VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

OCHRANA DAT V ORGANIZACI POMOCÍ DLP (DATA LOSS PREVENTION) ŘEŠENÍ

DLP SOLUTION AS AN ORGANIZATION DATA PROTECTION TOOL

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Jitka Drápalíková

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Sedlák

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Jitka Drápalíková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2018/19

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

Ochrana dat v organizaci pomocí DLP (Data Loss Prevention) řešení

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Navrhnout a představit možnost ochrany dat v organizaci pomocí DLP (Data Loss Prevention) řešení.

Základní literární prameny:

ANONYMOUS. Maximální bezpečnost. 4. vyd. Praha: Softpress, 2004. ISBN 80-86497-65-8.

DOBDA, Luboš. Ochrana dat v informačních systémech. Praha: Grada, 1998. ISBN 80-7169-479-7.

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

DOUCEK, Petr. Řízení bezpečnosti informací. 2. přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

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

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

V Brně dne 28.2.2019

L. S.

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

Abstrakt

Bakalářská práce se zabývá vypracováním návrhu ochrany dat pomocí technologie Data Loss Prevention pro konkrétní organizaci. Teoretická část se věnuje problematice dat ve firemním prostředí a samotné technologii DLP. Práce také pokrývá porovnání DLP produktů na trhu, výběr řešení, jeho rozsah, návrh nastavení i kalkulaci.

Klíčová slova

ochrana dat, Data Loss Prevention, DLP, únik dat, interní únik dat, externí únik dat, bezpečnost dat, bezpečnost informací, opatření

Abstract

The bachelor thesis deals with elaboration of data protection proposal using Data Loss Prevention technology for a particular organization. The theoretical part is focused on data problematics in company's environment and the DLP technology itself. The work also covers the comparison of DLP products on the market, selection of the product, its scope, proposal of setting and calculation.

Key words

data protection, Data Loss Prevention, DLP, data leakage, data loss, information exposure, internal data leakage, internal threat, external data leakage, external threat, information security, remedy

Bibliografické citace

DRÁPALÍKOVÁ, Jitka. *Ochrana dat v organizaci pomocí DLP (Data Loss Prevention) řešení* [online]. Brno, 2019 [cit. 2019-05-06]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119826. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

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

V Brně dne 24. 4. 2019

.....

podpis studentky

Poděkování

Za odborné vedení děkuji Ing. Petru Sedlákovi, vedoucímu bakalářské práce. Děkuji také mamince za její nekonečnou podporu. Poděkování patří i Bc. Michalovi Mezerovi MSc. a Bc. Jakubovi Mazalovi za předané zkušenosti, čas a ochotu k diskusím o problematice DLP.

OBSAH

ÚVOD

Data v konkurenčním boji organizací na trhu nabírají na důležitosti. Organizace si střeží svá výrobní tajemství, obchodní plány, osobní data i citlivá data zákazníků. V souvislosti s vydáním GDPR důležitost chránit osobní údaje nabírá ještě více na významu.

Příčinou úniku dat z organizace může být vnější i vnitřní útočník. Případy, kdy hackeři prolomili bezpečnostní opatření organizace a zcizili citlivá data, jsou známé. Organizace ale často opomíjejí riziko vnitřního útočníka. Osoby, která má k datům legitimní přístup. Zatímco dříve bylo pro zaměstnance poměrně obtížné z firmy odnést konkurenci data uložená v kartotéce, dnes mohou být celé rozsáhlé složky jedním kliknutím během sekundy v nesprávných rukou.

Společnosti se snaží držet krok s digitalizací, jež jim přináší mnoho výhod, ale také mnoho nástrah v podobě bezpečnostních hrozeb, jímž je třeba čelit vhodnými opatřeními. Technologie DLP (Data Loss Prevention) může být jedním z mozaiky opatření. DLP řešení může být velkým pomocníkem při ochraně dat, které může společnosti ušetřit velké finanční náklady a ztráty vzniklé případným datovým únikem. Klíčové je vhodné nastavení DLP a integrace technologie do stávajícího systému bezpečnosti informací a firemních procesů.

.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem práce je navrhnout systém ochrany dat v konkrétní organizaci pomocí DLP (Data Loss Prevention) řešení. Konkrétní organizace plánuje zavedení DLP, ale neformulovala přesné požadavky. Dílčím cílem tedy bude provedení analýzy organizace, zformulování požadavků na dané DLP řešení, vybrání konkrétního řešení a určení rozsahu implementace, tak aby bylo řešení z hlediska ekonomického i funkčního nejlepší variantou pro organizaci. Dalším dílčím cílem je vypracování plánu projektu implementace a návrhu samotného nastavení DLP. Je důležité, aby byl návrh v praxi realizovatelný, odpovídal požadavkům investora a jeho cena korespondovala s přínosy pro organizaci.

Práce je rozdělena do tří částí. Teoretická východiska práce se věnují základní teorii, jejíž znalost je nutným předpokladem pro pochopení problematiky úniků dat a technologie DLP, jež je specializovaným nástrojem ochrany proti datovým únikům. Druhá část je věnována analýze organizace. Analytická část obsahuje analýzu vybraných dokumentů ISMS, popis práce s daty, požadavky investora a popis komunikační infrastruktury. Třetí část se věnuje samotnému výběru vhodného DLP řešení včetně jeho kalkulace, návrhu postupu implementace i návrhu nastavení samotného DLP.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této části bakalářské práce je problematika ochrany dat na základě užitých literárních pramenů vysvětlena v teoretickém rámci.

1.1 Základní definice užitých pojmů

Tato část je věnována vysvětlení základních pojmů, které se frekventovaně vyskytují v dalších částech práce. Jejich znalost je klíčová pro celkové pochopení problematiky.

IT (Information Technology) - informační technologie

ICT (Information Communication Technology) - informační a komunikační technologie

IS (Information System) – informační systém

Data - chápeme jako posloupnost znaků, které samy o sobě mohou a nemusí nést význam. Lze je zaznamenat v digitální formě v paměti počítače, graficky na papír nebo zapamatované v mozku člověka [1]. Při ochraně dat obecně je třeba brát v úvahu všechny možné formy záznamu dat [2].

Informace - data se mohou stát informací za předpokladu, že uživateli dávají význam a snižují jeho neznalost. Např. řada číslic se stává informací, pokud je uživateli známo, že představuje peněžní částku. [1; 3; 4]

Znalosti - vznikají na základě informací pomocí přechozích zkušeností a již nabytých znalostí [1; 4].

Důvěrnost (Confidentiality) - vlastnost udávající, že informace není dostupná nebo není odhalena neautorizovaným osobám, entitám nebo procesům [5].

Integrita (Integrity) - zajištění správnosti a úplnosti informací [5].

Dostupnost (Availability) - vlastnost přístupnosti a použitelnosti na žádost autorizované entity [5].

Bezpečnost informací - ochrana důvěrnosti, integrity a dostupnosti informací. Navíc může také zahrnovat další vlastnosti jako autenticitu (authenticity), odpovědnost (accountability), nepopiratelnost (non-repudiation) nebo spolehlivost (reliability). Pokud mluvíme o bezpečnosti informací, mluvíme tedy i o bezpečnosti dat, jež jsou nositeli informací. [6; 5]

DLP systémy - Označovány jako DLPD (Data Leak Prevention and Detection) či DLP systémy (Data Loss Prevention, někdy také Data Leakage Prevention). V oblasti není jasně vymezena terminologie. Jsou to systémy, které identifikují, monitorují a chrání důvěrná data uvnitř organizace. Zaměřují se na ochranu proti interním hrozbám, které jsou spojeny s únikem dat. [7; 4] V rámci bakalářské práce bude užit termín Data Loss Prevention a jeho zkratku DLP.

Únik dat (data leakage / data loss) - je z hlediska problematiky technologie DLP, jíž je tato práce věnována, situace, kdy citlivá data opustí organizaci jako výsledek neautorizované komunikace skrz komunikační kanály - aplikace, fyzická zařízení nebo síťové protokoly [8; 9; 10].

Interní únik dat - úniky dat způsobeny samotnými zaměstnanci organizací, dodavateli nebo spolupracujícími třetími stranami [10; 7].

Externí únik dat - úniky dat způsobeny útočníky mimo danou společnost - hackery, aktivisty, konkurencí, autory mallwaru apod. [10; 7].

V bakalářské práci se v souvislosti s DLP, či obecně ICT, problematikou mohou vyskytovat některé názvy prvků infrastruktury v anglickém jazyce. Jde o zaběhlé termíny a užívané názvy, a proto nebyly překládány.

1.2 Data ve firemním prostředí

Tato podkapitola má za cíl přiblížit problematiku dat ve firemním prostředí a na základě výzkumů popsat, jaká data jsou z hlediska úniků nejvíce v ohrožení.

1.2.1 Základní typologie dat v organizacích

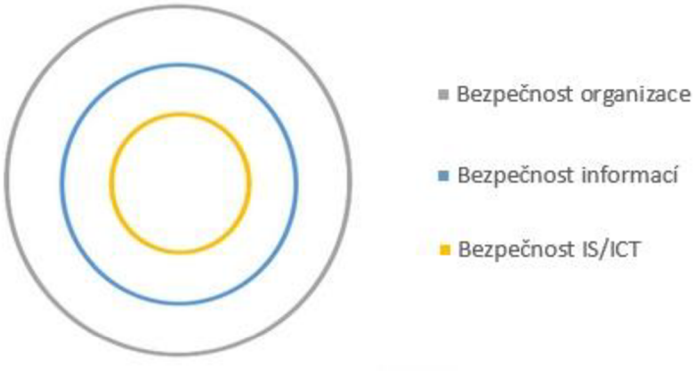
Data řadíme mezi významná aktiva organizace, která se velkou měrou podílí na jejím ekonomickém a tržním zdraví. Ve firemním prostředí můžeme identifikovat následující tři tipy dat, které souvisí s aktivitami podniku:

- **Data o společenských podmínkách podnikání** - zaznamenané známé skutečnosti o vnějších faktorech ovlivňujících činnost organizace (např. sociální, ekonomické a technologické trendy, vývoj cen nákladů, predikce vývoje politické situace).
- **Data o trhu** - data o poptávce po zboží a službách podniku, o stavu konkurence, data o očekávaných fúzích a akvizicích v okolí podniku apod.
- **Interní data podniku** - jsou předpokladem pro správné fungování podniku. Zpravidla popisují jeho interní prostředí (např. finanční plány, informace o pracovní síle, kapitálu, podnikových procesech, data o zákaznících apod.). [11]

Z hlediska bezpečnosti dat největší pozornost vyžadují interní data podniku, která zpravidla chceme chránit nejvíce, protože narušení jejich integrity, dostupnosti a důvěrnosti by společnosti přineslo nejvyšší škody. Interní data je důležité chápat jako množinu dalších typů dat, která mají pro organizaci různou hodnotu a různý účel a tedy i různý stupeň ochrany a přístupu k nim (např. marketingové podklady, účetní data, osobní údaje, výrobní tajemství). Tyto typy dat je nutné identifikovat a zvážit, jakou úroveň bezpečnosti je vhodné zvolit - viz. přiměřená bezpečnost dále. Tuto skutečnost bereme v potaz při identifikaci a následném hodnocení aktiv, které je vstupem do tvorby analýzy rizik, důležitého dokumentu řízení bezpečnosti informací dle ISMS. [2]

1.2.2 Ochrana dat v kontextu bezpečnosti organizace

Ochrana dat je v kontextu organizace velmi specifickým pojmem. Pro správné uchopení problematiky je třeba pochopení širšího kontextu, jež je znázorněn na obrázku níže.



Obrázek 1: Vztah úrovní bezpečnosti v organizaci
Zdroj: vlastní zpracování dle [5]

Nejširším pojmem je **bezpečnost organizace**, které podléhá zajištění bezpečnosti objektů organizace a jejího majetku, řízení přístupu do budov, jejich místností apod., čímž se podílí i na **bezpečnosti informací** a **bezpečnosti IS/ICT**. Kromě dalších oblastí je součástí bezpečnosti organizace i **bezpečnost informací**. Cílem řízení **bezpečnosti informací** je chránit důvěrnost, integritu a dostupnost informací, zachycených nejen v digitální formě. V dnešních organizacích jde zejména o data zaznamenaná v papírové a digitální formě. Patří sem způsob zpracování, uložení a správy nedigitálních dat, jejich skartace, zásady pro poskytování informací osobám mimo organizaci apod. Nejužší oblastí je oblast **bezpečnosti IT/ICT**, která má za úkol chránit pouze ta **aktiva**, která jsou součástí informačního systému firmy, podporovaného informačními a komunikačními technologiemi. [5; 12]

Aktivum (asset) můžeme definovat jako cokoli, co má pro organizaci či jednotlivce nějakou hodnotu, jež může být snížena působením určité hrozby [12]. V oblasti bezpečnosti IT/ICT pod tímto pojmem rozumíme všechny **hmotné** i **nehmotné** komponenty IT/ICT, které mají pro organizaci určitou hodnotu [5]. Hodnota se odvíjí od výše nákladů na pořízení či vývoj aktiva, jeho důležitosti pro chod IT/ICT, výše

prostředků vynaložených na překlenutí případné škody apod. [12]. Mezi **hmotná aktiva** patří zejména **technické prostředky výpočetní techniky** - počítače, tiskárny, datové rozvody, síťové prvky, servery apod. Do **nehmotných aktiv** řadíme **data** (organizací vytvořené nebo převzaté soubory, které jsou důležité pro provoz organizace), **služby** (komunikační a počítačové služby), **programové vybavení** (operační systém počítačů, textové editory, grafické programy, ERP systémy, BI aplikace apod.). [5; 2]

Zranitelnost (vulnerability) je slabé místo aktiva, které může být využito hrozbou pro uplatnění jejího nežádoucího vlivu [2; 5]. **Hrozba** (threat) je potenciální příčina nechtěného incidentu [5]. Je to síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo která může způsobit škodu [2; 6]. Mezi typické hrozby patří lidé, poruchy počítačů, nosičů dat nebo jiných technologických komponent, živelné pohromy, viry, trojské koně a další [5].

Opatření (control) znamená řízení rizika v rámci politik, směrnic, obvyklých postupů nebo organizačních struktur, jehož hlavním cílem je snížení rizika hrozby [2; 5]. Příkladem opatření může být používání hesel při přístupu k systému, omezení fyzického přístupu formou uzamykání objektů a místností, vytvoření záloh datových úložišť, odhlášení uživatele z počítače po určité době nečinnosti, používání bezpečnostních řešení (firewall, antivir, IPS, DLP), vyhodnocování auditních záznamů apod. [5].

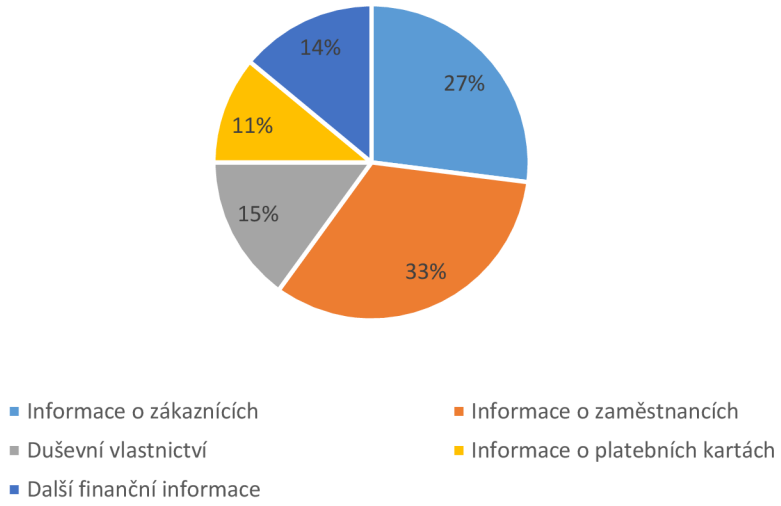
Riziko (risk) je míra ohrožení aktiva. Jde o vyjádření míry nebezpečí, že dojde k využití zranitelnosti aktiva hrozbou, a tak nežádoucímu výsledku vedoucímu ke vzniku škody. [2]

Po výběru vhodných opatření vždy zůstává určitá míra rizika - tzv. **zbytkové riziko**. Pro zbytkové riziko může být nadále hledáno další vhodné opatření, které ale může být příliš nákladné či zbytečné. Další možností je akceptace rizika ze strany vedení organizace. [2]

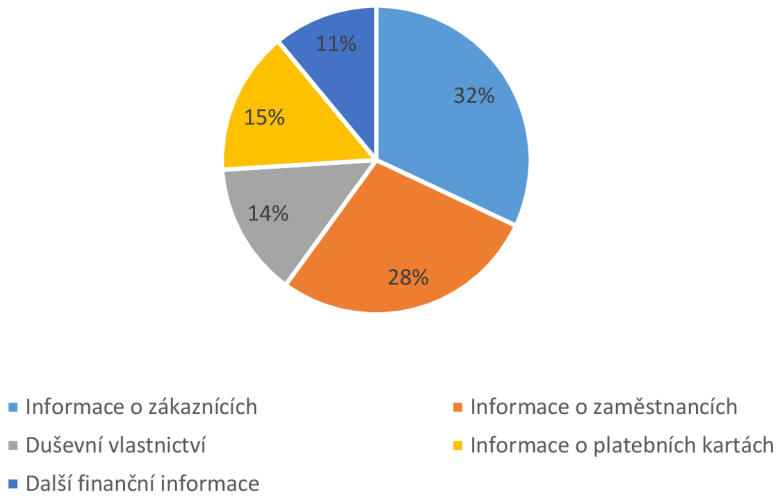
Ochranou dat tedy rozumíme ochranu části nehmotných aktiv IT/ICT, kdy na základě jejich zranitelností a hodnoty vybíráme vhodná opatření, jež dostatečně zmírňují rizika vybraných hrozeb, ale k jejichž zabezpečení musíme přistupovat komplexně (např. přihlížet i k ochraně sítě, ve které se s daty pracuje, k ochraně fyzických nosičů dat se zálohami apod.) [8; 5].

1.2.3 Úniky dat z firemního prostředí

Studie Intel Security z roku 2017 uvádí, že nejčastějším předmětem úniků dat z firemního prostředí, jsou v případě interních úniků data o zaměstnancích. V případě externích úniků jsou nejčastějším cílem data o zákaznících. Rozdíl je však minimální, v rozsahu 1 %. Dalšími nejčastějšími cíli úniků dat jsou finanční data a data nesoucí duševní vlastnictví (intellectual property). [13] Data jsou znázorněna v grafech dále.

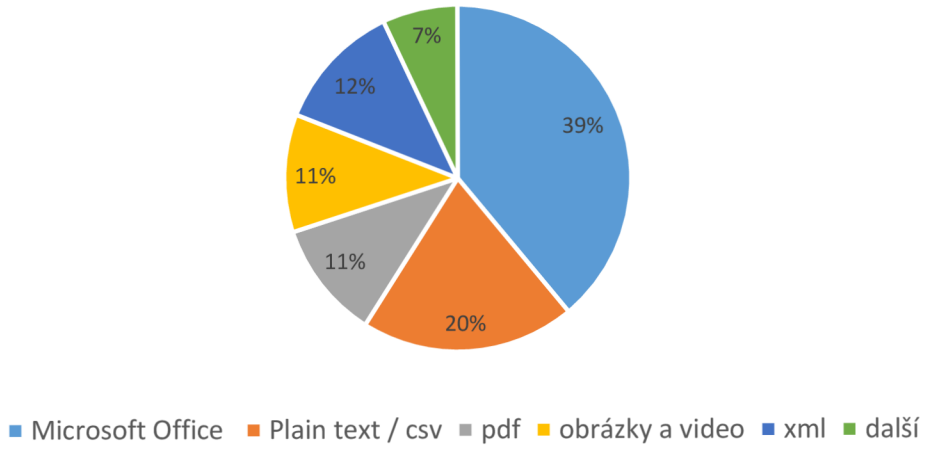


Graf 1: Cíle interních úniků dat z firemního prostředí
Zdroj:vlastní zpracování dle [13]

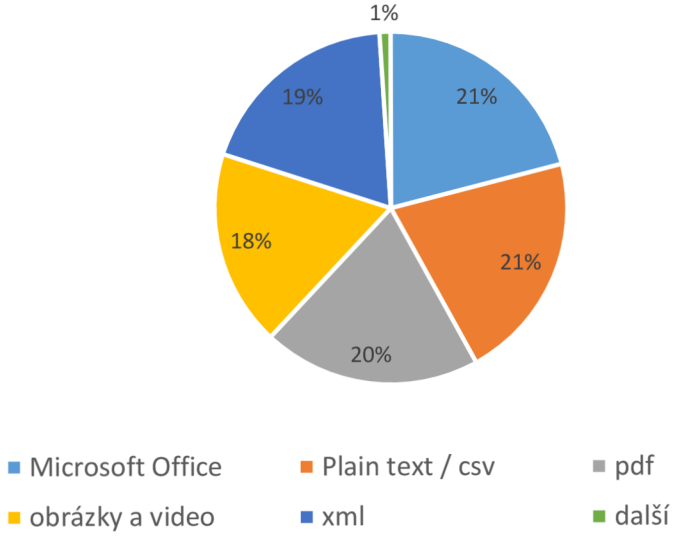


Graf 2: Cíle externích úniků dat z firemního prostředí
Zdroj: vlastní zpracování dle [13]

Mezi nejfrekventovaněji kradené soubory patří dokumenty Microsoft Office (PowerPoint, Excel, Word) pdf. soubory a cvs soubory, které jsou určeny pro jednoduchou výměnu tabulkových dat [13]. Výsledky výzkumu jsou znázorněny v grafech níže.

