamestnancov bez ich súhlasu na pokyn CEO, pričom prevedenie má byť neinvazívnou metódou, aby zamestnanci nemali pocit, že sú neustále pod dohľadom.

Zjednodušenie autentifikácie na jednu platformu, ktorá zároveň umožňuje ľahké prideľovanie licencií.

Zjednodušenie komunikačnej kaskády pri prideľovaní prístupov.

Možnosť spravovať a blokovať počítače na diaľku pri prípadnom odcudzení alebo pre prípady Homeofficu.

3.6 Vyhodnotenie analýzy

Firma spracováva dáta v CRM Salesforce a v ERP programe Target process. Dáta sú ukladané lokálne, v centrálnej intranetovej databáze ale aj vo verejnom Cloude. Externé úložné médiá sú regulované vnútrofiremnými smernicami, preto ich pri návrhu riešenia netreba brať do úvahy. Firma má dostatočnú sieťovú vybavenosť vďaka ktorej je zabezpečená dostupnosť dokumentov prístupných pomocou internetu. Do toho spadá LAN Cat.6, Wifi s pásmom 5G a redundantná optická sieť.

Na autentifikáciu firma využíva viacero metód bez možnosti SSO alebo BYOID, pričom každá vyžaduje samostatné unikátne heslo. Firma produkuje veľké množstvo dát, pričom sú tieto dáta zdieľané medzi oddeleniami a teamami bez logickej štruktúry.

Autorizácia je viazaná na identitu. Je s ňou spojená až do doby, kým ju na vyžiadanie nadriadeného pracovník IT-Supportu nezruší. V prípade odchodu zamestnanca z firmy identita nezaniká, čo znamená, že prístupy zostávajú. Aktuálny Identity Based Access Control je pri aktuálnom počte zamestnancov neudržateľný.

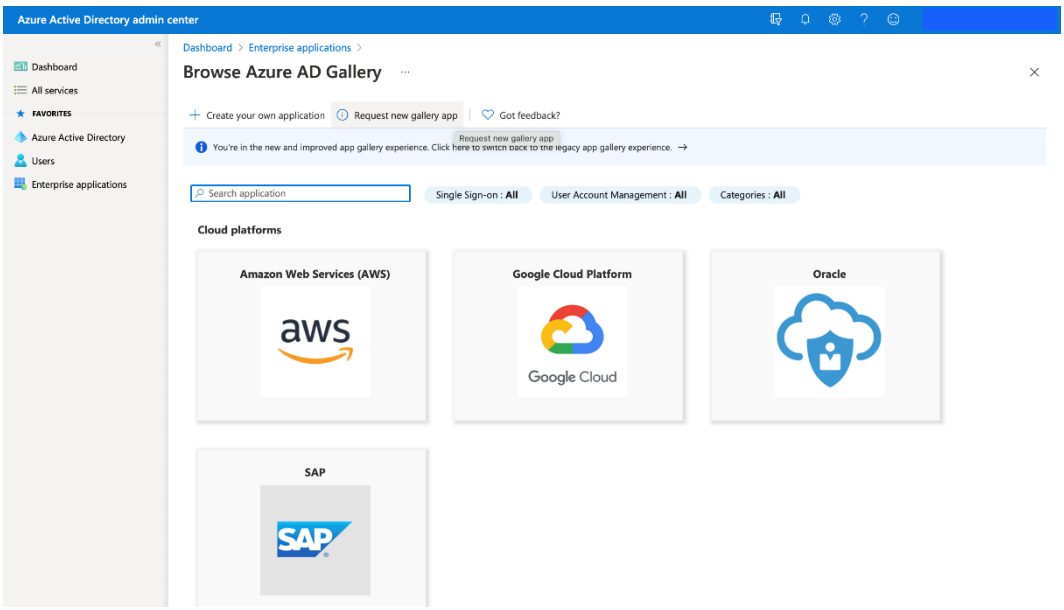
Pre zdieľanie dát medzi firmou a klientom sa používa veľké množstvo komunikačných kanálov, pričom sú často odosielané aj údaje spadajúce pod GDPR regulácie. Dáta sú zdieľané často redundantne cez ERP, CRM a cloud. Firma momentálne využíva verejný cloud, na ktorom má každý zamestnanec vyhradený úložný priestor spojený s jeho identitou. Nevýhodou tohto riešenia je absencia dohľadu nad tokmi dát užívateľov.

4 Navrhované riešenia

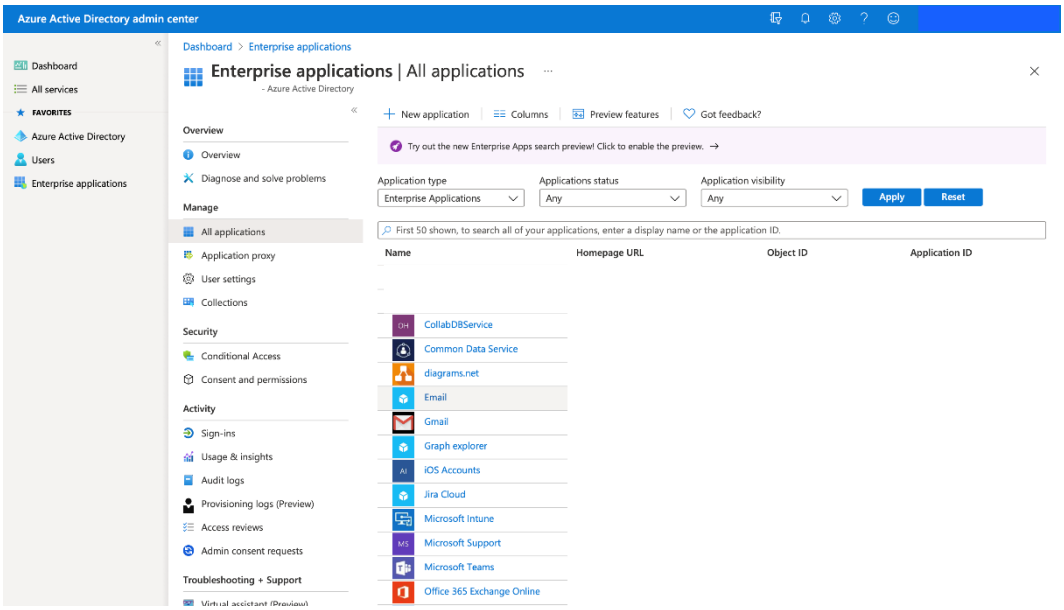
Na základe analýzy sa budú navrhované riešenia deliť na tri oblasti. Prvou bude zmena autentifikácie zamestnancov integrovaním SSO, druhou bude zmena spôsobu autorizácie na kombináciu RBAC a ABAC a treťou zmena spôsobu uchovávania dát vo firme prechodom na hybridný Cloud.

4.1 Zmena spôsobu autentifikácie

Zmena spôsobu autentifikácie prinesie menšiu potrebu pamätania hesiel a prístupových údajov na strane zamestnancov a lepšiu kontrolu na strane IT - Supportu. Keďže z analýzy je možné vidieť, že aj klienti firmy používajú Microsoft na autentifikáciu, bude jeho implementácia potrebná aj tu. Na autentifikáciu navrhujem využívať nástroj Active Directory, ktorý podporuje SSO a umožňuje autentifikuje užívateľa na základe jeho prihlasovacích údajov do služby Microsoft Office 365. Pridelenie autentifikácie pre aplikácie 3. strán ako napríklad ERP alebo CRM je priamo v administrácií. V prípade použitia Active Directory na interné prístupy je možnosť implementácie API.

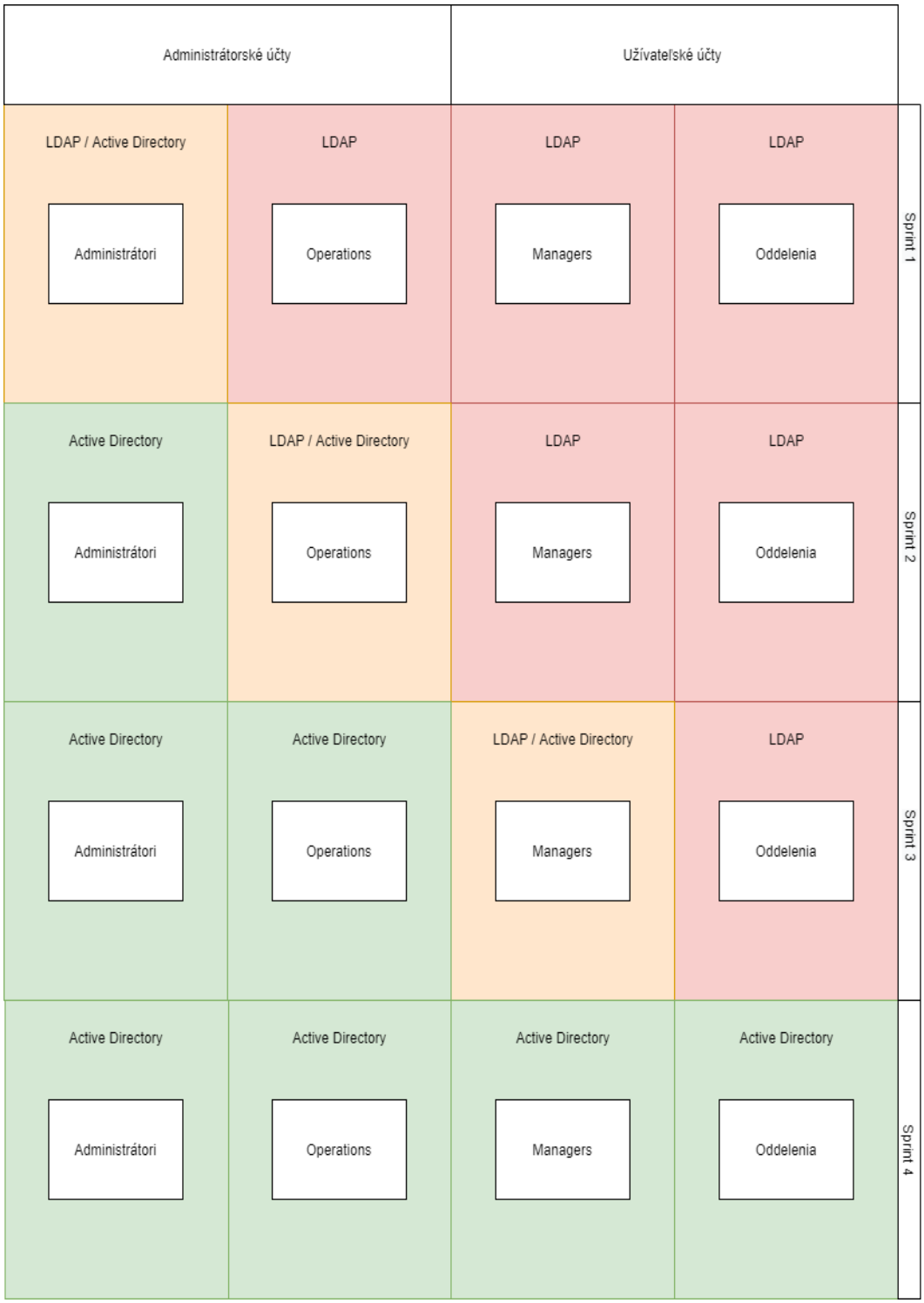


Obrázok 12 Pridávanie aplikácií na Office365 autentifikáciu [Zdroj: vlastné spracovanie]



