Vysoká škola logistiky o.p.s.

Využití cloudových služeb v logistické společnosti s ohledem na bezpečnost dat

Bakalářská práce

Přerov 2022 Pavlína Záhorovská

Vysoká škola logistiky o.p.s.

Zadání bakalářské práce

studentka	**Pavlína Záhorovská**
studijní program	LOGISTIKA
specializace	Informatika pro logistiku

Vedoucí Katedry bakalářského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v bakalářském studijním programu určuje tuto bakalářskou práci:

Název tématu: **Využití cloudových služeb v logistické společnosti s ohledem na bezpečnost dat**

Cíl práce:

Na základě zhodnocení modelů cloudových systémů a jejich služeb představit typické možnosti využití v logistických procesech firmy. V typových příladch se zaměřit především na bezpečnostní aspekty řešení. Navržené příklady zhodnotit.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Bakalářskou práci zpracujte v těchto bodech:

Úvod
1. Logistické procesy firmy
2. Cloudové služby
3. Bezpečnost zpracování dat
4. Typové příklady řešení informačních procesů
5. Zhodnocení návrhu

Závěr

Rozsah práce: 35 – 50 normostran textu

Seznam odborné literatury:

BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy. Grada 2012. ISBN: 978-80-247-4307-3.

GROS, Ivan, BARANČÍK, Ivan a Zdeněk ČUJAN. Velká kniha logistiky. Praha: VŠCHT, 2016. ISBN 978-80-7080-952-5.

SCHOLL, Boris; SWANSON, Trent a Peter JAUSOVEC. Cloud Native: Using Containers, Functions, and Data to Build Next-Generation Applications. O'Reilly Media 2019. ISBN 9781492053828

Vedoucí bakalářské práce: doc. Dr. Ing. Oldřich Kodym

Datum zadání bakalářské práce: 31. 10. 2021
Datum odevzdání bakalářské práce: 6. 5. 2022

Přerov 31. 10. 2021

Ing. et Ing. Iveta Dočkalíková, Ph.D.
vedoucí katedry

prof. Ing. Václav Cempírek, Ph.D.
rektor

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a že jsem ji vypracovala samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem v práci neporušila autorská práva ve smyslu zákona č. 121/2000 Sb., o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Prohlašuji, že jsem byla také seznámena s tím, že se na mou bakalářskou práci plně vztahuje zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé bakalářské práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědoma povinnosti informovat o této skutečnosti Vysokou školu logistiky o.p.s.

Prohlašuji, že jsem byla poučena o tom, že bakalářská práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované bakalářské práce v její tištěné i elektronické verzi. Tímto prohlášením souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.

Prohlašuji, že odevzdaná tištěná verze bakalářské práce, elektronická verze na odevzdaném optickém médiu a verze nahraná do informačního systému jsou totožné.

V Přerově, dne 30.4.2022 …….

podpis

Poděkování

Tímto děkuji svému vedoucímu práce doc. Dr. Ing. Oldřichu Kodymovi za odborné a pedagogické rady a spolupráci při zpracování této bakalářské práce.
S láskou děkuji svému životnímu partnerovi Ing. Vítu Štěpánkovi, Ph.D., DBA za dlouhodobý koučink, odborné zhodnocení průběhu práce a za nekončící podporu při tvorbě této bakalářské práce.

Anotace

V této bakalářské práci se zabývám zhodnocením využití cloudových služeb v logistické společnosti. V rámci ní jsem analyzovala také práci s daty uživatelů ve firmě a jejich bezpečnost v cloudu.
Popisuji v ní cloudové systémy a nabízené služby globálních provozovatelů cloudových služeb.
Dále představuji informační systémy, které používá smyšlená logistická firma, a to včetně typových příkladů, procesů jimi podpořenými. Takto zjištěné informace jsem zasadila do prostředí logistické společnosti s návrhem jejich efektivního využití. V závěrečné části jsem shrnuta doporučení pro provoz cloudových služeb s ohledem na bezpečnost dat v oblasti podnikání logistické společnosti.

Klíčová slova

Logistické procesy, cloud, bezpečnost, logistická společnost, procesy

Annotation

In this bachelor thesis, I deal with the evaluation of the use of cloud services in a logistics company. As part of it, I also analyzed the work with user data in the company and their security in the cloud. In it, I describe cloud systems and offered services of global cloud service providers. I also present information systems used by a fictional logistics company, including type examples, and processes supported by them. I put the information obtained in this way into the environment of a logistics company with a proposal for their effective use. In the final part, I summarize the recommendations for the operation of cloud services about data security in the field of business logistics company.

Keywords

Logistics processes, cloud, security, logistics company, processes

1 Logistické procesy firmy 10

1.1 Rozdělení logistických procesů 12

1.1.1 Logistická strategie 15

1.2 Nabídka služeb logistické společnosti 17

1.2.1 Působení logistické společnosti na trhu 18

2 Cloudové služby 18

2.1 Druhy modelů cloudu a služeb 19

2.1.1 Výhody a nevýhody využívání cloudových služeb 22

2.1.2 Poskytovatelé cloudových služeb 23

2.2 Migrace služeb do prostředí cloudu 25

2.2.1 Kritéria a faktory úspěchu nasazení 25

3 Bezpečnost zpracování dat 27

3.1 Doporučené zásady bezpečné práce s daty 28

3.1.1 Hackerské útoky na organizace 30

3.1.2 Doporučované kroky pro eliminaci hrozeb hackerských útoků 30

3.1.3 Penetrační testy 32

3.2 SWOT analýza 34

4 Typové příklady informačních procesů 36

4.1 Zálohování dat 37

4.2 Proces instalace nových zařízení a služeb ve firmě 38

4.2.1 Instalace nové stanice 39

4.2.2 Přidání nového uživatele v cloudových službách Microsoftu 40

4.3 Zadávání požadavků do Helpdesk systému 42

5 Zhodnocení návrhu 45

5.1 Zhodnocení návrhu na zajištění bezpečnosti ve firmě 45

5.2 Zhodnocení návrhu zefektivnění práce IT administrátorů 47

Závěr

Seznam grafických objektů 55

Seznam zkratek 56

Úvod

Dnešní doba digitalizace ve firmách nahrává využití cloudových služeb. Čím dál více firem se snaží do informačních a komunikačních technologií investovat nemalé finanční prostředky [1]. Cílem digitalizace a investice do cloudových technologií je podpora, zefektivnění stávajících či zavedení nových firemních procesů. Tím je zpravidla dosaženo zjednodušení práce zaměstnanců tak, aby jejich pracovní doba mohla být co nejefektivněji využita. Tedy aby systémy obstaraly část jejich dosavadní práce a automatizovaly jednotlivé kroky a procesy v organizaci. Současně dochází k poskytování kvalitnějších a rychlejších služeb koncovému zákazníkovi těchto společností a jejich partnerů. Zvyšuje se tím jejich konkurenceschopnost [2]. Cloudové služby a služby datových center umožňují také bezpečný a vysoko dostupný provoz firemní infrastruktury. Menší pořizovací náklady a rozložení investic jsou pro firmy značnou výhodou.

Logistické služby jsou náročným oborem podnikání, kde je kladen vysoký důraz na kvalitu, rychlost dodávky a informovanost o jejích aktuálním stavu. Tento důraz je kladený interními i externími zákazníky společností nabízejících logistické služby. A právě proto se firmy uchylují k digitalizaci těchto procesů pomocí technologie Cloud Native [3]. Mezi výhody této technologie se řadí vysoká bezpečnost dat, jejich dostupnost a škálovatelnost spojená s filozofií rychlého nasazování nových verzí aplikací s cílem zvýšit jejich atraktivitu u uživatelů. V neposlední řadě umožňuje využití Cloud Native principů nasazení firemních aplikací co nejblíže koncovému uživateli, a to distribuovanou formou v lokálních či globálních datových centrech.

V této bakalářské práci se budu snažit ukázat na příkladu smyšlené logistické společnosti možnosti využití cloudových služeb s ohledem na bezpečnost dat v organizaci a zacházení s daty v rámci firmy.

V první části práce popisuji logistické procesy. Představuji modely cloudových služeb a cloud computing. Dále zkoumám potřeby firmy a definuji možnosti využití konkrétních cloudových služeb. Dle zjištěných potřeb následně specifikuji potřeby zákazníka

s důrazem na bezpečnost a vyberu se vhodné cloudové technologie včetně definice firemních procesů.

V druhé části práce se zabývám vytipovanými cloudovými službami a jejich detailnějšímu popisu využití ve smyšlené logistické společnosti. V další části popisuji implementaci a nasazení vybraných cloudových služeb do prostředí zákazníka. Hodnotí se dosah a úspěšnost nasazení cloudových služeb, zajištění bezpečného přenosu a práci s firemními daty ve společnosti podnikající v oboru logistiky.

V závěru bakalářské práce jsou uvedeny přínosy těchto služeb v logistických službách na předem definovaných okruzích. Ty se týkají již zmiňované bezpečnosti, vysoké dostupnosti, efektivity práce a zjednodušení firemních procesů.

Práce zhodnocuje výběr co nejvhodnější technologie pro koncového uživatele působícího v logistických službách, které bude využívat cloudové technologie globálních poskytovatelů.

Důležitým zdrojem informací byly kromě uvedené doporučené literatury také dokumenty vydané společností Microsoft, její webové stránky, propagační materiály lokálních a globálních datových center. Dalším zdrojem byli někteří pracovníci působící v oblasti informatiky, cloudových služeb a služeb lokálních datových center. Informace o lokálních datových centrech byly čerpány z katalogu Cloud computingu, který poskytuje Ministerstvo vnitra České republiky.

1 Logistické procesy firmy

Vlivem rozsáhlé digitalizace podniků můžeme v současné době mluvit o celosvětovém rozvoji průmyslu. V rámci procesu digitalizace dochází Vzhledem k digitalizaci dochází v mnohých firmách k redefinici procesů. Cílem je rozvoj služeb pro podporu interních procesů a služeb zákazníkům. Stále se rozšiřujícím tokem informací jsou firmy mnohdy nuceny reorganizovat své interní procesy, aby dosáhly co nejvyšší míry efektivity služeb, plnohodnotné využití náplně práce zaměstnanců, rychlejšího zpracování dat a hlavně spokojenosti zákazníka. Cílem je realizovat dodávanou službu nebo produkt co nejrychleji, s co nejefektivněji využitým procesy společnosti. Procesy jsou nastaveny dle koncepce společnosti (výrobní, výrobková, prodejní, marketingová nebo sociální marketingová koncepce). Například u výrobkové koncepce společnosti je kladen velký důraz na konkrétní typ produktu, jeho výrobu, manipulaci, naskladnění, skladování, dopravu a prodej [4]. Mezi další služby patří zejména balení, kompletace, ocenění zboží, nebo jeho proclení. Tyto služby jsou označovány za doplňkové, nejsou tedy hlavní činností firmy, ale nabízí se zákazníkovi, aby se rozšířilo portfolio služeb zákazníkům a získala konkurenční výhoda.

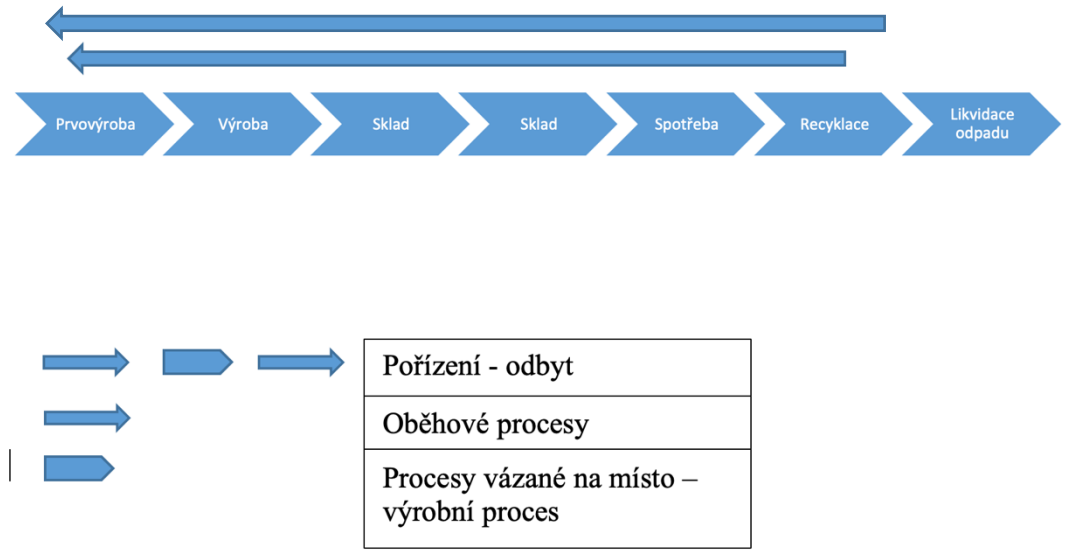
V případě výrobkové koncepce je konkurence na trhu firem tak vysoká, že jsou procesy zcela zásadním klíčem k tomu, aby si společnost udržela zákazníky [5]. Výsledky logistických procesů ovlivňují, za jak dlouho zboží/službu obdrží zákazník od objednání. Platí přímá úměra, čím dříve bude zákazníkova objednávka vyřízena, tím více bude zákazník spokojen. Ovlivňujících faktorů, ale může být více. Dle typu zákazníka může dojít k tomu, že zákazník upřednostní cenu výrobku, cenu dodání před rychlostí dodání. Spokojenost zákazníka tedy můžou ovlivnit tyto faktory: čas a místo dodání, kvalita a cena.

Správně nastavené logistické procesy jsou výsledkem konkurenceschopnosti na trhu [6]. Institute of Logistic Cambridge (1995), definoval logistiku takto: „Logistika uvádí do vztahů zboží, lidi, výrobní kapacity a informace, aby byly na správném místě ve správném čase, ve správném množství ve správné kvalitě, za správnou cenu.“. Touto definicí bych shrnula to, jak je logistický proces rozsáhlý a komplikovaný soubor činností s mnoha ovlivňujícími faktory. V případě správně stanových logistických procesů je míra spokojenosti zákazníka/ odběratele vyšší, čímž se firma staví na trhu do výhodné a konkurenceschopné pozice, která vede k vysokému odběru zboží či služeb.

Díky tzv. logistickému desateru mohou firmy jednodušeji určitě funkční logistický proces. Toto logistické desatero specifikuje skupinu zásad vedoucí ke stanovení procesů a konkurenceschopnosti.
Logistické desatero definoval Pernica ve své publikaci Logistický management: teorie a podniková praxe [7], kde sepsal desatero takto:

- Zaměření na zákazníka – dělá se vše pro uspokojení potřeb zákazníka.
- Integrace logistického systému – firmy se dnes již neobejdou bez informačního a logistického systému, který kontroluje procesy, zajišťuje správný tok informací, a to vše v reálném čase, data jsou tedy vždy aktuální (změny objednávek, kontrola skladových zásob, dostupnosti zboží aj.).
- Propojení strategií – synchronizace logistiky výrobku/služeb s cíli, které si stanovila společnost.
- Pružné logistické řetězce – včas reagovat na změnu poptávky na trhu a úpravu logistických procesů pro úspěšné dokončení procesů.
- Tvorba logistického informačního systému – sběr informací o zákaznících, produktech objednávkách je centralizován do jednoho systému, a v něm rozdělenou do modulů (objednávek, produktů, ceníků, dopravy).
- Vstup do strategických spojenectví – rozhodnutí společnosti část služeb outsourcovat (převést) pod externí poskytovatele (například pojištění výrobků, přepravu výrobků).
- Kvantifikace, měření a počítání – sběr dat do systému, který následně data umí vyhodnocovat, reportovat (například v grafech) uživatelům a navrhovat efektivnější řešení (například software Power BI od společnosti Microsoft).
- Aplikace logistického controllingu – zpětné kontroly nad daty a porovnání dat s cíli společnosti. Zejména v oblasti zisků nebo ztrát.
- Sledování finančních vztahů – administrace související s platbami dodavatelů a odběratelů. Kontrola splatností dodavatelských a odběratelských faktur za zboží/služby.
- Kvalifikovaný personál – snaha firmy a zaměstnanců o neustále vzdělávání a v oboru, díky kterému je firma schopna pružně reagovat na změny a novinky v legislativě, logistice, výrobě.