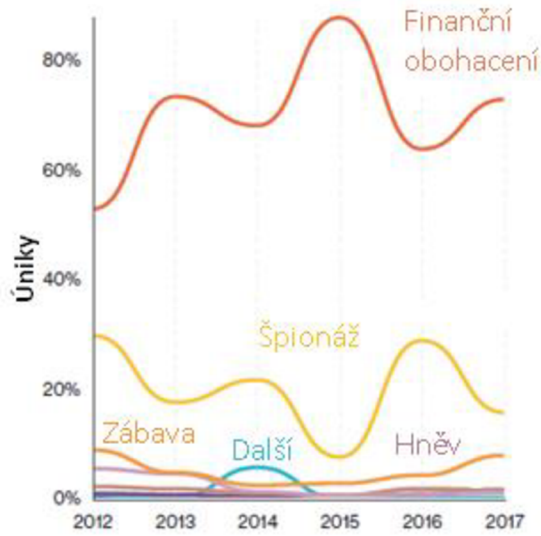


Graf 3: Typy souborů - interní úniky dat
Zdroj: vlastní zpracování dle [13]



Graf 4: Typy souborů - externí úniky dat:
Zdroj: vlastní zpracování dle [13]

Za úniky dat většinou stojí motiv finančního zisku (téměř 70 %) a špionáže (20 %). Některé kybernetické útoky jsou prováděny s pocitem osobní výzvy útočníka a s účelem zabavení se, či z hněvu a touhy po pomstě. Viz graf níže.



Graf 5: Úniky dat - motiv
Zdroj: přeloženo z [14]

1.3 Nejdůležitější vektory úniku dat

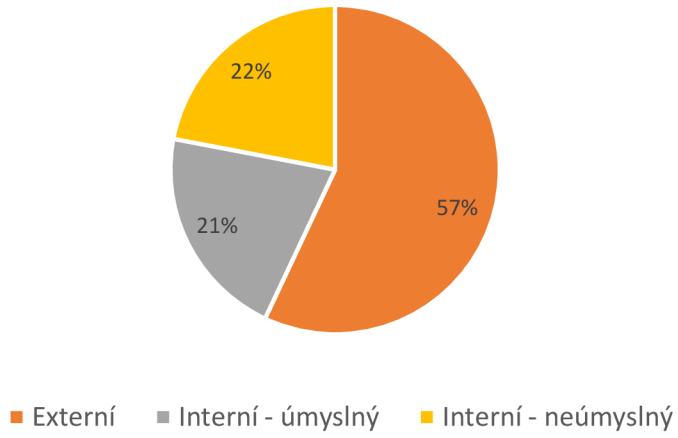
V této části bakalářské práce budou popsány nejčastější příčiny úniků dat, jejich základní rozdělení a výsledky studií zabývající se touto problematikou. Výsledky studií se mírně liší v závislosti na použitých metrikách, definicích (např. jak studie chápe pojem „interní únik dat“) a použitém vzorku dat.

1.3.1 Základní dělení úniků dat

Úniky dat z organizací můžeme zjednodušeně dle příčiny rozdělit na dvě skupiny: interní a externí úniky.

Interní úniky dat jsou způsobeny samotnými zaměstnanci organizací, dodavateli nebo spolupracujícími třetími stranami. Mohou být spáchány úmyslně či omylem. Za **externími úniky** stojí útočníci mimo danou společnost - hackeři, aktivisti, konkurence, autoři mallwaru apod. [7]. Mnoho externích útoků ale pro úspěšné provedení vyžaduje interakci uživatele uvnitř napadeného prostředí - tedy interakci interní (např. kliknutí zaměstnance na útočníkem podsunutý odkaz v emailu nebo otevření útočníkem zaslaného souboru). Výzkum Cyber Security Intelligence Index, publikovaný společností IBM, uvádí, že až v 95 % úniků dat figuruje nějakým způsobem lidský faktor. [15]

Dle studie od Intel Security z roku 2017 je 43 % úniků dat způsobeno přímo interními faktory a zbylých 57 % faktory externími (znázorněno na grafu níže).

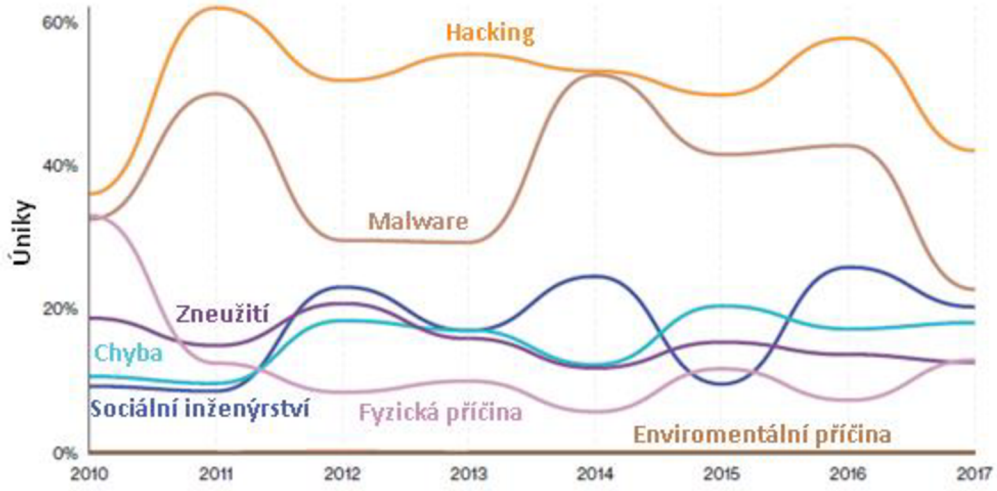


Graf 6: Příčiny úniků dat
Zdroj: vlastní zpracování dle [13]

Podíl interních a externích příčin se liší v závislosti na sektoru a geolokaci. V Asii a Pacifiku stojí za úniky dat až v 50% interní faktory, zatím co ve Spojené království Velké Británie a Severního Irska jde o méně než 40 %. Dle studie Verizonu [16] na interní úniky dat nejvíce trpí zdravotnictví a veřejný a finanční sektor. Ve zdravotnictví je téměř 60 % úniků dat způsobeno přímo interními faktory. [16]

1.3.2 Vývoj bezpečnostních hrozeb v čase

Na grafu níže můžeme vidět vývoj hlavních bezpečnostních hrozeb v čase dle studie *2018 Data Breach Investigations Report*, který ve zkoumaných incidentech rozlišoval 7 základních kategorií hrozeb, akcí či příčin.



Graf 7:Úniky dat - akce v čase
Zdroj: přeloženo z [14]

V únicích dat nejčastěji figuruje hacking (42 %) a malware (22 %) [14]. Hacking a malware zařazujeme do kategorie externích hrozeb, ale jak už bylo zmíněno dříve, zejména tyto dvě kategorie velmi často vyžadují pro úspěšný exploit interakci interního zaměstnance. [15]

Zastoupena je i kategorie sociálního inženýrství, která přímo využívá lidských slabin interních osob organizací. Sociální inženýrství samo o sobě může vyústit v únik informací, často je však prostředkem sběru informací pro přípravu mnohem

rozsáhlejšího úniku dat (např. následný útok formou hackingu, krádež zařízení apod.). [10; 14]

V grafu jsou dále zastoupeny tyto kategorie: zneužití pravomocí (zejména zneužití přístupu k datům), chybovost a fyzická příčina (ztráta, krádež, neadekvátní fyzická bezpečnost). V těchto kategoriích na straně příčiny dominují interní faktory organizace [14].

1.3.3 Specifika interních úniků dat

Jak už bylo zmíněno, interní úniky dat jsou způsobeny samotnými zaměstnanci organizací, dodavateli nebo spolupracujícími třetími stranami, které data organizace využívají v rámci svých dodavatelských procesů. V rámci bezpečnosti dat se zde významně projevuje tzv. lidský faktor. [17]

Interní úniky dat mohou být spáchány úmyslně (ve formě špionáže, v touze o obohacení apod.) nebo neúmyslně (zaměstnanec omylem sdílí data nebo pošle email s informacemi špatnému adresátovi). [7] Velkou roli zde hrají chyby z nepozornosti nebo z nevědomosti, kdy se projevuje nedostatečné povědomí o informační bezpečnosti, slabá motivace či únava. [18] Velký vliv má i samotné nastavení interních procesů práce s daty a jejich adekvátnost [10].

Detekce interních úniků je velmi složitá, protože se na nich podílí subjekty, které mají k datům legitimní přístup, znají firemní prostředí a mohou si být vědomi způsobů, jak zamaskovat důkazy o vynesení informací [7]. Bylo zjištěno, že až v 45 % organizací zaměstnanci úmyslně tají, ať už úmyslné či neúmyslné, bezpečnostní incidenty [16].

1.4 Bezpečnostní opatření

S cílem ochrany aktiv IS/ICT jsou v organizacích na základě jejich zranitelností a hodnot vybírána vhodná opatření, jež přiměřeně zmírňují rizika vybraných hrozeb. Ochranná opatření mohou snížit pravděpodobnost výskytu hrozby (např. školení uživatelů může vést k nižšímu množství úniků dat), odstranit zranitelnost, či zranitelnost učinit méně závažnou (firewall na perimetru sítě učiní síť méně zranitelnou) a omezit nebo vyloučit dopad (dostupné zálohy dat) [2; 5].

1.4.1 Základní dělení opatření

Opatření rozdělujeme **dle charakteru** na:

- administrativní,
- fyzická,
- technická a technologická [5].

Mezi **administrativní opatření** patří zejména nastavení interních procesů firmy popsaných ve směrnicích pro práci s aktivy IS/ICT a kontrola jejich dodržování. Příkladem mohou být např. směrnice pro zálohování dat nebo samotnou práci s daty. Jako administrativní opatření můžeme chápat také zavedení systému pravidelných školení informační bezpečnosti pro zaměstnance [5; 2].

Pod **fyzickými opatřeními** chápeme zejména používání zámků, trezorů pro ukládání kopií dat, tokenů (klíče, čipová karta) pro přístup do prostor s omezeným přístupem (např. vstup do serverovny) apod. [5].

Technická a technologická opatření formou aplikace různých bezpečnostních technologií. Mezi tato opatření řadíme např. využívání principů redundance, systém pravidelného zálohování dat na různá fyzická úložiště, plošné užívání antivirového či antimalware softwaru, šifrování provozu v síti, implementace bezpečnostních prvků (firewall, IPS, IDS, DLP, monitorovací sondy, proxy systémy, Active Directory apod.) nebo užití protokolu IEEE 802.1X pro síťovou autentizaci. [2; 5]

Opatření můžeme také **dle hlediska** ochrany dat rozdělit do těchto základních skupin:

- ochrana fyzického přístupu k datům,
- ochrana logického přístupu k datům,
- ochrana uložených dat,
- ochrana dat přenášených počítačovou sítí,
- ochrana dat před zničením [19].

Ochrana fyzického přístupu k datům - pod tímto pojmem myslíme nutnost zamezení fyzického přístupu k zařízením (USB disky, hard disk počítače, diskové pole v serverovně) neoprávněným osobám [19].

Ochrana logického přístupu k datům - neoprávněná osoba se může dostat k datům i bez toho, aby fyzicky získala zařízení s uloženými daty. Únik dat může způsobit např. chybné nakonfigurování cloudového/síťového úložiště, které umožní přístup k datům neoprávněným osobám. [19]

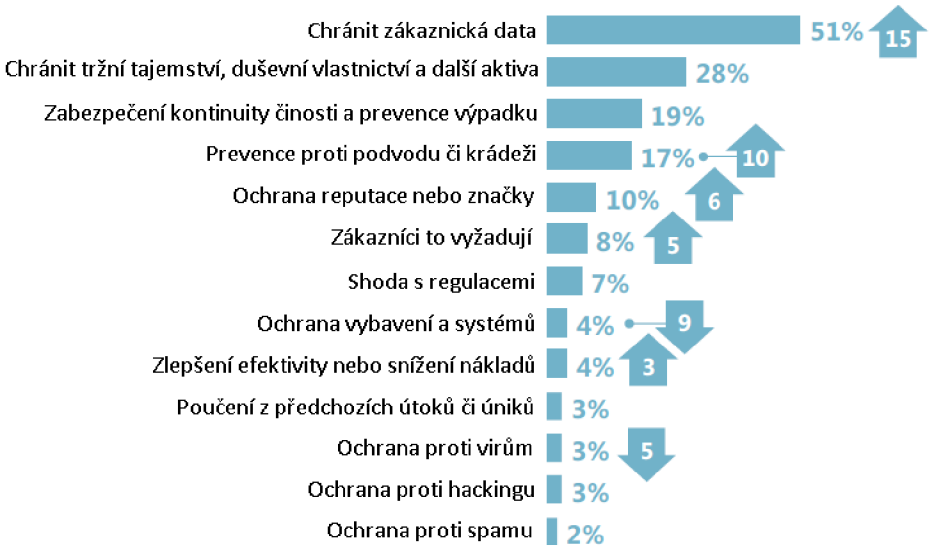
Ochrana uložených dat - nutnost zabezpečit uložená data (pevný disk počítače, data přenášená na USB discích) vhodnými metodami jako např. šifrováním proti neoprávněnému přečtení [19].

Ochrana dat přenášených počítačovou sítí - pokud má být zabezpečena důvěrnost dat, data musí být přenášena v zabezpečené podobě - šifrovaně [19].

Ochrana dat před zničením - ke zničení dat může dojít následkem přírodní katastrofy, selhání datového úložiště nebo následkem úmyslného chování zaměstnance [19].

1.4.2 Investice organizací do opatření

Institute for Criminal Justice Studies britské univerzity v Portsmouth zjistil, že společnosti investují finanční prostředky do bezpečnosti IT/ICT, zejména, aby ochránily data týkající se zákazníků. V posledních letech můžeme pozorovat, že tento trend se stále více prosazuje.

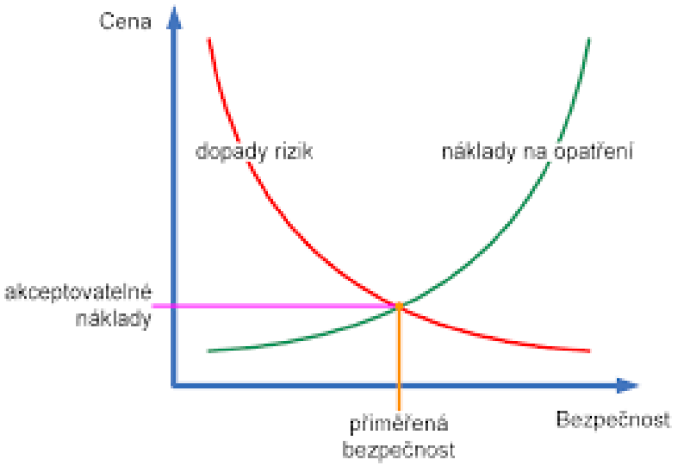


Graf 8: Motivace pro investice do bezpečnostních opatření
Zdroj: přeloženo z [20]

Další motivací pro společnosti je ochrana duševního vlastnictví, tržních tajemství a dalších aktiv, na třetím místě se nachází zabezpečení kontinuity činnosti organizace [20].

1.4.3 Přiměřená bezpečnost

Investice a usílí vložené do bezpečnostních opatření společnosti se musí odvíjet od hodnot aktiv společnosti a míře možných rizik - je třeba stanovit tzv. „přiměřenou bezpečnost“.



Graf 9: Graf přiměřené bezpečnosti
Zdroj: [2]

1.5 Technologie Data Loss Prevention

Kapitola má za cíl rámcově představit technologii DLP, a tak poskytnout výchozí znalost pro praktickou část, která je věnována výhradně ochraně dat pomocí DLP řešení.

1.5.1 DLP v kontextu bezpečnosti informací v organizaci

S cílem ochrany integrity, dostupnosti a důvěrnosti dat jsou v organizacích vedle administrativních a fyzických opatření užívána i technická opatření ve formě implementací různých bezpečnostních technologií [5]. Mezi ně patří např. autorizace a autentizace přístupu uživatelů k aktivům IS/ICT, zálohování dat, implementace firewallu, vytvoření demilitarizované zóny v síti nebo např. instalace antivirového softwaru na koncových stanicích. Každá z těchto technologií informační aktiva chrání pouze proti určitým typům hrozeb. [5; 7; 21]

DLP (Data Loss Prevention) systémy, které jsou předmětem této bakalářské práce, se specializují na ochranu proti interním hrozbám spojených s únikem dat. Cílem DLP systémů je identifikovat, monitorovat a chránit důvěrné informace před neoprávněnými aktivitami, na základě samotného obsahu dat, metadat nebo jejich kontextu v systému. Tyto systémy tedy cílí na ochranu důvěrnosti dat [7].

DLP systémy chrání před úmyslným i neúmyslným únikem dat. Účinnost ochrany je dána výběrem řešení, konfigurací, nastavením procesů organizace a součinností s ostatními prvky infrastruktury.

DLP systémy jsou rozdělovány do 2 základních kategorií: síťová DLP (network DLP) a DLP koncových bodů (tzv. host based DLP nebo také endpoint DLP). Pro zajištění maximální ochrany se oba přístupy často kombinují. [2]

1.5.2 Síťová DLP

Síťová DLP, či tzv. network DLP, představují síťová zařízení v interní síti organizace, která analyzují procházející komunikaci (email, ftp, http, https) a vyhledávají transakce obsahující klasifikované informace. Mohou také analyzovat data v úložištích. Zpravidla jsou umístěná v blízkosti perimetru sítě. Často je nutné je kombinovat s proxy

systémy - webovým proxy serverem nebo emailovým proxy agentem. Některá řešení mohou být ve formě softwarového modulu implementována na bezpečnostní brány na perimetru (firewally). Počet síťových DLP zařízení v organizaci se odvíjí od její velikosti a zvolené přiměřené ochraně, ale řádově se pohybuje v jednotkách kusů. [2; 22]

Síťová DLP jsou v případě většiny výrobců tradičně rozdělena do **3 funkčních modulů:**

- DLP Monitor - pro analýzu datových úložišť,
- DLP Network - pro monitorování síťové komunikace,
- DLP Prevent - v součinnosti s proxy systémy pro povolení či blokaci emailové nebo webové komunikace [22].

1.5.3 DLP koncových bodů

DLP koncových bodů, či tzv. DLP endpoint, jsou systémy, které jsou v podobě softwaru instalovány na koncových stanicích (počítačích, noteboocích, serverech apod.), kde, podobně jako síťová DLP, analyzují aktivity a probíhající komunikaci (mezi interními skupinami uživatelů i komunikaci mezi interními a externími subjekty). DLP koncových bodů umožňují kontrolu přístupu k přenosným fyzickým zařízením (externí disky, CD, DVD, mobilní zařízení) a zpravidla i šifrování (disků nebo souborů a složek). Počet spravovaných jednotek DLP endpoint se odvíjí od počtu chráněných koncových stanic. Řádově jde o desítky, stovky až tisíce stanic v závislosti na velikosti organizace. Jak zmíněná čísla napovídají, efektivní centralizovaná správa je nutností. [2; 22]

1.5.4 Princip fungování DLP

1.5.4.1 Bezpečnostní pravidla a klasifikace

Bezpečnostní pravidla - nastavení DLP. Jde o bezpečností pravidla definující, jak se má DLP chovat, když kontroluje aktivity s daty (data přenášená emailem mimo síť, data uložená na sdíleném úložišti v síti, uživatel na koncové stanici kopírující soubor apod.). Bezpečnostní pravidla jsou uplatňována na určité klasifikace dat. [22; 9]

Klasifikace dat - skupina dat mající určité vlastnosti a společný stupeň a způsob ochrany [22].

Klasifikování - proces udělování klasifikace [22].

1.5.4.2 Analýza dat - kontext a obsah

Data Loss Prevention užívá pro analýzu, a tak i jejich klasifikování, dva základní přístupy - analýzu na základě obsahu a na základě kontextu. Problematika může být přiblížena na základě analogie dopisu. Obsah je samotný dopis a kontext je obálka, informace na ní a prostředí kolem. [22]

DLP na **základě analýzy kontextu dat** dokáže rozeznat velikost či formát datového souboru, jeho odesílatele a příjemce, místo jeho uložení (např. konkrétní složka na sdíleném síťovém úložišti) apod. DLP v se v tomto případě vůbec nezabývá obsahem dat.

Kontextová analýza např. může brát v potaz:

- vlastnictví souboru a oprávnění,
- zašifrování souboru,
- síťový protokol přenášející data,
- roli uživatele a jeho začlenění v rámci organizace (na základě integrace s Active Directory),
- specifické webové služby,
- informace o USB disku (výrobce nebo číslo modelu),
- aplikaci pracující se souborem apod. [22]

Při analýze **založené na samotném obsahu dat** DLP využívá tzv. *filecraking* metodu, jež umožňuje technologii číst obsah souboru i přes mnoho vrstev (např. analyzovat soubor typu Excel vložený do zazipovaného dokumentu typu Word). Mnoho produktů na trhu s DLP podporuje kolem 300 typů souborů, analýzu vloženého obsahu, dvoubajtové znakové sady pro asijské jazyky či extrahování prostého textu z neznámých typů souborů. Některé nástroje mohou analyzovat šifrovaná data, pokud k jejich šifrování byly užity evidované podnikové šifrovací klíče. [22]

Techniky **analýzy obsahu** jsou založeny např. na:

- rozeznání specifických vzorů dat - např. specifický formát rodného čísla, čísla platební karty či IBAN kódu,

- vyhledávání klíčových slov,
- principu přesného porovnávání dat (zejména s daty z databáze) - vhodné pro strukturovaná data,
- principu přesného porovnávání souborů,
- porovnávání tzv. hashů (bezpečnostních otisků) důležitých souborů,
- porovnávání částí dokumentů (např. typický úvodní list, patička či hlavička dokumentu, či přímo celý utajovaný dokument) - vhodné pro ochranu duševního vlastnictví, výrobních plánů apod.,
- statistických metodách hledajících podobnost dokumentů apod. [22].

1.5.4.3 **Ochrana dat**

Cílem DLP je chránit data skrz celý jejich životní cyklus - v úložišti, při pohybu v síti i na koncových stanicích. V souvislosti s touto problematikou jsou používány následující pojmy:

- **data at rest** - uložená data,
- **data in use** - data, která jsou právě používána,
- **data in motion** - data v pohybu, data přenášená. [22]

Data at rest - ochranou je skenování úložišť a identifikace citlivých dat. V případě, že určitá data na daném úložišti nemají být uložena, mohou být přesunuta do karantény či zašifrována. [22]

Data in use - ochrana používaných dat je realizována pomocí endpoint modulů, které monitorují akce s daty, jež uživatelé provádějí [22].