Obrázok 13 Prehľad aplikácií, kde je autentifikácia Office365 [Zdroj: vlastné spracovanie]

Implementácia bude rozdelená na dve fázy. V prvej je potrebné umožniť aplikáciám komunikáciu s Azure Active Directory. Väčšina aplikácií používaná firmou na spracovanie a prenos dát sa už nachádza v zozname podporovaných aplikácií. Pre tie bez podpory bude potrebné implementovať API. Táto fáza pri aktívnom prístupe zaberie obdobie jedného sprisntu (dva týždne). Potom nasleduje druhá fáza, fáza migrácie užívateľov. Táto fáza bude rozdelená na štyri etapy trvajúce každá v období jedného sprintu (dokopy osem týždňov), aby prípadné problémy nenarušili projekty. Administrátorské účty budú mať počas testovania možnosť prihlasovania cez oba typy autentifikácií. Po úspešnom otestovaní sa zmení spôsob autentifikácie pre užívateľské účty pričom sa bude jednať o manažérov oddelení. Tento krok je potrebný aby si užívatelia zvykli a nahlásili chyby. Poslednou etapou je kompletný prechod na Active Directory. Podpora v tomto prípade vychádza z postupnej migrácie užívateľov, pričom užívatelia z predošlého sprintu budú podporou pre práve aktívny sprint. Pri aktívnom prístupe všetkých zúčastnených strán, je možné zmeniť spôsob autentifikácie za jeden kvartál.



Obrázok 14 Časový plán implementácie zmeny autentifikácie [Zdroj: vlastné spracovanie]

4.2 Zmena spôsobu autorizácie

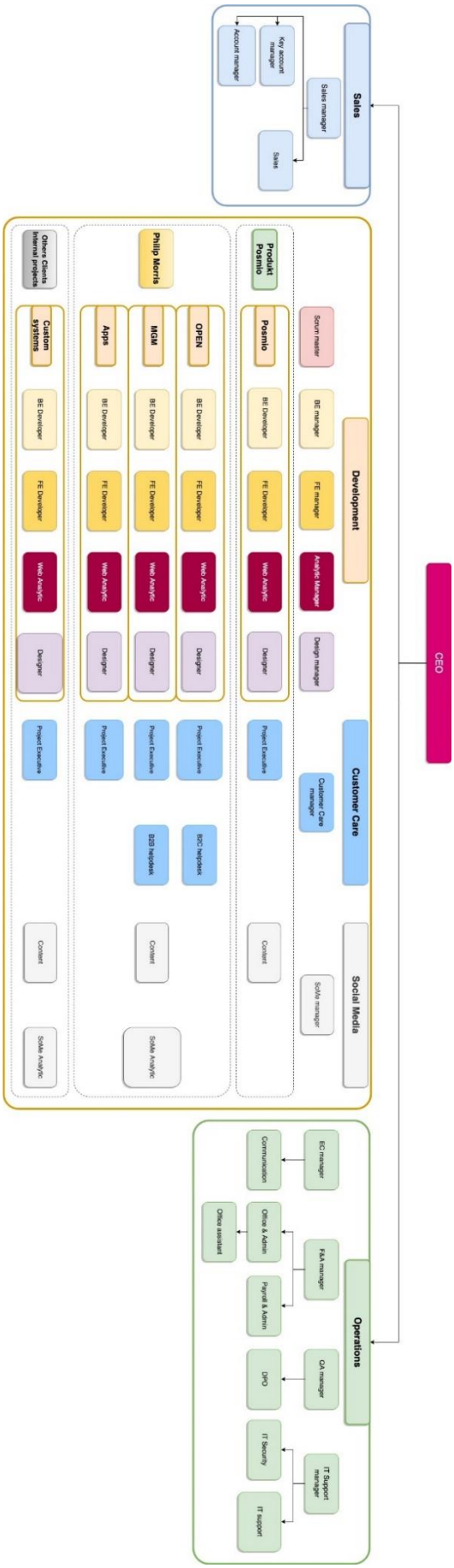
Pre jasné určenie, kto má kam prístup a kto môže o ktorý prístup žiadať, je potrebné lepšie nastaviť organizačnú štruktúru, aby zodpovedala oddeleniam a teamom. Následne na základe organizačnej štruktúry vytvoriť nový spôsob autorizácie prístupu k dátam, na základe ktorého budú neskôr upravené smernice. Nakoniec je potrebné implementovať MDM pre lepšiu správu autentifikácie a ochranu dát .

4.2.1 Úprava organizačnej štruktúry

Nová štruktúra lepšie znázorní rozdelenia na produkčné teamy, ktoré sa ďalej delia na jednotlivé projekty. Zároveň znázorňuje oddelenia, ktoré sa v produkčných teamoch nachádzajú. Na základe Tabuľky č.1-3 je určené, ktoré oddelenia vytvárajú aké dáta, a preto je možné určiť aké dáta tvoria a spracovávajú jednotlivé projekty.

Prerušovanou čiarou sú znázornené projektové teamy. V nich oranžovou oddelenia, zodpovedné za vývoj a za nimi mimo označenia oddelenia, ktoré sa starajú o podporu projektov.

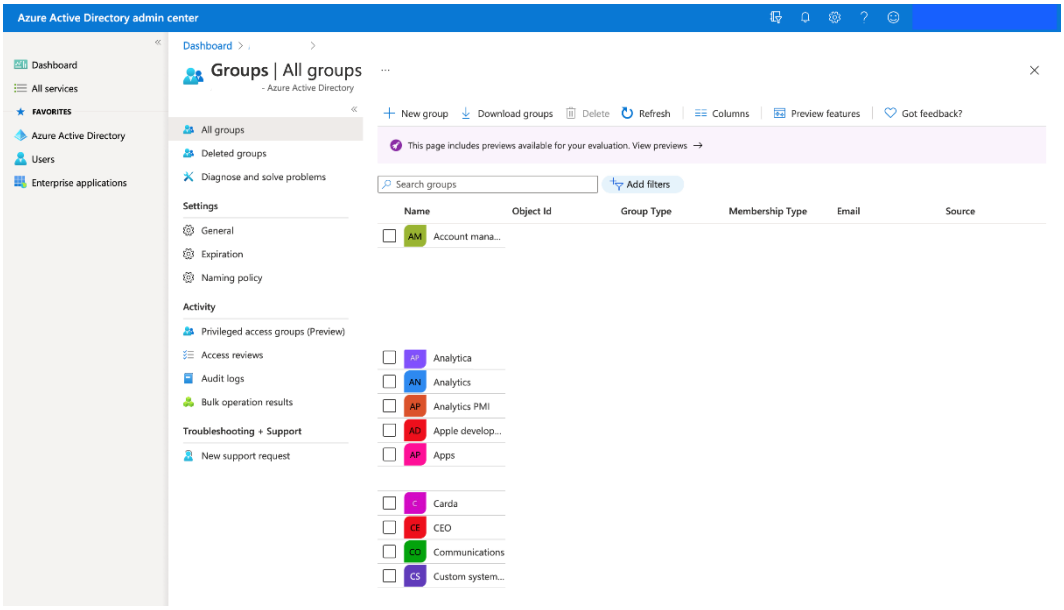
Na rozdiel od predošlej štruktúry sa CEO priamo zodpovedajú len Operations a Sales, čím odpadla nutnosť potreby konzultovať pridelenie prístupov k produkčným dátam.



Obrázok 15 Návrh organizačnej štruktúri [Zdroj: Matěj Kostka]

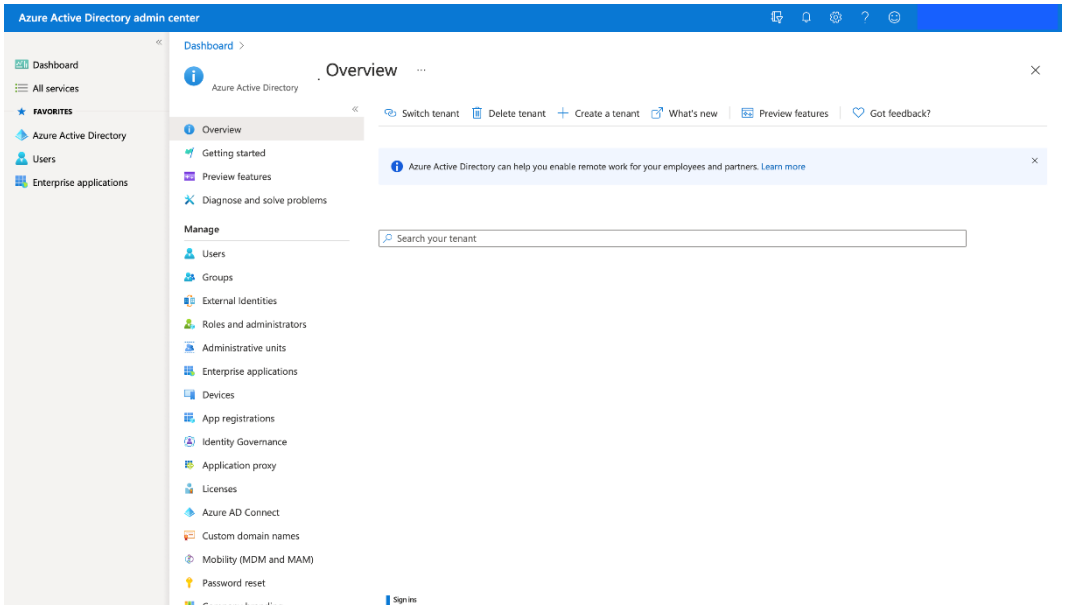
4.2.2 Nový spôsob prideľovania prístupu k dátam

Po implementácií Azure Active Directory a úprave organizačnej štruktúry vie administrátor rozdeľovať užívateľov na skupiny podľa teamov - ABAC a oddelení - RBAC. Daným skupinám vie ďalej automaticky prideliť prístup už pri Onboardingu.