Logistický proces ovlivňují mimo jiné i logistické technologie, které do logistických procesů vstupují jako ucelené a optimalizované operace. Jejich cílem je tedy zjednodušit a zefektivnit logistické procesy. Jako logistická technologie se označuje například služba Just in time (právě včas), která je podle slov Cempírka, Kampfa a Širokého nejrozšířenější logistickou technologií v oblasti zásobování, výroby a distribuce [8]. Tato technologie se řídí smluvenými termíny dle potřeb zákazníka. Mezi další logistické technologie patří například Systém rychlé odezvy, Počítačem podporované objednávání nebo Automatická identifikace.
Proces probíhá od získání prvotních zdrojů přes samostatné fáze zpracování k zákazníkovi (spotřebiteli) znázorňuje **Chyba! Nenalezen zdroj odkazů.**.



Obr. 1.1 Schéma logistického procesu

Zdroj: vlastní zpracování 2022

1.1 Rozdělení logistických procesů

Logistické procesy mají zajistit podporu hladkého chodu společnosti napříč celou strukturou společnosti. Strukturou myslíme oddělní, divize nebo skupiny zaměstnanců a technologií které se těmito procesy řídí. S definicí logistiky a jejích procesů souvisí ve společnosti řada činností. Jedná se například o management logistiky, plánování, řízení

materiálových toků. Aby firma byla plně samostatná v oblasti logistiky, měla by mít pod kontrolou procesy pro činnosti jsou je rozhodování, rozdělení logistických činností, informací, úkolů a zejména komunikaci. V logistickém řetězci se jedná o komunikaci vnitrofiremní, ale hlavně komunikaci napříč celým logistickým řetězcem.
Logistické procesy jsou děleny na několik způsobů. Správný a úspěšný proces řídí tok materiálu, financí, plánování, informací a řízení a všechny tyto kroky sdružuje.
V případě, že by nebyly zahrnuty v procesu, ale fungovaly samostatně nedosáhly by synergie, efektivity práce a nenaplnily by ekonomické cíle společnosti.
Díky dobře stanoveným logistickým procesům může firma získat významné postavení na trhu mezi konkurencí. I to je důvodem, proč by se logistické procesy měly považovat za nezbytnou součást firemní strategie [9].

Obecné rozdělení logistických procesů

Podle Blancharda [10] můžeme logistické procesy rozdělit na tři skupiny. Do první skupiny řadíme identifikaci a řízení dodavatelů, zadávání veřejných zakázek a zpracování objednávek od zákazníků. Patří sem také fyzické dodávky služeb nebo materiálu poskytnutých od dodavatelů směrem k výrobci nebo producentovi.
Druhou skupinou je manipulace se samotným materiálem a řízení skladových zásob při výrobním procesu. Třetí skupinou je přeprava a fyzická distribuce zboží od výrobce k zákazníkovi.

Rozdělení podle šíře zaměření na studium materiálových toků [11]

- Mikrologistické procesy
  Jsou vnitropodnikové procesy, na které nemají přímý vliv procesy třetích stran. Díky tomu jsou řízeny z jednoho místa (centrály) nebo z více míst stejné společnosti (centrála + pobočky) v rámci jedné společnosti. Cílem je uspokojení potřeb výrobní společnosti napříč celým logistickým procesem.

- Makrologistické procesy
  Jedná se o mezipodnikové procesy, jež jsou komplexně řízeny z více míst a společností. Makro-logistika zahrnuje má širší rozsah působnosti, a to od například samotné těžby materiálu pro výrobek, výrobu až po prodej nebo dodání

koncovému zákazníkovi. Díky její široké působnosti není tento typ procesu pouze v jedné společnosti, ale je rozšířen mezi všechny dodavatele podílející se na tomto logistickém řetězci. Tyto procesy jsou řízeny z národně hospodářského pohledu.

Rozdělení logistických činností

Rozdělení logistických činnosti za účelem zajištění hladkého chodu produktů celým logistickým řetězcem [12]:

- zákaznický servis,
- prognózování a plánování poptávky,
- řízení stavu zásob,
- logistická komunikace,
- manipulace s materiálem,
- vyřizování objednávek,
- balení,
- podpora servisu a náhradní díly,
- stanovení místa výroby a skladování,
- nákup,
- manipulace s vráceným zbožím,
- zpětná logistika,
- doprava a přeprava,
- skladování.

Dle Pernici [7], který použil data z výzkumu vytvořeného mezi manažery z Německa, kterého se zúčastnilo 384 respondentů, je rozdělení důležitosti činností znázorněno v

Materiálové hospodářství	78–94 %
Skladování	86–92 %
Odbyt	75–90 %
Vnitropodnikovou dopravu	64–84 %
Zásobování	53–83 %

Vnější dopravu	64–83 %
Distribuci	58–78 %
Vyřizování objednávek	53–76 %
Řízení výroby	47–71 %
Nákup	42–60 %
Informační systémy	25–44 %
Kontrolu jakosti	12–20 %
Výrobu	7–8 %

Tab. 1.1 Rozdělení logistický činností dle jejich důležitosti

Zdroj: [7]

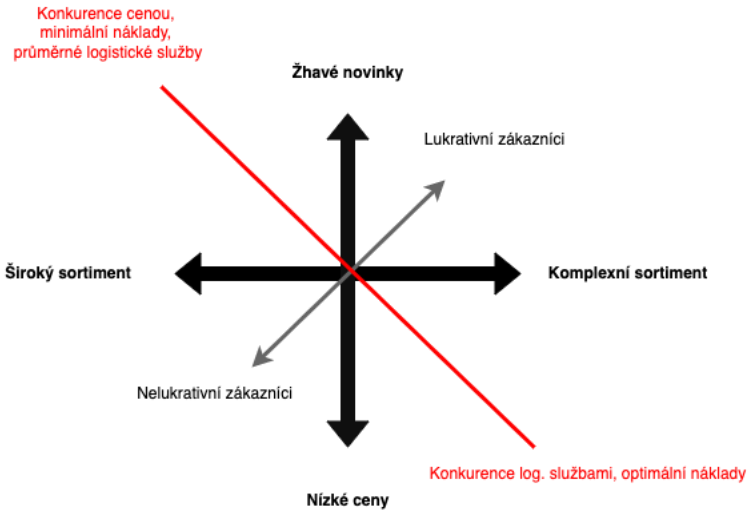
V logistické společnosti můžeme logistické procesy definovat hlavně dle jejich funkcí (činností, typů, operací).

1.1.1 Logistická strategie

Pro optimální funkci celého logistického řetězce je důležité spojit logistiku a strategii společnosti co jednoho funkčního celku. Logistický proces je úzce svázán se strategií podniku, můžeme tedy tuto strategii pojmenovat jako logistickou strategii. Ta klade důraz na potřeby zákazníků, strategii společnosti a její cíle. Strategie neboli soubor metod, přístupů a řídících procedur je funkční v případě, že její výsledky vedou k optimalizaci logistického řetězce a minimalizace logistických nákladů. Její součástí jsou také informační, komunikační a řídící procesy [13].

Úspěšnou strategií je ta, která se řídí potřebami zákazníků, zná svou konkurenci, je schopna se přizpůsobit změnám na trhu a umí na ně pružně reagovat. Dalším z bodů, které jsou součástí strategie je také definování cíle a taktiky společnosti. Může tím být nejnižší cena, nejkratší termín dodání, kvalita zboží a další. Tyto hodnoty společnosti by měli jít ruku v ruce s technologiemi a systémy, za kterými si firma stojí a plně je podporuje. Ke stanovení hodnot společnosti můžeme použít tzv. EST model, který definuje profil společnosti a její vnímání okolím. Profilovat se může na nejlepší ceny na trhu, největší výběr produktů na trhu nebo nejkvalitnější poskytování služeb. Je dobré se soustředit na jeden hlavní cíl, nikoli na všechny. Díky vynikání v jedné konkrétní oblasti, může firma být na trhu více vidět a lépe tak uplatnit své kvality. Logistické strategie jsou na **Chyba! Nenalezen zdroj odkazů.** rozděleny do vzájemně odlišných

skupin, které na příkladu retailingových firem zobrazují preferované skupiny orientace jejich produktů na zákazníky.



Obr. 1.2 Polarizace logistických strategií na příkladu retailingových firem

Zdroj: [7]

Polarizace logistických strategií na příkladu retailingových firem

Do logistické strategie z pohledu informačních technologií zasahují informační systémy. Technologie jsou jedním z klíčů dobré logistické strategie. Logistický informační systém sdružuje informace s informačními prostředky a dalšími kroky logistiky z celého logistického řetězce. Mezi ty patří tvorba zásob, poskytuje pracovníkům informace mezi jednotlivými úseky, informace k produktům a jejich dostupnosti, může také obsahovat modul plánování. Systémy nazývané ERP [14] (systém pro plánování podnikových zdrojů) mohou řešit ve společnosti oblasti dopravy a distribuce, finance, výplatu mezd a personalistiku, servis vozidel. Logistické společnosti dále používají systém pro sledování vozů a jejich reporting (stav vozu, výpočty tras aj.). Systémy pro sledování vozů určují polohu vozu, čas nakládky a vykládky převáženého zboží, spotřebu paliva nebo stav tachometru. Systémy pro řízení skladů se nazývají WMS systémy (Warehouse Management System). Cílem těchto systému je docílit přesnosti a včasnosti dodávek, zefektivnit skladové operace, zvýšit efektivitu zaměstnanců skladu, jednoduše udržovat skladové karty a přesuny a provádět inventury [15]. WMS systémy jsou dynamické systémy, které definují a řídí operace, které jsou součástí logistického řetězce díky naprogramovaným algoritmům.

Pro vyšší komfort zákazníků mohou společnosti svým zákazníků nabídnout online sledovací systém, který monitoruje operace spojené s přepravou jejich zboží. Přístup do takových aplikací obvykle bývá zákazníkovi poskytnut přes webovou aplikaci.

Dobrý informační systém obstará celý interní tok logistického procesu. Informační systém by měl být jednotný, uživatelé však mají rozděleny role, kterými do systému přistupují. Role definují, ke kterým datům má uživatel mít přístup a která data jsou pro jeho pozici důležitá. Systém by neměl být užíván jednotně a měl by se řídit jednotlivým rozdělením rolí (dle pozic zaměstnanců v logistickém řetězci). Správně implementovaný a používaný informační systém optimalizuje logistický proces.

1.2 Nabídka služeb logistické společnosti

V této kapitole je představena nabídka služeb, které mohou být součástí portfolia logistické společnosti. Společnosti, která sama nevyrábí, ale pouze zajišťuje proces od příjmu zboží po přepravu k zákazníkovi.

Nabídku logistické společnosti můžeme rozdělit do těchto kategorií

- Doprava – tzn. přeprava zboží do cílové destinace k zákazníkovi. Kromě dovozu zboží, může společnosti nabízet také jeho vývoz ze země. Dle zaměření společnosti se může jednat o mezinárodní nebo vnitrostátní (tuzemskou) dopravu. Z pohledu mezinárodní dopravy se mnoho logistických společnosti soustředí na konkrétní země, do kterých dopravu nabízí. To může být z mnoho důvodů, například jazyková vybavenost zaměstnanců, znalost právních norem pro danou zemi aj [16].
- Logistika a distribuce – součástí celkového logistického řešení jsou také sklady. Tato služba zajišťuje poskytnutí prostor pro uchování, manipulaci, balení a expedici zboží. Zaměstnanci skladů zboží přijmou, zavedou jej do systému vedení zásob, mohou zboží také vyskladňovat, polepovat etiketami, balit a finálním krokem je pak distribuce cílovému zákazníkovi. Výhodou skladování u logistických společností mohou být proškolení zaměstnanci, vysoké pojištění zboží, možnost proclení zboží, kvalitní informační systémy aj [16].

- Servis – mezi doplňkové služby mnoha logistických společností na trhu patří také servis vozidel. Dle značky vozů jsou servisy certifikovanými poskytovateli servisních služeb [17]. Může se jednat například o značky Volvo, DAF, Iveco, Mercedes nebo MAN.

1.2.1 Působení logistické společnosti na trhu

Stejně jako podniky v jiném oboru podnikání, i ty logistické zažívají poslední dobou transformaci svých služeb a interních procesů. Vliv na to má zejména situace související s onemocněním Covid-19. Řada společností se potýkala se ztrátou zákazníků, omezením vycestování do zemí, kde své služby poskytují nebo nedostatku zaměstnanců způsobeným nákazou tímto onemocněním.
Dalším důvodem pro transformaci jsou stále vyšší nároky zaměstnanců, růst cen na celém trhu, rozvoj technologií a nové výrobky na trhu.
Všechny tyto důvody vedou k neustávající snaze společností se přizpůsobit trhu a nabídnout zákazníkům co nejvýhodnější podmínky tak, aby společnosti dosáhla zisku. Společnost se musí zároveň vypořádat s rostoucí konkurencí. Zodpovědný přístup k logistice a správně nastavené procesy vedou ke zvýšení úspěšnosti společnosti na trhu. Logistická společnost na trhu mezi konkurencí může obstát, pokud nabídne zákazníkům krátké dodací lhůty, je spolehlivá a flexibilní.

2 Cloudové služby

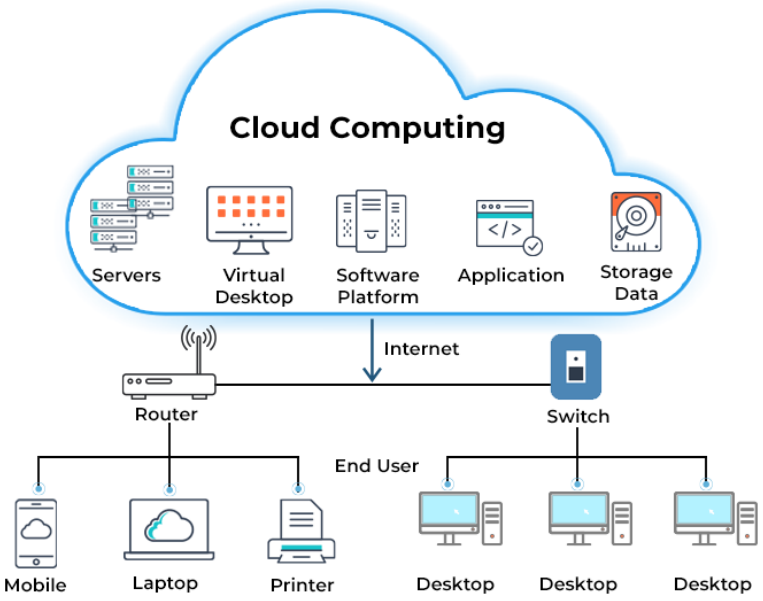
Pod názvem cloudové služby si mnoho lidí představí ikonu mraku, a data uložená neznámo kde. Cloud je možné definovat také jako internetová úložiště [18].
Pojem cloudové služby se stávají v České republice stále častěji diskutovaným tématem. Nároky dnešního podnikání ve spojení se zvyšující se poptávkou po větším množství dat a bezpečnosti vyžaduje škálovatelné řešení. Provoz služeb, serverů, aplikací či úložišť v cloudu je z pohledu dnešní doby jednoduché, výkonné a bezpečné řešení [19].
Cloudové služby umožňují zákazníkům získat špičkové a drahé technologie, do kterých globální či lokální společnosti poskytující cloud investují za dostupné finanční prostředky již pro malé až korporátní podniky. To je možné díky sdílení nákladů na

provoz. Firmy platí za to, co opravdu využijí. Cloudové služby jsou natolik škálovatelné, že je téměř nemožné nenajít pro poptávku firmy vyhovující řešení podle potřeb firmy, času i nutných investic. Nespornou výhodou cloudu je vysoký standard služeb. Všichni uživatelé pracují se stejnou verzí aplikace, jsou pravidelně nastavené aktualizace a vysoká úroveň bezpečnosti dat v cloudu. To je jedním z důvodů, proč IT administrátoři stále více vyhledávají pro firmy provoz jejich infrastruktury v cloudu. Dalším důvodem je také to, že se administrátorům výrazně sníží nutnost infrastrukturu spravovat. Většinu z potřebných zásahů zajistí poskytovatel cloudu. Příkladem může být například růst společnosti. Firmě se daří, zvyšuje svůj obrat i počet zaměstnanců, a současná infrastruktura na to již nestačí. Výhodou cloudových služeb je to, že se výkon dá navýšit „na kliknutí“. A to jak výkon, tak i retenci záloh, kapacitu úložiště, přístupové licence a další.