Data in motion - ochranou dat v pohybu je monitoring, případně filtrace, síťového provozu skrz specifické komunikační kanály (zejména emailová či webová komunikace) [22]. Rámcově může být prováděna díky network i endpoint modulu.

2 ANALÝZA SOUČASNÉHO STAVU

Kapitola má za úkol představit investující organizaci, jejímž cílem je zavést DLP řešení. Kapitola pokrývá popis fungování organizace, postupů práce s daty, výstupů analýz vybraných oblastí a požadavků na výsledné řešení.

Vzhledem k povaze bakalářské práce si investor nepřeje být identifikován ani jmenován. Z toho důvodu bude společnost investora označována pouze jako „organizace" či „společnost". Údaje, které by mohly vést k identifikaci organizace nebudou zmíněny, popř. budou zobecněny či jinak anonymizovány.

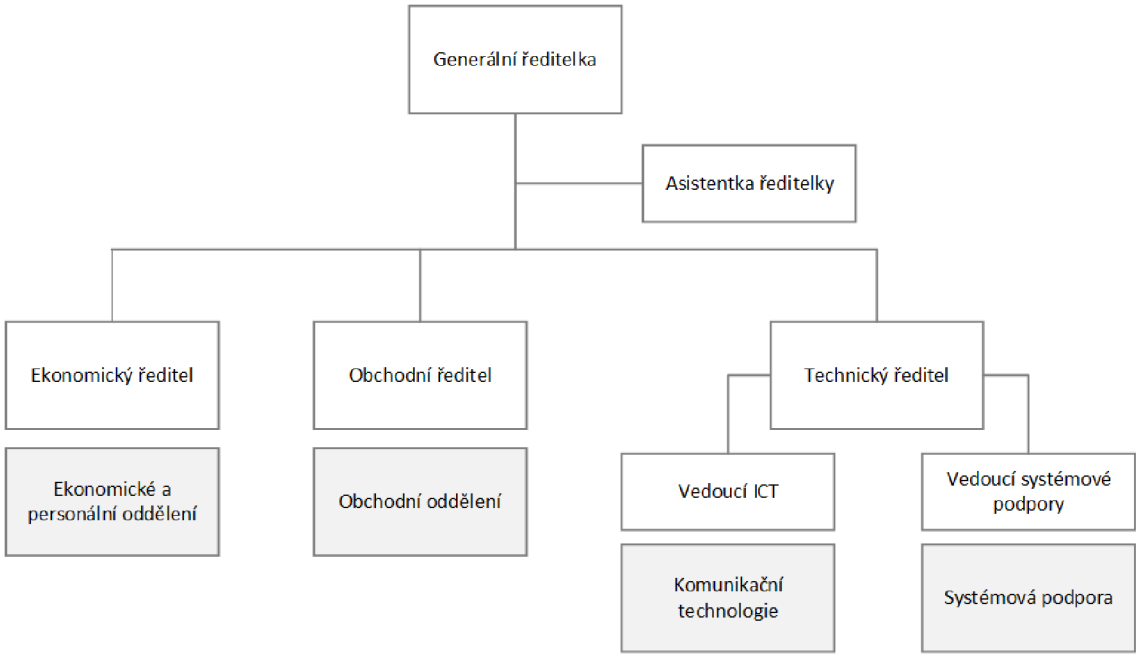
2.1 Základní informace o investorovi a předmět podnikání

Investorem je menší společnost podnikající v oblasti správy ICT řešení na poli B2B. Právní formou společnosti je společnost s ručením omezeným. Společnost sídlí v Čechách, ale podniká na celém území České republiky.

Společnost se v oblasti ICT řešení zabývá analýzami ICT prostředí, konzultacemi, návrhy, implementací a správou řešení ICT infrastruktury, pokrývající hardwarové i softwarové prvky, včetně prodeje a následné podpory. Kromě standardních servisních služeb nabízí i službu vzdáleného dohledu ICT infrastruktury. V portfoliu organizace nejdeme produkty mnoha výrobců jako např. Microsoft, Symantec, Cisco, GFI nebo Fortinet.

Zákazníky společnosti jsou organizace spadající do kategorií malých, středních i velkých podniků. Společnost poskytuje služby organizacím v oblasti státní a veřejné správy, školství i soukromého sektoru. Někteří zákazníci spadají do kategorie kritické a významné infrastruktury, proto je pro společnost samotnou informační a kybernetická bezpečnost prioritou, což v minulosti vedlo i k implementaci ISMS dle řady norem 27 000. Organizace sama nespadá pod působnost zákona o kybernetické bezpečnosti (ZKB). Zákazníci, na které spadá působnost ZKB, si soulad se zákonem zajišťují vedle splnění požadavků ze své strany i nastavením pravidel vůči dodavatelům. Jedním z takových pravidel může být např. podmínka zavedeného ISMS v organizaci dodavatele.

2.2 Organizační struktura společnosti



Obrázek 2: Organizační struktura společnosti
Zdroj: vlastní zpracování

Organizační struktura se promítá i do řízení Active Directory. Následující seznam uvádí rozřazení rolí do skupin AD.

- **mng** - generální ředitelka a její asistentka, ekonomický, obchodní a technický ředitel
- **hr** - všichni zaměstnanci ekonomického a personálního oddělení
- **obchod** - všichni zaměstnanci obchodního oddělení
- **tech** - všichni zaměstnanci technického oddělení
- **admin** - vybraní zaměstnanci technického oddělení mající i účet s oprávněním administrátora.

2.3 Požadavky investora

Organizace by ráda zvýšila bezpečnost práce s daty v organizaci, zejména s ohledem na data týkající se ICT řešení zákazníků. Samotné procesy práce s daty, spadající do skupiny organizačních opatření, jsou již nastaveny. Organizace nyní plánuje implementaci DLP technologie, jako technického opatření ochrany dat. DLP řešení musí

být implementováno v souladu s ISMS. Investor sám přesně nezformuloval požadavky na dané DLP řešení, pouze má představu, jaká data chce chránit. Konkrétní požadavky budou v součinnosti s vedením organizace zformulovány na základě výstupů analýzy společnosti.

2.4 Analýza vybraných dokumentů

Organizace v minulosti implementovala systém řízení bezpečnosti informací ISMS dle ČSN EN ISO 27001:2014 a systém managementu kvality dle ČSN EN ISO 9001:2016, ke kterým byla vypracována dokumentace. V rámci analýzy současného stavu došlo i k analýze vybraných dokumentů z této dokumentace, zejména Bezpečnostního manuálu uživatele ICT, Bezpečnostního manuálu administrátora ICT, Prohlášení o aplikovatelnosti a Příručky kvality.

2.4.1 Rozsah ISMS

V organizaci je zavedeno ISMS v následujícím rozsahu:

- Poskytování služeb v oblasti ICT.
- Správa komunikační infrastruktury.
- Služby a dodávky HW a SW.

Momentálně ISMS nepokrývá informace vedené v systému účetnictví, obchodní data (fakturace, nabídky) a personální data. Rozsah ISMS koresponduje s cílem organizace chránit důvěrná data zákazníků spojená s řešením ICT. V rámci tohoto rozsahu jsou popsány klíčové procesy organizace, způsoby práce s daty a další důležité skutečnosti, jež jsou jedním z podkladů pro správný výběr a konfiguraci DLP technologie.

2.4.2 Důležité body ISMS

Cílem následující části práce je na základě dokumentace ISMS popsat části dokumentace a jejich body, které mají návaznost na implementaci DLP. V následující části tedy nebudou zmíněny okruhy jako např. bezpečnost lidských zdrojů, řízení

kontinuity, řízení fyzického přístupu, používání hesel či dodržování zasad čistého stolu a čisté obrazovky při opouštění pracoviště apod. Zmíněné a podobné okruhy jsou vzhledem k informační a kybernetické bezpečnosti organizace velmi důležité, ale nejsou přímo relevantní pro řešení problematiky implementace DLP.

2.4.2.1 Školení zaměstnanců

Zaměstnanci jsou dle ISMS pravidelně školeni v oblasti ISMS, obecného povědomí o informační bezpečnosti a v případě potřeby i v návaznosti na nové projekty či technologie. Noví zaměstnanci absolvují řadu vstupních školení. V rámci implementace DLP by měla proběhnout série školení (plošné a pro administrátory).

2.4.2.2 Používání uživatelských jmen

V organizaci je pro přístup k počítačům, IT službám a k aplikacím vyžadováno zadání individuálních uživatelských přihlašovacích údajů v podobě uživatelského jména a hesla. Uživatel odpovídá za všechny úkony učiněné pod svým jedinečným přihlašovacím jménem. Uživatelská jména jsou dle vzoru vygenerována na začátku pracovního poměru daného zaměstnance a zaznamenávána spolu s hesly v AD (Active Directory).

2.4.2.3 Používání elektronické pošty

Každý zaměstnanec má zřízenou emailovou adresu dle vzoru *jmeno.prijmeni@nazevorganizace.cz*. Posílání pracovních emailů je dovoleno pouze přes tuto emailovou schránku. Pro přístup do emailové schránky je užívána výhradně desktopová aplikace Microsoft Outlook. Emaily, jejichž obsah je klasifikován jako citlivý nebo velmi citlivý, mohou být dle bezpečnostních směrnic posílány pouze v zaheslované (ZIP soubor s heslem) nebo šifrované podobě. Větší soubory nesmí být posílány emailem - pro jejich sdílení slouží úložiště OneDrive.

2.4.2.4 Používání internetu

V organizaci je zakázáno ukládat či sdílet informace společnosti nebo jejích zákazníků v prostředí Internetu. Jedná se zejména o úložiště typu Letecká Pošta,

Úschovna, Google Docs, Uložto, Dropbox apod. Je povolené používat interně schválené úložiště OneDrive (SharePoint). Pokud je nezbytně nutné použít pro výměnu dat veřejných služeb v Internetu, je nutné schválení časově omezené výjimky, kterou uděluje garant Komunikačních systémů. Data uložená na veřejných uložištích musí být zabezpečena šifrováním nebo minimálně zaheslována heslem, dle pravidle uvedených v části *Používání elektronické pošty*. Zaměstnanci nesmí vkládat do webových formulářů, aplikací či podobných služeb interní, citlivé nebo velmi citlivé informace (např. pro překlady v automatizovaných překladačích).

Zaměstnanci jsou obeznámeni s tím, že jejich činnost na internetu může být z bezpečnostních důvodů průběžně monitorována.

2.4.2.5 **Vzdálený přístup**

Pro vzdálené připojení firemních počítačů do sítě společnosti je možné využít pouze VPN přístup a to aplikací schválenou společností. Jiné vzdálené přístupy nejsou technicky dovoleny na úrovni firewallu.

2.4.2.6 **Používání přenosných zařízení**

Všichni zaměstnanci společnosti využívají k práci přenosné notebooky s operačním systémem Windows, zařazené do domény organizace. Dále jsou používány mobilní telefony a občasně tablety. Všechna zařízení mají šifrovaná uložiště, pro bezpečné ukládání dat. Dle bezpečnostních směrnic musí být notebook připojen do sítě minimálně jednou za 14 dní.

2.4.2.7 **Používání tiskáren a kopírovacích zařízení**

V organizaci je umístěno několik síťových tiskáren, které zaměstnanci mohou k výkonu práce používat. Dle bezpečnostních směrnic smí docházet k tisku či kopírování citlivých nebo velmi citlivých dokumentů jen na zařízením umístěném v chráněném prostoru. Všechny síťové tiskárny tuto podmínku splňují.

2.4.2.8 Přenosná paměťová média

Na přenosná paměťová média, mezi které řadíme USB flash disky, externí pevné disky, CD, DVD, paměťové karty apod., zaměstnanci mohou data organizace ukládat, ale za specifických podmínek. Pokud jsou ukládaná data klasifikována jako citlivá či velmi citlivá, mohou být nahrána pouze šifrovaně a musí být označena popiskem. Je zakázáno používat paměťová média z neznámých nebo nedůvěryhodných zdrojů (např. nalezené USB flash disky, neznámá CD/DVD, rozdávaná paměťová média).

2.4.2.9 Klasifikace aktiv dle ISMS

Společnost chápe, že data jsou důležitým aktivem společnosti a v systému řízení bezpečnosti tak k této problematice přistupuje. Klasifikace informací je dle interních směrnic součástí klasifikace aktiv. Aktiva klasifikuje Vlastník aktiva dle tří bezpečnostních atributů (důvěrnosti, integrity a dostupnosti). Dle kritérií uvedených v tabulce níže (obecné klasifikační schéma) určí klasifikační stupeň (Nízký až Velmi vysoký) pro každý z bezpečnostních atributů. Klasifikační stupeň je zaznamenán do registru aktiv.

Tabulka 1: Klasifikační stupně dle ISMS

Klasifikační stupeň	Popis
Nízký	Aktiva, u kterých porušení bezpečnostních atributů (dostupnost, integrita, důvěrnost) může vést v nejhorších případech pouze k nevýznamnému (akceptovatelnému) negativnímu dopadu.
Střední	Aktiva, u kterých porušení bezpečnostních atributů může vést k postřehnutelným dopadům, ale může být snadno zvládnuto.
Vysoký	Aktiva, u kterých porušení bezpečnostních atributů může vést k výrazným negativním důsledkům na procesy a aktivity organizace.
Velmi vysoký	Aktiva, u kterých porušení bezpečnostních atributů může ohrozit existenci společnosti.

Zdroj: vlastní zpracování dle dokumentace organizace

Z hlediska problematiky DLP je pro nás relevantní klasifikace aktiv v aspektu důvěrnosti. Vzhledem k obsáhlosti této problematiky bude jejímu popsání věnována samostatná kapitola *2.5.1 Klasifikace dat*.

Vlastníkem aktiva je osoba s manažerskou odpovědností za přístup k informaci. Vlastník aktiva je uveden v Registru aktiv. Mezi jeho odpovědnosti a pravomoci dle interních dokumentů patří:

- Identifikovat a dokumentovat informace nezbytné pro fungování firemních procesů.
- Určit u každé informace její hodnotu na základě požadavků společnosti.
- Klasifikovat informaci podle tří bezpečnostních atributů (důvěrnost, integrita a dostupnost), a prověřit splnění bezpečnostních požadavků spojené s daným klasifikovaným aktivem.

U nestrukturovaných a semistrukturovaných dat (např. dokumentů MS Word, Excel) je za Vlastníka informace považován ten, kdo dokument vytvořil, pokud nejsou stanoveny jiné požadavky na vlastnictví.

Zaměstnanci jsou si vědomi, že smí používat pouze takové zdroje informací (včetně výkazů a listinných dokumentů), k jejichž používání jsou oprávněni nebo k nimž mají oprávněný přístup. Musejí dodržovat zásady stanovené vlastníkem aktiva a bez jeho souhlasu nesmějí sdělovat informace či předávat aktiva třetím osobám mimo společnost, pokud to neumožňuje klasifikace aktiva.

2.5 Práce s daty v organizaci

V organizaci existuje systém klasifikace informací, jež je součástí systému klasifikace aktiv. Více o klasifikaci aktiv v organizaci lze najít v kapitole *2.4.2.9 Klasifikace aktiv dle ISMS*. V následující kapitole je popsána klasifikace dat z hlediska důvěrnosti a z toho vyplývající pravidla práce s nimi.

2.5.1 Klasifikace dat

Data jsou vzhledem k aspektu důvěrnosti informací, které nesou, rozdělena do čtyřech skupin (Nízký, Střední, Vysoký, Velmi vysoký klasifikační stupeň). Každý ze stupňů nese název klasifikace, pod kterým jsou data nesoucí dané informace v organizaci označována. Tento vztah je znázorněn na tabulce níže.

Tabulka 2: Klasifikace dat v organizaci z aspektu důvěrnosti

Název	Popis	Klasifikační stupeň pro atribut „Důvěrnost“	Příklad
Veřejné *Public*	Informace určené ke zveřejnění (např. marketingové materiály, tiskové zprávy, prohlášení).	Nízké	Informační letáky, text na webových stránkách apod.
Interní *Internal*	Informace vytvořené pro vnitřní použití v rámci běžné obchodní činnosti, jejichž zveřejnění neoprávněným osobám by nemělo žádný nebo omezený negativní dopad (např. pracovní pokyny, informace jinak běžně přístupné na intranetu).	Nízké nebo	Interní a účetní dokumenty společnosti, obchodní nabídky, ekonomická data apod.
		Střední	
Citlivé *Confidental*	Informace, jejichž zpřístupnění neoprávněným osobám by mohlo mít významný negativní dopad na společnost.	Vysoké	Osobní údaje, zákaznická data apod.
Velmi citlivé *Stritctly confidental*	Informace, jejichž zpřístupnění neoprávněným osobám by mohlo ohrozit existenci společnosti.	Velmi vysoké	Citlivá zákaznická data, přístupové údaje, popis řešení ICT v prostředí zákazníka.

Zdroj: dokumentace organizace

O určení stupně utajení informace typu listinný dokument, nebo elektronický dokument (např. MS Word, Excel, email) rozhoduje v organizaci autor dokumentu nebo zaměstnanec, který jej přijal jako první.

2.5.2 Pravidla pro práci s daty s ohledem na klasifikaci

Pravidla pro práci s daty v organizaci v závislosti na klasifikaci jsou popsána v tabulkách následujících podkapitol. Pravidla jsou rozdělena do dvou skupin - všeobecná pravidla a pravidla práce s daty mimo organizaci.

2.5.2.1 Všeobecná pravidla práce s daty

V následující části jsou popsána pravidla, které zaměstnanci organizace při práci s daty musí všeobecně dodržovat. Pravidla se týkají zejména výkonu práce na pracovišti. Pravidla jsou zaznamenána v tabulkách dle jednotlivých činností. Každá činnost podléhá různým pravidlům v závislosti na klasifikaci dat, s kterými daná činnost souvisí. V levém sloupci jsou uvedeny v organizaci používané klasifikace. V pravém sloupci jsou uvedena pravidla. Daná činnost je jmenována vždy vpravo nahoře.

Tabulka 3: Pravidla práce s daty - označování dokumentů

Klasifikace	Označování dokumentů
Veřejné	
Interní	Autorem označeny „ORG INTERNÍ“* • MS Office dokumenty - na úvodní stránce • Emaily - označení v předmětu emailu • Na přenosném médiu (CD, USB, ...) • Listinné dokumenty - na úvodní stránce dokumentu/složky
Citlivé	Autorem označeny „ORG CITLIVÉ“* • MS Office dokumenty - na úvodní stránce • Emaily - označení v předmětu emailu • Na přenosném médiu (CD, USB, ...) • Listinné dokumenty - na úvodní stránce dokumentu/složky • Informační systém - upozornění při přihlášení
Velmi citlivé	Autorem označeny „ORG VELMI CITLIVÉ“* • MS Office dokumenty - na úvodní stránce • Emaily - označení v předmětu emailu • Na přenosném médiu (CD, USB, ...) • Listinné dokumenty - na úvodní stránce dokumentu/složky • Informační systém - upozornění při přihlášení

	Dokumenty týkající se ICT zákazníků navíc musí obsahovat v záhlaví signaturu (popř. jejich kombinaci) určující typ dokumentu dle následujících specifik: • ZI - dokumenty obecné analýzy prostředí zákazníka • ZK - informace o konfiguraci řešení • ZP - obsahující přístupové údaje • ZL - obsahuje logy z prostředí zákazníka

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

* ORG zastupuje zkratku názvu organizace (anonymizováno)

Tabulka 4: Pravidla práce s daty - opakovaná klasifikace dokumentů

Klasifikace	Opakovaná klasifikace dokumentu
Veřejné	Vlastník udržuje aktuální klasifikaci
Interní	Vlastník udržuje aktuální klasifikaci
Citlivé	Vlastník aktiva Min. 1krát ročně
Velmi citlivé	Vlastník aktiva Min. 1krát ročně

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 5: Pravidla práce s daty - šíření v rámci organizace

Klasifikace	Šíření v rámci organizace
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Schválení garantem aktiva
Velmi citlivé	Distribuční seznam Schválení garantem aktiva

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 6: Pravidla práce s daty - fyzické uložení

Klasifikace	Uložení fyzických dokumentů a přenosných médií s daty (USB, CD apod)
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Při opuštění místnosti uzamčené (stůl, skříňka, celá místnost apod.)
Velmi citlivé	Při opuštění místnosti uzamčené (stůl, skříňka, trezor, celá místnost)

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 7: Pravidla práce s daty - uložení elektronických dokumentů

Klasifikace	Uložení elektronických dokumentů
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Šifrovaně nebo omezený přístup k zálohám
Velmi citlivé	Šifrovaně nebo omezený přístup k zálohám

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 8: Pravidla práce s daty - zálohování

Klasifikace	Zálohování
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Šifrovaně nebo omezený přístup k zálohám
Velmi citlivé	Šifrovaně nebo omezený přístup k zálohám

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 9: Pravidla práce s daty - smazání el. dat

Klasifikace	Smazání elektronických dat
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Bezpečné smazání
Velmi citlivé	Bezpečné smazání

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 10: Pravidla práce s daty - tisk, kopírování, skenování

Klasifikace	Tisk, kopírování, skenování
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Tisk v uzavřených prostorách - kancelář Dokument okamžitě bezpečně uložit
Velmi citlivé	Tisk v uzavřených prostorách - kancelář Dokument okamžitě bezpečně uložit

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

2.5.2.2 Pravidla práce s daty mimo organizaci

V následující části jsou popsána pravidla, které zaměstnanci společnosti při práci s daty mimo organizaci musí dodržovat. Pravidla jsou zaznamenána v tabulkách dle jednotlivých činností. Každá činnost podléhá různým pravidlům v závislosti na klasifikaci dat, s kterými daná činnost souvisí. V levém sloupci jsou uvedeny v organizaci používané klasifikace. V pravém sloupci jsou uvedena pravidla. Daná činnost je jmenována vždy vpravo nahoře.