Obrázok 16 Návrh skupín Azure Active Directory [Zdroj: vlastné spracovanie]

Na stránke Overview bude administrátor vidieť prehľad prihlasovania užívateľov.



Obrázok 17 Overview užívateľov Azure Active Directory [Zdroj: vlastné spracovanie]

Vďaka novej štruktúre vieme rozdeľovať dva hlavné druhy prístupov.

Interné dáta - medzi ktoré radíme strategické dokumenty firmy, vnútorné dokumenty, účtovníctvo a personalistiku

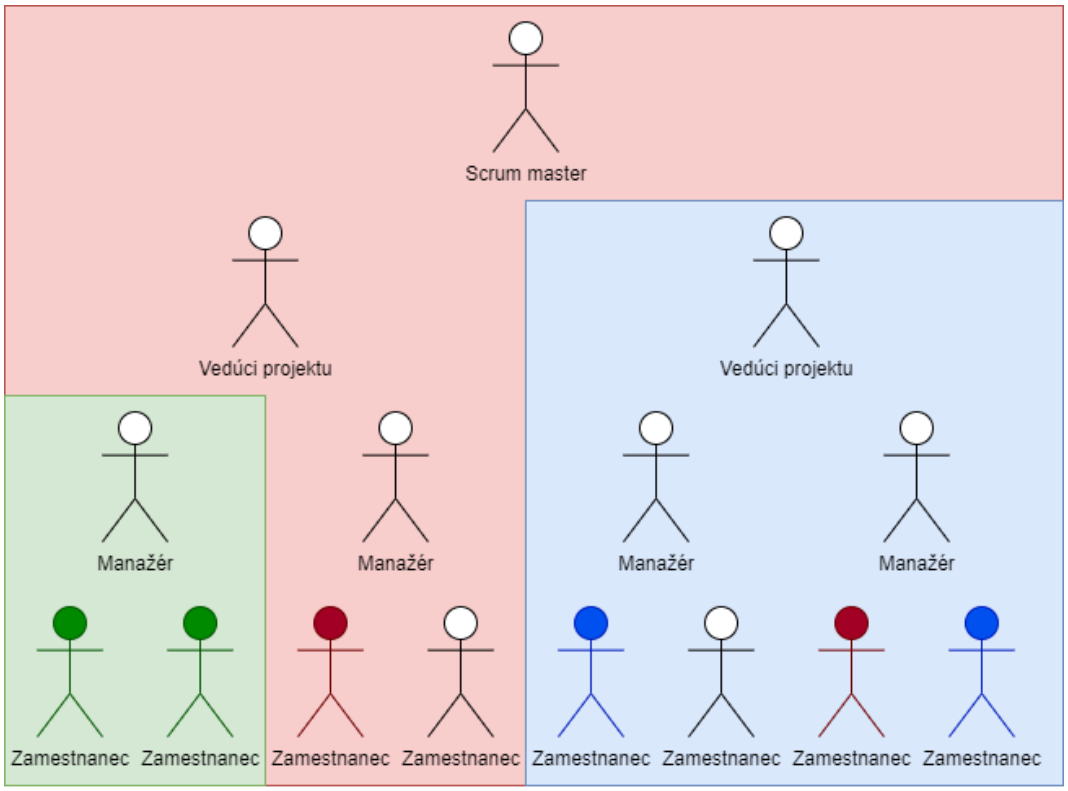
Produkčné dáta - pod ktoré spadajú obchodné dáta, vyvíjaný softvér, databázy a logy. Tie sú zdieľané medzi produkčnými teamami na rôznych úrovniach.

Pre interné dáta je automaticky Data owner a Data supervisor CEO, ktorý rozhoduje, komu budú prístupy pridelené. Pre tento prípad má RACI matica len troch aktérov a to CEO v roli Data Owner/ Data Supervisor, zamestnanca čo o prístup žiada v roli Data User/ Data Spectator a zamestnanca, ktorý dáta aktuálne vytvára alebo s nimi aktuálne pracuje v roli Data Creator/ Data User.

Pridelenie prístupu pre Interné dáta	Procesné kroky				
R - Responsible A - Accountable C - Consulted I - Informed	Požiadanie	Rozhodnutie o udelení prístupu	Úprava dát	Sprístupnenie dát	Overenie prístupu
Data Creator / Data User	C	C	A/R		
Data User / Data Spectator	A/R	I	I	I	A/R
Data Supervisor / Data Owner	I	A/R	C	A/R	I
Výstup procesu	Zamestnanec požiada o prístup	CEO rozhodne, či je prístup pridelený	Podľa dohody CEO a zamestnanca sú dáta upravené	Finálne udelenie prístupov ku dátam v dohodnutej forme	Zamestnanec potvrdí, či má prístup tak, ako bolo pôvodne dohodnuté

Obrázok 18 RACI interné dáta [Zdroj: vlastné spracovanie]

Pre produkčné dáta ďalej rozlišujeme 3 úrovne prístupov.



Obrázok 19 Typy prístupu pri produkčných dátach [Zdroj: vlastné spracovanie]

Zelenou farbou je znázornený prístup v rámci rovnakého projektu a v rámci rovnakého oddelenia. Rieši situácie, v ktorých si medzi sebou zamestnanci rozdeľujú prácu pre rýchlejšie spracovanie dát. Na tejto úrovni sú v RACI matici štyria aktéri a to manažér oddelenia v roli Data Ownera, zamestnanec ktorý žiada prístup v roli Data User/ Data Spectator, zamestnanec, ktorý dáta aktuálne vytvára alebo používa v roli Data Creator/ Data User a IT – Support v roli Data Supervisor. Zodpovednosť za prístup je na strane manažéra oddelenia, ktorý zároveň rozhoduje aký prístup sa nakoniec žiadateľovi pridelí. Za samotnú úpravu dát zodpovedá zamestnanec v roli Data Creator/ Data User.

Pridelenie prístupu 1	Procesné kroky				
R - Responsible A - Accountable C - Consulted I - Informed	Požiadanie	Rozhodnutie o udelení prístupu	Úprava dát	Sprístupnenie dát	Overenie prístupu
Data Creator / Data User	C	C	A/R		
Data User / Data Spectator	A/R		I	I	A/R
Data Owner	I	A/R	C	C	I
Data Supervisor		I		A/R	
Výstup procesu	Zamestnanec požiada o prístup	Manažér rozhodne, či je prístup pridelený	Podľa dohody Manažéra a zamestnanca sú dáta upravené	Finálne udelenie prístupov ku dátam v dohodnutej forme	Zamestnanec potvrdí, či má prístup tak, ako bolo pôvodne dohodnuté

Obrázok 20 RACI Rovnaký projekt Rovnaké oddelenie [Zdroj: vlastné spracovanie]

Modrou farbou je znázornená matica žiadania prístupu k dátam v rámci rovnakého projektu, ale iných oddelení. Táto úroveň má v RACI matici 6 aktérov a to zamestnanec, ktorý žiada prístup v roli Data User/ Data Spectator, zamestnanec, ktorý dáta aktuálne vytvára alebo používa v roli Data Creator/ Data User, manažéra oddelenia, z ktorého zamestnanec o prístupy žiada, manažér oddelenia, z ktorého majú dáta pochádzať, vedúci projektu v roli Data Owner a IT – Support v roli Data Supervisor. V tomto prípade o pridelenie dát nežiada Data Ownera priamo zamestnanec, ale jeho manažér, ktorý zodpovedá za to, že zamestnanec dáta skutočne potrebuje. Na strane druhej je manažér, ktorý rozhoduje aký prístup a aké dáta nakoniec pridelí. Za samotnú úpravu dát ale opäť zodpovedá zamestnanec v roli Data Creator/ Data User.

Pridelenie prístupu 2	Procesné kroky						
R - Responsible A - Accountable C - Consulted I - Informed	Požiadanie	Zhodnotenie žiadosti o prístup	Rozhodnutie o dátach a typu prístupu k nim	Rozhodnutie o udelení prístupu	Úprava dát	Sprístupnenie dát	Overenie prístupu
Data Creator / Data User					R		
Manažér poskytovateľa			A/R	C	A		
Data User / Data Spectator	A/R	I				I	A/R
Manažér žiadateľa	C	A/R	C		I		
Data Owner			I	A/R	C	C	I
Data Supervisor				I		A/R	
Výstup procesu	Zamestnanec požiada o prístup	Manažér rozhodne, či je prístup potrebný	Manažér poskytovateľa rozhodne v akej forme budú dáta sprístupnené	Data Owner schváli prístup	Podľa dohody Manažérov sú dáta upravené	Finálne udelenie prístupov ku dátam v dohodnutej forme	Zamestnanec potvrdí, či má prístup tak, ako bolo pôvodne dohodnuté

Obrázok 21 RACI Rovnaký projekt Iné oddelenie [Zdroj: vlastné spracovanie]

Červenou farbou je prípad, kedy sa prideľujú prístupy nad úrovňou projektových teamov. Táto úroveň zapája všetkých 8 aktérov. Rozdiel v predošlej úrovni je ten, že kým manažér určoval, či je prístup potrebný a aké dáta sa budú presúvať, na tejto úrovni o tom rozhodujú vedúci projektov. Rolu Data Owner má v tomto prípade Scrum master a IT – Support zostáva v roli Data Supervisor. Zodpovednosť za úpravu dát má Manažér oddelenia, z ktorého dáta pochádzajú.