2.1 Druhy modelů cloudu a služeb

Cloud obecně dělíme na modely Saas, Paas, Iaas. Distribuční model cloud computingu zobrazen na **Chyba! Nenalezen zdroj odkazů.** je model, který zahrnuje servery, aplikace, služby a úložiště, ty nabízí jako službu poskytující uživateli, který se připojuje přes síť vzdáleně. Díky tomu není přetěžována kapacita hardware a software zákazníka.

Pokud se například jedná o provoz webové služby, zapotřebí je kombinace všech těchto tří modelů. Modely totiž na sebe pro plnou funkcionalitu navazují, Iaas zajišťuje infrastrukturu, Paas poskytuje provoz služeb a model Saas již používané aplikace běžící v cloudu.



Obr. 2.1 Architektura cloud computingu

Zdroj: [20]

Saas

SaaS - Software as a Service (software jako služba). Uživatel si pronajímá aplikaci, která se licencována jako služba. Uživatel si tedy za peníze kupuje přístup k potřebné aplikaci, ne přímo aplikaci jako takovou. Jedná se vlastně o tzv. pronájem aplikací. Tento model je vhodný pro společnosti, jejíž uživatelé pracují často vzdáleně, a potřebují mít k aplikaci přístup kdykoli a odkudkoli na světě [21]. Obvykle se jedná o klasické aplikace typu Microsoft Office 365, sady nástrojů Google Apps nebo například aplikaci Cargopass pro logistické společnosti.

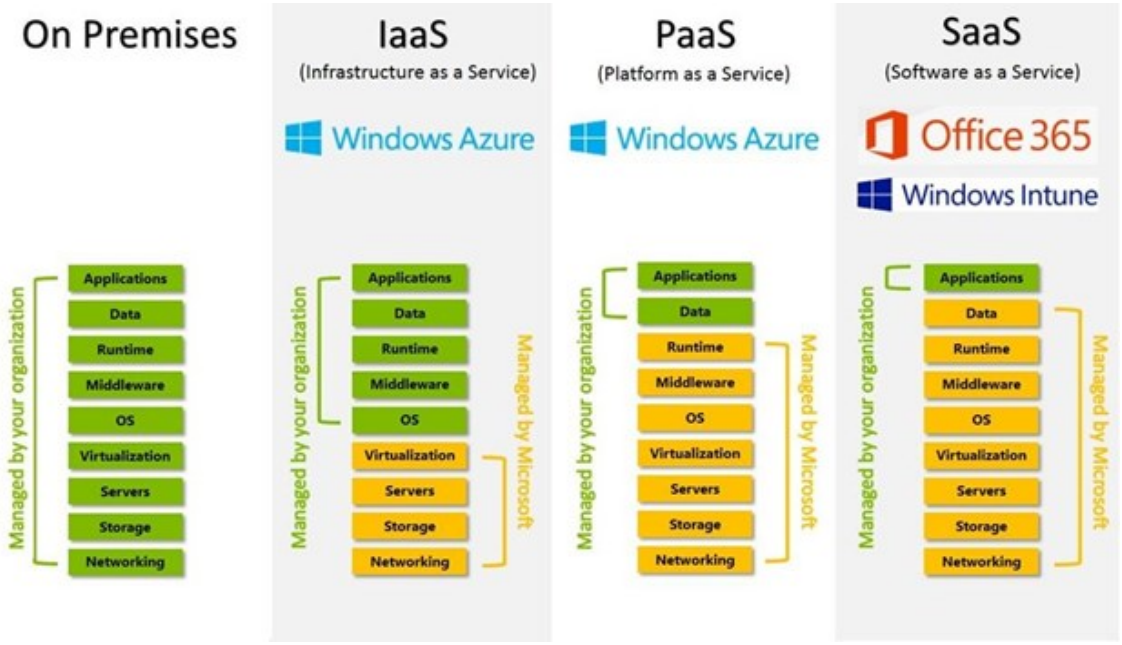
Paas

Paas – Platform as a service (platforma jako služba). Model, kdy jsou zákazníkovi poskytovány veškeré prostředky pro provoz jeho interně využívaných aplikací a služeb. Může se jednat například o provoz ekonomické systému, ERP systému a dalších klíčových firemních systémů. Jedná se o přístup do aplikací přes internet. Software je aplikován na platformě poskytovatele, a není možné jej nějakým způsobem stáhnut off-

line do stanice uživatele. Velmi často je tento model cloudu využíván vývojáři a testery, nebo provozovatele software, například lokální společnost Kvasar s.r.o. Služby tohoto typu poskytuje například globální lídr na trhu, společnost Microsoft, jejíž služba se nazývá Microsoft Azure. Dále také lokální poskytovatelé datových center, mezi ně patří na území České republiky na příklad společnosti O2 Czech Republic a.s. [22], České Radiokomunikace a.s. [23], NWT a.s. [24], ALEF Distribution CZ s.r.o. [25] a další.

Iaas

Iaas – Infrastructure as a Service (infrastruktura jako služba). Tato služba, jak již název napovídá poskytuje zákazníkovi infrastrukturu. Poskytuje potřebné hardwarové a softwarové prostředky pro provoz požadované infrastruktury firmy, a to jak hardwarové, tak softwarové prostředky [18]. Firmy si tuto možnost oblíbily zejména proto, že tato služba zajišťuje bezproblémové zajištění chodu infrastruktury, o kterou se stará poskytovatel. Firmě tak odpadá starost zajištění lidských zdrojů a energií pro provoz hardwarové infrastruktury. Na poskytovatele padá odpovědnost starat se o aktualizace software, jeho správu, rozšíření a dodávky energií. Služby tohoto typu poskytuje stejně jako u Paas modelu například společnost Microsoft v Azure, stejně tak výše zmíněná lokální datová centra. **Chyba! Nenalezen zdroj odkazů.** zobrazuje rozdělení aplikační služby dle druhů modelů cloudu do kategorií poskytovaných služeb společnosti Microsoft.



Obr. 2.2 Rozdělení aplikačních služeb dle druhu modelů cloudu

Zdroj: [26]

2.1.1 Výhody a nevýhody využívání cloudových služeb

Na cloudové služby koluje mnoho odlišných názorů. Pro část lidí pohybující se v oboru informačních technologií, je cloud výhodný. Důvodem je, že se o něj nemusí starat, z jejich pohledu je flexibilnější i bezpečnější z pohledu použití a zabezpečení dat. Druhá skupina lidí cloud spíše odsuzuje. Dle jejich názoru není bezpečné mít data mimo prostředí organizace, mnohdy neznámo kde. Tato skupina lidí preferuje mít fyzický server v prostředí organizace, kde ho vidí, může si na něj doslova sáhnout. Vidí výhodu v tom, že si správu zajišťují sami a přesně vědí, co na dané serveru je nasazeno, v jaké verzi, jak je server zabezpečen a kdy je potřeba provádět aktualizace. Jednoduše je pro něj přijatelnější přijmout odpovědnost za správu infrastruktury na sebe než ji předat na poskytovatele cloudových služeb.

Mezi prodejní argumenty, výhody poskytovatelů služeb, které se dají považovat za výhody je například elasticita, takřka neomezený výběr konfigurace služeb, rozložené finanční náklady do měsíců (tyto služby se obvykle platí měsíčním paušálem), nízké počáteční investice, což je výhodou pro nově vznikající společnosti nebo start-upy. Mezi další výhody se řadí patří vysoká kvalita dodávaných služeb, vzhledem

k bezpečnostním rizikům firmy poskytující cloudové služby investují nemalé finanční prostředky do bezpečnosti, což zákazníkovi nabízí vysoký standard poskytovaných služeb.
Za nevýhody cloudu se dá považovat menší možnost škálovatelnosti, na on-premise serverech je daleko složitější zajistit vyšší kapacitu úložiště, zvýšit výkon nebo povýšit licence pro software. Vše zmíněné souvisí s dalším nákupem disků, úložiště nebo licencí a fyzickou instalací na serveru. Mezi nevýhody také můžeme řadit bezpečnost. Z pohledu poskytovatelů cloudových služeb, není zákazník na svém vlastním on-premise řešení zajistit stejnou bezpečnost, jako mají globální či lokální datová centra. Toto bezesporu souvisí s finančním prostředky vynaloženými na zajištění bezpečnosti. Firmy obvykle nemají možnost investovat stejné finanční prostředky do testování a bezpečnosti dat jako datová centra. Důvodem je samozřejmě fakt, že datová centra jsou poskytována širokému portfoliu zákazníků a ze smluvního vztahu mezi poskytovatelem a zákazníkem plyne zajištění bezpečnosti dat a informací. Při úniku informací hrozí poskytovatelům cloudových služeb velké finanční postihy. Důležité je také zmínit, že přístup ke cloudovým službám je přes internet, čímž se firma na internetu stává závislou, aby umožnila chod infrastruktury svým uživatelů. Připojení by mělo být kvalitní, vysokou rychlostí a hlavně stabilní.
Obecně nelze říci, která varianta je správná, názory se různí a každá společnost má jiné nároky a finanční možnosti na provoz infrastruktury.

2.1.2 Poskytovatelé cloudových služeb

Firmy poskytující cloudové služby můžeme základě rozdělit na lokální a globální.

Lokální, tedy působící v České republice, poskytují cloudové služby zejména z vlastních datových center v případě Paas nebo Iaas. (viz druhy modelů a služeb), nebo v případě Saas poskytují pronájem konkrétní softwarové platformy. Lokální společnosti se doporučují firmám, které nechtějí svá data poskytovat mimo území České republiky. Často lidé, kteří se cloudu bojí, mají pocit, že data v cloudu jsou bezpečnější a jim bližší v České republice než v globálních datových centrech v zahraničí. U datových center globálních poskytovatelů totiž nejde přesně říci, kde se vlastně data nacházejí.

Mezi globální poskytovatele řadíme velké hráče na trhu cloudových technologií. Patří sem společnosti Microsoft [27]
Amazon web services [28], nebo Google [29].
Tyto společnosti nabízí všechny zmíněné cloudové modely Saas, Paas, Iaas. Kalkulaci cludových služeb u globální společností poskytující cloud se dají spočítat, a tedy predikovat náklady na cloud na webových stránkách těchto společností. Služby těchto technologických gigantů využívají obvykle firmy s velkým kapitálem, s moderním přístupem k informačním a komunikačním technologiím. Tyto firmy nemají obvykle tak velký strach o únik jejich dat a věří globálním poskytovatelům, kteří investují miliardy dolarů do bezpečnosti v těchto datových centrech [30].

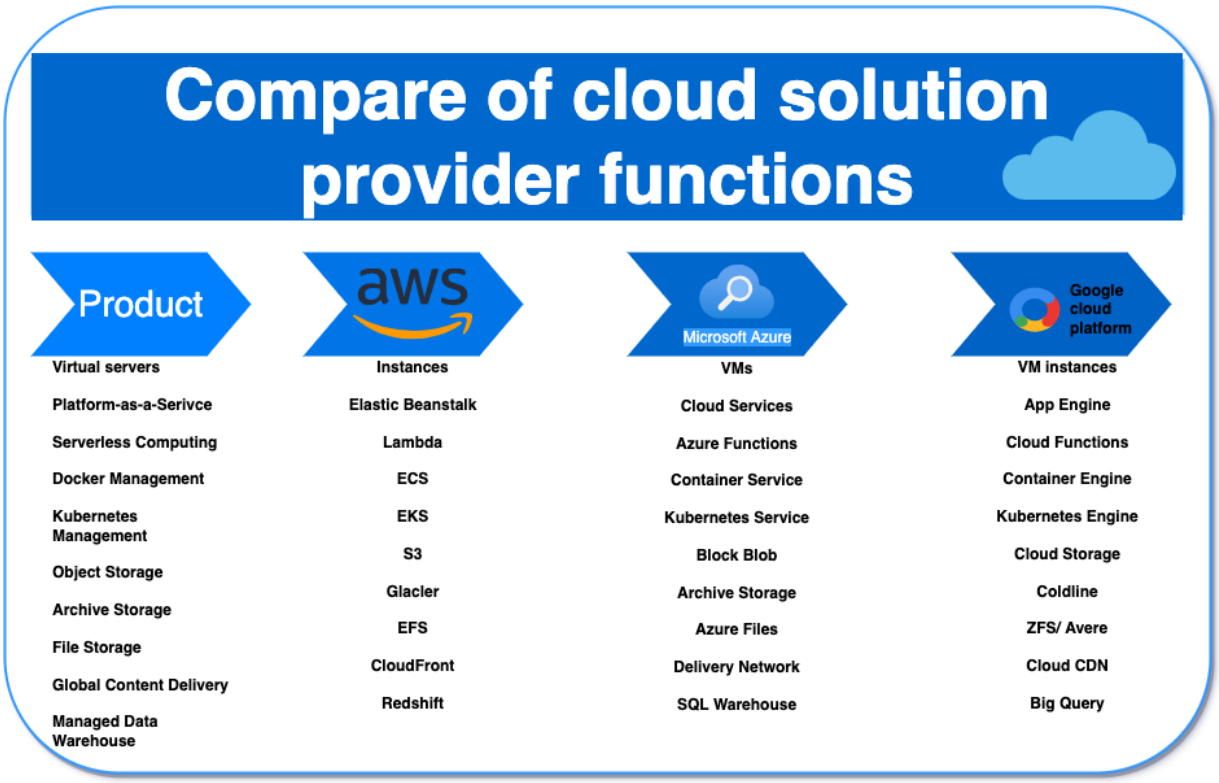
Příklady lokálních poskytovatelů cloudových služeb

- O2 Czech republic a.s. [22]
- Autocont a.s. [31]
- Forpsi, Internet CZ a.s. [32]
- ČMIS s.r.o. [33]
- NWT a.s. [24]
- TOTAL SERVICE a.s. [34]

Příklady globálních poskytovatelů cloudových služeb [35], [36]

- Amazon Web Services,
- Google Cloud Platform,
- Microsoft Azure,
- IBM Cloud,
- Salesforce.

Porovnání cloudových služeb globálních poskytovatelů zobrazující produkty v jejich vlastním názvosloví **Chyba! Nenalezen zdroj odkazů..Chyba! Nenalezen zdroj**



Obr. 2.3 Porovnání služeb globálních cloudových poskytovatelů

Zdroj: vlastní zpracování 2022

odkazů.

2.2 Migrace služeb do prostředí cloudu

Převod ze stávajícího řešení do světa cloudových služeb se nazývá migrace nebo také implementace.

Implementace zahrnuje nastavení všech služeb, nastavení koncových stanic, převod domén, v případě migrace řešení Saas i migraci pošty, migrace prostředí, zaškolení správců a uživatelů a všechny práce s tím spojené.

Vyšší efektivitě práce a úspoře financí přispěje školení a seznámení uživatelů s technologiemi, zejména po nasazení vybraného řešení.

Například migraci poštovního serveru do cloudu, můžeme provést následujícími nástroji

- migrace pomocí PST souborů,
- migrace pomocí systému Linux,
- migrace pomocí kliku v Microsoft Exchange,
- migrace pomocí migračního nástroje BitTianu [37].