Tabulka 11: Pravidla práce s daty - šíření mimo organizaci

Klasifikace	Šíření informace mimo organizaci
Veřejné	Žádné požadavky
Interní	Pouze k pracovním účelům
Citlivé	NDA (dohoda o mlčenlivosti) Distribuční seznam Schválení vedoucím zaměstnancem
Velmi citlivé	NDA (dohoda o mlčenlivosti) Distribuční seznam Schválení vlastníkem informace a vedoucím zaměstnancem

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 12: Pravidla práce s daty - přenosná média

Klasifikace	Přenosná média
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Šifrovaná
Velmi citlivé	Šifrovaná

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 13: Pravidla práce s daty - předávání mimo organizaci

Klasifikace	Předávání mimo organizaci
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Bezpečný způsob (osobní předání, kurýr, zapečetěné apod.)
Velmi citlivé	Bezpečný způsob (osobní předání, kurýr, zapečetěné apod.)

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 14: Pravidla práce s daty - emailová komunikace

Klasifikace	Emailová komunikace
Veřejné	Žádné požadavky
Interní	Zákaz zasílání přes osobní (nefiremní) emaily
Citlivé	Šifrovaný obsah Zákaz zasílání přes osobní (nefiremní) emaily
Velmi citlivé	Šifrovaný obsah Zákaz zasílání přes osobní (nefiremní) emaily

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 15: Pravidla práce s daty - Instant Messaging

Klasifikace	Instant Messaging komunikace
Veřejné	Žádné požadavky
Interní	Pouze k pracovním účelům
Citlivé	Pouze schválenými nástroji
Velmi citlivé	Zákaz komunikace

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

Tabulka 16: Pravidla práce s daty - používání úložišť

Klasifikace	Používání sdílených internetových uložišť (uloz.to, dropbox.com,)
Veřejné	Žádné požadavky
Interní	Pouze schválené služby - firemní SharePoint, OneDrive
Citlivé	Pouze schválené služby - firemní SharePoint, OneDrive
Velmi citlivé	Pouze schválené služby - firemní SharePoint, OneDrive

Zdroj: vlastní zpracování na základě dat z dokumentace organizace

2.6 Popis současné komunikační infrastruktury

Obsah popisu komunikační infrastruktury byl vybrán, popř. zestručněn, na základě relevance k zaměření bakalářské práce.

2.6.1 Síťová infrastruktura

Lokální datová síť společnosti je tvořena pevnými metalickými datovými rozvody kategorie Cat.5E zakončenými na patch-panelech v komunikačních datových

rozvaděčích *DRC1* a *DRC2,* které jsou spolu se serverovými rozvaděči umístěny v hlavní a vedlejší serverovně, a dále bezdrátovou WIFI sítí zajišťující pokrytí prostor společnosti v pásmu 2,4GHz a 5GHz dle standardů IEEE 802.11.

Lokální datová síť je rozdělena na provozní a laboratorní síť. Provozní síť zajišťuje datovou komunikaci společnosti. Laboratorní síť slouží pro testování a přípravu zákaznických řešení. Obě datové sítě jsou dále rozsegmentovány do virtuálních LAN sítí (VLAN) a odpovídajících IP podsítí.

Důležitým prvkem infrastruktury společnosti je UTM (Unified Threat Management) bezpečnostní brána, která zajišťuje následující funkcionality:

- směrování provozu z/do internetu,
- NGFW - Next-Generation Firewall,
- IPS - Intrusion Prevention System (detekce anomálií síťového provozu),
- filtrování webového provozu dle obsahu a kategorizace webu,
- VPN - zajištění vzdáleného přístupu pro zaměstnance a dodavatelské organizace.

2.6.2 Serverová infrastruktura

Provozní serverovou infrastrukturu tvoří 4 fyzické servery v clusteru a sdílené úložiště s interními SSD disky s využitím automatického tieringu pro optimalizaci výkonu. Zálohování se provádí na externí úložiště NAS a SharePoint. V organizaci je provozována virtualizační platforma Hyper-V, na které běží virtuální servery s následujícími rolemi:

- 2x domain controller - Active Directory, DNS, DHCP
- ePO server - SQL databáze + ePolicy Orchestrator (Windows Server 2012)
- Certifikační autorita
- DB server - SQL Server
- Proxy server
- Backup server
- Aplikační server - ERP
- MGMT Server - Archivace pošty, CCTV

Na ePO serveru je nainstalována platforma ePolicy Orchestrator, která slouží ke správě Endpoint Security (dále jen ENS), produktu od firmy McAfee. ENS je anti-malwarový a antivirový program pro firemní prostředí, chránící mimo jiné před útoky nultého dne. Pro potřeby ePolicy Orchestratoru je na ePO serveru také SQL databáze *SQL_EPO*.

2.6.3 Uživatelské stanice

V organizaci se nyní aktivně využívá 52 notebooků s operačním systémem Windows 10 a 45 pracovních mobilních telefonů s operačním systémem Android. Tablety pro práci nejsou využívány. Pevný disk všech počítačů je šifrován.

Na koncových stanicích pracují zaměstnanci, kteří pro svůj výkon práce využívají aplikaci Help Desk, produkty Microsoft Office a další software pro správu lokálních či zákaznických ICT řešení. Mezi nejčastěji využívané aplikace Microsoft Office patří Outlook, primárně pro odesílání emailů, a Microsoft Word s Excelem pro tvorbu pracovních dokumentů. Zaměstnanci sdílí dokumenty na firemní SharePoint a používají také osobní OneDrive.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

3.1 Souhrnný popis řešení

V rámci vlastního řešení došlo k návrhu ochrany dat v konkrétní organizaci pomocí technologie DLP, včetně potřebných kroků pro zahájení implementace.

V první fázi byla provedena analýza a zváženy všechny její výstupy (stávající zabezpečení, požadavky a preference investora, bezpečnostní směrnice organizace, počet zaměstnanců apod.). Na základě výstupů analýzy organizace a potřeb investora byly zformulovány požadavky na DLP řešení. Proběhla analýza několika DLP řešení různých výrobců, jejich porovnání i přibližná kalkulace případné implementace. Na základě analýz bylo vybráno konkrétní DLP řešení vhodné právě pro danou organizaci. Následně byl určen rozsah budoucí implementace i výběr konkrétní licence. V rámci praktické části také došlo k vypracování postupu implementace, který se skládá z klíčových činností, jejich popisu a délky trvání. Pro hladké řízení projektu implementace byl vypracován harmonogram spolu s časovou analýzou a RACI maticí zodpovědností. Následně došlo k samotnému návrhu nastavení DLP v testovacím prostředí a jeho vyladění tak, aby mohlo být použito v rámci budoucí reálné implementace.

3.2 Formulace požadavků na DLP řešení

Investorův požadavek implementovat DLP technologii nedoprovází konkrétní zadání - specifikace výrobce, rozsah implementace, způsoby ochrany. Požadavkem organizace je, vedle monitorování dat nesoucích osobní údaje, pouze zvýšení ochrany dat zákazníků díky DLP, jehož implementace by měla být provedena v souladu s ISMS. Proto v první řadě musí dojít k formulaci požadavků na dané DLP řešení na základě analýzy společnosti.

Požadavky, které byly v rámci praktického řešení navrhnuty ve spolupráci s odpovědnými osobami organizace, jsou uvedeny v následujících podkapitolách.

3.2.1 Obecné požadavky

- Možnost synchronizace DLP s údaji z Active Directory zachovávající kontejnerizaci a skupiny uživatelů pro následné nastavování politik a výjimek.
- Podpora Digital Rights Management.
- Při potenciálním rozšíření funkcionalit implementací dalších dílčích modulů možnost spravovat všechny moduly z jedné konzole.

3.2.2 Požadavky na klasifikace a definice

- Možnost vytvářet vlastní klasifikační stupně a pravidla pro udělování těchto klasifikací.
- Možnost ručního oklasifikování dokumentů při jejich vzniku (zejména souborů MS Office).
- Možnost automatického oklasifikování dat na základě ručně nastavených pravidel pro udělování klasifikací.
- Použití vlastních slovníků klíčových slov. Tyto slovníky budou sloužit pro nastavení pravidel pro klasifikování. (např. seznam zákazníků společnosti, seznam používaných signatur označující citlivé dokumenty apod.).
- Možnost porovnání celých částí dokumentu a na základě toho přiřazení klasifikace danému dokumentu. (např. dokument obsahující speciální hlavičku, která se používá u citlivých dokumentů).
- Možnost tvorby vlastních definic užitých v bezpečnostních pravidlech. (např. vydefinování USB disku konkrétního výrobce, na který bude možno ukládat citlivá data, ale na jiné USB disky ne)

3.2.3 Požadavky na bezpečnostní pravidla

- Možnost nastavovat vlastní bezpečnostní pravidla.
- Možnost chránit tyto kanály možných úniků dat:
    - Emailová komunikace - Outlook.

- Data vkládaná do webového rozhraní - např. do textového pole psaného emailu veřejné emailové služby Google nebo překladače otevřeného v prohlížeči.
- Tzv. clipboard ochrana - ochrana kopírování a vkládání v paměti počítače (typicky klávesové zkratky CTRL C + CTRL V).
- Ochrana dat snímaných pomocí snímku obrazovky (tzv. screen capture).
- Přenos na přenosná datová úložiště (USB zařízení, DVD apod.)
- Vkládání na známá cloudová úložiště přes desktop aplikace.

- Možnost definování bezpečnostních pravidel pro kontejner zařízení nebo skupinu uživatelů z AD.
- Možnost přiřazení výjimky pro konkrétní uživatele nebo zařízení.
- Při porušení bezpečnostního pravidla ideálně možnost zobrazení edukační zprávy týkající se daného porušení.
- Možnost uživatele vyžádat si od administrátora pro danou akci, která není v souladu s bezpečnostní politikou, výjimku.
- Bezpečnostní pravidla zůstávají aktivní i po odpojení od sítě organizace (např. notebooky u zaměstnanců doma nebo na pracovní cestě).

3.3 Výběr konkrétního řešení

Na základě zformulovaných požadavků je třeba vybrat konkrétního výrobce DLP technologie, jehož řešení bude v organizaci implementováno. Postup výběru je popsán v následujících kapitolách.

3.3.1 Možnosti výběru - trh s DLP technologií

Na trhu s DLP řešeními můžeme rozlišit několik hlavních hráčů. Na vrcholu tohoto žebříčku se léta drží společnosti Symantec, McAfee (dříve Intel Security) a Forcepoint, jejichž DLP produkty získali za rok 2018 ocenění Gartner Customers‘ Choice. Tito výrobci patří k výrobcům tzv. enterprise řešení, tedy řešení určených zejména pro větší firmy. Situace na trhu DLP výrobců na základě široce uznávané analýzy Gartner je znázorněna dále.

Graf 10:Situace na trhu DLP
Zdroj: upraveno na základě [23]

Produktová výkonnost je měřítko popisující schopnost výrobce dodat na trh řešení, jehož funkcionality, výkon, výsledky i zákaznická podpora splňují očekávání a požadavky zákazníka. Významně zde figuruje kompletnost, vhodnost řešení i univerzálnost (integrace s dalšími třetími stranami, podpora různých operačních systémů apod.) a jeho schopnost se vyvíjet na základě potřeb trhu. Na míru produktové výkonosti analýzy Gartner má vliv i aktuální obchodní (vztahy s distributory, prodejní kanály) a cenová politika spolu s marketingovou strategií. [23]

Úplnost vize je měřítko popisující jak komplexně a důkladně se výrobce zaměřuje na inovace a splnění budoucích požadavků trhu - přicházející regulace, nové hrozby, trendy a potřeby zákazníků. Plnění vize se měří nejen v oblasti samotného DLP produktu a přidružených služeb, ale i v oblastech obchodního modelu, prodeje a marketingu. [23]

Po dohodě s investorem bylo na základě jeho přání rozhodnuto, že při výběru DLP řešení budou zvažovány DLP řešení od firem Symantec, McAfee (v analýze Gartner Intel Security), Forcepoint a Digital Guardian, jež patří mezi leadery na trhu. Do výběru se dále zařadí i výrobce Sophos, který se zaměřuje spíše na menší podniky a mohl by být v porovnání k ostatním výrobcům jednodušší a levnější variantou.

3.3.2 Symantec

Obrázek 3: Logo Symantec
Zdroj: [26]

Na poli DLP řešení je společnost Symantec, americká společnost, zaměřující se na vývoj softwaru, absolutním leaderem. Tato společnost vede trh, transformuje ho a určuje směr inovací. Na trhu představuje laťku, podle které jsou ostatní řešení srovnávána. Symantec DLP je považováno za nejobsáhlejší, ale také nejdražší DLP řešení. Malé a střední podniky mohou mít problém s jeho komplexností a správou. [24]

Symantec DLP je řešeno čistě na softwarové bázi. Obsahuje mnoho komponent, jež se dají zakoupit v rámci jedné zlevněné licence nebo zvlášť. Téměř každá komponenta může být instalována na Windows či Red Hat Enterprise Linux, a to jak na fyzický či virtuální stroj. Symantec DLP je strukturováno do těchto komponent:

- Symantec DLP Enforce Console (konzole pro správu řešení),
- Symantec DLP Cloud Services,
- Symantec DLP for Network,
- Symantec DLP for Network,
- Symantec DLP for Storage,
- Symantec DLP Sensitive Image Recognition,
- Symantec Information Centric Tagging,
- Symantec Information Centric Encryption,
- Symantec Information Centric Analytics,
- Symantec Information Centric Analytics. [25]

Network Monitor využívá metodu Port Mirroring neboli tzv. SPAN (Switched Port Analyzer) či RSPAN port (Remote Switched Port Analyzer), jež dokáže na daný port přeposílat komunikaci z celé sítě. V blokaci webové a emailové komunikace Symantec DLP využívá existující emailovou infrastrukturu organizace a proxy systémy [24]. Velkou výhodou Symantec DLP je, že v rámci DLP řešení zahrnuje také Data Insight, produkt společnosti Veritas, specializující se na bezpečnost nestrukturovaných dat [23].

Cena řešení se odvíjí od počtu licencí a jejich rozsahu. Symantec je softwarové řešení, ale pro implementaci je třeba počítat i s náklady na hardware, jež řešení využívá a s dalšími nutnými úpravami ICT prostředí. Výrobce neposkytuje zkušební verzi. [25]

Implementace Symantec DLP je velmi rozsáhlá a nákladná. Jednotlivé komponenty musí být zvlášť instalovány a konfigurovány. Je vhodné spíše pro velké firmy, které před nižšími náklady upřednostní velmi rozsáhlé a spolehlivé řešení. [23; 24]

3.3.3 Forcepoint

Obrázek 4: Logo Forcepoint
Zdroj: [27]

Základy pro tuto americkou společnost vznikaly v roce 2015 sloučením podniků Raytheon and Vista Equity Partners. Došlo ke sloučení portfolií těchto dvou společností (produktová řada Websense a linii bezpečnostních produktů Raytheon Cyber Products). O rok později společnost koupila 2 produktové linie Intel Security (firewally Stonesoft a Sidewinder) a vstoupila na trh oficiálně jako Forcepoint. V roce 2017 společnost získala Skyfence CASB a RedOwl, výrobce stojící za produkty bezpečnostní analýzy. Raytheon nyní vlastní většinu společnosti. Forcepoint nabízí kromě DLP i firewally nové generace, ochranu webové a emailové komunikace, bezpečnost cloudových řešení ad. [25; 24]

Forcepoint DLP obsahuje tyto komponenty, jež mohou fungovat zvlášť či se implementovat dohromady:

- Forcepoint DLP Endpoint (ochrana dat na koncových stanicích operačních systémů Windows, Mac OS i Linux),
- Forcepoint DLP Cloud Applications (rozšíření platnosti bezpečnostních pravidel i do cloudových aplikací - Microsoft Office 365, Google G Suite, Box, ServiceNow a Salesforce),

- Forcepoint DLP Network (monitoruje data posílaná ze sítě organizace a uplatňuje na ně nakonfigurovaná bezpečnostní pravidla, funkce OCR),
- Forcepoint DLP Discover (skenuje data na serverech, v databázích a poštovních serverech, spolučinnost s podporovanými třetími stranami - SharePoint apod., funkce OCR) [25].

Podporuje ochranu strukturovaných i nestrukturovaných dat, OCR (Optical Character Recognition), ochranu dat skrze tisk, email, cloudové aplikace a přenosná media. Síťové i endpoint moduly lze spravovat skrz jednu konzoli. Řešení DLP Forcepoint je považováno za řešení, které lze poměrně levně implementovat, jednoduše konfigurovat a dlouhodobě spravovat. Představuje velmi přímočarý přístup k ochraně dat vhodný i pro menší organizace. Výrobce poskytuje zkušební verzi. [23; 25; 24]

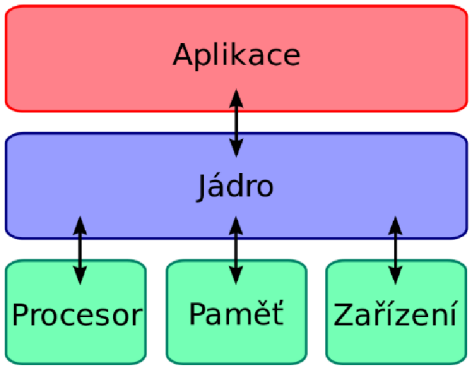
3.3.4 Digital Guardian

Obrázek 5: Logo Digital Guardian
Zdroj: [28]

Digital Guardian, oficiálně Verdasys, je americká společnost zaměřující se od svého vzniku v roce 2003 na vývoj bezpečnostní platformy pro ochranu dat. Společnost se vyznačuje silným porozuměním trhu, samotné bezpečnostní technologie, což vede k adekvátním inovacím produktu a posílení pozice leadera. [25; 24]

Z technického hlediska se Digital Guardian DLP (dále jen DG DLP) ve svém pojetí liší od tradičního pojetí DLP leadery trhu, kteří rozdělují hlavní komponenty do 3 skupin: Network (data in motion), Discovery (data at rest) a Endpoint (data in use).

Základem DG DLP je agent koncových stanic pracující na daném stroji přímo na úrovni jádra (tzv. DG Agent - DGA). Agenti na koncových stanicích komunikují s řídícím serverem v síti. Součinnost agenta s operačním systémem přímo na úrovni jádra poskytuje řešení komplexní přehled a kontrolu nad aktivitami ve stroji. Tento přístup může přinést potenciální problémy v kompatibilitě dalších aplikací s operačním systémem, které jsou ale ze



Obrázek 6: Jádro v kontextu systému
Zdroj: [29]

zkušeností zákazníků Gartner vyváženy benefity DG Agenta. [24]

Po koupi společnosti Code Green Networks v roce 2015 organizace rozšířila své řešení i o moduly network a dicovery. I po přidání modulů zůstává endpoint DG Agent jádrem řešení. [24]

DG DLP je vhodným řešením pro organizace, které kladou velmi silný důraz na přesné dodržování regulačních pravidel, specificky ve zdravotnictví nebo finančním sektoru. Produkt je také vhodný pro organizace zaměřující se na ochranu duševního vlastnictví. Velkou výhodou také může být schopnost DG DLP spravovat zařízení s Windows, Mac OS i Linux operačními systémy. Digital Guardian nabízí zkušební verzi zdarma. [23; 25; 24]

3.3.5 McAfee

Obrázek 7: Logo McAfee
Zdroj: [30]

Společnost McAfee, LLC. byla založena roku 1987 Johnem McAfeem, počítačovým programátorem. Přiřazuje se jí prvenství za vytvoření prvního komerčního antivirového softwaru. Nyní nabízí široké portfolio bezpečnostních produktů. [25; 24]

Na trh s DLP řešením vstoupila v roce 2006 po akvizici s výrobcem endpoint DLP řešení, společností Onigma. O dva roky později došlo k získání společnosti Reconnex, tehdejšího leadera v oblasti network DLP. V roce 2010 koupila společnost firma Intel. Došlo ke změně názvu a společnost McAfee je od té doby známa jako Intel Security. Po akvizici nedocházelo k dostatečnému vývoji McAfee DLP a produkt se na žebříčku trhu začal propadat. V roce 2016 došlo k oddělení společnosti Intel Security od společnosti Intel nákupem 51 % podílu společností TPG Capital. Společnost po oddělení dostala opět své původní jméno a po personální krizi se výrazně orientuje na inovaci DLP produktu. [25; 24]

McAfee DLP je členěno do několika komponent, které můžeme rozdělit do dvou skupin - host a network. Host moduly (Device Control a DLP Endpoint) jsou instalovány přímo na koncových zařízeních a network moduly (DLP Discover, Prevent a Monitor) ve formě appliance v síti. Některé moduly, podobně jako moduly Symantec DLP, fungují v součinnosti s proxy systémy. Moduly jsou spravovány přes centrální konzoli ePolicy

Orchestrator instalovanou na serveru v síti, kterou je možné spravovat i další produkty McAfee. Je možná pouze částečná implementace. [23]

Velkou výhodou je široké portfolio společnosti, jež nabízí vzájemné provázání a kompatibilitu jednotlivých řešení, která lze navíc spravovat přes jedinou konzoli (SIEM, antivirová řešení apod.). McAfee DLP integruje v ochraně dat mnoho třetích stran (doplňky do webových prohlížečů, kompatibilita s širokým spektrem cloudových úložišť, synchronizace s Active Directory, součinnost s produkty Microsoft Office - Outlook, Excel, Word apod.). Chrání strukturovaná i nestrukturovaná data skrz tisk, emailovou a webovou komunikaci, zachycování obrazovky, nahrávání na cloudová úložiště i přenosná datová zařízení. Podporuje OCR. [23; 25; 24]

Cena řešení se odvíjí od počtu licencí a jejich rozsahu. Finanční náklady mohou být vyšší při plné implementaci ačkoli na jejich snížení se podílí možnost instalace komponent na virtuální stroje. Výrobce nabízí zkušební verzi. [24; 25]

3.3.6 Sophos

Obrázek 8: Logo Sophos
Zdroj: [31]

Sophos je evropská společnost založená v roce 1985 Peterem Lammerem a Janem Hruskou. Sophos se zaměřuje na vývoj bezpečnostního softwaru v oblasti ochrany koncových stanic, šifrování, síťové, emailové a mobilní bezpečnosti pro střední a velké společnosti. V portfoliu jsou i produkty řady pro domácnost. Sophos Endpoint má některé funkcionality DLP.