Pridelenie prístupu 3	Procesné kroky						
R - Responsible A - Accountable C - Consulted I - Informed	Požiadanie	Zhodnotenie žiadosti o prístup	Rozhodnutie o dátach a typu prístupu k nim	Rozhodnutie o udelení prístupu	Úprava dát	Sprístupnenie dát	Overenie prístupu
Data Creator / Data User					I		
Manažér poskytovateľa			R		R		
Vedúci projektu poskytovateľa			A	I	A		
Data User / Data Spectator	A/R	C				I	A/R
Manažér žiadateľa	C	R					
Vedúci projektu žiadateľa	I	A	C				
Data Owner			I	A/R	C	C	I
Data Supervisor				I		A/R	
Výstup procesu	Zamestnanec požiada o prístup	Manažér a vedúci projektu rozhodnú , či je prístup potrebný	Manažér poskytovateľa rozhodne v akej forme budú dáta sprístupnené	Data Owner schváli prístup	Podľa dohody vedúcich projektov sú dáta upravené Manažérom	Finálne udelenie prístupov ku dátam v dohodnutej forme	Zamestnanec potvrdí, či má prístup tak, ako bolo pôvodne dohodnuté

Obrázok 22 RACI prideľovanie prístupov medzi projektami [Zdroj: vlastné spracovanie]

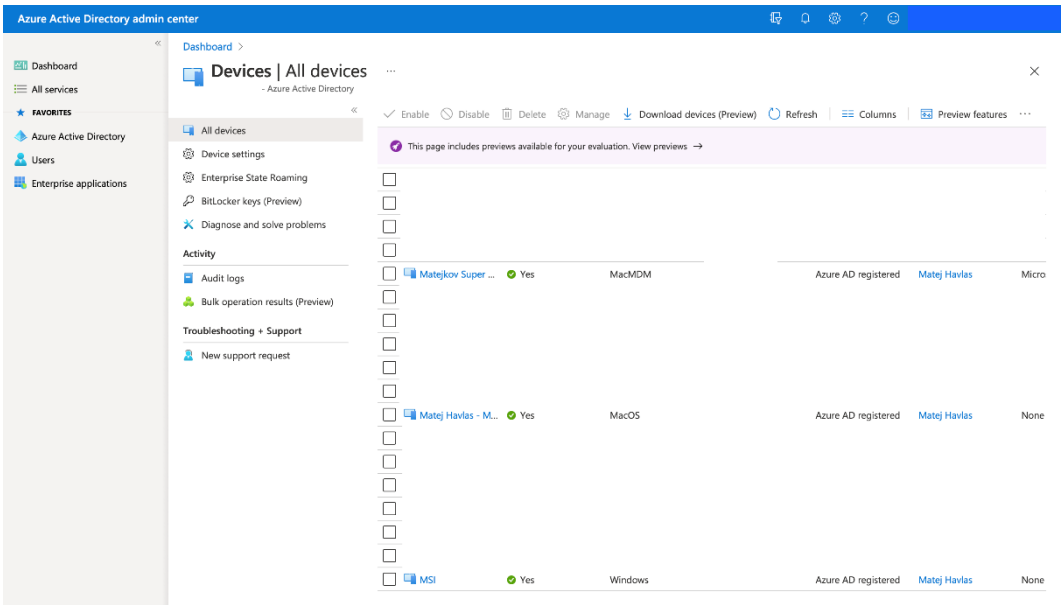
Po udelení prístupu priradí administrátor zamestnanca do príslušnej skupiny, v ktorej sú dáta dostupné. Dobu trvania prístupu budú upravovať vnútrofiremné smernice.

4.2.3 Úprava smerníc

Pre dva druhy prístupov treba upraviť smernice tak, aby v nich bolo jasne vymedzené časové obdobie, po ktoré má zamestnanec platnú autorizáciu prístupu k dátam. Pre interné firemné dáta bude tento prístup garantovaný schváleným zamestnancom nepretržite až do doby, kým ho Data Owner, ktorým je v tomto prípade CEO nezruší. Prístupy bude Data Supervisor, ktorým je v opäť CEO revidovať kvartálne. Pre produkčné dáta bude platiť, že prístup bude platný po dobu dvoch sprintov a po jej uplynutí sa zruší. O predĺženie prístupu je možné opätovne žiadať, treba však nanovo prehodnotiť žiadosti o prístup. Ak sa počas tejto doby stane z Data User Data Creator, predlžovanie sa na neho nevzťahuje, nakoľko Data Creator má autorizáciu k dátam garantovanú.

4.2.4 Mobile Device Management

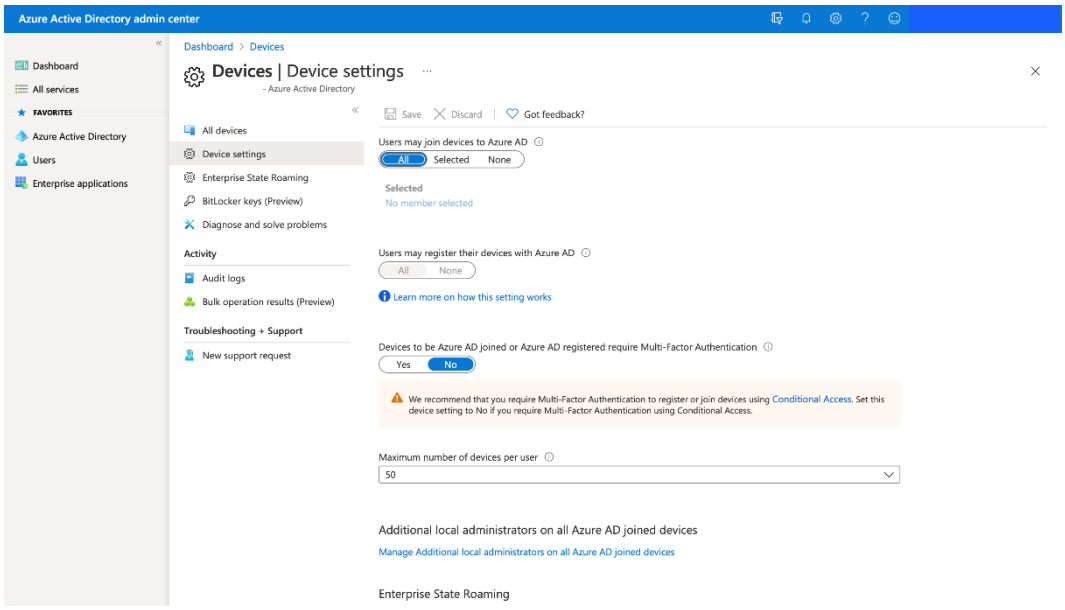
Azure Active Directory podporuje priradenie zariadení do domény, ktorá umožňuje nielen určovať, ktorý zamestnanec má prístup k dátam, ale aj z ktorého konkrétneho zariadenia sa ku ním vie dostať.



Obrázok 23 Zariadenia v Azure Active Directory [Zdroj: vlastné spracovanie]

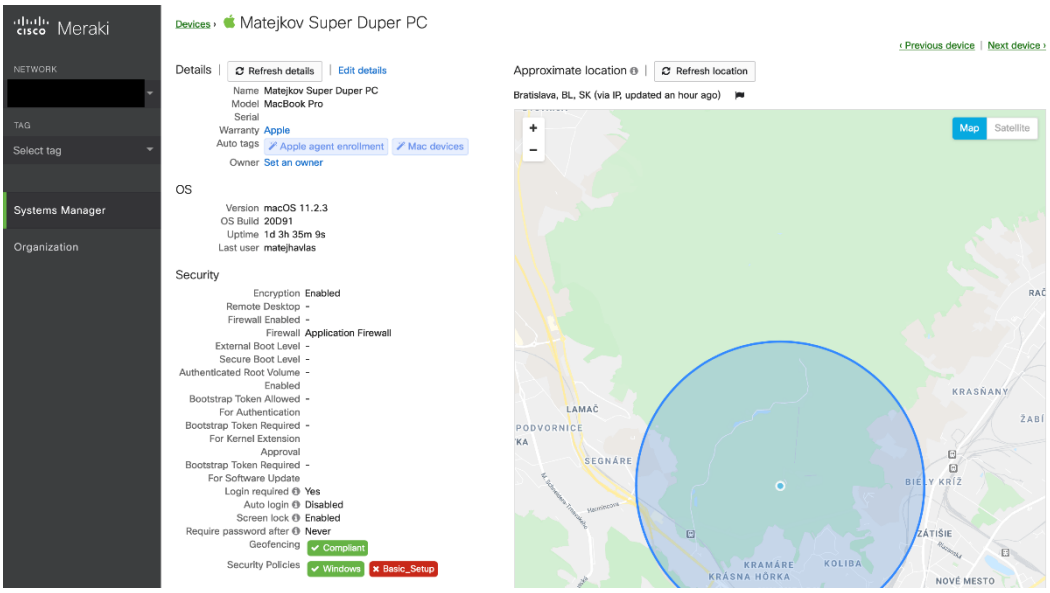
Na obrázku sú viditeľné vzostupne MSI – súkromný notebook zaregistrovaný do domény s operačným systémom Windows, Pracovný notebook pridaný cez MDM Intune od Microsoftu s typom zaradenia Personally owned s operačným systémom

Mac OS a nakoniec Matejkov Super Duper PC, pridaný cez Intune, zaregistrovaný cez Meraki. Tento typ pridania vyhodnocuje Active Directory ako Mac MDM. Na úrovni Active Directory je možné donastaviť prístup notebookov do siete a následne synchronizovanie nastavení naprieč zariadeniami.