2.2.1 Kritéria a faktory úspěchu nasazení

Mezi identifikované faktory k dosažení cílů projektu patří:

- spolupráce s dalšími dodavateli odběratele (registrátor DNS, poskytovatel internetu, stávající poskytovatel e-mailového řešení apod.),
- podpora projektu ze strany vedení zákazníka,
- akceptace smluvního vztahu, například mezi Microsoft Operations Ltd. Ireland a objednatelem,
- součinnost klíčových uživatelů,
- trvání na projektových standardech řízení projektu,
- přístup do prostor odběratele nebo zajištění vzdáleného přístupu k infrastruktuře,
- základní znalost aplikace Microsoft Outlook u koncových uživatelů,
- nasazení aplikace Microsoft Outlook minimálně ve verzi 2007 na koncových zařízeních,
- odpovídající šířka pásma internetu pro připojení v jednotlivých lokalitách,
- plný přístup administrátorů (dodavatele nebo objednatele) ke schránkám uživatelů, jejichž data budou migrována,
- dostupná technologická infrastruktura (internetové připojení, pracovní stanice odpovídající současnému výkonovému standardu pro provoz Microsoft Office - min. 2GB RAM, CPU min. 2GHz).

Postup migrace zahrnuje

Příprava na účet – jedná se připravení systému na migrace, otestování účtu + sledování logu a chyb. Délka migrace je omezena výkonem migrovaného serveru a objemu migrované schránky. Obecně se dá říct 1 GB je cca 5 hodin, pokud je u řešení předpoklad migrace 10 GB, odhad doby migrace je přes 48 hodin, přesný čas bohužel říci nejde, jelikož migraci ovlivňuje velké množství faktorů, které ve velké míře nelze dopředu predikovat. Například u migrace poštovního serveru můžeme dohromady migrovat až 10 účtů, větší počet mnohdy zahltí migrovaný server a ten začne odmítat spojení, doporučený počet migrovaných účtů najednou je dle odborníků ale 6.

Technik při migraci provádí následující kroky

- aplikace pořízených licencí a zkontrola platnosti,
- kontrola certifikátů a jejich platností,
- kontrola serverů, blacklistů, SPF, logů, testovací zprávy,
- příprava řešení migrace uživatelů a sdílených mailboxů do cloudu,
- migrace a konfigurace admin prostředí,
- kontrola migračních vln,
- konfigurace dynamických skupin,
- konfigurace tenantu [38],
- konfigurace hybridní koexistence [39],
- konfigurace Exchange serverů a konektorů,
- konfigurace federation trusts [40],
- zajištění změny MX záznamů [41],
- testování odesílání a přijímání pošty přes cloud,
- vytváření nového uživatele v cloudu,
- řešení odinstalace a podmínek pro odinstalaci serverů.

Přínosy migrace

Přínosem migrace je následně úspora času a finančních prostředků. Cloudové prostředí umožní zvýšit pružnost a v mnoha případech rychleji reagovat na potřeby firmy. Cloud může dokonce přispět ke snížení celkových nákladů na vlastnictví [42].

Tím firmě poskytne obrovské úspory finančních prostředků, které může investovat zpět do firmy, například na modernizaci. Navíc nabízené možnosti řešení PaaS a SaaS, které umožňují snížit celkové náklady na vlastnictví a zároveň rozšíří vaše schopnosti v oblasti IT.

3 Bezpečnost zpracování dat

Data patří v dnešní době k jedné z nejcennějších věcí, které firma má [43]. Zahrnují informace o chodu společnosti, mezi které můžeme zařadit například databáze zákazníků, bankovní údaje, výrobní patenty, receptury či postupy a vůbec know-how celé společnosti. Tyto klíčové informace mohou při jejich ztrátě mnohdy znamenat až krach společnosti.

Odborníci z oblasti informačních technologií se shodují, že v České republice je cennost dat stále podceňována. Zároveň se také shodují, že až 40% firem svá data vůbec nezálohuje [44]. Administrátoři IT ve firmách nejsou v této oblasti dostatečně seznámeny s možností, jak data zálohovat a jaké jsou „best practices“ pro ochranu firemních dat.

Právě z těchto důvodů je důležité, aby zaměstnanci společností byli pravidelně proškolování v oblasti práce s daty, bezpečného chování na internetu, nebo také práce na firemní síti mimo sídlo společnosti, například na home office.

3.1 Doporučené zásady bezpečné práce s daty

K vyššímu zabezpečení společnosti lze zásadně přispět. Za bezpečnost dat ve společnosti obvykle zodpovídají interní administrátoři informačních technologií.
V některých společnostech interní administrátoři vůbec nejsou, v takových případech si firmy najímají externího dodavatele pro informační technologie.

O tom, jakým způsobem budou data zabezpečena tedy odpovídá administrátor. Práci s daty definují nastavené firemní procesy, které se stávají oficiální směrnicí pro zaměstnance, případně externisty pracující s firemními daty.

Práci s daty výrazně ovlivnilo nařízení Evropské unie o ochraně osobních údajů, tzv. GDPR [45]. Nástupem tohoto nařízení začalo bezpečnost ve firmách řešit výrazně více společností, které hledaly lidské zdroje a nástroje na to, aby toto nařízení Evropské unie byly schopny plnit.

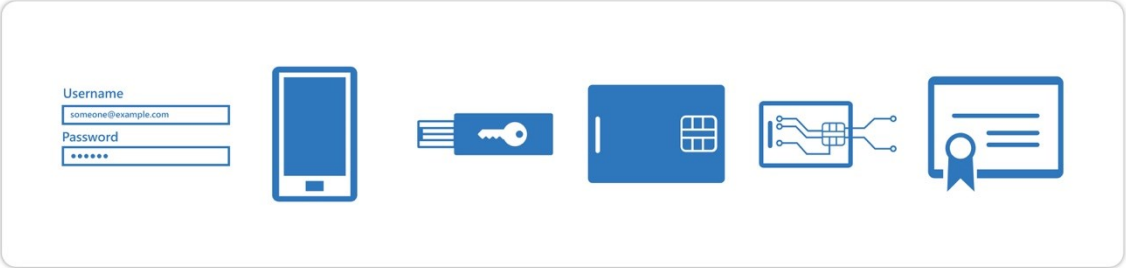
Bezpečnost ve společnosti se dělí na tří základní části.

- bezpečnost infrastruktury,
- bezpečnost stanic a serverů,
- bezpečnost uživatelů.

Mezi kroky vedoucí ke zvýšení zabezpečení firemních dat a zamezení jejich úniku patří:

- Šifrování stanic - počítačů, notebooků, mobilních telefonů, tabletů. Cílem šifrování stanic je eliminovat riziko úniku dat a informací, ke kterému může dojít v případě ztráty nebo odcizení zařízení. Šifrování zařízen nabízí společnosti poskytující na trhu antivirová řešení. Mezi ty patří například společnosti Eset, Bitdefender, Kaspersky nebo česká společnosti Avast.
- Zabezpečení firemního e-mailu a dokumentů uživatelů – nejrozšířenějším komunikačním nástrojem ve firmách je e-mail. Skrze něj si vyměňují uživatelé z interní i externí sítě velké množství informací, citlivých firemních údajů. Zabezpečení e-mailových konverzací a dokumentů, které mohou být přílohou e-mailů je pro firmy velice důležité. Jeden z nástrojů, kterým se dají e-maily zabezpečit je například od společnosti Microsoft s názvem Azure Information Protection [46].
- Pravidelné aktualizace používaného software ve firmě – vlivem kybernetických útoků a stále nových verzí hrozeb útočníků, vydávají firmy poskytující software pravidelné aktualizace, které reagují na hrozby hackerů bezpečnostními záplatami.

- Dvoufaktorové ověřování, tzv. MFA [47] – jedná se o metodu ověřování, jejíž cílem je při ověření přístupu, například do aplikace, nutnost ověřit uživatele minimálně dvěma faktory. Čím vyšší počet ověřených faktorů, tím větší míra zabezpečení a menší pravděpodobnost útoku hackera. Na **Chyba! Nenalezen zdroj odkazů.** je zobrazen proces ověření při použití druhého faktoru pomocí bezpečnostního tokenu



Obr. 3.1 Proces druhého faktoru ověření pomocí bezpečnostního tokenu

Zdroj: [48]

- Využití nástrojů pro správu přístupu – například nastavení oprávnění přístupu k dokumentům a při úniku dat jejich případné zneplatnění přístupu. Pro nastavení oprávnění k dokumentům může ve společnosti sloužit například funkce tzv. labellingu, česky štítkování. V rámci organizace může mít firma stanovené určité množství štítku citlivosti, které klasifikují dokumenty dle toho, jak citlivé údaje dokument obsahuje. Tuto funkci nabízí v jednom ze svých předplatných například společnost Microsoft.

3.1.1 Hackerské útoky na organizace

Ve firmách je důležité zajistit zabezpečení a dodržování předpisů, které si vynucují stále sofistikovanější kybernetické hrozby a složitá ochrana údajů vyžadovaná předpisy, jako je obecné nařízení o ochraně osobních údajů (GDPR). Průzkumy globálních společností poskytující IT služby ukazují, že více než 77 % firem není vybaveno záložním plánem pro potřeby případného kybernetického útoku, to ukazuje například průzkum společnosti IBM [49].

Profesionální hackeři se denně pokusí po celém světě až o XY útoků, z toho XY je úspěšných. Nejčastějším typem útoků je phishing. Phising útočí přímo na konkrétní uživatele ve firmě, na jejich e-mailové účty, přístupy do podnikových systémů. Vysoká úspěšnost této metody je způsobena neznalostí uživatelů. Zejména administrativní pozice nejsou vůbec, nebo jen minimálně poučeny o tom, jak se bezpečně chovat na internetu a ve firemní síti. Mnoho firem se těmto „slabým“ článkům celé organizace snaží pomoci nejen školením, ale také nastavením globální firemní politiky zabezpečení. Může se jednat například o vyžadování časté změny hesla, požadavků na skladbu hesla – počet znaků, speciální znaky, číslice apod. Ještě vyšší formou zabezpečení pomocí dvou faktorového ověřování, tzv. MFA [50].

3.1.2 Doporučované kroky pro eliminaci hrozeb hackerských útoků

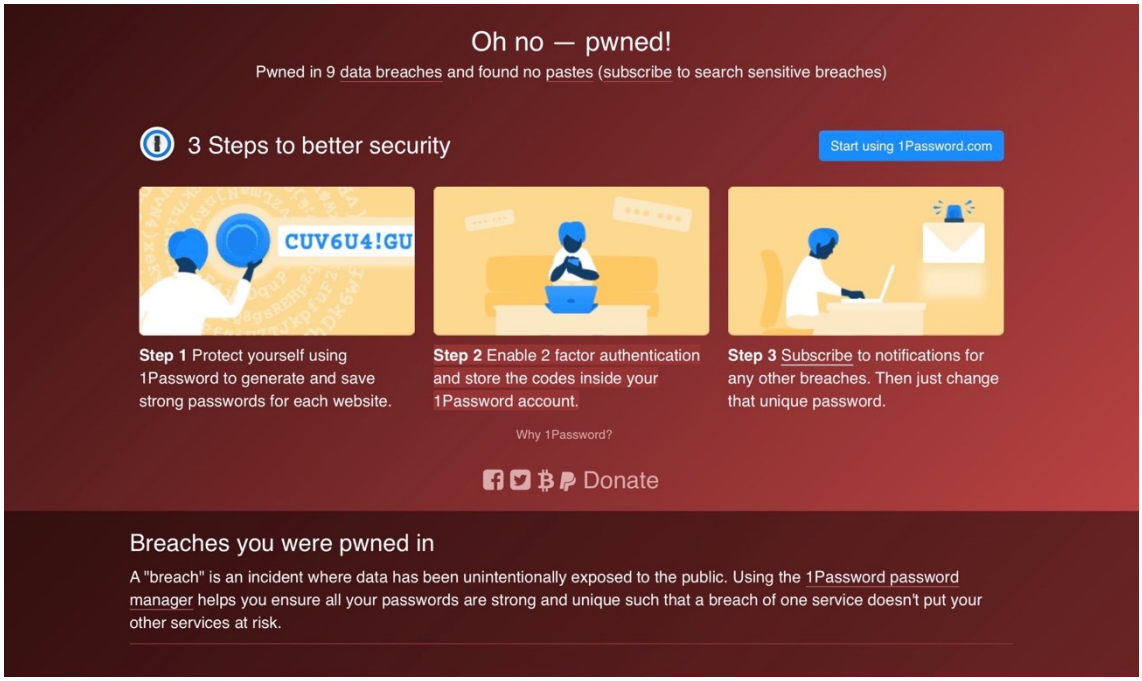
Jednou z prvních zásad je nepřipojování k neznámé a veřejné Wifi. V případě nutnosti lze připojení provést vytočením VPN, která u firemních počítačů bývá chráněna antivirovým systémem. Z neznámých sítí není vhodné přistupovat k „citlivým údajům“ (bankovnictví, firemní zdroje, aj.)
Webové stránky, které nejsou zabezpečeny, není vhodné navštěvovat. Zabezpečené webové stránky začínají zkratkou HTTPS:// a nejsou označené jako nedůvěryhodné. Mají bílý nebo zelený zámek u adresy, zatímco ty nezabezpečené jsou označeny červeným trojúhelníkem s vykřičníkem uvnitř.

Firemní počítač je obvykle přidělen pouze jedné osobě a není vhodné dovolit přístup komukoli dalšímu, mimo informačního specialisty nebo technika, který je autorizovaný. Do stanic není vhodné vkládat cizí média jakou jsou flash disky, CD, DVD a další externí zdroje.

Vzhledem k častým útokům tzv. phishingu, je důležité, aby uživatelé byli proškoleni na zásady bezpečnosti chování na internetu, s firemními daty a aplikacemi. Útočníci v dnešní době využívají loga bank, státních institucí a dalších orgánů, pod kterými se vydávají za danou organizaci a vymáhají zaplacení nemalých finančních obnosů. Formou e-mailů pak hromadně rozesílají žádosti o zaplacení finančních prostředků. Pouhým kliknutím na odkaz v e-mailu může uživatel hackera vpustit do firemní sítě a to

postupně hackera vede k napadení sítě celé organice. Proto je důležitým krokem proškolení uživatelů a instuktáž, jak poznat pravé e-maily od těch s falešnou žádostí o poskytnutí finančních prostředků nebo čísel bankovních účtů. Rozeznat lze často dle e-mailové adresy, která není oficiální e-mailovou adresou dané instituce, nebo také pravopisnými chybami v textu e-mailu. Hackeři texty nepíší, uměle je překládají v překladači, což vede k četným chybám. Phishing se vyskytuje nejen formou e-mailů a také SMS zpráv. Všechny tyto falešné zprávy a e-maily mají jediný cíl, kompromitovat uživatelský účet a dostat se do sítě společnosti [51].

Dalším doporučovaným krokem je pravidelná kontrola hesel. Například na webové stránce https://haveibeenpwned.com lze ověřit, zda se některé z uživatelských hesel nenachází na seznamu tzv. uniklých hesel. V případě, že se jedná o uniklé heslo, jako příklad je uveden **Chyba! Nenalezen zdroj odkazů.** je doporučeno hesla ve všech službách ihned změnit.



Obr. 3.2 Ukázka webu pro zjištění úniku hesel

Zdroj: [52]

Jak má vypadat správné heslo

- mělo by být komplexní (VELKÉ, malé písmo, čísla, speciální znaky .:?+*),
- mělo by mít minimálně 12 znaků,
- mělo by být náhodné.

Slovníkový útok je běžný a nahrazování písma čísly není pro hackera překážka, stejně tak stupňující se číslo na konci nebo přidávání teček umí hackeři algoritmizovat.