3.3.7 Srovnání funkcionalit

Tabulka 17: Porovnání DLP řešení

Funkcionalita:	McAfee DLP ver. 11. 2	Digital Guardian - Threat Aware Data Protection Endpoint	Forcepoint DLP 8.6	Symantec DLP 15.5	Sophos Endpoint
Obecné požadavky		100+**		100+**	
synchronizace s Active Directory	ANO	ANO	ANO	ANO	ANO
synch. s AD zachovávající kontejnerizaci	ANO	NE	ANO	ANO	ANO
synch. s AD zachovávající groups	ANO	ANO	ANO	ANO	ANO
podpora Digital Rights Management	ANO	NE, podpora DRM s Microsoft v plánu (2020)	ANO	ANO	NE
správa dalších modulů (pokud jsou) z jedné konzole	ANO	ANO	ANO	ANO	ANO
Požadavky na klasifikace a definice					
vytváření vlastních klasifikačních stupňů a pravidel pro jejich udělování	ANO	ANO	ANO	ANO	ANO
možnost ručního oklasifikování souborů MS Office při jejich vzniku	ANO	NE	NE	NE	NE
možnost automatického oklasifikování dat na základě ručně nastavených pravidel pro udělování klasifikací	ANO	ANO	lze integrovat	lze integrovat	ANO
použití vlastních slovníků klíčových slov pro nastavení pravidel pro klasifikování	ANO	ANO	ANO	ANO	ANO
možnost porovnání celých částí dokumentu (např. hlavičky nebo patičky docx dokumentu)	ANO	ANO	ANO	ANO	NE
možnost tvorby vlastních definic užitých v bezpečnostních pravidlech (např. vydefinování USB disku konkrétního výrobce)	ANO	ANO	ANO	ANO	NE
Požadavky na bezpečnostní pravidla					
možnost nastavovat vlastní bezpečnostní pravidla	ANO	ANO	ANO	ANO	ANO
možnost definování bezpečnostních pravidel pro kontejner zařízení nebo skupinu uživatelů z AD	ANO	ANO	ANO	ANO	ANO
možnost definování výjimky z bezpečnostních pravidel pro skupinu uživatelů z AD nebo konkrétní uživatele	ANO	ANO	ANO	ANO	ANO
při porušení bezpečnostního pravidla ideálně možnost zobrazení edukační zprávy týkající se daného porušení	ANO	ANO	ANO	ANO	ANO, ale ne vlastní
možnost uživatele vyžádat si od administrátora pro danou akci, která není v souladu s bezpečnostními pravidly, výjimku	ANO	ANO	ANO	ANO	ANO
bezpečnostní pravidla zůstávají aktivní i po odpojení od sítě organizace	ANO	ANO	ANO	ANO	NE
Chráněné kanály možných úniků dat:					
emailová komunikace - outlook	ANO	ANO	ANO	ANO	ANO
webové rozhraní	ANO	ANO	ANO	ANO	ANO
clipboard ochrana (ctrl v + ctrl c)	ANO	ANO	ANO	ANO	NE
snímek obrazovky (screen capture)	ANO	ANO	ANO	ANO	NE
přenos na přenosná datová úložiště	ANO	ANO	ANO	ANO	ANO
vkládání na známá cloudová úložiště přes desktop aplikace	ANO	ANO	ANO	ANO	NE
Cena licence s podporou výrobce (rok)	69 USD (101 USD - CDA)	66 USD*	553,- bez DPH	3 494,- bez DPH	36 USD
Cena licence s podp. výr. (prodloužení)	18 USD (22,27 USD - CDA)	63,96 USD*	553,- bez DPH	3 494,- bez DPH	36 USD

Zdroj: vlastní zpracování

Vysvětlivky k tabulce:

* nejde o koncovou cenu řešení - je ještě nutné počítat s náklady na databázový systém *Oracle Standard Edition 2 for Data Loss Prevention* (viz. přibližná kalkulace)

** minimální objednávka počtu licencí je 100ks

Tabulka porovnává funkcionality a ceny licencí DLP koncových stanic různých výrobců. Ceny jsou uvedeny v Kč, případně v USD.

3.3.8 Přibližná kalkulace

V následující tabulce je uvedena přibližná pořizovací cena jednotlivých řešení zahrnující cenu licencí (bez DPH). Kalkulace není výpočtem TCO (Total Cost of Ownership) a nezahrnuje pořízení případného HW vybavení, implementační práce technika ani cenu údržby řešení.

Tabulka 18: Finanční porovnání DLP řešení

	cena licence (rok)	cena licence prodloužení (rok)	počet licencí ks	cena celkem v prvním roce	cena celkem 2. rok	cena celkem pro všechny stanice (5 let)
McAfee DLP	1 576 Kč	408 Kč	60	94 560 Kč	24 480 Kč	192 480 Kč
Digital Guardian DLP	1 508 Kč	1 461 Kč	100**	150 800 Kč	146 100 Kč	735 200 Kč
Forcepoint DLP	553 Kč	553 Kč	60	33 180 Kč	33 180 Kč	165 900 Kč
Symantec DLP	3 494 Kč	3 494 Kč	100**	525 209 Kč	525 209 Kč	2 626 045 Kč
Sophos Endpoint	824 Kč	824 Kč	60	49 440 Kč	49 440 Kč	247 200 Kč

Zdroj: vlastní zpracování

pozn. pro převod cen v USD na CZK byl použit směnný kurz 22,884 Kč za 1 USD

Do ceny řešení Symantec je třeba počítat i každoroční náklady na databázový systém *Oracle Standard Edition 2 for Data Loss Prevention v* hodnotě 175 810 Kč bez DPH ročně.

3.3.9 Konečný výběr řešení

Došlo k porovnání funkcionalit jednotlivých řešení a jejich ceny. Nejlepším řešením se z dlouhodobého hlediska pro organizaci jeví DLP Forcepoint (pětileté přímé náklady rovny 165 900 Kč) či McAfee DLP (pětileté přímé náklady rovny 192 480 Kč). V organizaci se ale již používá Endpoint Security od McAfee s centrální správou ePolicy Orchestrator, jež umožňuje spravovat i další produkty, včetně McAfee DLP, z jediné konzole. Tento fakt byl rozhodující při výběru řešení. Rozdíl ceny řešení je z dlouhodobého hlediska minimální. Případné personální i technické náklady spojené s integrací nového systému Forcepoint by v dlouhodobém horizontu převýšily úsporu za pořízení mnohonásobně. Z těchto důvodů bylo rozhodnuto o implementaci McAfee DLP verze 11.2.x, které je momentálně nejnovější verzí McAfee DLP.

3.4 Výběr způsobu správy DLP

Pro efektivní správu DLP řešení je třeba centrální management. Existují dva základní přístupy ke správě McAfee DLP - cloudové řešení a on premis řešení. Všechny produkty McAfee lze spravovat jedinou centrální správou, což je výhodou při implementaci dalších bezpečnostních technologií.

3.4.1 Cloudové řešení správy

DLP lze spravovat přes centrální správu v cloudu - MVISION. Server, na kterém ePO konzole, běží je mimo organizaci, stejně tak na něm uložená data. Logy DLP se posílají ze společnosti na server poskytovatele služby.

3.4.2 On premis řešení správy

DLP lze také spravovat přes konzoli ePolicy Orchestrator, jež je nainstalována jako software na serveru (tzv. ePo serveru) přímo v síti organizace - tzv. on premis řešení. Všechna data jsou uložena přímo na serveru ve společnosti.

3.4.3 Možnosti správy McAfee DLP

Konzole ePolicy Orchestrator je přístupná přes webové rozhraní a umožňuje komunikaci přes https protokol (možnost využít certifikát podepsaný interní certifikační autoritou). Skrz konzoli je možné spravovat všechny komponenty DLP (endpoint i network), nastavovat bezpečnostní pravidla, instalovat software na koncová zařízení, prohlížet statistiky o systémech, uživatelích a monitorovaných bezpečnostních událostech, exportovat manažerské výstupy apod. Konzole nabízí v praxi velmi využívanou synchronizaci s adresářovými službami LDAP (např. Active Directory od Microsoft), jež umožňuje import databází uživatelů a systémů, včetně možnosti zachování kontejnerizace a skupin uživatelů. Lze tak definovat bezpečnostní pravidla pro uživatelské skupiny, konkrétní uživatele i organizační jednotky (nebo kombinací vícero parametrů) definované v adresářové struktuře AD/LDAP. V samotném ePolicy Orchestratoru lze také nastavovat oprávnění (přístup k logům, statistikám, správě politik apod.) na základě rolí a uživatelské identity v AD, a s podporou autentizace pomocí klientských certifikátů. Konzole i samotné DLP jsou podporovány mnoha třetími stranami - integrace s cloudovými datovými úložišti či aplikacemi Office.

3.4.4 Konečný výběr způsobu správy

Po společné konzultaci s investorem bylo zvoleno on-premis řešení centrální správy. Rozhodující byl fakt, že organizace je již zvyklá používat konzoli ePolicy Orchestrator, jímž spravuje produkt Endpoint Security. Toto řešení je vyhovující a zaběhlé, a proto bylo rozhodnuto, že nebude docházet ke změně přístupu. ePO server organizace je však zastaralý, stejně tak, jako verze ePolicy Orchestratoru. V rámci implementace tedy musí dojít k migraci na nový server a upgradu softwaru konzole na novou verzi.

3.5 Výběr rozsahu implementace

McAfee DLP má několik komponentů, z nichž každý poskytuje další vrstvu bezpečnosti dat a zastává v jejich ochraně jinou roli:

- Device contorol
- DLP Discover
- DLP Endpoint
- DLP Prevent
- DLP Monitor

Tabulka 19: Přehled modulů McAfee DLP

Název	Forma	Hlavní účel	Typ dat
Device Control	SW	Kontrola připojených zařízení a přenosných datových úložišť ke koncovému zařízení.	Data in use
DLP Discover	Nainstalovaný SW na Windows Server	Skenování síťových a podporovaných cloudových úložišť	Data at rest
DLP Endpoint	SW	Řízení aktivit s daty na koncových stanicích, skenování lokálního úložiště na PC.	Data in use, data at rest
DLP Prevent	Virtuální systém (appliance) vč. SW v rámci dodaného OS	Kontrola webové anebo emailové komunikace.	Data in motion
DPL Monitor	Virtuální systém (appliance) vč. SW v rámci dodaného OS	Monitoring síťové komunikace (SMTP, HTTP, FTP, LDAP, Telnet, IRC, SMB…).	Data in motion

Zdroj: vlastní zpracování

3.5.1.1 Device Control

Device control (dále jen DC) kontroluje zařízení připojená k danému koncovému zařízení a přístup k nim. Většinou jde o přenosné USB disky nebo telefony, připojené jak fyzicky, tak i přes Bluetooth. Připojená zařízení můžeme na základě definicí:

- bez omezení povolit,

- blokovat,
- nastavit možnost pouze pro čtení.

3.5.1.2 **DLP Discover**

DLP Discover skenuje data v lokálních síťových a podporovaných cloudových úložištích, data klasifikuje, sbírá jejich metadata a následně vytváří statistiky. Statistiky jsou vytvářeny na základě analýz, kdy DLP Discover nabízí dva základní pohledy na data v úložištích:

- z hlediska specifikace **souborů** (velikost souborů, typy souborů, datum poslední práce se souborem),
- z hlediska **klasifikací** (jaké klasifikace jsou v úložišti přítomny a jaké je jejich zastoupení).

3.5.1.3 **DLP Endpoint**

DLP Endpoint pracuje přímo na daném koncovém zařízení, kde skenuje lokální souborový systém a sleduje aktivity s daty. DLP Endpoint dané akce (jako např. poslání emailu s přílohou nebo přesun souboru s účetními dokumenty na flash disk) může na základě klasifikací:

- ignorovat,
- blokovat,
- vytvořit záznam o dané akci,
- předmět (data) akce pomocí spolupráce s vybraným šifrovacím klíčem zašifrovat.
- atd.

3.5.1.4 **DLP Prevent**

Modul DLP Prevent je ve formě virtuální jednotky vč. OS na bázi Linux na fyzicky přítomném serveru v síti organizace. Prochází webovou anebo emailovou komunikaci, analyzuje ji a na základě bezpečnostních pravidel rozhoduje, zda

komunikaci povolí či nikoli. Pracuje v součinnosti s poštovním serverem (MTA server) anebo webovým proxy serverem.

Modul dostává od MTA serveru pomocí SMTP protokolu (Simple Mail Transfer Protocol) emailovou komunikaci. Pokud modul daný email na základě analýzy zablokuje, odesílatel je o tom informován a email nemůže být poslán. Pokud je email modulem schválen, dojde k přidání X-RCIS-Action hlavičky a odeslání emailu zpět MTA serveru, který se postará o jeho hladké odeslání adresátovi. MTA server musí podporovat funkci analýzy hlaviček (header inspection) na základě které vynutí požadovanou akci.

Kontrola webového provozu modulem DLP Prevent probíhá obdobně. Modul dostává od webového proxy serveru pomocí protokolu ICAP (Internet Content Adaptation Protocol) webovou komunikaci jako nadřazená ICAP proxy. DLP Prevent komunikaci analyzuje a na jejím základě posílá proxy serveru pokyn, zda má být daná komunikace uskutečněna, či zamítnuta. Tímto způsobem mohou být analyzovány např. emaily posílané přes webový prohlížeč či nahrávané soubory do internetových úložišť.

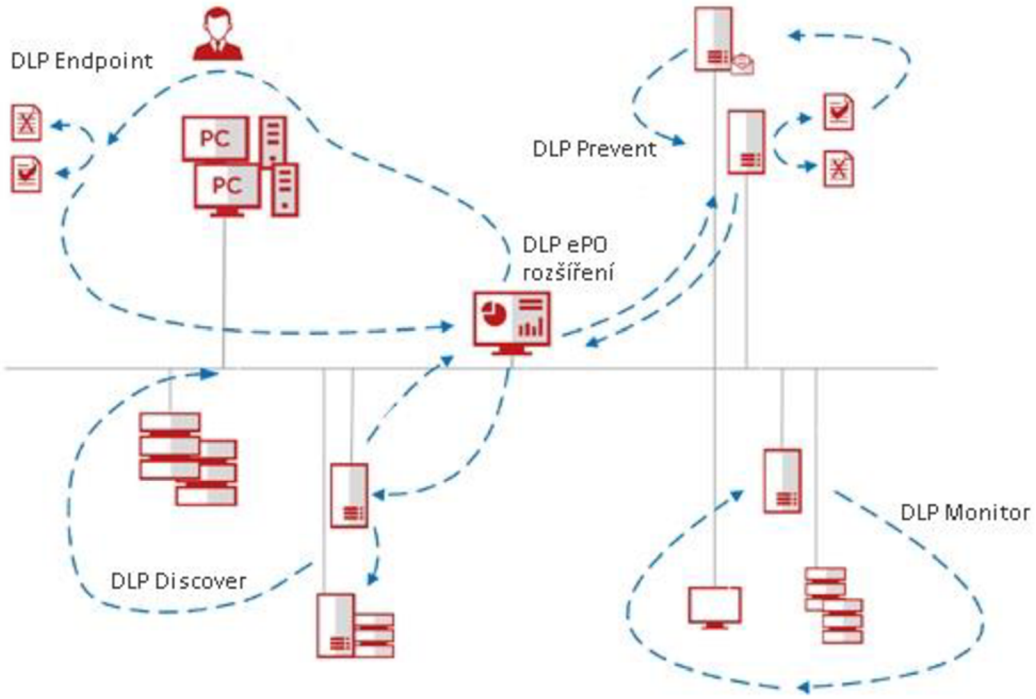
Je možné také analyzovat emaily posílané na mobilní zařízení. Funkcionalita ActiveSync Microsoft Exchange umožňuje mobilním aplikacím přímé připojení k Exchange serveru, a tak i posílání a přijímání emailů. Protože tato komunikace nevyužívá SMTP protokol, její kontrola probíhá na úrovni AciveSync proxy a podporuje standardní řešení, např. MobileIron Mobile Device Management (MDM) serveru.

3.5.1.5 **DLP Monitor**

Modul DLP Prevent je ve formě appliance instalován na virtuální jednotce na fyzicky přítomném serveru v síti organizace. Pomocí interní infrastruktury, za využití SPAN či Mirror portů na switchích a nebo TAP zařízení modul dostává kopie paketů síťové komunikace, analyzuje je a výsledky analýzy odesílá ePO serveru. Lze analyzovat komunikaci využívající následující protokoly: SMTP, HTTP, FTP, IMAP, POP3, LDAP, Telnet, IRC, SMB. Za běžných okolnostní nedochází k analýze šifrované komunikace.

3.5.1.6 **Součinnost McAfee DLP komponent**

Na následujícím obrázku je znázorněna součinnost DLP komponent.



Obrázek 9: Součinnost McAfee DLP komponent
Zdroj: přeloženo a přejato z [9]

3.5.1.7 Kalkulace možných rozsahů implementace

Komponenty se navzájem doplňují a dohromady poskytují komplexní ochranu proti úniku dat způsobeného interními faktory při práci s daty. Nutné je ale také přihlížet k míře přiměřené bezpečnosti v závislosti na rizicích a finančních výdajích za opatření. McAfee momentálně nabízí možnosti licencování dle tabulky níže.

Tabulka 20: Licenční balíčkyMcAfee DLP

	Mc Afee Data Protection licenční balíčky		
Produkty	TDL	CDA	CDB
DLP Endpoint			
Device Control			
Drive Encryption - šifrování celých PC			
File and Removable media Protection - šifrování souborů			
Management of Native Encryption) - správa šifrování*			
DLP Monitor, DLP Prevent, DLP Discover - síťové řešení			

Zdroj: vlastní zpracování

* centrální správa pro šifrování typu BitLocker (Windows) nebo File Vault (Mac)

TDL - McAfee Total Protection for Data Loss Prevention Appliance Software

CDA - McAfee Complete Data Protection Advanced

CDB - McAfee Complete Data Protection

Při výběru licence byla zvážena následující kalkulace, jež zahrnuje přibližnou nákupní cenu licencí bez DPH pro 60 koncových stanic.

Tabulka 21: Přibližná kalkulace - porovnání DLP Endpoint a DLP CDA licence

	cena licence (rok)	cena licence prodloužení (rok)	počet nakoupených licencí ks	cena celkem v prvním roce	cena celkem 2. rok	cena celkem (5 let) pro všechny stanice
McAfee DLP CDA	2 307 Kč	508 Kč	60	138 420 Kč	30 480 Kč	260 340 Kč
McAfee DLP Endpoint	1 576 Kč	408 Kč	60	94 560 Kč	24 480 Kč	192 480 Kč

Zdroj: vlastní zpracování

3.5.1.8 **Zvolený rozsah implementace**

Na základě konzultace s investorem byl vybrán licenční balíček CDA (McAfee Complete Data Protection Advanced). Investor preferuje používat DLP pouze na koncových stanicích (bez appliance síťového řešení), vítá možnost centrálního šifrování disků v podobě produktu Drive Encryption i možnost šifrování souborů díky File and Removable media Protection. Předpokládá vyšší bezpečnost a úsporu času oproti dosavadnímu řešení, které neumožňuje centrální správu šifrování. Základní součástí balíčku je i produkt Device Control. Bylo dohodnuto, že v rámci první fáze dojde pouze k implementaci DLP Endpoint a případně konfiguraci možných pravidel pro Device Control.

3.6 Vytvoření plánu implementace

Před vytvořením plánu průběhu implementace DLP bylo nutné formulovat požadavky. Na základě těchto požadavků bylo vybráno konkrétní DLP řešení (výrobce) a určen jeho rozsah vhodný pro organizaci. Na základě rozsahu a znalosti konkrétního řešení, znalosti organizace, jejích procesů a požadavků lze vypracovat podrobný plán implementace.

3.6.1 Klíčové činnosti plánu implementace

Klíčové činnosti implementace jsou rozděleny do 9 okruhů a popsány v následující tabulce:

Tabulka 22: Klíčové činnosti implementace

Činnost
1. Příprava technického zázemí 1.1. kontrola požadavků v dokumentaci 1.2. formulace požadavku na technické zázemí 1.3. alokace serverového prostoru a vytvoření přístupů
2. Příprava ePolicyOrchestratoru 2.1. export politik ze staré ePo konzole 2.2. instalace ePO na novém serveru (nová SQL databáze* + instalace SW) 2.3. obnovení nastavení v nové verzi konzole dle původního nastavení (import politik, přístup uživatelů, synchronizace s AD apod.) 2.4. komunikace klientských stanic s novým serverem beze změny nastavení
3. Příprava hrubého návrhu politik 3.1. organizace poskytne vzorové soubory dat a požadované slovníky 3.2. navrhnutí pravidel pro klasifikování a formulace definic 3.3. navrhnutí bezpečnostních politik 3.4. konzultace hrubého návrhu s organizací 3.5. zapracování námětů 3.6. vytvoření finální verze hrubého logického návrhu nastavení
4. Testovací prostředí 4.1. alokace testovacích PC 4.2. instalace DLP na ePo server (DLP v repozitáři ePO) 4.3. vytvoření speciálního testovacího prostředí komunikujícího s ePo serverem, na kterém bude testováno nastavení dle dokumentace hrubého logického návrhu 4.4. nastavení definic, klasifikací a politik pro DLP 4.5. postupné uplatňování politik, testování a jejich úprava 4.6. testování politik se vzorovými soubory a případná úprava nastavení
5. Školení administrátorů 5.1. základní proškolení 5.2. detailní proškolení (administrátoři schopni DLP řešení spravovat)

6. Pilotní implementace 6.1. výběr uživatelů zapojených do pilotní instalace (reálný + placebo vzorek) 6.2. školení uživatelů 6.3. distribuce agentů a instalace DLP Endpoint na vybrané uživatelské stanice 6.4. průběh testování a podpora uživatelům 6.5. sběr zpětné vazby od testovací skupiny zaměstnanců 6.6. analýza výsledků testování dle logů DLP v ePO konzoli 6.7. vypracování reportu o pilotní implementaci a příprava návrhů na zlepšení 6.8. zhodnocení testování a rozhodnutí o dalších případných změnách 6.9. úprava politik pro plnou implementaci
7. Plná implementace 7.1. distribuce DLP Endpoint na zbylé stanice 7.2. průběh testování a podpora uživatelům 7.3. sběr zpětné vazby od zaměstnanců 7.4. analýza výsledků testování dle logů DLP v ePO konzoli 7.5. zajištění finální vyhovující verze politik (případná úprava politik, otestování)
8. Zpřísnění politik 8.1. v určených případech změna reakce DLP „warning“ na „block“ 8.2. testování, podpora uživatelům a řešení tzv. false positive 8.3. finalizace a kontrola nastavení
9. Ukončení implementace 9.1. zhodnocení implementace 9.2. předání DLP řešení

Zdroj: vlastní zpracování

Dodržení principů PDCA cyklu (Plan-Do-Control-React) je pro správnou implementaci DLP klíčové. Plán implementace i jednotlivé klíčové činnosti musí tento fakt respektovat. V rámci procesu implementace musí v několika cyklech docházet ke kontrole bezpečnostních pravidel a jejich případné úpravě. I po skončení projektu a předání DLP řešení do správy organizace je třeba neustále celé řešení kontrolovat a případně upravovat dle právě aktuální potřeby organizace. Jde o nikdy nekončící proces zlepšování.