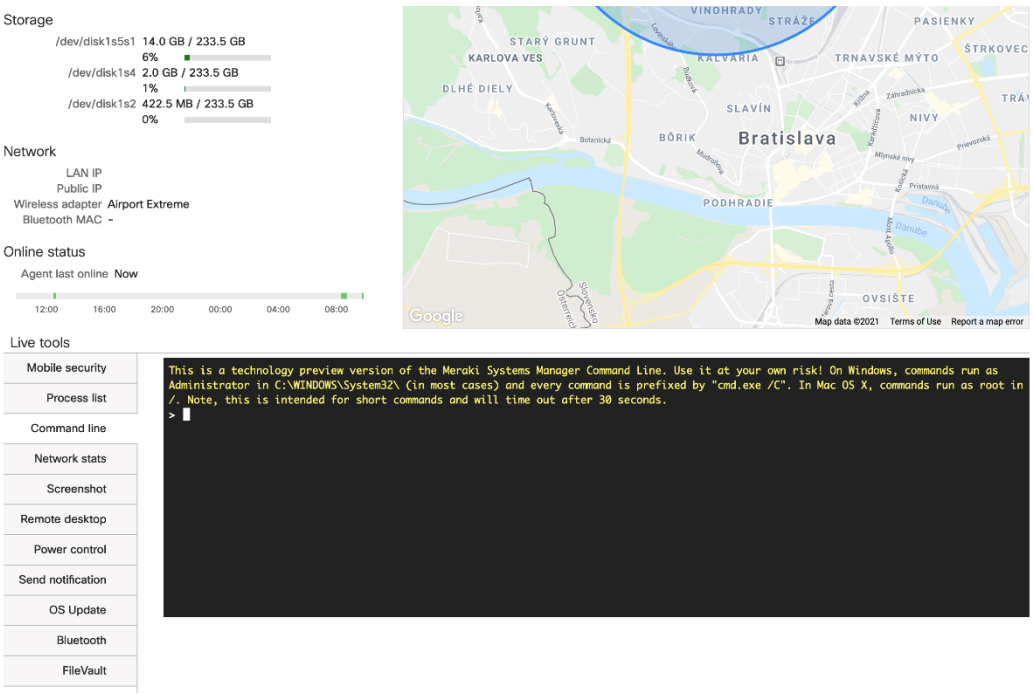
Obrázok 24 Nastavenia zariadení v Azure Active Directory [Zdroj: vlastné spracovanie]

Azure Active Directory natívne podporuje zariadenia s operačným systémom Windows. Firma ale používa Mac OS, a preto je potrebné notebooky priraďovať cez Mobile Device Management. Intune je služba ponúkaná k licenciám E3 v rámci Office 365, ale toto MDM je primárne stavané na Windows. Z tohto dôvodu treba zvoliť Meraki od spoločnosti Cisco. Mobile Device Management umožňuje administrátorovi pridávať zariadenia jednotlivo, alebo skupinovo a to buď cez klasické pridanie alebo cez Apple DEP priamo pri kúpe zariadenia. Po pridaní vie administrátor zobraziť základné informácie o zariadení.



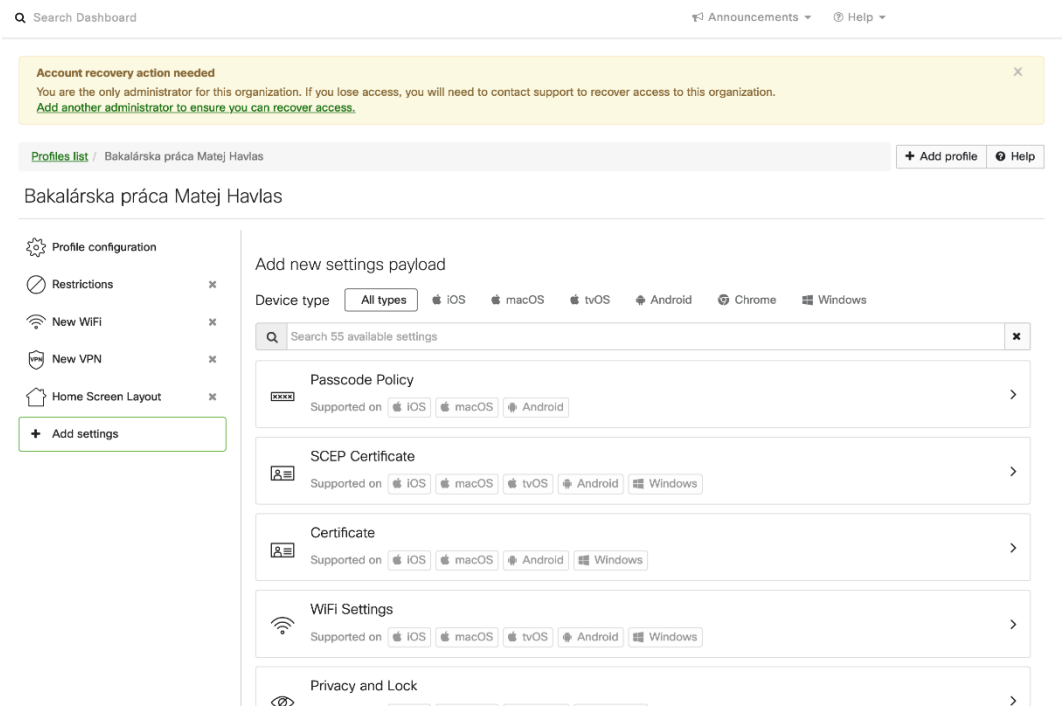
Obrázok 25 Prehľad zariadenia v Meraki od spoločnosti CISCO [Zdroj: vlastné spracovanie]

Pri pridaní zariadenia ako Company owned má administrátor prístup do počítača na úrovni užívateľa a to bez nutnosti samostatného administrátorského účtu.



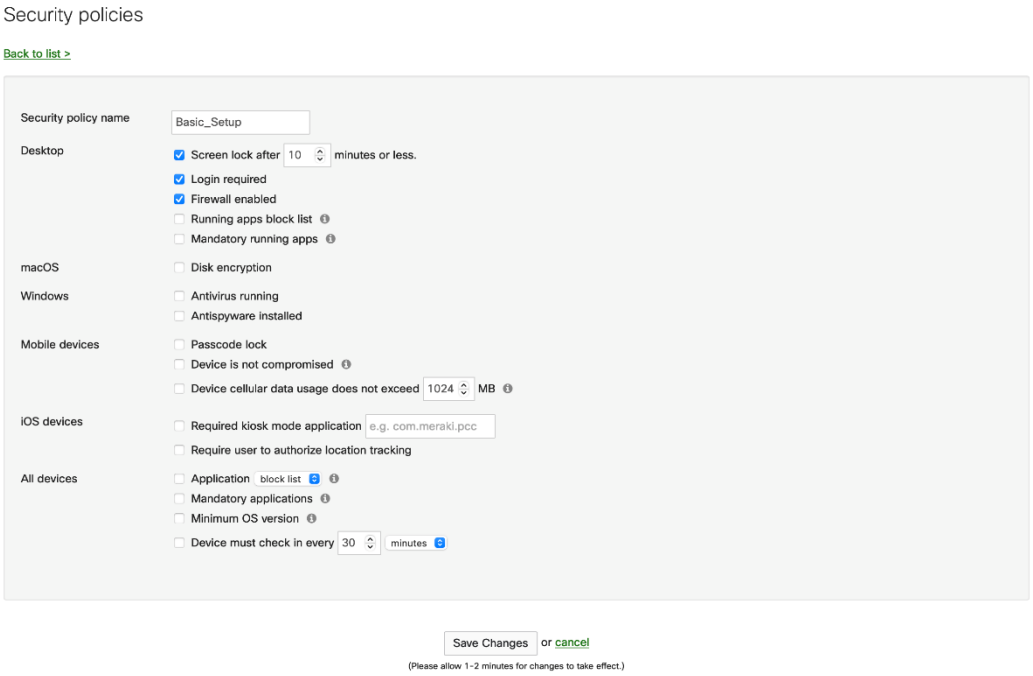
Obrázok 26 Funkcie Meraki v reálnom čase [Zdroj: vlastné spracovanie]

Administrátori budú môcť spravovať nastavenia tak, aby boli v súlade so štandardami organizácie.



Obrázok 27 Nastavenie profilu pre zariadenie v Meraki [Zdroj: vlastné spracovanie]

Základným nastavením bude obmedzenie inštalácie softvéru tretích strán, aby sa predchádzalo únikom dát. Nastavenie Wifi a VPN, pre zníženie rizika úniku shared secret hesla. Bezpečnostnú politiku je vidieť na nasledujúcom screenshote.



Obrázok 28 Nastavenie bezpečnostnej politiky zariadenia v Meraki [Zdroj: vlastné spracovanie]

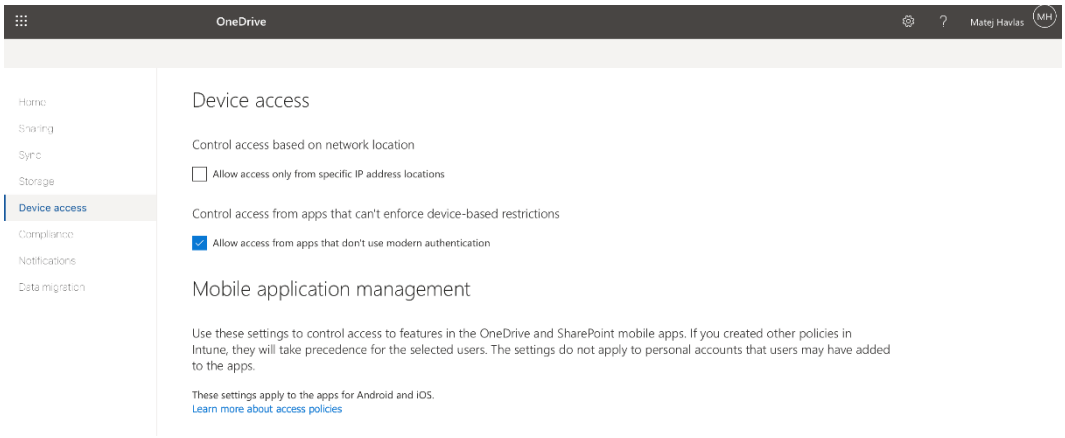
Takto nastavené počítače budú následne pridané do Azure Active Directory a priradené k zamestnancom. Azure Active Directory poskytuje podporu pre Meraki Dashboard, čo znamená, že notebooky budú do Active Directory pridané automaticky. Na základe nastavenia skupín budú práva spadať nielen na užívateľa ale k tomu aj na konkrétne zariadenie, čím sa zníži riziko zneužitia prístupov.