3.1.3 Penetrační testy

Penetrační test je komplexnější test, který vychází z OWASP TOP 10 - 10 nejčastějších technik pronikání do sítí. Skládá z otestování sítě a zařízení na zranitelnosti a známé chyby zabezpečení. Dále se provádí kontrola antivirového řešení, nastavení a zapnutí bezpečnostních prvků stanic a serverů, kontrola aktivních prvků (jako jsou například switche, Wi-Fi, routery). Řeší se také aktuálnost software a hardware a jejich chyby. Test lze doplnit o reálný test zranitelnosti a pokus zneužití nebo o sociální inženýrství a přípravu kampaně na uživatele k otestování míry odolnosti k těmto sociotechnikám. Velkým firmám je standardně doporučováno dělat penetrační test minimálně 1x ročně nebo po významnější změně infrastruktury a z jeho výsledků pak dělat nápravná opatření.
Výsledkem testu je rozsáhlá zpráva o stavu infrastruktury společnosti, zhodnocení topologie sítě a konkrétní návrhy řešení zjištěných nedostatků. Výsledkem je komplexní přehled o stavu, rizik, problémů a návrh opatření k jejich nápravě – s ohledem na využití nových technologií, efektivitu i ekonomiku.
Testy provádí specialisté, většinou zaměstnanci společností zabývající se informačními technologiemi. Profesionálové jsou oficiálně certifikováni. Mezi certifikační autority patří například společnosti EC-Council, TAYLLORCOX, CYBERSECURITY.EYE a další [53].
Samy společnosti z oblasti informačních technologií by měly umět pracovat s bezpečností dat. Proto je mnoho z nich certifikováno certifikací ISO 27001. „Jedná se o mezinárodně platný standard, který definuje požadavky na systémgementu bezpečnosti informací“ [54].
Mezi kroky zahrnující úspěšné dokončení penetračních testů patří například:

- kolik zařízení bude předmětem testu (počet IP adres/ zařízení včetně popisu: server, pevné stanice, switche),

- zjištění kondice interní a externí formy sítě (útok z vnitřní sítě nebo i z internetu),
- kontrola nastavení Virtuální privátní sítě (VPN),
- kontrola systému prevence proti útoku, tzv. IPS,
- kontrola systému pro detekci a prevenci průniku, tzv. IDPS, Systém prevence průniku – Wikipedie (wikipedia.org)
- ověření fyzické bezpečnosti - kamerová zařízení, přístupy do počítačů zaměstnanců, přístup do budovy,
- provedení DOS a DDOS útoků - vyřazení služby útokem - zahlcením požadavky,
- realizace útoku na hesla zaměstnanců,
- audit legálnosti software,
- posouzení používání cloudových služeb,
- posouzení nakládání zaměstnanců s citlivými údaji,
- test sociálního inženýrství -manipulace nebo phishing.

3.2 SWOT analýza

Níže zpracovaná SWOT analýza na **Chyba! Nenalezen zdroj odkazů.** (silné stránky, slabé stránky, příležitosti, hrozby) definuje aspekty připravenosti logistické společnosti schopnost odrazit hackerský útok. Pro tvorbu SWOT analýzy jsem použila vlastní zkušenosti z práce a mého portfolia zákazníků, konkrétně zákazníka působícího v oblasti logistických služeb.

Silné stránky

Mezi silné stránky obecně patří zájem společnosti investovat definovanou výši finančních prostředků do IT bezpečnosti. Společnost v letech 2020-2021 investovala do ochrany všech uživatelských koncových stanic v podobě nasazení antivirového programu Bitdefender v pokročilé variantě Ultra [55].
Ta chrání stanice uživatelů, filtruje příchozí poštu, zabezpečuje VPN připojení. Další investicí do ochrany dat společnosti bylo zakoupení a nasazení bezpečnostních prvků společnosti Fortinet, světového leadera na trhu v oblasti bezpečnosti sítí. Odborníci ve společnosti nasadili zařízení Fortigate, tzv. Next Generation Firewall, jejíž cílem je

chránit celou topologii sítě na centrále a všech pobočkách společnosti v České republice i zahraničí [56], [57].

Slabé stránky

Do slabých stránek řadíme fakt, že společnost vlastní téměř 500 kamionů a v nich je umístěn stejný počet tabletů, běžících na operačním systému Android. Tento druh operačního systému je velice náchylný na viry a má slabé zabezpečení, takže může být lehkým terčem při případném hackerském útoku na organizaci.
Řidiči kamionů cestují nejen v rámci České republiky, ale také do zahraničí. Z toho plynou další rizika mobilních zařízení a tabletů, a to zejména připojováním řidičů těchto náprav na veřejné WiFi sítě.
Přestože firma v letech 2020-2021 investovala větší množství finančních prostředků do IT bezpečnosti, od té doby k dalším investicím zatím nedošlo. Z tohoto důvodu uvádím jako slabou stránku, jelikož hrozby útočníků používají každým dnem nové algoritmy, na které je potřeba reagovat v čase.

Příležitosti

Společnost se snažila v určitém období investovat nemalé finanční prostředky do zabezpečení koncových stanic a firemní sítě. Tím využila většinu možných dostupných prostředků pro zamezení hackerského útoku.

Hrozby

Tým Check Point Research vytvořil analýzu, která říká, že české firmy čelí až 640 útokům týdně. Což je více, než je celosvětový průměr. V porovnání s tím, jaký mají firmy v České republice na IT bezpečnost rozpočet, se jedná o velice vysoké číslo [58].
Vlivem častého cestování více než ½ zaměstnanců této organizace mezi různými zeměmi EU ale i zemí mimo EU je zde vysoké riziko ztráty nebo odcizení tabletů a mobilních telefonů. Toto riziko představuje vyšší pravděpodobnost odcizení dat ze zařízení uživatele a následnému zneužití dat.

Předmět analýzy: **Připravenost logistické společnosti odrazit hackerský útok**

	POMOCNÉ (k dosažení cíle)	**ŠKODLIVÉ** (k dosažení cíle)
VNITŘNÍ (atributy organizace)	**STRENGHTS** (silné stránky) • Investice do penetračních testů • Používání pokročilé verze antivirového software na stanicích uživatelů • Ochrana serverů a switchů pomocí firewallu • Školení uživatelů jak se	**WEAKNESSES** (slabé stránky) • Velké množství externích zařízení (mobilních telefonů, tabletů) • Uživatelé na cestách mimo ČR • Malé množství finančních prostředků na další rozvoj
VNĚJŠÍ (atributy prostředí)	**OPPORTUNITIES** (příležitosti) • Použití silných stránek pro zamezení hrozeb	**THREATS** (hrozby) • Hackerské útoky na data organizace • Ztráta koncového zařízení uživatele v exteriéru

Obr. 3.3 SWOT analýza zabezpečení podniku

Zdroj: vlastní zpracování 2022

Doporučení

Pro rozšířenější zabezpečení koncových zařízení pohybující se v terénu, by bylo vhodné za tato zařízení nasadit pokročilejší verzi antivirového software, který by nechránil pouze notebooky a počítače, ale také mobilní zařízení a tablety. Tento krok by pomohl při záchraně dat u ztraceného zařízení. V případě ztráty uživatel odcizení nahlásí administrátorovi, který pomocí příkazu v systému zařízení a uživatelský účet vzdáleně deaktivuje.

Dalším doporučením je pravidelné školení uživatelů (interních i externích) na práci s firemními daty a bezpečnou práci v síti. Uživatelé bývají z pohledu bezpečnosti vyhodnocováni jako ten nejslabší článek při ztrátě nebo odcizení dat v organizaci.

4 Typové příklady informačních procesů

Náplní práce IT administrátora, ať už zaměstnance společnosti, nebo externí administrátora patří správa firemního software, drobné opravy HW, správa stanic uživatelů, komunikace se zaměstnanci společnosti a případně školení zaměstnanců. Administrátoři by měli zajistit bezpečnost firemních dat, jejich správné zálohování a omezení přístupu k datům uživatelům dle organizační struktury ve společnosti.

Firmy se neobejdou bez globálních poskytovatelů služeb. Dle údajů z roku 2018 používalo operační systém Windows od společnosti Microsoft 96 % počítačů v České republice [59].
„Microsoft je dle analytiků společnosti IDC CEMA lídrem tuzemského trhu. [60]“
Vývoj cloudových služeb je enormní, toto odvětví patří je nejvíce rozvíjejícím se technologickým oborům za poslední tři roky.
Obvykle interními směrnicemi stanovené postupy vedoucí k údržbě systémů a jejich funkčnosti se stávají rutinními kroky administrátorů. Vzhledem k fluktuaci zaměstnanců ve společnostech, způsobenou také vývojem nemoci Covid-19, tak mnohdy až na týdenní bázi rutinně opakují například od instalaci stanice zaměstnance ve výpovědní lhůtě, nebo naopak instalují novou stanici pro nové zaměstnance [61].
Ve středních a velkých společnostech není dlouhodobě udržitelné, aby celé IT oddělení společnosti zastupoval pouze jeden člověk. Nejčastěji firmy od desítek a více zaměstnanců obsazují na IT oddělení více zaměstnanců [62]. Rozdělení pozic na tomto oddělení obvykle plyne z rozdělení na správu software nebo hardware. Velké firmy používající robustní ERP systémy, mají mnohdy přímo zaměstnance spravující pouze tento systém, ostatní pozice se starají o komunikaci se zaměstnanci, řešení interních požadavků, nákupu nového hardware a software, školení zaměstnanců a správu ostatních systémů ve společnosti. Další samostatnou pozicí může být na IT oddělení zaměstnanec zabývající se bezpečností. Tato pozice odpovídá za návrh interních směrnic pro bezpečnou práci s daty. Dále je odpovědná za výběr a implementaci

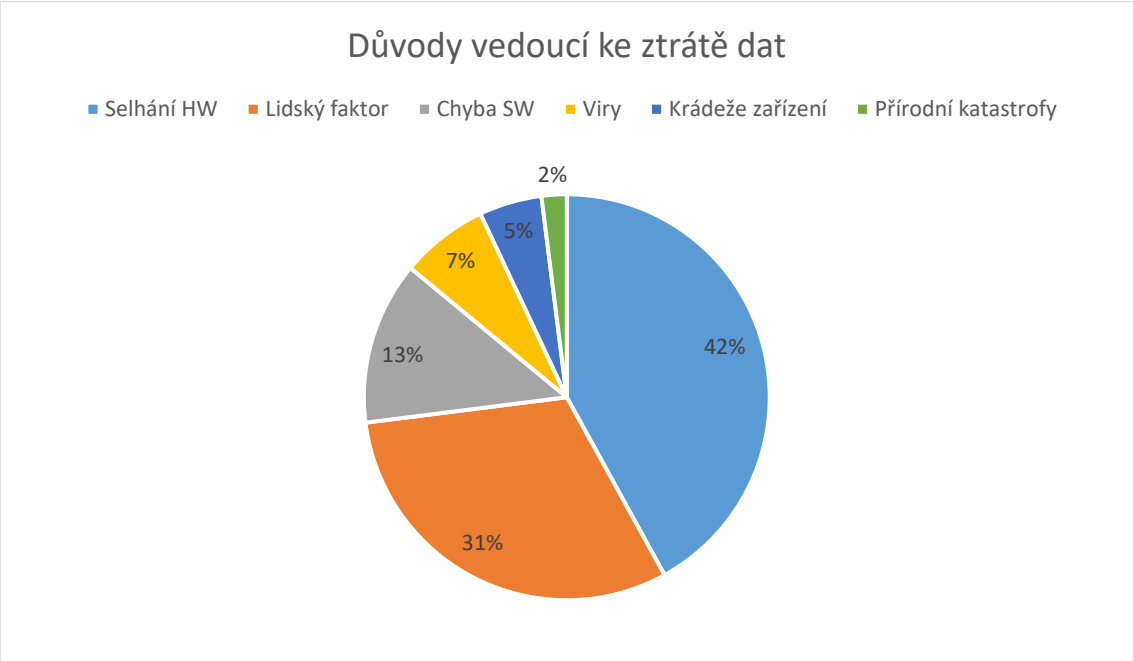
antivirového řešení ve společnosti, za topologii sítě, nasazené firewally. Přes veškerou snahu zajištění dat proti úniku, se nelze před hackerským útokem 100 % ubránit.

4.1 Zálohování dat

Záchranou v případě úniku dat jsou pro firmu správně zálohovaná data. Záloha dat je tím pádem pro firmu zcela klíčová. Zálohovat data se dá mnoha způsoby – lokálně, na flash disky, disky, na druhý server umístěný ve stejné místnosti (což není vhodně kvůli riziku požáru, výpadku nebo odcizení dat). Za nejmodernější způsob, jak data zálohovat se v dnešní době považuje odliv záloh dat do datových center. Výhodou této formy zálohování je velmi snadná obnova. Transport a ukládáním dat probíhá šifrovaným připojením. Poskytovatelé datových center mají pro bezpečný přístup dat zákazníkovi často vyvinut uživatelský portál. Přístup k datům tak mají pouze společností vlastníci data definovaní uživatelé pomocí přístupových údajů do portálu a více faktorovým ověřováním.

Doporučená forma zálohování je mít tři kopie na dvou lokalitách a mít jednu off-line verzi záloh. Při nastavení zálohování je také důležité myslet na to, jak často budeme zálohu dat provádět, to zpravidla určuje, jak jsou pro nás data důležitá. Čím častější retence (provádění záloh) bude, tím jsou pro nás data důležitější a jejich ztráta by mohla být pro firmu velmi ohrožující. Co je nejčastějším důvodem ztráty dat zobrazuje **Chyba! Nenalezen zdroj odkazů.**.

Zálohovat se doporučují fyzické servery, virtuální servery, data aplikací, aplikace (například Microsoft 365) [63].



Graf 4.1 Nejčastější důvody ztráty dat

Zdroj: vlastní zpracování 2022

4.2 Proces instalace nových zařízení a služeb ve firmě

Příchod nového zaměstnance do společnosti znamená pro IT administrátory přípravu uživatelské stanice, notebooku nebo pevného počítače pro daného uživatele, vytvoření e-mailové adresy, uživatelského učtu do počítače a mimo jiné i generování přístupů do firmou používaných aplikací, jako jsou ekonomický software, CRM systém, podnikový informační systém, tzv. ERP systém, aplikace pro zadávání dovolené a další. Směrnice ve firmách definují, jak má administrátor zařízení pro nového zaměstnance nastavit, co vše má do zařízení nainstalovat, definuje, jaká má uživatel (dle zařazení a pozice) práva v aplikacích a k jakým datům má přístup. Obvykle se také uživateli přiřazuje a instaluje Office licence pro tvorbu a čtení dokumentů, tabulek, aplikaci pošty, nebo tvorbu prezentací.

Na níže popsaných procesech popisuji nejčastější postup IT administrátorů při instalaci nového zařízení a uživatelského účtu.