Souhrnná tabulka v následující kapitole vychází ze zmíněných klíčových činností, ale obsahuje také dobu trvání jednotlivých oblastí činností a zakomponovanou RACI matici pro jednodušší řízení projektu implementace.

3.6.2 Souhrnná tabulka projektu (s RACI maticí)

IMPL = implementátor **ITA=** administrátor organizace **VO** = vedení organizace **ZRPI** = zaměstnanci reální pilotní implementace **ZPPI** = zaměstnanci placebo pilotní implementace **ZO** = ostatní zaměstnanci

Tabulka 23: Souhrnná tabulka projektu implementace

Činnost	Doba trvání (dny)	Výstup	Poznámka	Role (RACI matice)						
				Označení činnosti	IMPL	ITA	VO	ZRPI	ZPPI	ZO
1. Příprava technického zázemí 1.1. kontrola požadavků v dokumentaci 1.2. formulace požadavku na technické zázemí 1.3. alokace serverového prostoru a vytvoření přístupů	**2 dny**	Prostředí připravené pro migraci ePO konzole na nový server a následnou implementaci DLP.	Příprava prostředí	**1. Příprava technického zázemí**						
				1.1.	A, R					
				1.2.	A, R	I				
				1.3	I, C	R	A			
2. Příprava ePolicyOrchestratoru 2.1. export politik 2.2. instalace ePO na novém serveru (nová SQL databáze* + instalace SW) 2.3. obnovení nastavení v nové verzi konzole dle původního nastavení (import politik, přístup uživatelů, synchronizace s AD apod.) 2.4. komunikace klientských stanic s novým serverem beze změny nastavení	**2 dny**	Plně funkční ENS a ePO, klienti bez problému komunikující s ePo serverem.		**2. Příprava ePolicyOrchestratoru**						
				2.1.	A, R	C				
				2.2	A, R	C				
				2.3.	A, R	C				
				2.4.	A	R	I	I	I	I
3. Příprava hrubého návrhu politik 3.1. organizace poskytne vzorové soubory dat a požadované slovníky 3.2. navrhnutí pravidel pro klasifikování a formulace definic 3.3. navrhnutí bezpečnostních politik 3.4. konzultace hrubého návrhu s organizací 3.5. zapracování námětů 3.6. vytvoření finální verze hrubého logického návrhu nastavení	**5 dní**	Kompletní návrh hrubého logického nastavení zpracovaného v dokumentu odsouhlaseného vedením organizace.	Příprava bezpečnostních pravidel	**3. Příprava hrubého návrhu politik**						
				3.1.	C	R	A, R			
				3.2.	A, R					
				3.3.	A, R					
				3.4	A, R	R	R			
				3.5	A, R		I			
				3.6.	A, R	C	I			
4. Testovací prostředí 4.1. alokace testovacích PC 4.2. instalace DLP na ePo server (DLP v repozitáři ePO) 4.3. vytvoření speciálního testovacího prostředí komunikujícího s ePo serverem, na kterém bude testováno nastavení dle dokumentace hrubého logického návrhu 4.4. nastavení definic, klasifikací a politik pro DLP	**5 dní**	Vyhovující verze politik pro ostrý provoz (částečná pilotní implementace), založených na funkcích „warning“ a „monitor“.	Nastavení bezpečnostních pravidel bez jejich aplikace v provozu.	**4. Testovací prostředí**						
				4.1.	I	A, R				
				4.2.	A, R	C				
				4.3.	A, R	C				
				4.4.	A, R					

4.5. postupné uplatňování politik, testování a jejich úprava 4.6. testování politik se vzorovými soubory a případná úprava nastavení				4.5.	A, R					
				4.6.	A, R	C	C			
5. Školení administrátorů 5.1. základní proškolení 5.2. detailní proškolení (administrátoři schopni DLP řešení spravovat)	**4 dny**	Administrátoři rozumí DLP technologii a jsou schopni její samosprávy.	Administrátoři jsou postupně v několika kolech obeznámeni s DLP řešením	**5. Školení administrátorů**						
				5.1.	R	R	A	I	I	I
				5.2.	R	R	A	I	I	I
6. Pilotní implementace 6.1. výběr uživatelů zapojených do pilotní instalace (reálný + placebo vzorek) 6.2. školení uživatelů 6.3. distribuce agentů a instalace DLP Endpoint na vybrané uživatelské stanice 6.4. průběh testování a podpora uživatelům 6.5. sběr zpětné vazby od testovací skupiny zaměstnanců 6.6. analýza výsledků testování dle logů DLP v ePO konzoli 6.7. vypracování reportu o pilotní implementaci a příprava návrhů na zlepšení 6.8. zhodnocení testování a rozhodnutí o dalších případných změnách 6.9. úprava politik pro plnou implementaci	**10 dní**	Vyhovující verze politik pro ostrý provoz (plná implementace), založených na funkcích „warning“ a „monitor“.	Bezpečnostní pravidla v provozu pouze monitorují a podávají hlášení. .	**6. Pilotní implementace**						
				6.1.	R	R	C, A			
				6.2.	R	C	R, A	R	R	R
				6.3.	R, A	I	I	I	I	I
				6.4.	R, A	R	I	R	I	I
				6.5	R, A		I	R	R	I
				6.6.	R, A					
				6.7.	R, A	C				
				6.8.	R	R	R, A			
				6.9.	R, A		I			
7. Plná implementace 7.1. distribuce DLP Endpoint na zbylé stanice 7.2. průběh testování a podpora uživatelům 7.3. sběr zpětné vazby od zaměstnanců 7.4. analýza výsledků testování dle logů DLP v ePO konzoli 7.5. zajištění finální vyhovující verze politik (případná úprava politik, otestování)	**10 dní**			**7. Plná implementace**						
				7.1.	R, A	I	I	I	I	I
				7.2.	R, A	R		R	R	R
				7.3.	R, A		I	R	R	R
				7.4.	R,A					
				7.5.	R, A	C	C			
8. Zpřísnění bezpečnostních pravidel 8.1. v určených případech změna reakce DLP „warning“ na „block“ 8.2. testování, podpora uživatelům a řešení tzv. false positive 8.3. finalizace a kontrola nastavení	**10 dní**	Plně funkční DLP.	Bezpečnostní pravidla blokují, monitorují a podávají hlášení.	**8. Zpřísnění bezpečnostních pravidel**						
				8.1.	R, A	I				
				8.2.	R, A	R	I			
				8.3.	R, A	I	I			
9. Ukončení implementace 9.1. zhodnocení implementace 9.2. předání DLP řešení	**2 dny**	Ukončení projektu.		**9.Ukončení implementace**						
				9.1.	R		R, A			
				9.2.	R,A	R	R			

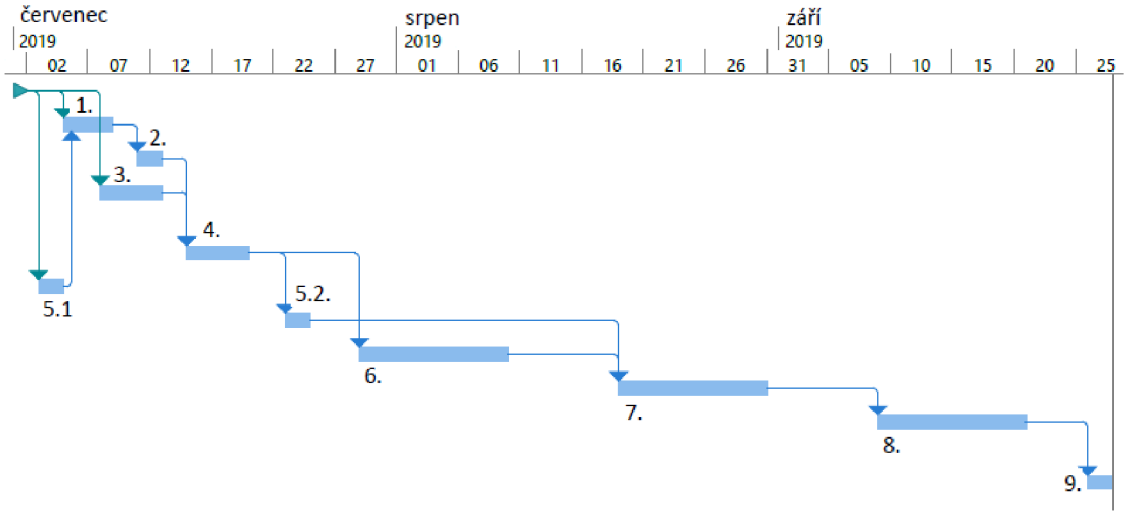
Zdroj: vlastní zpracování

3.6.3 Časová analýza implementace

V rámci předprojektové části projektu implementace DLP došlo k časové analýze projektu. Byl vypracován Ganttův diagram.

Název úlohy	Trvání	Začátek	Dokončení
Zahájení implementace	0 dnů	Po 01.07.19	Po 01.07.19
1. Příprava technického zázemí	2 dny	Pá05.07.19	Po 08.07.19
2.Příprava ePolicyOrchestratoru	2 dny	Čt 11.07.19	Pá12.07.19
3.Příprava hrubého návrhu politik	5 dní	Po 08.07.19	Pá12.07.19
4. Testovací prostředí	5 dní	Po 15.07.19	Pá19.07.19
5.1 Základní proškolení	2 dny	St 03.07.19	Čt 04.07.19
5.2.Detailní proškolení	2 dny	Ut 23.07.19	St 24.07.19
6. Pilotní implementace	10 dní	Po 29.07.19	Pá09.08.19
7. Plná implementace	10 dní	Po 19.08.19	Pá30.08.19
8. Zpřísnění bezpečnostních pravidel	10 dní	Po 09.09.19	Pá 20.09.19
9. Ukončení implementace	2 dny	Čt 26.09.19	Pá 27.09.19

Obrázek 11: Ganttův diagram - úlohy
Zdroj: vlastní zpracování



Obrázek 10: Ganttův diagram - časová osa úloh
Zdroj: vlastní zpracování

Pro délku jednotlivých činností a jejich návaznost byla započítána mírná časová rezerva. Pro organizaci není kritické případné posunutí termínu dokončení projektu, které

by mohlo být způsobeno zpožděním jednotlivých navazujících činností. Tento fakt byl zohledněn při určení výše časových rezerv.

Riziko případného zpoždění by mohlo nastat zejména z možných prodlení na vyhovění požadavkům implementace ze strany organizace (např. technik organizace připravující technické zázemí nebude k dispozici, organizace nepošle včas požadované podklady, dojde k pozdnímu schválení návrhu politik organizací apod.) či v případě neočekávaných technických problémů. Tato rizika je před začátkem samotné implementace nutno komunikovat, aby je bylo možné v rámci projektu adekvátně řídit.

Vzhledem k přehlednosti a povaze projektu byly v Ganttově diagramu použity pouze hlavní oblasti činností (označeny číslováním jedné úrovně) z tabulky projektu v kapitole *3.6.2 Souhrnná tabulka projektu (s RACI maticí)*, bez zmínění daných pod-činností, s výjimkou školení administrátorů (bod 5.1 a 5.2.), které bude dle plánu projektu probíhat ve dvou na sebe navzájem nenavazujících termínech. Ostatní chronologicky uspořádané pod-činnosti v rámci hlavních oblastí činností souhrnné tabulky projektu na sebe přímo navazují nebo jejich přesné chronologické uspořádání v rámci oblasti činnosti není klíčové.

3.7 Návrh nastavení bezpečnostních pravidel pro ochranu dat

Příprava první verze bezpečnostních pravidel pro reálnou implementaci v organizaci probíhá v rámci oblastí klíčových činností **3. Příprava hrubého návrhu politik** a **4. Testovací prostředí**.

Nastavení bezpečnostních pravidel, neboli DLP politik, funguje na základě definicí a klasifikací. DLP. V sekci DLP lze nastavovat několik tipů pravidel:

- Application File Access Protection,
- Cloud Protection,
- Email Protection,
- Network Communication Protection,
- Network Share Protection,
- Printer Protection,
- Removable Storage Protection,

- Screen Capture Protection,
- Web Protection.

DLP politiky - nastavení DLP. Jde o bezpečností pravidla definující, jak se má DLP chovat, když uživatel na koncovém stanici pracuje s daty. DLP může danou akci (např. odeslání souboru emailem, přesun na USB disk, zachycení dat snímkem obrazovky apod.) zablokovat, povolit, zaznamenat do databáze incidentů a v některých případech dokonce uložit i soubor, jež byl předmětem akce (např. uložit snímek obrazovky s citlivými údaji, který chtěl daný uživatel pořídit). V určitých případech může DLP daná data zašifrovat pomocí FRP klíčů.

Klasifikace - účinnost McAfee DLP politik se vztahuje vždy na určitá data. Některá data chceme chránit více či jinak, než jiná, a proto je třeba je rozdělit do tzv. klasifikací. Klasifikujeme data, která chceme chránit či monitorovat. McAfee DLP umožňuje automaticky udělovat klasifikace na základě **obsahu** (tzv. content classification) nebo na základě tzv. **otisků** (v originále „content fingerprint"), tedy např. na základě toho, jaká aplikace soubor s daty vytvořila, kde se daný soubor nachází nebo na základě toho, přes jakou webovou URL adresu došlo ke stažení nebo otevření souboru.

Definice - jsou používány pro vytváření klasifikací a samotných politik. Definice jsou naprostým základem pro správné nastavení DLP. Jsou to například slovníky klíčových slov nebo nadefinované vzory, podle kterých lze v textu například rozeznat rodné číslo či číslo kreditní karty. Definice definují objekty užívané v bezpečnostních politikách. Na základě definic např. DLP rozlišuje, co chápe jako běžné USB zařízení, co jako organizací specifikované USB zařízení a co jako SD kartu.

3.7.1 Návrh kategorií klasifikací

V první řadě na základě povahy dat v organizaci a požadavků na ochranu specifikujeme jednotlivé klasifikace a představu o jejich specifikaci.

Dle požadavků organizace a souladu s ISMS jsou navrženy následující klasifikace:

- Osobní údaje (zkratka OSB),
- Interní (zkratka INT),
- Citlivé (zkráceně C),
- Velmi citlivé (zkráceně VC).

Osobní údaje chce společnost pouze monitorovat. Za objekt s osobními údaji bude považován soubor, popř. email, který jich nese větší množství - viz. tvorba klasifikačních pravidel. Faktura obsahující jméno a příjmení osoby spolu s telefonním číslem nebo emailem nebudeme z hlediska klasifikace považovat za osobní údaj, protože udělení takové klasifikace není v souladu s cílem zavedení DLP a bylo by nesmyslné. Za objekt obsahující osobní údaje by měla být považována také data nesoucí rodná čísla. Tato klasifikace dat dle logiky ISMS spadá pod data interní. V rámci sledování práce s osobními údaji byla ale tato klasifikace z hlediska DLP osamostatněna.

Objekty nesoucí **Interní data** jsou dle ISMS společnosti povinně označovány jako „ORG INTERNÍ“, kde ORG zastupuje zkratku názvu organizace. MS Office dokumenty jsou označovány na úvodní stránce. Emaily jsou označovány v předmětu.

Objekty nesoucí **Citlivá data** musí být stejně jako data interní označována klíčovým slovem „ORG CITLIVÉ“, kde ORG zastupuje zkratku názvu organizace..

Objekty nesoucí **Velmi citlivá data** musí být dle ISMS, stejně jako data spadající pod klasifikace Interní a Citlivé, označována slovním spojením „ORG VELMI CITLIVÉ“, kde ORG zastupuje zkratku názvu organizace. Dokumenty týkající se ICT zákazníků spadající pod tuto klasifikaci navíc musí být označovány speciální signaturou, popř. jejich kombinací, v záhlaví dokumentu

3.7.2 Tvorba klasifikačních pravidel

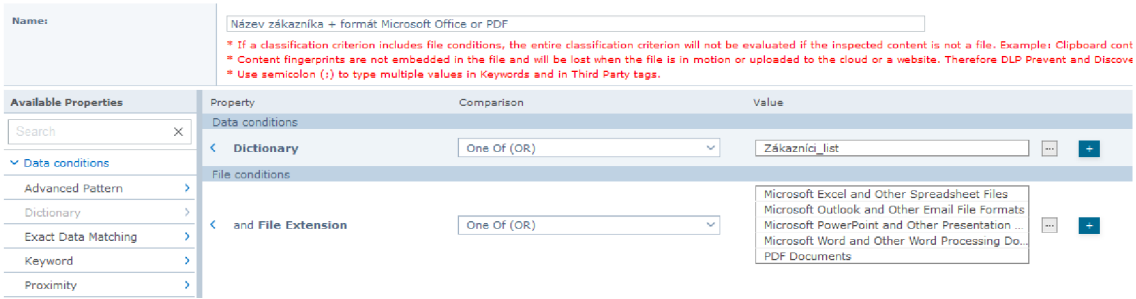
Následně přichází na řadu tvorba samotných klasifikačních pravidel. McAfee DLP při automatické klasifikaci na základě těchto pravidel přiděluje souborům s daty klasifikaci. Nastavení klasifikačních pravidel je klíčové pro správné fungování DLP.

Osobní údaje - OSB

- importovány a použity slovníky nejčastějších českých jmen a příjmení, českých poštovních směrovacích čísel a slovník rodinných stavů (obsahuje klíčová slova jako vdaný, vdaná, svobodný, rozvedená apod.)
- klasifikační pravidlo na základě CNTC (content classification)
- podmínky přidělení klasifikace (stačí splnit jeden z bodů):
    - obsahuje české jméno i příjmení z importovaných slovníků a také (logický operátor AND) PSČ nebo rodinný stav
    - obsahuje 4 česká jména a 4 česká příjmení a minimálně jedno rodné číslo (české či slovenské)

Interní - INT

- klasifikační pravidlo na základě CNTC (content classification)
- podmínky přidělení klasifikace (stačí splnit jeden z bodů):
    - obsahuje spojení „org interní“
    - obsahuje název společnosti, jež je zákazníkem organizace a zároveň jde o PDF dokument či soubor MS Office



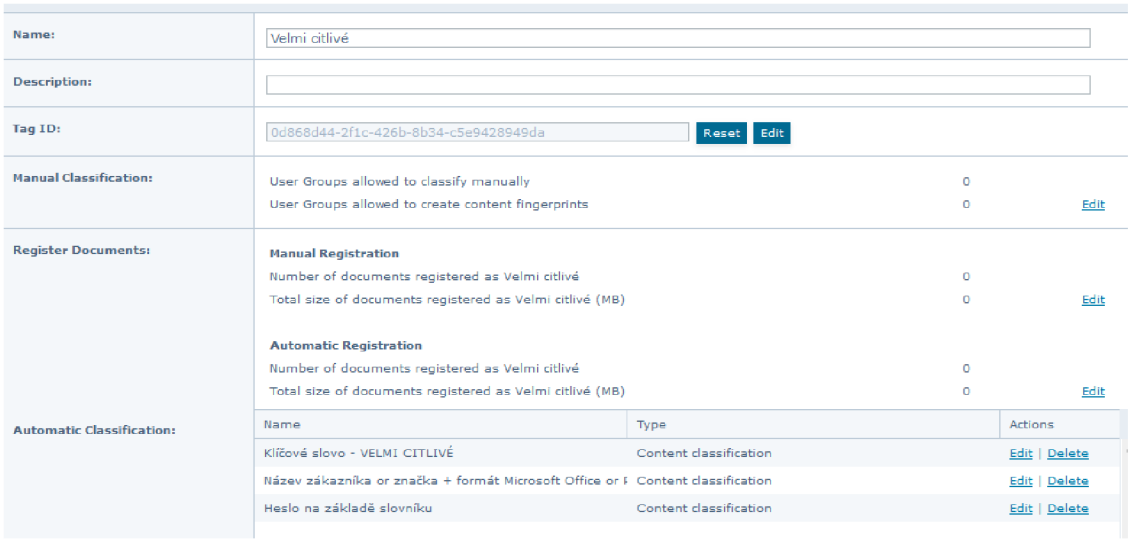
Obrázek 12: Nastavení DLP - příklad nastavení klasifikačního pravidla
Zdroj: vlastní zpracování

Citlivé - C

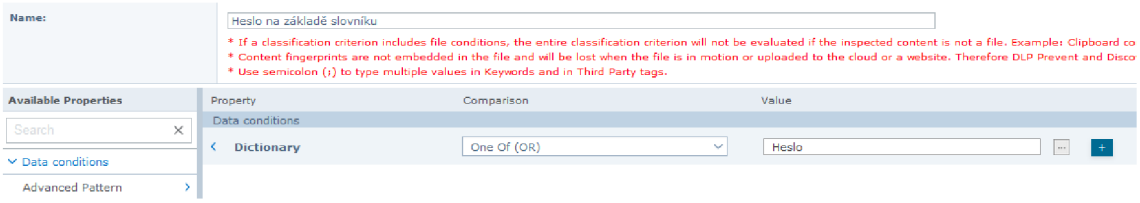
- importován a použit slovník obsahující názvy zákazníků organizace
- klasifikační pravidlo na základě CNTC (content classification)
- podmínky přidělení klasifikace (stačí splnit jeden z bodů):
    - obsahuje spojení „org citlivé“ v jakémkoli používaném slovním tvaru

Velmi citlivé - VC

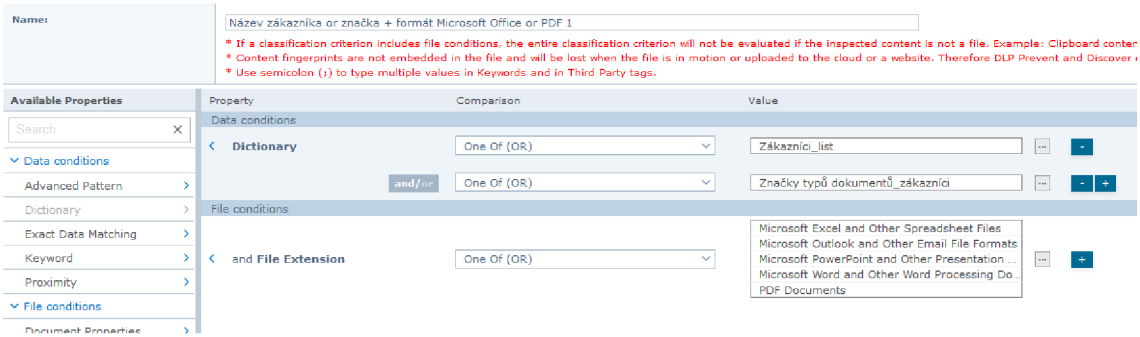
- importovány a použity slovníky obsahující názvy zákazníků organizace, signatur používaných pro označování souborů dokumentujících ICT zákazníků org. a slovník s klíčovými slovy týkající se hesel (obsahující slova jako heslo, password apod.)
- klasifikační pravidlo na základě CNTC (content classification)
- podmínky přidělení klasifikace (stačí splnit jeden z bodů):
    - obsahuje slovní spojení „org velmi citlivé“ v jakémkoli používaném slovním tvaru
    - obsahuje položku z importovaného slovníku *Heslo*
    - obsahuje název společnosti, jež je zákazníkem organizace, zároveň jde o PDF dokument či soubor MS Office a zároveň obsahuje alespoň jednu ze signatur pro označování velmi citlivých dokumentů



Obrázek 13: Nastavení DLP - přehled nastavení klasifikace
Zdroj: vlastní zpracování



Obrázek 14: Nastavení DLP - příklad klasifikačního pravidla
Zdroj: vlastní zpracování



Obrázek 15: Nastavení DLP - příklad nastavení klasifikačního pravidla pro VC klasifikaci
Zdroj: vlastní zpracování

3.7.3 Vlastní definice

Při konfiguraci DLP byly užity výchozí McAfee DLP definice i vlastní definice, jež byly vytvořeny, aby bylo možno lépe chránit data společnosti na základě jejich specifik a užití v českém prostředí.