Implementácia jednotlivých súčastí bude prebiehať paralelne. Vytvorenie novej organizačnej štruktúry bude trvať jeden sprint, Následne budú počas ďalšieho sprintu vydané nové smernice, ktoré budú upravovať autorizáciu. Vytváranie skupín v Azure Active Directory bude prebiehať zároveň s nastavovaním profilov v MDM. Táto fáza bude trvať dva sprinty kvôli testovaniu, nakoľko po spustení to bude ovplyvňovať všetkých zamestnancov naraz. Pridávanie zariadení a zamestnancov do skupín bude trvať jeden kvartál. Predpoklad pre implementáciu celej zmeny spôsobu autorizácie je úspešná implementácia zmeny spôsobu autentifikácie. Organizačnú štruktúru a smernice zmena spôsobu autentifikácie neovplyvňuje.

4.3 Zmena spôsobu ukladania dát

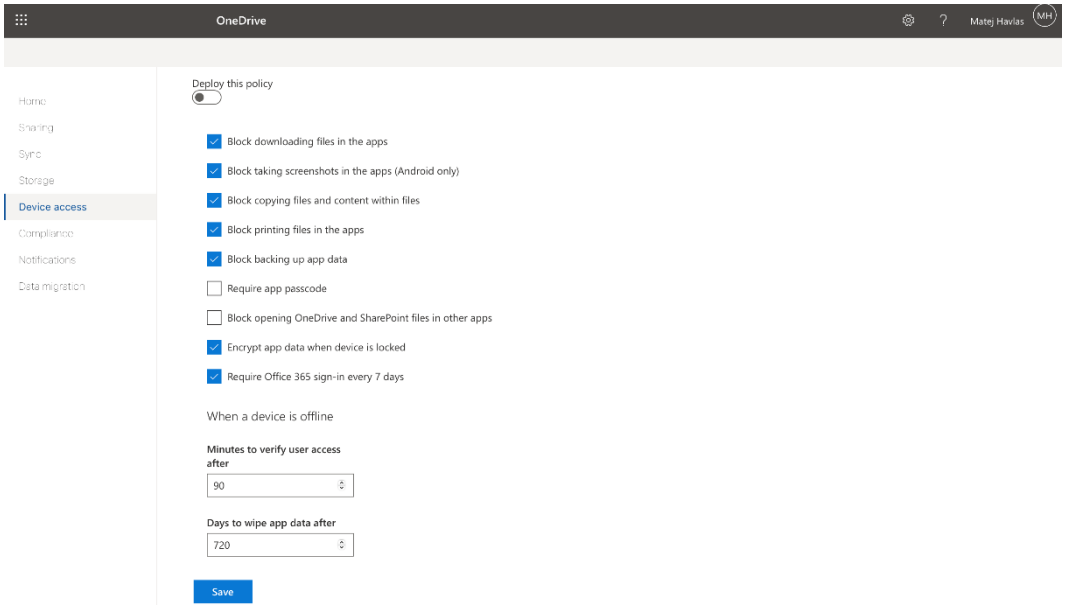
Pre jednoduchšiu kontrolu dát v súkromnom cloud priestore je potrebná adaptácia služby SharePoint. Stránka v službe SharePoint je vytvorená vždy buď manuálne, alebo po vytvorení teamu v Microsoft Teams. Službu Microsoft teams už firma využíva, takže stránky sú vytvorené. Adaptácia SharePointu bude rozdelená na dve hlavné časti.

Prvou časťou je využívanie služby OneDrive na ukladanie súborov do súkromného cloudu. S každou licenciou na Office 365 má užívateľ nárok na 1TB úložného priestoru. Po synchronizácií Online cloudu s počítačom bude nastavená funkcia On-Demand pre všetky súbory, pri ktorých zamestnanec nefiguruje ako Data Creator. Funkcia On-Demand znamená, že dáta sú v Cloude a pre prácu s nimi si ich vie užívateľ stiahnuť. Po uplynutí nastavenej doby sa dáta z počítača automaticky odstránia. Pri použití OneDrive na úrovni jednotlivcov si tieto nastavenia nastavuje sám užívateľ. Pri používaní SharePoint sú tieto nastavenia automaticky aplikované na celý úložný priestor skupiny. Implementácia prvej časti je možná behom jedného sprintu a nevyžaduje žiadnu z predošlých etáp.



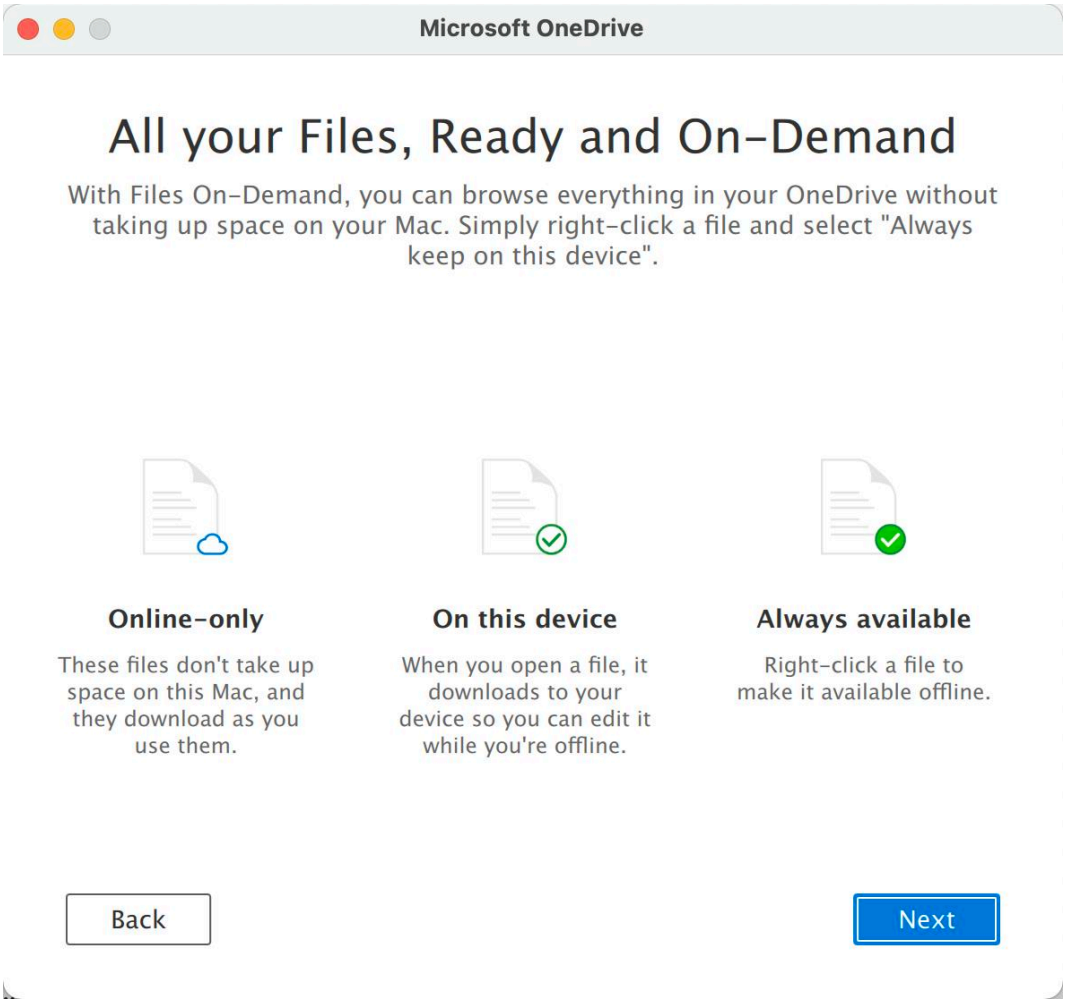
Obrázok 29 Nastavenie Onedrive aplikácie pre mobilné zariadenia [Zdroj: vlastné spracovanie]

Mobilná aplikácia je často používaná zamestnancami na súkromných mobilných telefónoch, preto musí byť prístup k dátam obmedzený natoľko, aby nenastalo riziko úniku.

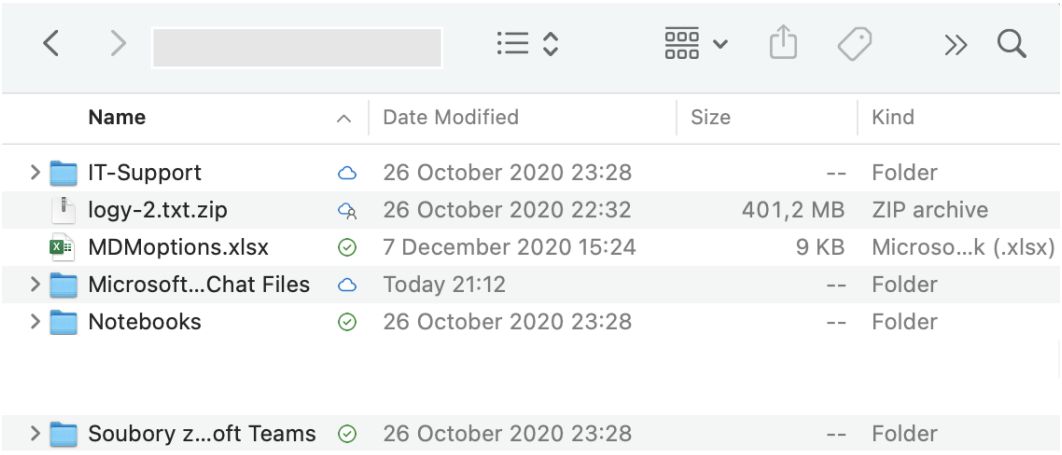


Obrázok 30 Nastavenie Onedrive aplikácie pre mobilné zariadenia detail [Zdroj: vlastné spracovanie]

Po synchronizácií je nastavená funkcionalita On-Demand, ktorá automaticky odstraňuje súbory zo zariadenia.