4.2.1 Instalace nové stanice

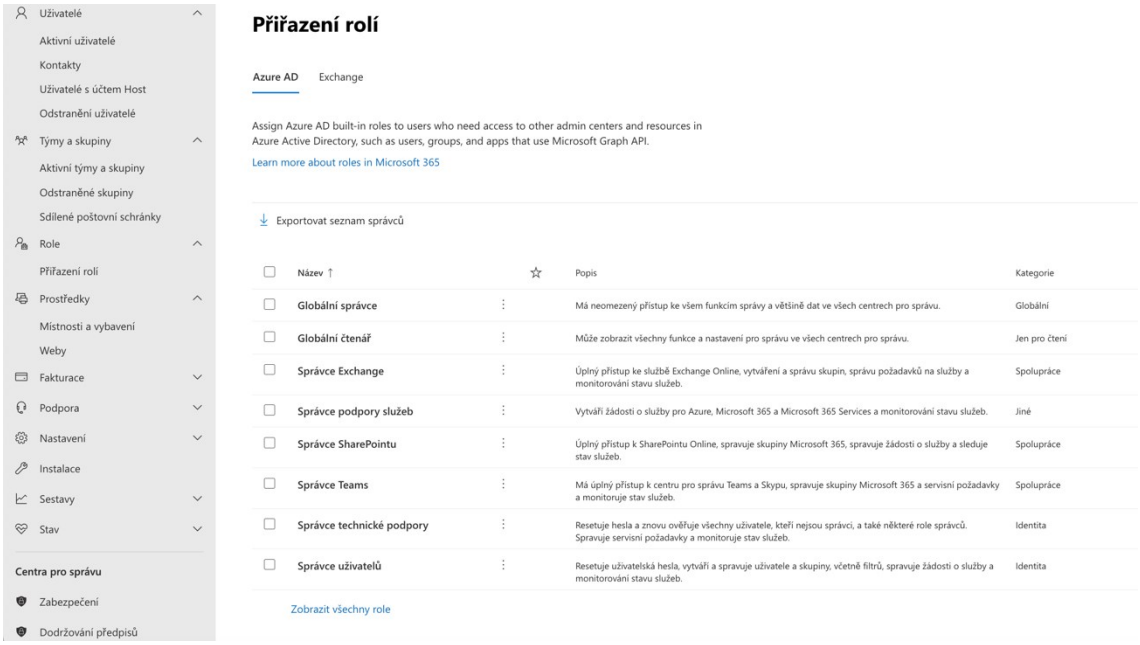
Instalace uživatelské stanice zahrnuje následující kroky

- Instalace operačního systému – zpravidla Windows Professional v aktuální verzi, nyní verze 11. Administrátorům může pomoci automatizace tohoto procesu, kdy se operační systém pomocí upraveného Image balíčku, který se spustí po připojení počítače k síti, připojí do domény a následně nainstaluje aktualizace a vybraný software. To vše automaticky.
- Windows 10 pomocí instalačního balíčku připojí operační systém administrátor do domény, následně pojmenuje zařízení. Může být předem definováno směrnicí, například zkratka oddělení a příjmení uživatele.
- Dalším krokem je zadání přihlášení k WiFi přes doménové jméno uživatele do zaheslované firemní sítě.
- Aktivace Windows pomocí zakoupeného licenčního klíče.
- Instalace používaných aplikací ve firmě (platí v případě, že administrátor nepoužil Image balíček. Mezi nejčastěji používané aplikace patří aplikace internetových prohlížečů, aplikace pro čtení PDF souborů, čtení ZIP souborů, antivirový software, Office aplikace, aplikaci pro přehrávání videí, instalace aplikace tiskáren.
- Nastavení VPN v rámci operačního systému pro možnost vzdáleného připojení mimo firemní doménu. Následně vytvoření zástupce na ploše pro přístup na vzdálenou plochu terminálů.
- V ideálním případě firma zálohuje data, v takovém případě je potřeba nastavit zálohování složek (plochy, stažených souborů nebo dokumentů na úložiště, například OneDrive daného uživatele).
- Konfigurace poštovního klienta, například Outlooku. Konfiguraci zahrnuje přihlášení uživatele do aplikace a připojení mailboxu zaměstnance, aktivace Office balíčku, test odeslané a příchozí pošty, nastavení firemních bezpečnostních politik (například dvoufaktorové ověřování při přístupu do aplikace).
- Instalace tiskáren, nastavení výchozí tiskárny a provedení testovacího tisku.
- Nastavení a přidání uživatele do skupin (například kolegove@, info@ a další).

4.2.2 Přidání nového uživatele v cloudových službách Microsoftu

Firmy využívající cloudové předplatné softwaru Office 365, Microsoft 365 nebo Microsoft Azure od společnosti Microsoft mají k dispozici tzv. tenant, tedy admin prostředí všech uživatelů a služeb na jednom místě. Díky tomu je správa uživatelů a bezpečnostních politik jednotlivých aplikací a dat v nich daleko jednodušší než při správě tzv. on-premise řešení.

V administrátorském rozhraní na **Chyba! Nenalezen zdroj odkazů.**, kde má oprávněná osoba (ve většině případů administrátor IT) přístup, je několik rolí, které můžou uživatelé v organizaci mít. Role jsou od nejnižších (běžní uživatelé) po ty nejvyšší (globální administrátor) rozděleny dle struktury společnosti a samotného IT oddělení ve firmě. Rozdělení těchto rolí určuje, kdo je za prostředí Microsoft cloudových služeb zodpovědný.

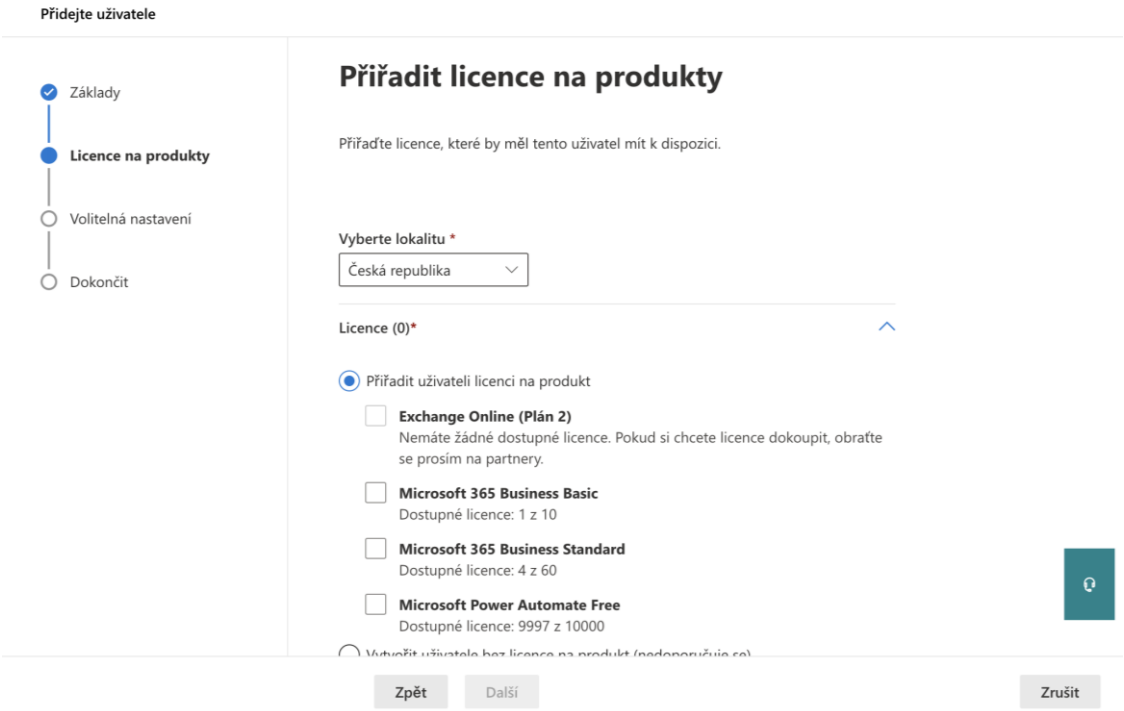


Obr. 4.1 Ukázka admin prostředí Microsoft 365

Zdroj: vlastní zpracování 2022

Vytvoření nového uživatele (zaměstnance) do Microsoft 365/ Office 365 zahrnuje následující kroky

- Přihlášení IT administrátora na webovém rozhraní office.com do rozhraní správce.
- Vytvoření nového uživatele v položce Aktivní uživatelé – přidat uživatele.
- Vyplnění údajů o uživateli – jméno, příjmení, telefonní číslo, zobrazované jméno, e-mail, generování hesla.
- Přiřazení Microsoft 365/ Office 365 licence uživatelskému účtu (typ licence je obvykle přiřazen dle pracovní pozice). Licence určené pro firmy jsou například Business Basic, Business Standard nebo Business Premium. Zobrazeno na Obr. *4.1*.
- Zařazení uživatele do doménových skupin.
- Bezpečné předání uživatelského účtu uživateli.

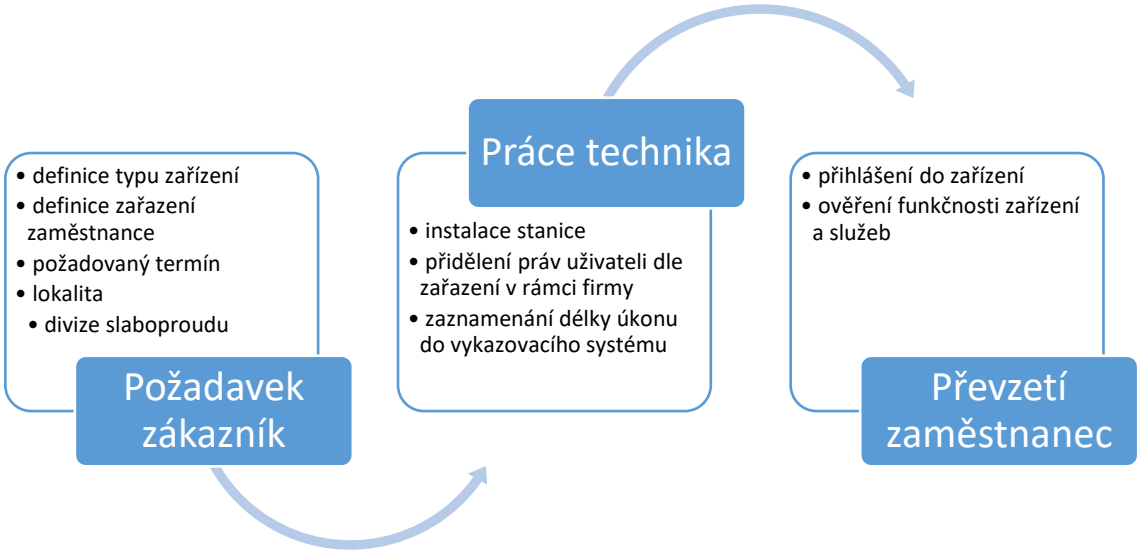


Obr. 4.1 Ukázka kroku přiřazení licencí uživateli z admin prostředí Microsoft 365

Zdroj: vlastní zpracování 2022

4.3 Zadávání požadavků do Helpdesk systému

Helpdesk je systém pro zadávání požadavků uživatelů. Cílem helpdesku je umožnit uživatelům zadat požadavky na podporu nebo pomoc při řešení problémů různého charakteru. To vše jednoduše, efektivně a na jednom místě. Způsob využití této aplikace závisí na oboru, kde je využívána. Ve firmách je často využíván jako vykazovací systém práce zaměstnanců, kteří pracují například externě, nebo jejich finanční ohodnocení závisí na počtu odpracovaných hodin. Typickou pozicí může být programátor, vývojář, IT technik, fakturantka, údržbář a další pozice závislé na výkonu. Naopak uživatelé do helpdesku zadávají požadavky na pracovníky konkrétních oddělení. **Chyba! Nenalezen zdroj odkazů.** znázorňuje proces výše zmíněné instalace počítače pro nového uživatele. Asistentka zadá pokyn na IT technika, formou ticketu. Zadá ticketu požadovaný termín splnění, prioritu (nízká, vysoká, urgentní) a informace potřebné pro technika k dokončení úkonu. Z pohledu technika, který takový ticket od uživatele obdrží je cílem ho včas a správně splnit. Práce technika začíná otevřením ticketu, zpracováním zadání, vykázáním stráveného času na zadaném požadavku a uzavření ticketu. Po uzavření obdrží zadávající upozornění (například formou e-mailu), že je zadaný úkol dokončen a připraven k převzetí.



Obr. 4.2 Proces vybavení koncové stanice pro nového zaměstnance

Zdroj: vlastní zpracování 2022

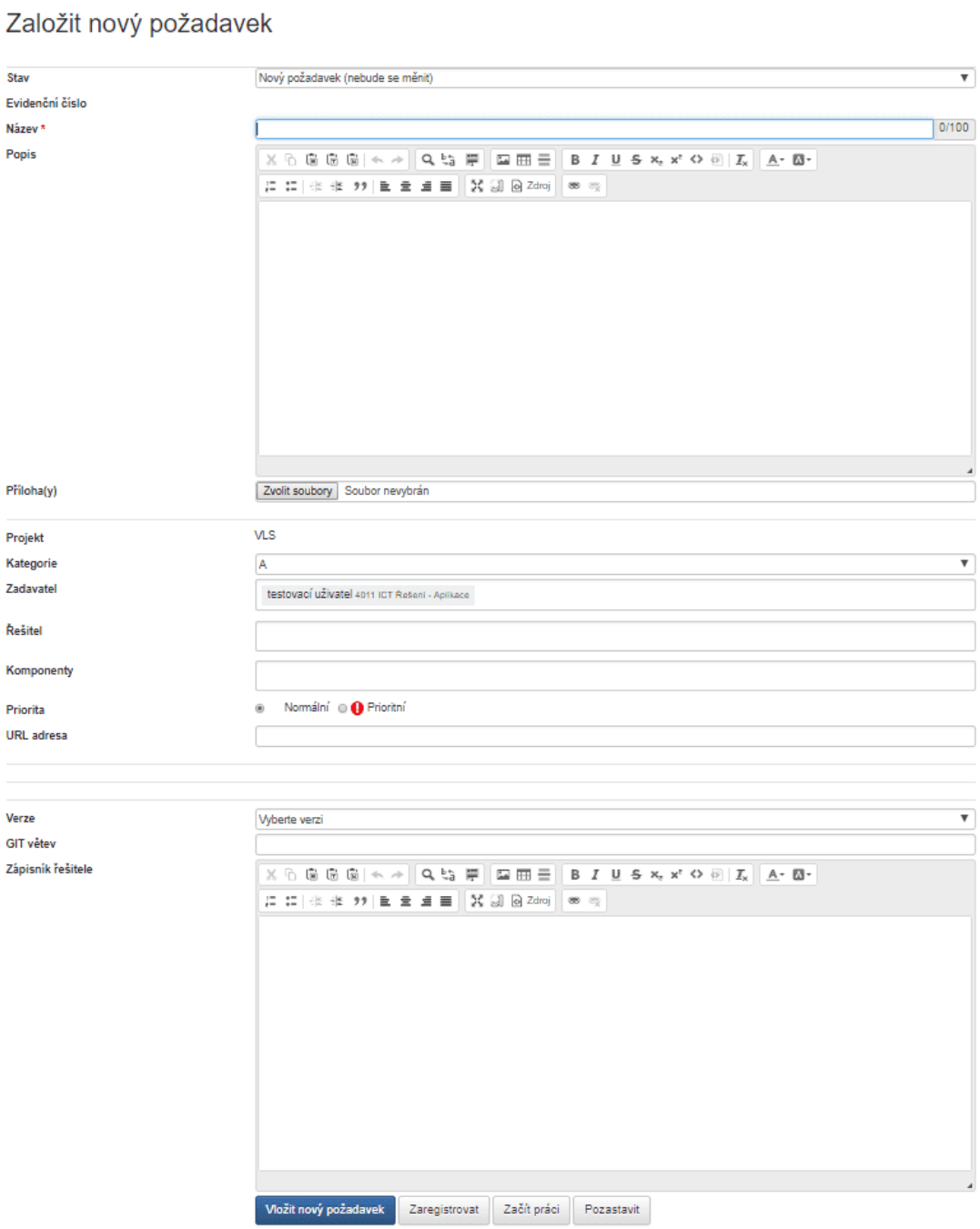
Druhy helpdesk systémů

- **Externí helpdesk**

  Takto je označován helpdesk, který poskytuje firma dalším stranám – zákazníkům, dodavatelům, spolupracujícím společnostem. V oblasti IT je často helpdesk poskytován IT firmou zákazníkovi, který si IT firmu najímá na externí správu IT. Helpdesk v tomto případě slouží nejen jako portál na zadávání požadavků zákazníka, ale také se z něj dají exportovat vykázané práce techniků na daného zákazníka, které mohou sloužit například jako podklady pro následnou fakturaci, a důkazní materiály pro zákazníka, že fakturace odpovídá odvedené práci.

- **Interní helpdesk**

  Forma interního helpdesku znamená, že aplikaci firma poskytuje svým zaměstnancům. Do něhož zaměstnanci zadávají například žádost o dovolenou, žádost o přezutí firemního vozu, potřebu nového vybavení k práci nebo instalaci hardwaru či softwaru. Výhodou firem, které pracují s helpdesk systémem je přehled o vytíženosti zaměstnanců, tvorba reportů, přehledy nejčastěji zadávaných požadavků. Vzorový systém helpdesku popisuje **Chyba! Nenalezen zdroj odkazů.**



Obr. 4.3 Ukázka helpdesk formuláře

Zdroj: [64]

- **Helpdesk aplikace**

  Firmy, které se zabývají službami zákazníkům a prodejem zboží, mají zřízená samostatná helpdesková pracoviště [65]. Ta slouží pro služby zákazníkům z oblastí reklamací, dotazů zákazníků ke zboží, opravy zboží nebo evidence komunikace se zákazníkem (například formy dotazníků). Výhodou samostatné

helpdeskové aplikace [66] je, že sdružuje klienty společnosti v jednom adresáři, zobrazuje historii požadavků či reklamací zákazníka, nabízí možnost prioritizace ticketů nebo vyhodnocování SLA (cyklus ticketu od zadání po vyřešení/uzavření) [67]. V samostatných helpdesk aplikacích se dá velké množství věcí automatizovat, což vede k šetření finančních prostředků společnosti a lidské práce. Další výhodu je možnost napojení na aplikace třetích stran, což může být například CRM systém, ERP systém a další.