3.7.3.1 Přehled užitých slovníků

Pro tvorbu klasifikačních pravidel byly do ePo konzole nahrány nové slovníky klíčových slov. Jde o tyto slovníky:

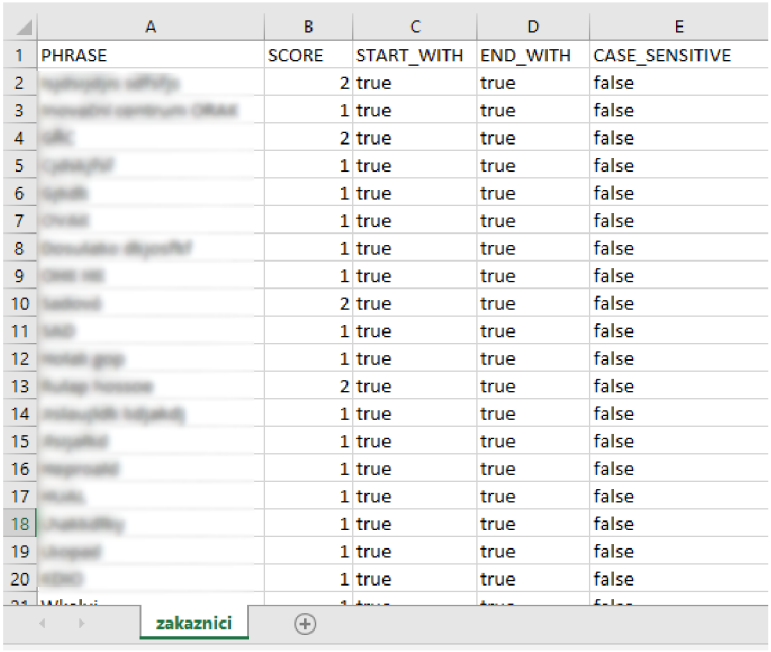
- 500 nejpoužívanějších českých jmen,
- 500 nejpoužívanějších českých příjmení,
- slovník názvů společností, jež jsou zákazníky organizace,
- česká poštovní směrovací čísla,
- slovník rodinných stavů (obsahuje slova jako vdaný, vdaná, svobodný, rozvedená apod.),
- slovník klíčových slov spojených s hesly,
- slovník užitých zkratek pro označování velmi citlivých dokumentů dle ISMS.

3.7.3.2 Tvorba vlastního slovníku

Slovníky pro McAfee DLP jsou nahrávány v sekci pro definice nebo skrz modul pro nastavování politik. Snímky obrazovky pocházející přímo z procesu definování

slovníku *Zákazníci_list* jsou přiloženy spolu s popsáním tvorby slovníku. Vzhledem k povaze bakalářské práce byly konkrétní názvy znečitelněny.

Nejprve je v excelu vytvořen slovník dle šablony (položky *PHRASE, SCORE, START_WITH, END_WITH, CASE_SENSITIVE*).



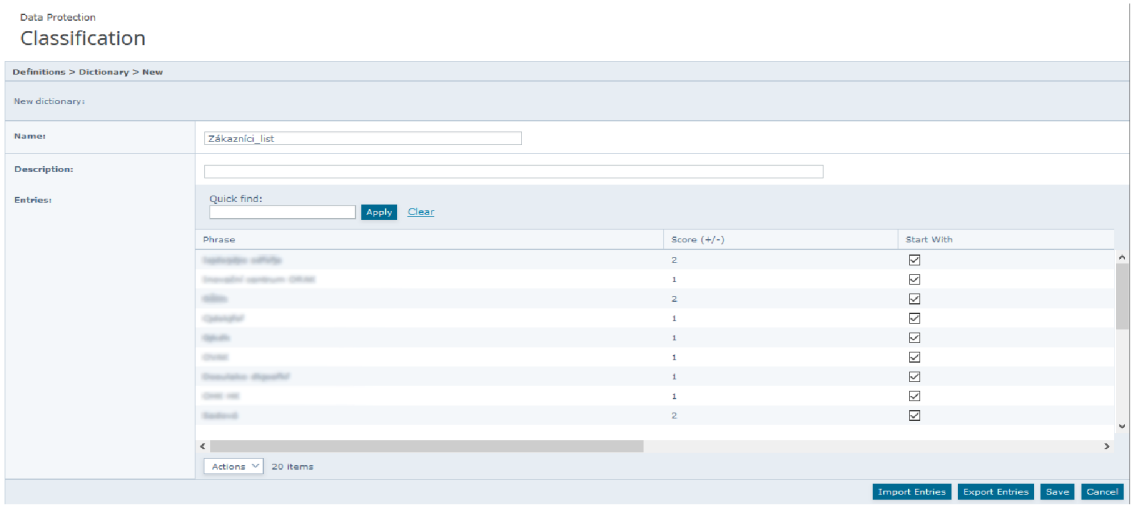
	A	B	C	D	E
1	PHRASE	SCORE	START_WITH	END_WITH	CASE_SENSITIVE
2	[redacted]	2	true	true	false
3	[redacted]	1	true	true	false
4	[redacted]	2	true	true	false
5	[redacted]	1	true	true	false
6	[redacted]	1	true	true	false
7	[redacted]	1	true	true	false
8	[redacted]	1	true	true	false
9	[redacted]	1	true	true	false
10	[redacted]	2	true	true	false
11	[redacted]	1	true	true	false
12	[redacted]	1	true	true	false
13	[redacted]	2	true	true	false
14	[redacted]	1	true	true	false
15	[redacted]	1	true	true	false
16	[redacted]	1	true	true	false
17	[redacted]	1	true	true	false
18	[redacted]	1	true	true	false
19	[redacted]	1	true	true	false
20	[redacted]	1	true	true	false

zakaznici

Obrázek 16: Tvorba slovníku
Zdroj: vlastní zpracování

Ve sloupci *phrase* jsou vypsány názvy zákazníků investující organizace. Atribut *score* slouží pro vyjádření důležitosti a relevantnosti klíčového slova a může nabývat kladných i záporných hodnot. Atributy *start_with* a *end_with* určují zda dané slovo musí být pro detekci užito v přesném znění ve smyslu jeho úplnosti od začátku či od konce slova. Např. slovo „Irka“ bude při obou atributech v hodnotě *true* identifikováno jako slovo ze slovníku jen pokud bude takto začínat i končit, tedy bude přesně v tomto znění. Pokud bude hodnota atributu *start_with* změněna na hodnotu *false*, pak budou jako slova ze slovníku identifikovány např. i slova jako Mirka či Jirka. Hodnota ve sloupci *case_sensitive* určuje citlivost na velká a malá písmena.

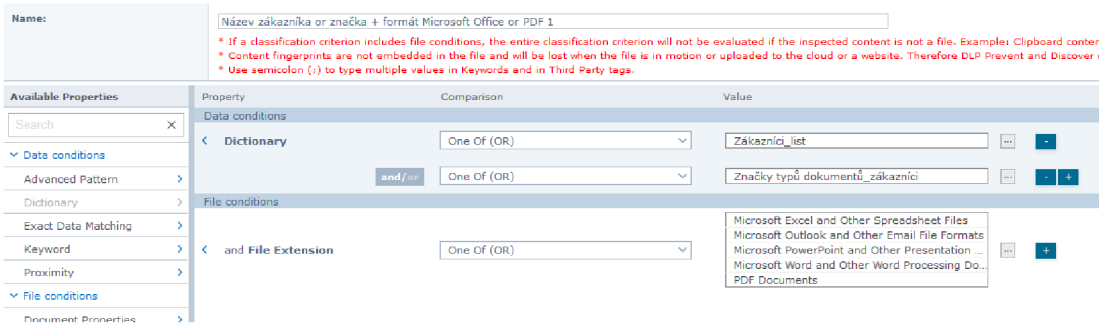
Následně je slovník importován do ePo konzole v modulu pro definice DLP, jak je vidět na obrázku dále.



Obrázek 17: Import slovníku do ePO konzole
Zdroj: vlastní zpracování

Do slovníku lze kdykoli přidat další záznam, což by bylo třeba v případě, kdy organizace získá nového zákazníka. Jde o příklad činnosti související s údržbou DLP řešení, jež by měla být začleněna do procesů organizace a zapracována do směrnic.

Slovník lze po uložení užívat v klasifikačních pravidlech či bezpečnostních politikách DLP. Příklad užití je zachycen na obrázku níže, kdy byl slovník použit pro jedno z klasifikačních pravidel klasifikace Velmi citlivé.



Obrázek 18: Příklad užití slovníku v klasifikačním pravidle
Zdroj: vlastní zpracování

3.7.4 Tvorba DLP politik

V následující části je popsán první návrh aplikovatelných DLP politik, tedy způsobu, jakým je DLP nastaveno. Jednotlivé podkapitoly jsou strukturovány dle konkrétních typů nastavených pravidel. Název je odvozen od názvu daného pravidla McAfee DLP, a proto není překládán.

Při tvorbě politik byly užity skupiny uživatelů z Active Directory, s kterým byla konzole ePolicyOrchestrator synchronizována. Jde o tyto skupiny uživatelů:

- **mng** - vedení organizace,
- **tech** - technické oddělení organizace,
- **hr** - personální a ekonomické oddělení,
- **obchod** - obchodní oddělení.

V rámci bezpečnostních pravidel se také nastavuje důležitost, neboli severita, bezpečnostní události, popř. incidentu. McAfee DLP rozlišuje následující stupně závažnosti, jež jsou seřazeny vzestupně dle významu:

- Info,
- Minor,
- Major,
- Critical.

3.7.4.1 Souhrnná tabulka

Souhrnné tabulky popisují reakci bezpečnostních pravidel na akce týkají se daných klasifikací.

První tabulka popisuje nastavení v rámci prvních fází implementace, kde jsou pravidla založena na monitorování.

Tabulka 24: Souhrnná tabulka DLP pravidel - první fáze

Reakční pravidlo	Klasifikace			
	OSB	Interní	Citlivé	Velmi citlivé
Application File Access Protection	Nenastaveno	Nenastaveno	Nenastaveno	Nenastaveno
Cloud protection rules	Info; Monitor	Info; Monitor	Minor; Monitor	Minor; Monitor
Email Protection	Nenastaveno	Warning; Monitor	Minor; Monitor	Major; Monitor
Network Communication Protection	Nenastaveno	Nenastaveno	Nenastaveno	Nenastaveno
Network Share Protection	Nenastaveno	Nenastaveno	Nenastaveno	Nenastaveno
Printer Protection	Nenastaveno	Nenastaveno	Major; Monitor	Major; Monitor
Removable Storage Protection	Info; Monitor	Info; Monitor	Minor; Monitor	Major; Monitor
Screen Capture Protection	Info; Monitor	Warning; Monitor	Minor; Monitor	Minor; Monitor

Web Protection	Warning; Monitor	Warning; Monitor	Minor; Monitor	Minor; Monitor

Zdroj: vlastní zpracování

Druhá tabulka popisuje nastavení, které by mělo odpovídat požadovanému stavu na konci implementace, kde jsou pravidla založena jak na monitorování, tak i na blokaci nepovolených akcí.

Tabulka 25: Souhrnná tabulka DLP pravidel - konečná fáze

Reakční pravidlo	Klasifikace			
	OSB	Interní	Citlivé	Velmi citlivé
Application File Access Protection	Nenastaveno	Nenastaveno	Nenastaveno	Nenastaveno
Cloud protection rules	Blokace (s výjimkou)	Blokace (s výjimkou)	Blokace (s výjimkou)	Blokace (s výjimkou)
Email Protection	Nenastaveno	Warning, User justification	Blokace (s výjimkou)	Blokace (s výjimkou)
Network Communication Protection	Nenastaveno	Nenastaveno	Nenastaveno	Nenastaveno
Network Share Protection	Nenastaveno	Nenastaveno	Nenastaveno	Nenastaveno
Printer Protection	Nenastaveno	Nenastaveno	Blokace (s výjimkou)	Blokace (s výjimkou)
Removable Storage Protection	Info; Šifrování	Info; Šifrování	Blokace (s výjimkou + šifrování)	Blokace (s výjimkou + šifrování)
Screen Capture Protection	Info; Monitor	Info; Monitor	Blokace (zvážit výjimku)	Blokace (zvážit výjimku)
Web Protection	Blokace	Blokace	Blokace	Blokace

Zdroj: vlastní zpracování

Obrázek dále byl pořízen na konci první fáze testovacího nastavování DLP a zobrazuje souhrnně pravidla Data Protection.

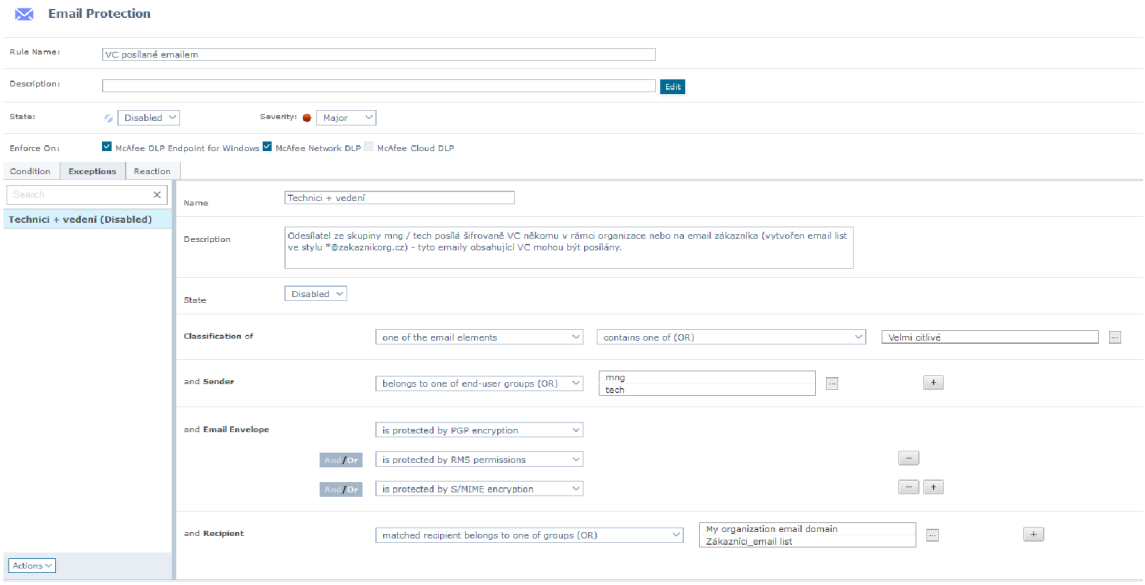
Obrázek 19: Souhrnné nastavení DLP - Data Protection
Zdroj: vlastní zpracování

3.7.4.2 Email Protection

Velmi Citlivé - VC

- Data označena jako VC se nesmí posílat emailem.
- V případě, že chce uživatel takový email poslat, DLP akci zablokuje (akce *block*) a zobrazí uživateli edukační hlášku (tzv. *user notification* v režimu *on*).
- **Výjimkou:**
  - Odesílatel ze skupiny mng či tech posílá šifrovaný email nesoucí VC data někomu s emailouvou doménou organizace investora (tzn. na interní emailovou adresu jiného zaměstnance) nebo na email zákazníka.
    Pro identifikaci emailu zákazníků byl vytvořen email list ve stylu **@nazevzakaznika.cz* (hvězdička zastupuje libovolný znak, emailová adresa je pouze pro znázornění nastavení).
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MAJOR*

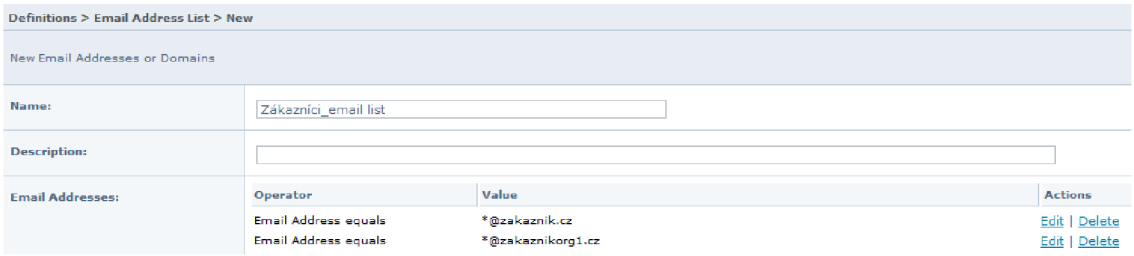
Nastavení výjimky pravidlu můžeme vidět na přiloženém snímku obrazovky, který byl pořízen během samotného nastavování.



Obrázek 20: Nastavení výjimky
Zdroj: vlastní zpracování

V sekci *Condition*, jež můžeme na obrázku vidět, se nastavují podmínky, za kterých bude toto pravidlo aplikováno. V tomto případě je to jednoduše tehdy, když některá část emailu nese klasifikaci Velmi citlivé.

Snímek obrazovky nastaveného email listu, jež byl importován podobně jako slovník. Skutečná doménová jména emailových adres nemohou být v samotné bakalářské práci použita, a proto byla pro užití v ní zaměněna za „zakaznik.cz“ či „zakaznikorg1.cz“.



Obrázek 21: Užití email listu
Zdroj: vlastní zpracování

Citlivé - C

- Data nesoucí klasifikaci C se nesmí posílat emailem.
- V případě, že chce uživatel takový email poslat, DLP akci zablokuje (akce *block*) a zobrazí uživateli edukační hlášku (tzv. *user notification* v režimu *on*).
- **Výjimkou:**
  - Odesílatel ze skupiny mng či tech posílá šifrovaný email nesoucí VC data někomu s emailouvou doménou organizace investora (tzn. na interní emailovou adresu jiného zaměstnance) nebo na email zákazníka.
    Byl použit stejný email list jako v přechozím případě.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MAJOR*

Interní - INT

- Data klasifikována jako interní smí být posílána pouze pokud uživatel vědomě DLP softwaru potvrdí jejich odeslání (tzv. vynucení *user justification*).
- **Výjimkou:**
  - interní data posílaná emailem mezi zaměstnanci (zaměstnanci si mezi sebou mohou interní informace volně posílat)
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím nevynucovat nic (akce *no action*), pouze hlášení se závažností *WARNING*

Osobní údaje - OSB

- v rámci email ochrany neřešeno

State	Rule	Desc	Severity	Incidents	Data To Protect	Applies To	Protection	Enforce On	DLP Endpoint Reaction
	C posílané emailem		Minor	0	Citlivé	any user	Email Protection		Report incident | Report incident |
	INT posílané emailem		Warning	0	Interní	any user	Email Protection		Report incident | Report incident |
	OSB posílané emailem - monitoring		Info	0	Osobní údaje	any user	Email Protection		Report incident | Report incident |
	VC posílané emailem		Major	0	Velmi citlivé	any user	Email Protection		Report incident | Report incident |

Obrázek 22: Přehled DLP pravidel pro Email Protection

Zdroj: vlastní zpracování

3.7.4.3 Screen capture

Velmi citlivé a Citlivé - VC a C

- Data nesoucí klasifikaci VC či C není možno snímat pomocí tzv. screen capture.
- **Výjimkou:**
  - Odesílatel ze skupiny mng či tech posílá šifrovaný email nesoucí VC data někomu s emailovou doménou organizace investora (tzn. na interní emailovou adresu jiného zaměstnance) nebo na email zákazníka.
    Byl použit stejný email list jako v přechozím případě.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MAJOR*

Interní - INT

- Všichni uživatelé bez omezení.
- Pouze monitorovat (*no action* + reportovat)
- závažnost WARNING

Osobní údaje - OSB

- závažnost INFO
- Všichni uživatelé bez omezení.
- Pouze monitorovat (*no action* + reportovat)

3.7.4.4 Web Protection

Velmi citlivé a Citlivé - VC a C

- Data klasifikovaná jako C či VC nesmí být vůbec vkládána přes webové rozhraní - akce blokování (*block*).
- **Aktuální nastavení:**
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MINOR*

Interní a Osobní údaje - INT a OSB

- Data klasifikovaná jako INT či OSB nesmí být vůbec vkládána přes webové rozhraní - akce blokování (*block*).
- **Aktuální nastavení:**
    - zatím neblokovat (*no action*), pouze hlášení se závažností WARNING

3.7.4.5 Clipboard Protection

Velmi citlivé - VC

- Data klasifikovaná jako VC nesmí být kopírována pomocí funkce uložení do paměti počítače (clipboard - klávesové zkratky ctrl, c a ctrl, v) - akce blokování (*block*).
- **Výjimkou:**
    - Uživatelé ze skupin mng a tech můžou vkládat odkudkoli do destinace Microsoft Office Application nebo přes Průzkumník souborů Windows (File Explorer Windows).
- **Aktuální nastavení:**
    - zatím nechat výjimku neaktivní (*disabled*)
    - zatím neblokovat (*no action*), pouze hlášení se závažností *MAJOR*.