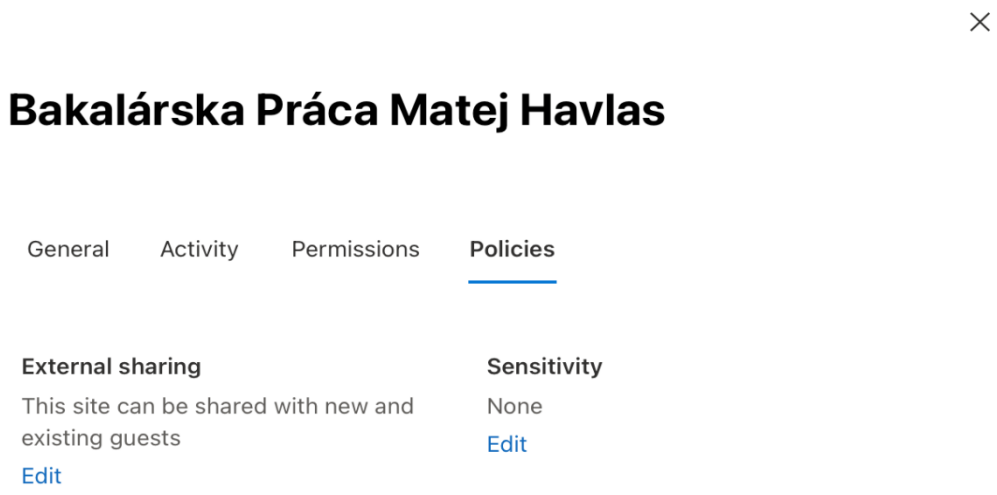


Obrázok 31 On-Demand nastavenie OneDrive [Zdroj: vlastné spracovanie]



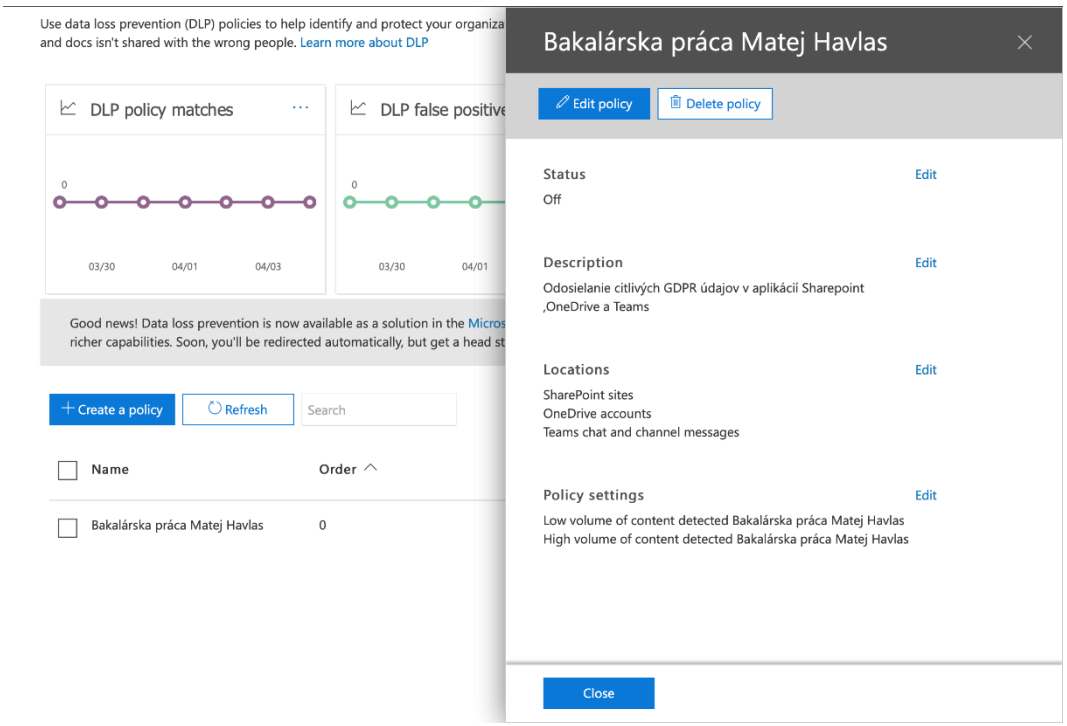
Obrázok 32 Pohľad na OneDrive priečinok u zamestnancov [Zdroj: vlastné spracovanie]

Druhou časťou je prechod na hybridný cloud SharePoint, ktorý umožňuje importovanie skupín z Azure Active Directory. Podľa novej organizačnej štruktúry budú vytvorené stránky do ktorých budú užívatelia nahrávať dáta. Skupiny, ktoré aktívne pracujú s klientami, budú mať nastavené povolenie na zdieľanie obsahu s hosťami organizácie. Skupiny, ktoré s klientami nerobia, budú mať povolené len zdieľanie s organizáciou.



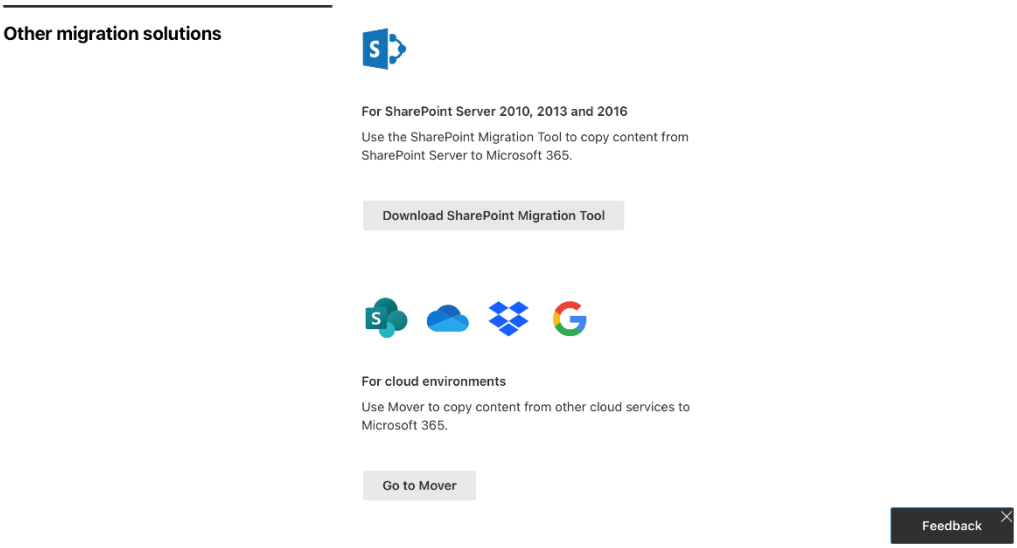
Obrázok 33 Bezpečnostné nastavenie SharePoint stránky [Zdroj: vlastné spracovanie]

Pre každú stránku je možné priradiť senzitivitu. V prípade, že senzitivitu nenastavíme na úrovni stránky ale súborov, sa senzitivita doplní automaticky. Označenie kritickosti bude priradené na základe tabuľky kritickosti z kapitoly 3.2.2. Pre zdieľanie dát mimo organizáciu je potrebné nastaviť základné pravidlá predchádzaniu straty dát.



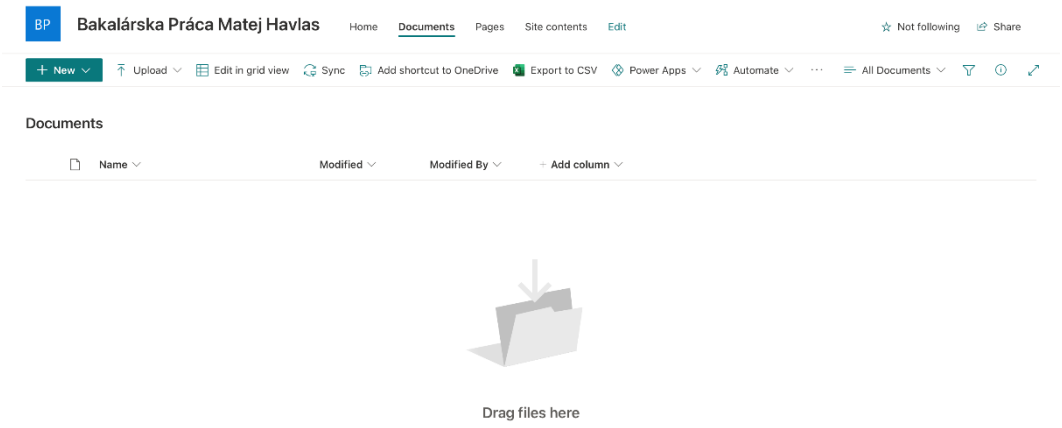
Obrázok 34 Nastavenie Data Loss Prevention politiky [Zdroj: vlastné spracovanie]

Toto pravidlo upozorňuje administrátorov v prípade, že sa v jednej zo spomínaných aplikácií vyskytuje súbor, ktorého súčasťou sú citlivé údaje. Po vložení súboru sa užívateľom odošle upozornenie, po ktorého potvrdení môžu súbor nahrať. To platí aj v prípade, že do Cloudu nahrá dáta Hosť. Pre prípad, že dáta sa posielajú častejšie budú zamestnancovi nastavené práva pre statickú IP adresu, čo znamená, že dáta budú môcť byť odoslané len z intranetu alebo cez VPN. Po aplikovaní pravidiel je bezpečné spustiť migráciu dát. Pre úspešnú migráciu je potrebná úspešná implementácia zmeny autentifikácie zamestnancov a zmeny spôsobu autorizácie. Implementácia základných pravidiel predchádzaní straty dát aj s testovaním bude trvať obdobie jedného sprintu.



Obrázok 35 Migrácia na SharePoint [Zdroj: vlastné spracovanie]

Po úspešnej migrácií nenastanú na front ende pre zamestnancov žiadne zmeny. Vizuálna stránka prostredia sa nemení, a nové priečinky sa synchronizujú automaticky. Jediní užívatelia, ktorí pocítia zmeny budú administrátori.