5 Zhodnocení návrhu

V následující kapitole se zabývám zhodnocením vybraných typových příkladů informačních procesů ve společnosti. Definuji návrhy na zlepšení těchto procesů z několika pohledů – zvýšení efektivnosti, zlepšení zabezpečení nebo zkvalitnění procesu v rámci nasazení nové technologie.
Vyhodnocuji návrh zálohování a bezpečnosti ve společnosti a jako druhý příklad hodnotím možnosti pro zefektivnění práce administrátorů. Tím cílím na optimalizaci práce administrátorů a automatizaci některých postupů. Návrhy na zlepšení byli konzultovány s odborníkem na implementaci cloudových služeb a bezpečnost Ing. Filipem Langem. Jedná se zároveň o certifikovaného etického hackera.

5.1 Zhodnocení návrhu na zajištění bezpečnosti ve firmě

Jak již bylo výše zmíněno, data jsou pro společnost velmi důležitá. Jejich hodnota je pro většinu firem vysoká a jejich případná ztráta může způsobit nemalé problémy. Pro vyšší míru zabezpečení by s ve společnosti mohli implementovat níže uvedené bezpečnostní požadavky, které by zvýšili zabezpečení dat, omezili přístup k datům uživatelům, kteří k nim nemusí mít přístup a omezili faktor lidské chybovosti. Lidský faktor je totiž nejslabším článkem bezpečnostních systémů. Uživatelé pracují mnohdy zmateně, neukázněně, což vede k případům jako je úspěšný zákrok phishingového pokusu o získání dat či finančních prostředků. V případě, že by přesto došlo k napadení

společnosti hackere a zhrozila ztráta dat, myslíme na zálohování, ze kterého se při správném nastavení data dají z poslední zálohy bez větší námahy obnovit zpět tak, aby se ztracená data nahrála zpět do systémů. Vyšší míra zabezpečení povede také k zachování důvěrnosti dat. Zajistí lepší průkaznost, díky logování akcí v jednotlivých systémech.

Ke zvýšení bezpečnosti vedou následující kroky

- Pravidelné vzdělávání nejen administrátorů ale hlavně zaměstnanců – můžeme rozdělit na teoretickou a praktickou část, jejíž součástí je ukázka z praxe. Školení může provádět vyškolený zaměstnanec společnosti nebo externí školitel (doporučeno).
- Politika hesel a plošná implementace MFA – uživatelé mají často nastavená hesla, jež se zobrazují na seznamech uniklých hesel, jsou lehce dešifrovatelná nebo zaznamenaná na papírku nalepeném na monitoru. Z tohoto důvodu je dobré zavést ve firmě dvoufaktorové ověřování, nejlépe jako druhý faktor použít firemní mobilní telefon, který má každý zaměstnanec společnosti k dispozici svůj.
  Zdroj: Důležité informace o nasazení pro Azure AD Multi-Factor Authentication | Microsoft Docs
- Aktualizace systémů na nejnovější ověřené verze – vývojáři globálně poskytovaných softwarů v dnešní době velice rychle reagují na prolomené šifry hackerů a na software vydávají formou nových verzí bezpečnostní záplaty. Proto je dobré mít vždy aktuální verze systémů, které eliminují riziko napadení systému, uživatelského účtu nebo dat v systému.
- Pravidelné provádění penetračních testů – cílem penetračních testů je definovat rizika, u kterých může dojít k napadení sítě útočníkem. Jedná se o definici konkrétní principů a postupů útoků. Analyzovat můžeme bezpečnost sítě a veškerá síťová zařízení, stanice uživatelů, používané systémy. Vyhodnocení pak poukazuje na možnosti vylepšení stavu sítě, které hackerovi ztíží nebo dokonce znemožní průnik do sítě.
- Nastavení Firewallu – implementace firewallu do sítě rozhoduje o blokaci nebo povolení přístupu do navazované komunikace na předem definovaných pravidel a politik pro síť. Firewall zjednodušeně rozhoduje o tom, koho do sítě pustí a komu přístup zamítne [68].

- Zálohování virtuálních serverů – díky zálohování společnost zajistí kontinuální, tedy nepřerušený provoz. Zálohování může zachránit data společnosti a v případě jejich ztráty zajistit rychlou a nenáročnou obnovu dat. Nejmodernější formou zálohování je zálohovat pomocí backup software. Zálohy samozřejmě potřebují být někam ukládány, v dnešní době například do datových center. Výhodou je flexibilní obnova dat a možnost nastavení individuální retence (tzn. nastavení četnosti záloh).
- Zálohování dat z účtů managementu podniku – kromě zálohování serverů, se také dají v tomto případě zálohovat i uživatelské účty. A to díky cloudové službě společnosti Microsoft. Data z Office účtů můžeme zálohovat zálohovacím softwarem, kterému definujeme, jaká data nás zajímají a jaká data tedy zálohovat, jak často zálohy provádět a kam zálohy ukládat. Použít můžeme například zálohovací software do společnosti Veeam [69].

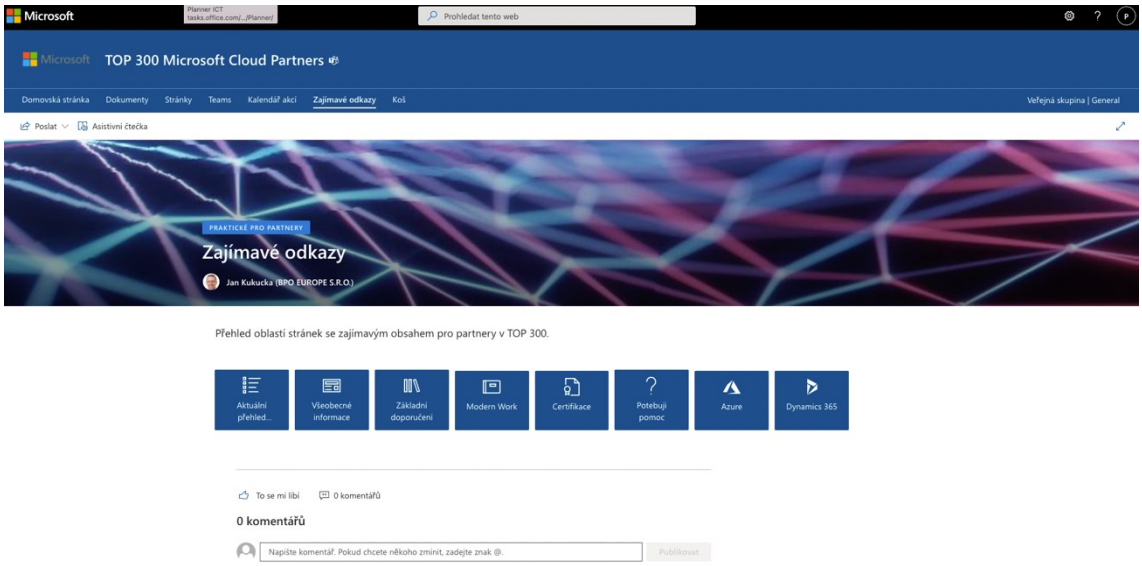
- Filtrování MAC adres – adres, které přistupují k síti. Tím se zamezí možnosti připojení uživatele do sítě přes jiné, než firemní zařízení.
  Zavedení politiky omezení připojení přes veřejné Wi-Fi – uživatelé, kteří nesedí vždy v sídle společnosti a nepřipojují se pouze na ověřenou Wi-Fi, ale dochází k připojení na hotelech, v kavárnách nebo u zákazníků, se mohou připojovat k neověřeným Wi-Fi sítím, bez nutnosti zadání hesla. Pro zvýšení bezpečnosti je možné v tomto uživateli zamezit, a připojit se k internetu pouze přes mobilní data, nebo ověřené Wi-Fi sítě.

5.2 Zhodnocení návrhu zefektivnění práce IT administrátorů

Vzhledem k výše zmíněným často se opakujícím postupům, které administrátoři vykonávají, je ve firmách snaha o co největší automatizaci procesů. Cílem automatizace je ulevit administrátorům od rutinních postupů, což vede k zefektivnění jejich práce a ušetření času při těchto úkonech. Mezi opakující se činnosti můžeme zařadit správu uživatelů, tvorbu nových uživatelských účtů, přihlášení nového zařízení do sítě, ruční zálohování dat aj.
Vhodným nástrojem pro část automatizace může být například AutoPilot od společnosti Microsoft. Tento nástroj umožňuje samoobslužnou hromadnou instalaci na několika

stanicích současně, a to díky Azure konzoli. Nasazení nových zařízení v organizaci, se díky tomuto nástroji stane pro administrátora mnohem jednodušším. V konzoli se předem definují pravidla a směrnice organizace, kterými se systém při nových instalacích řídí. Například omezení přístupu uživateli do firemního e-mailu mimo IP adresu společnosti. Díky funkci AutoPilot administrátor ušetří čas, který dříve potřeboval na kompletní přípravu stanice pro nového uživatele. Pomocí balíčku, který zahrnuje definované politiky a pravidla je instalace natolik jednoduchá, že administrátorovi stačí pouze zapnout nové zařízení se systémem Windows, vše ostatní již zajistí konzole AutoPilota. Celý tento proces tak vyžaduje minimální interakci administrátora do procesu. Podobně, jako například při koupi nového chytrého telefonu.

Dalším návrhem na automatizaci práce administrátorů může být digitalizace návodů k systémům ve společnosti. Fluktuací se administrátor ve firmě často dostává do pozice školitele, jež je nucen pravidelně novým zaměstnancům představovat používané systémy v organizaci, provádět školení jak používat firemní e-mail, jak se bezpečně chovat na internetu, jak se přihlásit do počítače mimo firemní síť nebo jak změnit heslo v jednotlivých aplikacích. Do práce administrátora však tato úloha mnohdy nezpadá a bere mu čas, který potřeboval na správu sítě.
Řešením může být příprava materiálů pro zaměstnance, které budou sloužit jako naučné materiály pro firemní systémy. Forma může být pojata mnoha způsoby. Může se jednat o prezentace, návody se screeny ze systému v PDF, videa nebo zřízení intranetové stránky. Vzhledem k častým aktualizacím aplikací a měnícím se vzhledům aplikací, považuji za nejlepší variantu intranetovou stránku, kde lze informace nejlépe a nejrychleji upravovat v případě, kdy dojde k aktualizacím informací.
Uživatelé tak formou hypertextového odkazu budou přistupovat na web, kde budou mít zpracovány návody pro užívání aplikací nebo nastavení jejich účtů. Portál s návody pro zaměstnance by mohl vypadat jako na **Chyba! Nenalezen zdroj odkazů.**.



Obr. 5.1 Portál s návody pro koncového uživatele

Zdroj: [27]

Závěr

Cílem práce bylo zhodnocení modelů cloudových systémů a jejich služeb. Dále představit možnosti využití v logistických procesech společnosti s návazností na bezpečnost a tyto možnosti zhodnotit. V úvodu se práce věnovala představení logistických procesů, které odráží aktuální stav na trhu a které se stále častěji mění a přetváří tak, aby bylo docíleno spokojenosti zákazníka, využito kapacit podniku a práce byla vykonávána efektivně. Práce se dále věnovala nabídce služeb logistických společností s ohledem na logistickou strategii.

V druhé části práce se věnovala jsou představeny a zhodnoceny cloudové služby a modely. Jsou zhodnoceny výhody a nevýhody cloudových služeb s ohledem na citlivá data společnosti a to, jak je možné realizovat migraci z on-premise řešení do cloudu, jaké jsou výhody migrace a jsou faktory pro úspěšné nasazení těchto služeb.

Pro dosažení cíle práce byla v další kapitole popsána bezpečnost dat, jak s daty bezpečně pracovat a co hrozí firmě v případě zasažení hackerským útokem. V rámci této kapitoly je také popsána prevence před únikem dat, kterou jsou penetrační testy a bezpečnostní analýzy.

Byla sestavena SWOT analýza, která cílí na definici aspektů připravenosti logistické společnosti na schopnost odrazit hackerský útok. Analýza hodnotí slabé a silné stránky, příležitosit a hrozby ve společnosti. Z analýzy vyplynulo, že společnost má dostatek silných stránek, které by mohly útok odrazit, avšak nevynakládá další finanční prostředky na zvýšení úrovně zabezpečení, což vede k tomu, že bezpečnostní technologie budou zaostávat a tím se bude riziko prolomení hackerského útoku časem zvyšovat. Analýza zahrnuje doporučení, které by vedlo k udržení nasazených systémů tak, aby při pokusu o útok ze strany hackera došlo k jeho zamezení.

Zpracovali jsme typové příklady informačních procesů, které jsme považovali za důležité a které jsou součástí většiny podniků. Zaměřili jsme se zejména na procesy zajišťující bezpečnost, ale také na nejčastěji se opakující procesy. Z bezpečnostních procesů bylo zhodnoceno zálohování dat a bezpečná práce s daty. Z nejčastěji se opakujícího procesu byl vybrán proces instalace nového zařízení ve společnosti. Ke každému identifikovanému problému jsme sepsali návrh na vylepšení procesu. Objevené poznatky byly popsány včetně možnosti nasazení. Výsledkem této práce je zjištění, jak hluboce je logistická společnost závislá na informačních systémech a jaké jsou doporučené kroky pro odstranění zranitelnosti systémů a zjednodušení práce IT administrátorů. V neposlední řadě i vzdělávání uživatelů.

Uvedená opatření mají za cíl automatizovat procesy, zefektivnit čas zaměstnanců z řad IT oddělení a vhodně zaškolit zaměstnance společnosti.

Díky mé bakalářské práci se podařilo v nejmenované logistické společnosti zahájit jednání o implementaci MFA a realizovat penetrační test.

Na mou práci by se dalo navázat širším zpracováním procesů zasahujících do informačních a cloudových systémů.

Seznam zdrojů

[1] The Cloud in 2022: Growth, Trends, Market Share & Outlook. *BMC Blogs* [online]. [vid. 2022-04-29]. Dostupné z: https://www.bmc.com/blogs/cloud-growth-trends/

[2] HØYLAND, Sindre, Janne Merete HAGEN a Ruth Østgaard SKOTNES. Exploring the benefits of cloud services and accountability tools from a competitiveness and return on investment perspective. *International Journal of Information Technology and Management* [online]. 2017, **16**(3), 215–236. ISSN 1461-4111. Dostupné z: doi:10.1504/IJITM.2017.085020

[3] SCHOLL, Boris, Trent SWANSON a Peter JAUSOVEC. *Cloud native: using containers, functions, and data to build next-generation applications*. First edition. Sebastopol, CA: O'Reilly Media, 2019. ISBN 978-1-4920-5382-8.

[4] *Koncepce marketingového řízení* [online]. 2017 [vid. 2022-04-29]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Koncepce_marketingov%C3%A9ho_%C5%99%C3%ADzen%C3%AD&oldid=15086992

[5] GROS, Ivan, Ivan BARANČÍK a Zdeněk ČUJAN. *Velká kniha logistiky*. 2016. ISBN 978-80-7080-952-5.

[6] KOUTNÝ, Stanislav. *Struktura logistických procesů ve výrobním podniku* [online]. B.m., 2015 [vid. 2022-04-29]. Jihočeská univerzita v Českých Budějovicích, Ekonomická fakulta. Dostupné z: https://theses.cz/id/8rfyph?info=1;isshlret=ve%3B;zpet=%2Fvyhledavani%2F%3Fsearch%3Dve%26start%3D79#panel_bibtex

[7] PERNICA, Petr. *Logistický management : teorie a podniková praxe* [online]. B.m.: Radix, 1998 [vid. 2022-04-29]. ISBN 978-80-86031-14-9. Dostupné z: https://is.vstecb.cz/publication/17887/cs/Logisticky-management-teorie-a-podnikova-praxe/Pernica

[8] CEMPÍREK, Václav, Rudolf KAMPF a Jaromír ŠIROKÝ. *Logistické a přepravní technologie*. Pardubice: Institut Jana Pernera, 2009. ISBN 978-80-86530-57-4.