Citlivé - C

- Data klasifikovaná jako C nesmí být kopírována pomocí funkce uložení do paměti počítače (clipboard - klávesové zkratky ctrl, c a ctrl, v) - akce blokování (*block*).
- **Výjimkou:**
    - Uživatelé ze skupin mng a tech můžou vkládat odkudkoli do jakékoli destinace přes libovolnou aplikaci.
- **Aktuální nastavení:**
    - zatím nechat výjimku neaktivní (*disabled*)
    - zatím neblokovat (*no action*), pouze hlášení se závažností *MINOR*.

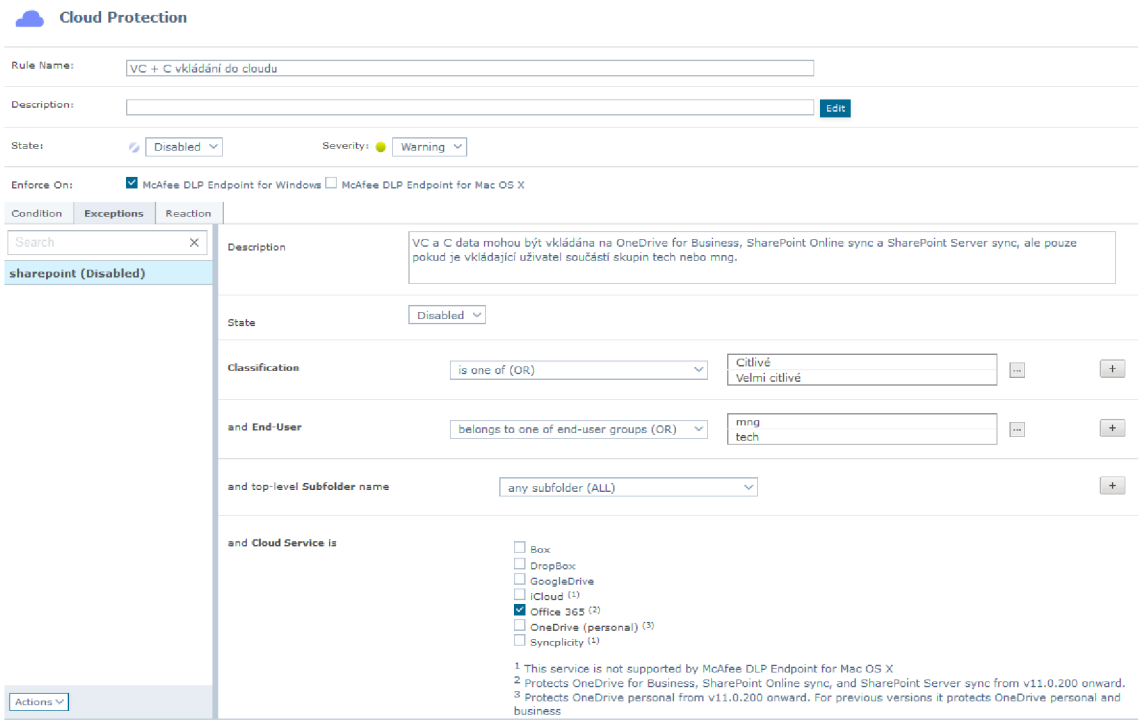
Interní a Osobní údaje - INT a OSB

- v rámci tohoto typu pravidel ochrany neřešeno

3.7.4.6 Cloud Protection

Velmi citlivé a Citlivé - VC a C

- Data klasifikovaná jako VC a C nemohou být kromě výjimky zmíněné níže vkládána na cloudová úložiště - akce blokování (*block*).
- **Výjimkou:**
  - VC a C data mohou být vkládána na OneDrive for Business, SharePoint Online sync a SharePoint Server sync, ale pouze pokud je vkládající uživatel součástí skupin tech nebo mng.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MINOR*.



Obrázek 23: Příklad nastavení výjimky pro Cloud Protection
Zdroj: vlastní zpracování

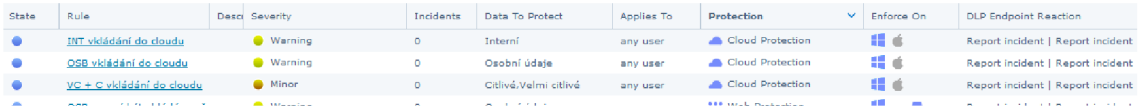
Interní - INT

- Data klasifikovaná jako INT nemohou být kromě výjimky zmíněné níže vkládána na cloudová úložiště - akce blokování (*block*).
- **Výjimkou:**
  - INT data mohou být vkládána všemi zaměstnanci společnosti, ale pouze na OneDrive for Business, OneDrive Personal, SharePoint Online sync a SharePoint Server sync, jež jsou oficiálně využívány organizací.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)

- zatím neblokovat (*no action*), pouze hlášení se závažností *MINOR*.

Osobní - OSB

- Data klasifikovaná jako OSB nemohou být kromě výjimky zmíněné níže vkládána na cloudová úložiště - akce blokování (*block*).
- **Výjimkou:**
  - OSB data mohou být vkládána pouze na OneDrive for Business, OneDrive personal, SharePoint Online sync a SharePoint Server sync, ale pouze uživatelem ze skupiny mng nebo hr.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MINOR*.



Obrázek 24: Přehled DLP pravidel pro Cloud Protection
Zdroj: vlastní zpracování

3.7.4.7 Printer Protection

Velmi citlivé a Citlivé - VC a C

- Data klasifikovaná jako VC a C nemohou být volně tisknuta - akce blokování (*block*).
- **Výjimkou:**
  - VC a C data mohou být tištěna uživateli, kteří jsou součástí skupiny tech nebo mng.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MINOR*.

Interní a Osobní údaje - INT a OSB

- v rámci tohoto typu pravidel ochrany neřešeno

3.7.4.8 Removable Storage Protection

Velmi citlivé - VC

- Data klasifikovaná jako VC nemohou být volně přenášena na přenosná úložiště, ani kopírována z přenosných úložišť do zařízení (počítače) - akce blokování (*block*).
- **Výjimkou:**
  - VC a C data mohou být obousměrně přenášena uživateli, kteří jsou součástí skupiny tech nebo mng.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MAJOR*.

Citlivé - C

- Data klasifikovaná jako C nemohou být volně přenášena na přenosná úložiště, ani kopírována z přenosných úložišť do zařízení (počítače) - akce blokování (*block*).
- **Výjimkou:**
  - C data mohou být obousměrně přenášena uživateli, kteří jsou součástí skupiny tech, mng nebo obchod.
- **Aktuální nastavení:**
  - zatím nechat výjimku neaktivní (*disabled*)
  - zatím neblokovat (*no action*), pouze hlášení se závažností *MINOR*.

Interní a Osobní údaje - INT a OSB

- Přenos INT a OSB dat pouze monitorovat - závažnost INFO.

Souhrnné šifrovací pravidlo pro VC, C, INT i OSB dat

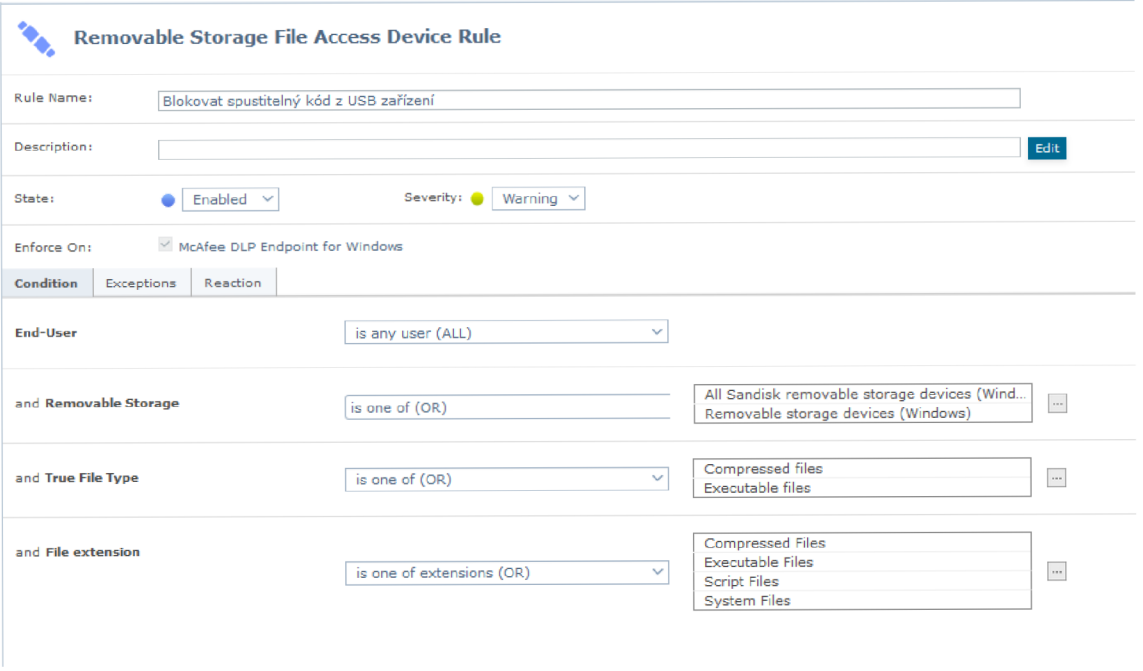
- Pokud dle výše zmíněných pravidel dojde k přenosu dat jakékoli ze sledovaných klasifikací, dojde k zašifrování dat - akce *encrypt*.
- **Aktuální nastavení:**
  - zatím nešifrovat

3.7.4.9 Removable Storage File Access Device Rule

Toto pravidlo je jedním z pravidel Device Control.

Blokovat spustitelný kód z USB zařízení

- Pokud na USB spustitelné soubory, pak blokace.
- **Výjimka:** uživatel ze skupiny admin



3.8 Kalkulace ceny

Na začátku implementace byla známa cena licence McAfee DLP typu CDA pro jedno koncové zařízení, což bylo jedním z aspektů zohledňovaných při výběru řešení i rozsahu.

Cena pořízení licence McAfee CDA na 1 rok:

- McAfee CDA **- 101,98 USD/koncové zařízení (PC, laptop a server)** - perpetuální licence s Business Software Support (podpora výrobce) na 1 rok

Obnova podpory v dalších letech licence McAfee CDA:

- Obnova Business Software Support na 1 rok **- 22,27 USD/koncové zařízení**

Prvotní pořízení technologie McAfee CDA je vyšší investicí, ale následná obnovení podpory v dalších letech tvoří pouze 22 % z pořizovací ceny.

Do ceny implementace včetně ceny licencí také vstupuje cena implementačních prací a případně i nákup potřebného HW vybavení. Organizace pro implementaci nemusí nakupovat další HW vybavení, proto ho celková přibližná kalkulace v následující tabulce nebere v potaz.

Tabulka 10: Kalkulace DLP řešení

	cena licence (rok)	cena licence prodloužení (rok)	počet nakoupených licencí ks	cena celkem v prvním roce	cena celkem 2. rok	cena celkem (5 let) pro všechny stanice
McAfee DLP CDA licence	2 307 Kč	508 Kč	60	**138 420 Kč**	**30 480 Kč**	**260 340 Kč**
		odhad náročnosti	odhad ceny	cena impl. prací		
+ implementační práce		cca 6 ČD	14 000 Kč / ČD*	**84 000 Kč**		
Přibližná pořizovací cena (bez DPH) celkem:				**222 420 Kč**		

Zdroj: vlastní zpracování

Celková odhadovaná pořizovací cena implementace DLP pro danou organizaci je rovna 222 420 Kč. V dalším roce organizace zaplatí 30 480 Kč (za licence při 60 ks). Organizace si plánuje chod DLP řešení spravovat sama, ale je možné, že bude muset občasně využít rad specializované bezpečnostní firmy, což by mohlo znamenat další

náklady. Podpora správy DLP může být součástí ceny za implementaci od specializované bezpečnostní firmy.

ZÁVĚR

Cíl práce, jímž bylo navrhnout a představit možnost ochrany dat v organizaci pomocí DLP (Data Loss Prevention) řešení, byl splněn kompletně. Možnostem ochrany dat v organizaci i samotné technologii se věnovala rámcově teoretická část a hlouběji pak praktická část, v rámci které došlo k aplikaci a hlubšímu vysvětlení poznatků na přípravě implementace DLP v konkrétní organizaci.

Technologie DLP byla rámcově představena v první kapitole, v rámci teoretické části bakalářské práce, kde byly zmíněny principy fungování DLP, typy DLP řešení, možné funkcionality a techniky ochrany dat. Došlo také k vysvětlení role DLP technologie v kontextu informační bezpečnosti organizace. Teoretická část představuje výchozí znalost pro porozumění problematiky ochrany dat pomocí DLP, kterému se věnuje hlouběji praktická část práce. Pro komplexní pokrytí problematiky se teoretická část také zabývá problematikou dat ve firemním prostředí, nejčastějšími vektory úniků dat a bezpečnostními opatřeními.

V analytické části došlo k představení organizace, která má zájem implementovat technologii DLP - oblast podnikání, fungování organizace a její struktura. Analytická část se vedle základních informací o organizaci věnuje oblastem, jejichž znalost je klíčová pro korektní implementaci DLP technologie - obsahu, formátu i uložení dat, postupům práce s daty v organizaci, systému klasifikace dat, výsledkům provedené analýzy vybraných dokumentů a oblastí ISMS či požadavkům organizace na DLP řešení.

Na problematiku DLP navázala praktická část, jež se věnuje formulaci požadavků na DLP technologii na základě výstupů analytické části, výběru DLP řešení pro danou organizaci, vysvětlení možností ochrany dat pomocí daného DLP řešení a výběru rozsahu implementace vhodného pro konkrétní společnost. Byl vytvořen seznam klíčových činností implementace DLP a plán implementace včetně časové analýzy a RACI matice. Došlo k detailnímu návrhu ochrany dat organizace pomocí DLP a jeho nastavení v testovacím prostředí. Následně došlo ke kalkulaci implementace DLP řešení pro danou organizaci.

SEZNAM POUŽITÝCH ZDROJŮ

[1] KOMINÁCKÁ, Jitka. *Moderní ICT pro podporu rozhodování*. První vydání. V Praze: C.H. Beck, 2014. C.H. Beck pro praxi. ISBN 978-80-7400-531-2.

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

[3] SKLENÁK, Vilém. *Data, informace, znalosti a Internet*. Praha: C.H. Beck, 2001. C.H. Beck pro praxi. ISBN 80-717-9409-0.

[4] HAUER, Barbara. Data and Information Leakage Prevention Within the Scope of Information Security. *IEEE Access* [online]. 2015, **3**, 2554-2565 [cit. 2019-02-12]. DOI: 10.1109/ACCESS.2015.2506185. ISSN 2169-3536. Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7348633

[5] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[6] *International Standard ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary*. 5. vydání 2018-02. Switzerland: ISO copyright office, 2018.

[7] CHENG, Long, Fang LIU a Danfeng Daphne YAO. Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* [online]. 2017, **7**(5), 14 [cit. 2019-02-12]. DOI: 10.1002/widm.1211. ISSN 19424787. Dostupné z: http://doi.wiley.com/10.1002/widm.1211

[8] ANONYMOUS, . *Maximální bezpečnost*. 4. vyd. Praha: Softpress, 2004. ISBN 80-864-9765-8.

[9] *McAfee Data Loss Prevention 11.1.x Product Guide* [online]. Revision B. McAfee, LLC, 2019 [cit. 2019-02-02]. Dostupné z: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/28000/PD28028/en_US/dlp_1110_pg_B00_en-us.PDF

[10] HARRIS, Shon. *CISSP exam guide*. Sixth edition. New York: McGraw-Hill, 2013. ISBN 978-0071781749.

[11] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-247-5457-4.

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

[13] *Grand Theft Data: Data exfiltration study: Actors, tactics, and detection* [online]. In: . b.r., s. 13 [cit. 2019-02-12].

[14] *2018 Data Breach Investigations Report: 11th edition* [online]. In: . Verizon, b.r., s. 1-68 [cit. 2019-02-14].

[15] *IBM 2015 Cyber Security Intelligence Index: Analysis of cyber attack and incident data from IBM's worldwide security services operations* [online]. In: . b.r., s. 1 - 24 [cit. 2019-02-13].

[16] *2017 Data Breach Investigations Report: 10th Edition* [online]. In: . Verizon, 2017, s. 1 - 76 [cit. 2019-02-19].

[17] POLLOCK, Tommy. *Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS)* [online]. Kennesaw State University, 2017 [cit. 2019-02-19]. Dostupné z: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1051&context=ccerp

[18] METALIDOU, Efthymia, Catherine MARINAGI, Panagiotis TRIVELLAS, Niclas EBERHAGEN, Christos SKOURLAS a Georgios GIANNAKOPOULOS.

The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia: Social and Behavioral Sciences* [online]. 2014, (147), 424-428 [cit. 2019-02-19]. DOI: 10.1016/j.sbspro.2014.07.133. ISSN 1877-0428. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1877042814040440

[19] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. První vydání. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[20] *Cyber security breaches survey 2017* [online]. In: . Institute for Criminal Justice Studies, University of Portsmouth, 2017, s. 1 - 66 [cit. 2019-02-19].

[21] *Corporate security. simply. make it happen: leveraging digitization through it security*. New York, NY: Springer Berlin Heidelberg, 2016. ISBN 978-3-319-46528-9.

[22] MOGULL, Rich a Mike ROTHMAN, Chris PEPPER, ed. *Understanding and Selecting a Data Loss Prevention Solution: Version 3.0* [online]. In: . Arizona: Securosis, L.L.C., 2017, s. 1 - 56 [cit. 2019-04-21].

[23] Magic Quadrant for Enterprise Data Loss Prevention. In: *Gartner* [online]. Gartner, Inc., 2017 [cit. 2019-03-20]. Dostupné z: https://www.gartner.com/doc/reprints?id=1-3TPE5D0&ct=170216&st=sb

[24] Data Loss Prevention Leading Vendor Review: A DLP Experts White Paper. In: *DLPX: Data Loss Prevention Experts* [online]. 2018 [cit. 2019-03-24]. Dostupné z: https://dlpexperts.com/wp-content/uploads/2018/11/DLPVendorReview_v8.1.pdf

[25] *Data Loss Prevention -- Market Quadrant 2018: An Analysis of the Market for Data Loss Prevention* [online]. In: . The Radicati Group, 2018 [cit. 2019-03-26]. Dostupné z: https://www.forcepoint.com/thank-you-your-interest-report-0?form_id=1363&file=35506&resource=27496&category=industry_analyst_reports

[26] Symantec logo. In: *Symantec* [online]. b.r. [cit. 2019-03-27]. Dostupné z: https://www.symantec.com/

[27] Forcepoint logo. In: *Forcepoint* [online]. b.r. [cit. 2019-03-27]. Dostupné z: https://www.forcepoint.com/

[28] Digital Guardian logo. In: *Digital Guardian* [online]. b.r. [cit. 2019-03-27]. Dostupné z: https://www.digitalguardian.com/

[29] Kernel_Layout_cs. In: *Wikipedia* [online]. b.r. [cit. 2019-03-27]. Dostupné z: https://cs.wikipedia.org/wiki/J%C3%A1dro_opera%C4%8Dn%C3%ADho_syst%C3%A9mu#/media/File:Kernel_Layout_cs.svg

[30] McAfee logo. In: *McAfee* [online]. b.r. [cit. 2019-03-27]. Dostupné z: https://www.mcafee.com/

[31] Logo Sophos. In: *Sophos* [online]. b.r. [cit. 2019-04-01]. Dostupné z: www.sophos.com

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ

SEZNAM ZKRATEK

AD - Active Directory

C - Citlivá data (klasifikace)

CDA - McAfee Complete Data Protection Advanced (licenční balíček)

CNTC - Klasifikační pravidlo na základě analýzy obsahu

ČD - Člověkoden

DC - Device Control

DG - Digital Guardian

DLP - Data Loss Prevention

DNS - Domain Name System

EPO - EPO server, případně ePO konzole pro správu DLP

FRP - File and Removable media Protection (McAfee produkt)

HW - Hardware

ICT - Informační a komunikační technologie

IDS - Intrusion Detection System

INT - Interní klasifikace

IPS - Intrusion Prevention System

IS - Informační systém

ISMS - Information Security Management Systém

IT - Informační technologie

OS - Operační systém

OSB - Osobní údaje (klasifikace)

SW - Software

UTM - Unified Threat Management

VC - Velmi citlivá data (klasifikace)

ZKB - Zákon o kybernetické bezpečnosti