Obrázok 36 Ukážka SharePoint stránky [Zdroj: vlastné spracovanie]

Nakoľko implementácia vyžaduje úspešné splnenie predošlých bodov, kompletný prechod na SharePoint je možný až v treťom kvartáli od začiatku nasádzania zmien. Po Implementácií všetkých troch bodov bude splnená požiadavka vedenia firmy a bude zaistená maximálna bezpečnosť pri pristupovaní k dátam, a to ako zo strany firmy tak zo strany jej klientov.

4.4 Prínosy navrhovaných riešení

Integrácia SSO prinesie vyššiu mieru zabezpečenia, nakoľko si zamestnanci musia pamätať iba jedno heslo pre jednu identitu. Heslo bez exspirácie zabraňuje užívateľom vytvárať cyklické heslá, ktoré sú neskôr ľahšie odhadnuteľné pri útokoch.

Autorizácia pomocou RBAC rozdelí zamestnancov podľa pracovnej pozície a ABAC na základe priradených atribútov do teamov. Komunikačná kaskáda popisovaná v obrázkoch 18 až 22 jasne definuje práva na udelenie autorizácie. MDM umožní pridanie notebookov do Active Directory.

Hybridný Cloud Sharepoint je bezpečný a pohodlný. Bezpečnosť zabezpečuje dvoj úrovňové šifrovanie. Disky v dátových centrách, na ktorých sú súbory uložené sú šifrované BitLockerom so štandardom AES 256-bit. Samotné súbory sú zašifrované vlastným kľúčom. Ak presahujú 64KB, sú rozdelené a časti sú náhodne rozdistribuované medzi dátové centrá. Počas prenosu sú dáta šifrované. Pohodlnosť spočíva v možnosti nastavenia prístupov pomocou emailových adries. Správcom SharePoint stránky môže byť aj zamestnanec bez administrátorských práv. Stránky si tak vedia spravovať manažéri oddelení a vedúci teamov, pričom pracovník IT-Supportu s administrátorskými právami vie nastavovať politiky na riadenie tokov dát. Do takto nastaveného cloudu je bezpečné ukladať všetky druhy súborov bez ohľadu na ich kritickosť. Obsah súborov automaticky kontrolujú pravidlá predchádzaniu straty dát, preto je možné touto cestou posielať GDPR údaje. Systém ale nevie rozpoznať heslá, a preto je zakázané ich ukladanie v akejkoľvek forme.

Cena navrhovaných riešení na jedného človeka je od 8 do 13 eur mesačne. V cene je zahrnutá základná licencia MS Office 365 Business Basic (5 eur), s ktorou užívateľ získa prístup do Azure Active Directory a licencia na MDM Cisco Meraki (3 eurá). Počas implementácie riešení sa bežné náklady firmy na zamestnanca zvýšia oproti doterajším o 3 eurá zakúpením licencie na MDM. Implementácia bude prebiehať interne, preto sú náklady na riešenie počas implementácie 1 620 eur (60 zariadení na 9 mesiacov). Celkové náklady na chod budú maximálne 780 eur mesačne.

Záver

Cieľom mojej práce bolo navrhnúť systém prístupu k dátam spoločnosti.

V teoretickej časti som rozobral dva hlavné druhy spracovania dát, najčastejšie používaný spôsob ukladania dát, autentifikáciu a autorizáciu. Na základe toho bola vypracovaná analýza, v ktorej sa riešili vyprodukované a spracované dáta, zakladanie identity zamestnancov a získavanie prístupov k dátam. Boli zistené nedostatky v oblastiach autorizácie, autentifikácie a spôsobu zdieľania dát medzi zamestnancami.

Navrhované riešenia vychádzali z analýzy a opierali sa o vlastné skúsenosti, skúsenosti odborníkov z praxe, o teoretické východiská práce a o zdroje (35, 36, 37, 38). Norma ČSN ISO/IEC 27001:2006 bola v roku 2014 nahradená normou ČSN ISO/IEC 27002:2014, no aj napriek tomu bola zahrnutá do tvorby návrhov riešenia. Samotné riešenia počítajú s predpokladaným vývojom informačných technológií, ktoré postupne prechádzajú do Cloudového priestoru. Aj napriek tomu, že práca nerieši implementáciu, som tieto teoreticky navrhnuté riešenia úspešne implementoval do praxe, avšak iba na svojom užívateľskom konte s administrátorskými právami. Umožnilo to však lepšiu predstavu a časový odhad navrhovaných riešení. Cieľ mojej práce bol týmto splnený.

Zoznam literatúry

1. **PERNA, Andrea a BARALDI, Enrico.** *CRM Systems in Industrial Companies: Intra- and Inter-Organizational Effects.* London : Palgrave Macmillan, 2014. ISBN 978-1-137-33565-4.

2. **BUNKER, Guy a FRASER-KING, Gareth.** *Data Leaks For Dummies.* Hoboken : Wiley Publishing, Inc., 2009. ISBN 978-0-470-38843-3.

3. **GAWRONSKI, Maciej.** *Guide To The GDPR.* Alpen aan den Rijn : Kluwer Law International B. V., 2019. ISBN 978-94-035-1414-7.

4. **NOVÁK, Lukáš.** Podnikové informační systémy. *Prednáška.* Brno : VUT, 15. 2. 2021.

5. **NOVÁK, Lukáš.** Podnikové informační systémy. *Prednáška.* Brno : VUT, 5. 4. 2021.

6. **What is MDM? [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.miradore.com/blog/mdm-mobile-device-management/

7. **What is Cloud. [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/?fbclid=IwAR2sp5DrZz-

8. **What is SaaS. [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.cloudflare.com/learning/cloud/what-is-saas

9. **Access a key distribution management. [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.ami.cz/publikujeme/blog/access-a-key-distribution-management-serial-o-idm-cast-4

10. **Azure AD Multi-Factor Autentication ovreview [Online]** [Cit. 2021-04-11.] Dostupné z: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

11. **What is Multi-Factor Autentication [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.onelogin.com/learn/what-is-mfa

12. **What is IAM? Identity access management explained [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

13. **What is SSO? [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.cloudflare.com/learning/access-management/what-is-sso/

14. **What is MDM? [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.miradore.com/blog/mdm-mobile-device-management/

15 **What is MDM? [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.manageengine.com/mobile-device-management/what-is-mdm.html

16 **Active Directory Domain Services Overview [Online]** [Cit. 2021-04-11.] Dostupné z: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

17. **Understanding the Active Directory logical model [Online]** [Cit. 2021-04-11.] Dostupné z: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

18. **Active Directory [Online]** [Cit. 2021-04-11.] Dostupné z: https://techterms.com/definition/active_directory

19. **Licence a delegace [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.ami.cz/publikujeme/blog/licence-a-delegace-serial-o-idm-cast-3

20. **Role Based Access Control [Online]** [Cit. 2021-04-11.] Dostupné z: https://docs.microsoft.com/en-us/windows-server/networking/technologies/ipam/role-based-access-control

21. **Co je GDPR? [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.gdpr.cz/gdpr/

22. **Co považuje GDPR za osobní údaje [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

23. **DATA [Online]** [Cit. 2021-04-11.] Dostupné z: https://dictionary.cambridge.org/dictionary/english/data

24. **Dáta, informácie, znalosti – kybernetika TUKE [Online]** [Cit. 2021-04-11.] Dostupné z: http://matlab.fei.tuke.sk/wiki/index.php?title=D%C3%A1ta,_inform%C3%A1cie,_znalosti

25. **CLAUS, Volker; SCHWILL, Andreas, eds.** *Lexikón informatiky*. Preklad Eva Stadtruckerová. 1. vyd. Bratislava : Slovenské pedagogické nakladateľstvo, 1991. 544 s. ISBN 80-08-00755-9.

26. **What is data storage? [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.dataversity.net/what-is-data-storage/

27. **What is data storage? [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.hpe.com/us/en/what-is/data-storage.html

28. **Pros and Cons of Local and Cloud Datastorage [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.kelsercorp.com/blog/pros-and-cons-of-local-and-cloud-data-storage

29. **Cloud storage vs Local storage [Online]** [Cit. 2021-04-11.] Dostupné z: https://mydatascope.com/blog/en/cloud-storage-vs-local-storage-what-is-the-right-for-your-business/

30. **Centralized Database Management System [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.tutorialspoint.com/Centralized-Database-Management-System

31. **Difference between Centralized Database and Distributed Database [Online]** [Cit. 2021-04-11.] Dostupné z: https://www.geeksforgeeks.org/difference-between-centralized-database-and-distributed-database/

32. **PIERER, M.** *Mobile Device Management.* Vienna: Springer Vieweg., 2016. ISBN 978-3-658-15046-4

33. **Dishan, F.** *Mastering Active Directory* Birmingham: Packt Publishing, Ltd., 2017. ISBN 978-1-78728-935-2

34. **OSMANOGLU E.** *Identity and Access Management: Business Performance Through Connected Intelligence.* Newnes, 2013. ISBN 9780124104334.

35**. ČSN ISO/IEC 27001:2006** *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky.* Český normalizační institut, 2006.

36. **ČSN ISO/IEC 27002:2005** *Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací.* Český normalizační institut, 2005.

37. **ČSN ISO/IEC 27002:2014** *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky* Český normalizační institut, 2014

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

Zoznam obrázkov

Zoznam tabuliek

Zoznam použitých skratiek

MDM	Mobile Device Management
AD	Active Directory
AD DS	Active Directory Domain Service
MS	Microsoft
NUKIB	Národní úřad pro kybernetickou a informační bezpečnost
VPN	Virtual Private Network
CEO	Chief executive officer
RACI	Responsible Accountable Consulted Informed
LDAP	Lightweight Directory Access Protocol
ERP	Enterprise Resource Planning
CRM	Customer Relations Management
IBAC	Identity-Based Access Control
RBAC	Role-Based Access Control
ABAC	Attribute-Based Access Control
IAM	Identity and Access Management
RBA	Risk Based Authentication
SSO	Single Sign On
BYOID	Bring Your Own Identity
GDPR	General Data Protection Regulation
SaaS	Software as a Service

PaaS	Platform as a Service
IaaS	Infrastructure as a Service
FaaS	Function as a Service