[9] BAZALA, Jaroslav. *Logistické činnosti a procesy | Logistická akademie* [online]. [vid. 2022-04-29]. Dostupné z: https://www.logistickaakademie.cz/blog/diskutovana-temata/logisticke-cinnosti-a-procesy

[10] BLANCHARD, Benjamin S. *Logistics engineering and management*. 6th ed. Upper Saddle River, N.J: Pearson Prentice Hall, 2004. ISBN 978-0-13-142915-4.

[11] RINNOVÁ, Kristýna. *Studie zásobovací logistiky ve zvolené společnosti; Ing. Kristýna Rinnová (2016 - 100153) – VUT* [online]. 8. červen 2017 [vid. 2022-04-29]. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/100153

[12] LAMBERT, Douglas M, James R STOCK a Lisa M ELLRAM. *Logistika*. Brno: CP Books, 2005. ISBN 978-80-251-0504-7.

[13] BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy: podnik v informačí společnosti*. Praha: Grada, 2012. ISBN 978-80-247-4307-3.

[14] *Plánování podnikových zdrojů* [online]. 2022 [vid. 2022-04-29]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Pl%C3%A1nov%C3%A1n%C3%AD_podnikov%C3%BDch_zdroj%C5%AF&oldid=20970644

[15] *WMS - Warehouse Management System | Informační systém KARAT* [online]. [vid. 2022-04-29]. Dostupné z: https://www.karatsoftware.cz/wms-warehouse-

management-system.dic
[16] MOSS logistics – Vaše spolehlivá cesta k cíli. *MOSS logistics* [online]. [vid. 2022-04-29]. Dostupné z: https://www.mosslogistics.cz/
[17] *O.K. TRANS PRAHA* [online]. [vid. 2022-04-29]. Dostupné z: https://www.oktrans.cz/cs/uvod
[18] *Cloudové služby – Wikisofia* [online]. [vid. 2022-04-29]. Dostupné z: https://wikisofia.cz/wiki/Cloudov%C3%A9_slu%C5%BEby
[19] *Cloudové služby na vzestupu, o miliardový byznys jde i v Česku - Novinky.cz* [online]. [vid. 2022-04-29]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/cloudove-sluzby-na-vzestupu-o-miliardovy-byznys-jde-i-v-cesku-40337663
[20] What Is Cloud Computing? Definition, Benefits, Types, and Trends. *Toolbox* [online]. [vid. 2022-04-29]. Dostupné z: https://www.toolbox.com/tech/cloud/articles/what-is-cloud-computing/
[21] *Cloud computing* [online]. 2022 [vid. 2022-04-29]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Cloud_computing&oldid=20828489
[22] O2 Datové centrum | Housing pro firemní servery. *O2* [online]. [vid. 2022-04-29]. Dostupné z: https://www.o2.cz/firmy-a-organizace/it-reseni/datove-centrum
[23] S.R.O, PIXMAN. *Datové centrum DC TOWER - bezpečný český server housing* [online]. [vid. 2022-04-29]. Dostupné z: https://www.cra.cz/datove-centrum-dc-tower
[24] *Datové centrum Silo | Efektivní ICT od NWT* [online]. [vid. 2022-04-29]. Dostupné z: https://ict.nwt.cz/produkty/datove-centrum-a-cloud/datove-centrum-silo/
[25] *Datové centrum | ALEF* [online]. [vid. 2022-04-29]. Dostupné z: https://www.alef.com/cz/datove-centrum.c-8.html
[26] SHIVAM, Kumar. A Walk through on IaaS, PaaS and SaaS. *Medium* [online]. 28. květen 2018 [vid. 2022-04-29]. Dostupné z: https://kumarshivam-66534.medium.com/a-walk-through-on-iaas-paas-and-saas-7e8a4e4793fb
[27] *Microsoft – cloud, počítače, aplikace a hry* [online]. [vid. 2022-04-29]. Dostupné z: https://www.microsoft.com/cs-cz
[28] Free Cloud Computing Services - AWS Free Tier. *Amazon Web Services, Inc.* [online]. [vid. 2022-04-29]. Dostupné z: https://aws.amazon.com/free/
[29] Data Centers - Google. *Google Data Centers* [online]. [vid. 2022-04-29]. Dostupné z: https://www.google.com/about/datacenters/
[30] *Šest varovných signálů v zabezpečení při hledání perfektního cloudového úložiště* [online]. [vid. 2022-04-29]. Dostupné z: https://www.microsoft.com/cs-cz/microsoft-365/business-insights-ideas/resources/6-security-red-flags-when-identifying-the-perfect-cloud-storage-solution
[31] AUTOCONT. *AUTOCONT a.s. | AUTOCONT* [online]. [vid. 2022-04-29]. Dostupné z: https://www.autocont.cz/
[32] *Registrace domény již od 49 Kč u největšího registrátora | FORPSI.COM | FORPSI.COM* [online]. [vid. 2022-04-29]. Dostupné z: https://www.forpsi.com/domain/?gclid=CjwKCAjwur-SBhB6EiwA5sKtjppe00BQcEBZ2op8lQ6A6-On5fLWxFhkoQbIfvQ8GXHBHYQd13xo3BoCDPQQAvD_BwE
[33] *Kontakt ČMIS* [online]. [vid. 2022-04-29]. Dostupné z: https://www.cmis.cz/kontakt
[34] Získejte cloud na míru. *TOTAL SERVICE* [online]. [vid. 2022-04-29]. Dostupné z: https://www.totalservice.cz/cloudova-infrastruktura/
[35] *Poskytovatelé cloud computingu Top 15 poskytovatelů služeb cloud computingu* [online]. [vid. 2022-04-29]. Dostupné z: https://cs.education-wiki.com/cs.education-wiki.com/3289454-cloud-computing-providers

[36] Public Cloud Providers | Overview on Top 7 Public Cloud Providers. *EDUCBA* [online]. 23. srpen 2020 [vid. 2022-04-29]. Dostupné z: https://www.educba.com/public-cloud-providers/
[37] *BitTitan MigrationWiz | Migrate to Microsoft 365, Exchange, and G Suite* [online]. [vid. 2022-04-30]. Dostupné z: https://www.bittitan.com/
[38] Co je to tenant? *Office 365* [online]. 5. říjen 2018 [vid. 2022-04-30]. Dostupné z: https://ms-office-365.cz/co-je-to-tenant/
[39] BRIANBLANCHARD. *Vytvoření konzistentního hybridního cloudu - Cloud Adoption Framework* [online]. [vid. 2022-04-30]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/cloud-adoption-framework/ready/considerations/hybrid-consistency
[40] *Trust federation* [online]. 2022 [vid. 2022-04-30]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Trust_federation&oldid=1082214602
[41] What is a DNS MX record? *Cloudflare* [online]. [vid. 2022-04-30]. Dostupné z: https://www.cloudflare.com/learning/dns/dns-records/dns-mx-record/
[42] Přemýšlíte vážně o firemním cloudu? Tady jsou nejčastější otázky, na které se nás firmy ptají. *O2* [online]. 23. září 2020 [vid. 2022-04-30]. Dostupné z: https://blog.o2.cz/2020/09/23/premyslite-vazne-firemnim-cloudu-tady-jsou-nejcastejsi-otazky-ktere-se-nas-firmy-ptaji/
[43] *[IT Systems] Data znamenají moc | Data & Business* [online]. [vid. 2022-04-30]. Dostupné z: https://www.databusiness.cz/2021/11/02/it-systems-data-znamenaji-moc/
[44] *Data a soubory nezálohuje 40 % Čechů* [online]. [vid. 2022-04-30]. Dostupné z: https://blog.avast.com/cs/data-a-soubory-nezalohuje-40-procent-cechu
[45] *Obecné nařízení o ochraně osobních údajů (GDPR): Úřad pro ochranu osobních údajů* [online]. [vid. 2022-04-30]. Dostupné z: https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr/ds-3938/p1=3938
[46] BATAMIG. *Co je Azure Information Protection (AIP)?* [online]. [vid. 2022-04-30]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/information-protection/what-is-information-protection
[47] What is Multi-Factor Authentication (MFA)? | OneLogin. *One Login* [online]. [vid. 2022-04-30]. Dostupné z: https://www.onelogin.com/learn/what-is-mfa
[48] *Vícefaktorové ověřování (MFA) – zabezpečení od Microsoftu* [online]. [vid. 2022-04-30]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/identity-access-management/mfa-multi-factor-authentication
[49] PETRELSIK. *Bezpečnost a penetrační testy – díl první | Efektivní ICT od NWT* [online]. 11. červen 2019 [vid. 2022-04-30]. Dostupné z: https://ict.nwt.cz/blog/bezpecnost-a-penetracni-testy-dil-prvni/
[50] PETRELSIK. *Pozor na podvodné aplikace! Phisheři se snaží obcházet Office365 MFA | Efektivní ICT od NWT* [online]. 3. červen 2020 [vid. 2022-04-30]. Dostupné z: https://ict.nwt.cz/blog/pozor-na-podvodne-aplikace-phisheri-se-snazi-obchazet-office365-mfa/
[51] PETRELSIK. *Jak probíhá analýza IT sítě | Efektivní ICT od NWT* [online]. 25. červen 2019 [vid. 2022-04-30]. Dostupné z: https://ict.nwt.cz/blog/jak-probiha-analyza-it-site/
[52] *Have I Been Pwned: Check if your email has been compromised in a data breach* [online]. [vid. 2022-04-30]. Dostupné z: https://haveibeenpwned.com/
[53] PETRELSIK. *Do šestice všeho dobrého – nový certifikát Manažer Kybernetické bezpečnosti „on board“ | Efektivní ICT od NWT* [online]. 7. leden 2022 [vid. 2022-04-30]. Dostupné z: https://ict.nwt.cz/blog/do-sestice-vseho-dobreho-novy-certifikat-manazer-kyberneticke-bezpecnosti-on-board/

[54] *ISO/IEC 27001* [online]. 2021 [vid. 2022-04-30]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=ISO/IEC_27001&oldid=20327591
[55] GravityZone Ultra. *Bitdefender.cz* [online]. [vid. 2022-04-30]. Dostupné z: https://www.bitdefender.cz/bitdefender-gravityzone-ultra
[56] Fortinet Centrum Valvera. *Valvera* [online]. [vid. 2022-04-30]. Dostupné z: https://www.valvera.cz/
[57] BOUSKAP@SAMURAJ-CZ.COM, Petr Bouška-Samuraj; e-mail: Fortinet FortiGate < články -> SAMURAJ-cz.com. *SAMURAJ-cz.com* [online]. [vid. 2022-04-30]. Dostupné z: https://www.samuraj-cz.com/clanek/fortinet-fortigate/
[58] PETRELSIK. *Nový trend: Kybernetické útoky na nemocnice a zdravotnická zařízení | Efektivní ICT od NWT* [online]. 18. březen 2020 [vid. 2022-04-30]. Dostupné z: https://ict.nwt.cz/blog/novy-trend-kyberneticke-utoky-na-nemocnice-a-zdravotnicka-zarizeni/
[59] *Microsoft v Česku zvýšil tržby na 1,72 miliardy korun. Operační systém Windows používá 96 procent lidí | Hospodářské noviny (HN.cz)* [online]. [vid. 2022-04-30]. Dostupné z: https://byznys.hn.cz/c1-66104220-microsoft-v-cesku-zvysil-trzby-na-1-72-miliardy-korun-operacni-system-windows-pouziva-96-procent-lidi
[60] *Český trh cloudových služeb v roce 2019 | CLOUD & BACKUP NETWORK NEWS* [online]. 28. září 2020 [vid. 2022-04-30]. Dostupné z: https://www.cb-nn.com/cesky-trh-cloudovych-sluzeb-v-roce-2019/
[61] *Fluktuace zaměstnanců: Jak jí zabránit? | Průvodce podnikáním | ČSOB* [online]. 4. únor 2021 [vid. 2022-04-30]. Dostupné z: https://www.pruvodcepodnikanim.cz/clanek/fluktuace-zamestnancu/
[62] *BLOG: V čele digitální proměny pro lepší budoucnost – Microsoft News Center* [online]. [vid. 2022-04-30]. Dostupné z: https://news.microsoft.com/cs-cz/features/blog-jste-pripraveni-stanout-v-cele-digitalni-promeny-a-zasadit-se-o-lepsi-budoucnost/
[63] *Zálohování dat - jak vytvořit datovou zálohu* [online]. [vid. 2022-04-30]. Dostupné z: https://www.acronis.cz/kb/zalohovani-dat/
[64] MKALETA. *ServisDesk | Efektivní ICT od NWT* [online]. 22. únor 2019 [vid. 2022-04-30]. Dostupné z: https://ict.nwt.cz/produkty/informacni-systemy-a-aplikace/servicedesk/
[65] *Technická podpora* [online]. 2022 [vid. 2022-04-30]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Technick%C3%A1_podpora&oldid=21056618
[66] Daktela Helpdesk. *Daktela* [online]. [vid. 2022-04-30]. Dostupné z: https://www.daktela.com/callcentrum/helpdesk/
[67] *Service-level agreement* [online]. 2021 [vid. 2022-04-30]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Service-level_agreement&oldid=20343312
[68] *Co je to firewall?* [online]. [vid. 2022-04-30]. Dostupné z: https://www.eset.com/cz/firewall/
[69] *VEEAM: Zálohování ve virtualizovaném prostředí | Odborná sekce | 3S.cz* [online]. [vid. 2022-04-30]. Dostupné z: https://www.3s.cz/cs/odborna-sekce/detail/id/132-veeam-zalohovani-ve-virtualizovanem-prostredi

Seznam grafických objektů

Obr. 1.1 Schéma logistického procesu 12
Obr. 1.2 Polarizace logistických strategií na příkladu retailingových firem 16
Obr. 2.1 Architektura cloud computingu 20
Obr. 2.2 Rozdělení aplikačních služeb dle druhu modelů cloudu 21
Obr. 2.3 Porovnání služeb globálních cloudových poskytovatelů 24
Obr. 3.1 Proces druhého faktoru ověření pomocí bezpečnostního tokenu 29
Obr. 3.2 Ukázka webu pro zjištění úniku hesel 32
Obr. 3.3 SWOT analýza zabezpečení podniku 36
Obr. 4.1 Ukázka admin prostředí Microsoft 365 41
Obr. 4.2 Proces vybavení koncové stanice pro nového zaměstnance 43
Obr. 4.3 Ukázka helpdesk formuláře 44
Obr. 5.1 Portál s návody pro koncového uživatele 49

Graf 4.1 Nejčastější důvody ztráty dat 38

Tab. 1.1 Rozdělení logistický činností dle jejich důležitosti 15

Seznam zkratek

Iaas	Infrastructure as a service
Paas	Platform as a service
Saas	Software as a service
WMS	Warehouse Management System
DNS	Domain Name Systém
MX	Mail Exchange
GDPR	General Data Protection Regulation
SWOT	Strenghts Weaknesses Opportunities Threats
IT	Information Technology
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning

Autor/ka BP	**Pavlína Záhorovská**
Název BP	**Využití cloudových služeb v logistické společnosti s ohledem na bezpečnost dat**
Studijní program	**IPL**
Rok obhajoby BP	**2022**
Počet stran	49
Počet příloh	0
Vedoucí BP	doc. Dr. Ing. Oldřich Kodym
Anotace	Tato bakalářská práce se zabývá zhodnocením využití cloudových služeb v logistické společnosti. V rámci ní je analyzována také práce s daty uživatelů ve firmě a jejich bezpečnost v cloudu. Jsou zkoumány cloudové systémy a nabízené služby globálních provozovatelů cloudových služeb. Jsou popsány informační systémy, které používá smyšlená logistická firma, a to včetně typových příkladů, procesů jimi podpořenými. Takto zjištěné informace jsou zasazeny do prostředí logistické společnosti s návrhem jejich efektivního využití. V závěrečné části jsou shrnuta doporučení pro provoz cloudových služeb s ohledem na bezpečnost dat v oblasti podnikání logistické společnosti.
Klíčová slova	Logistické procesy, cloud, bezpečnost, logistická společnost, procesy
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	