VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NASAZENÍ KONTEXTOVÉHO DLP SYSTÉMU V RÁMCI ZAVÁDĚNÍ ISMS

DEPLOYMENT OF THE CONTEXT DLP SYSTEM WITHIN ISMS IMPLEMENTATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN IMRICH
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2015

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2014/2015
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Imrich Martin, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Nasazení kontextového DLP systému v rámci zavádění ISMS

v anglickém jazyce:

Deployment of the Context DLP System within ISMS Implementation

Pokyny pro vypracování:

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

Seznam odborné literatury:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.
ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.
DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.
POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2014/2015.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 28.2.2015

Abstrakt

Diplomová práce se zabývá nasazením DLP systému do vybrané společnosti. Práce obsahuje analýzu současné situace společnosti a na základě zjištění poskytuje rozhodnutí pro výběr nejvhodnějšího DLP řešení. Nakonec popisuje reálné nasazení vybraného DLP systému do společnosti.

Abstract

This diploma thesis focuses on a DLP implementation within a specific organization. The thesis contains current situation analysis and provides decision for choice of the most suitable DLP based on the analysis findings. Eventually describes a real implementation of the chosen DLP system within the organization.

Klíčová slova

DLP, kontextové DLP, Data Loss Prevention, bezpečnost informací, ICT bezpečnost, ISMS

Keywords

DLP, context DLP, Data Loss Prevention, data security, ICT security, ISMS

Citace

IMRICH, M. *Nasazení kontextového DLP systému v rámci zavádění ISMS*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. 90 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

Prohlášení

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

V Brně dne 29. května 2015

……

Martin Imrich

Poděkování

Tímto bych chtěl poděkovat vedoucímu práce Ing. Viktoru Ondrákovi, Ph.D za odborné vedení práce. Dále děkuji Ing. Petru Sedlákovi za odborné technické konzultace a čas, který mi věnoval.

OBSAH

ÚVOD

Tato práce se zabývá výběrem vhodného DLP systému na řešení konkrétního problému v analyzované společnosti. Po provedení nutného výběru se budu také věnovat samotnému nasazení vybraného DLP řešení do prostředí společnosti.

Diplomovou práci jsem rozdělil na 3 hlavní kapitoly, které na sebe postupně navazují. V první kapitole se čtenář dozví nezbytná teoretická východiska mé práce. Vysvětlíme si základní bezpečnostní pojmy, které budou moji práci provázet. Dále se blíže podíváme na Systém řízení bezpečnosti informací, neboli ISMS, a mj. také na normy související s bezpečností informací. V poslední části první kapitoly se zaměřím na vysvětlení problematiky DLP.

Druhá kapitola se věnuje analýze současného stavu ve vybrané organizaci. Představím vybranou organizaci, kterou budu analyzovat, a následně provedu technickou a bezpečnostní analýzu. Tyto analýzy budu provádět pomocí workshopů a interview s klíčovými stakeholdery společnosti. Následně provedu identifikaci a ohodnocení aktiv společnosti a budu pokračovat analýzou rizik. Na závěr této kapitoly představím dostupná řešení a provedu ekonomické zhodnocení.

V třetí kapitole se budu zabývat návrhem vlastního řešení. Uvedu zde rozhodovací kritéria pro výběr toho nejvhodnějšího řešení. Po výběru konkrétního řešení se budu zabývat naplánováním samotného projektu nasazení. Uvedu nutnou dokumentaci a plán projektu i s časovou analýzou. Následně popíšu reálnou implementaci vybraného DLP řešení do prostředí společnosti. Představím implementační plán, dle kterého budu postupovat, a popíšu tak všechny části implementace včetně ukázky reálných dat z produktu.

Cíle práce, metody a postupy zpracování

Cílem této práce je výběr vhodného DLP systému pro řešení konkrétního problému analyzované společnosti.

Jako jednou z metod pro zajištění tohoto cíle zvolím formu workshopů a interview s klíčovými stakeholdery ve vybrané společnosti. Tím docílím zjištění konkrétních potřeb a udělám si obrázek o potřebném řešení. Jako další metodu zvolím analýzu rizik, kde na základě zjištěných detailů z prostředí mohu odhadnout rizika, která mohou ohrozit aktiva společnosti. K tomuto účelu tedy identifikuji a ohodnotím aktiva společnosti a následně provedu analýzu rizik a zranitelností.

Po provedené analýze definuji kritéria pro výběr toho nejvhodnějšího řešení. Porovnáním a vyhodnocením těchto kritérií u konkrétních dostupných řešení pak vyberu to nejlepší.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole si vysvětlíme základní pojmy v oblasti bezpečnosti, se kterými se budeme potkávat v rámci celé práce. Kromě pojmů se také zaměřím na popsání systému pro řízení bezpečnosti informací a příslušných norem, které napomáhají a standardizují tuto problematiku.

1.1 Informační bezpečnost

Informační bezpečnost stále více nabývá na důležitosti s rostoucím množstvím digitálních informací, širšího používání informačních a komunikačních technologií a potřebou chránit tyto informace před vyzrazením. Samotná ochrana informací zasahuje ještě do dob před vznikem informačních technologií, kdy se jednalo právě především o ochranu před vyzrazením. Dnes máme na informační bezpečnost větší nároky a kromě ochrany před vyzrazením, se zabýváme také zajištěním důvěrnosti, dostupnosti a integrity dat.

Dle autorů Ondrák, Sedlák a Mazálek bezpečnost informací řeší ochranu informací a dostupnost. Je ve vzájemném vztahu s pojmy bezpečnost organizace a bezpečnosti IS/ICT. Nejvýše je postavena bezpečnost organizace s úkolem zajištění bezpečnosti objektu a tím také majetku organizace. Zahrnuje automaticky také zajištění bezpečnosti IS/ICT a bezpečnost informací. Bezpečnost informací zahrnuje kromě bezpečnosti IS/ICT práci s informacemi v nedigitální formě. Bezpečnost IS/ICT chrání pouze aktiva informačního systému podporovaná informačními a komunikačními technologiemi (Ondrák, 2013). Situaci znázorňuje následující obrázek:

Obrázek 1 Rozdělení bezpečnosti (Zdroj: (Ondrák, 2013))

Důvěrnost, dostupnost a integrita dat jsou hlavní tři kritéria a zachování těchto kritérií je také hlavním cílem bezpečnosti informací (Doucek, 2008). Dostupnost je zajištění přístupnosti informace v požadovaný okamžik. Důvěrnost znamená zajištění přístupnosti k informaci pouze uživateli pro něj určené. Integrita pak zajištění správnosti a úplnosti informace (Požár, 2005).

1.2 Systém řízení bezpečnosti informací jako metodika pro ochranu dat

Systém řízení bezpečnosti informací (neboli ISMS), jak již z názvu vyplývá, je zavedený systém pro řízení bezpečnosti informací. ISMS je založeno na tzv. PDCA cyklu, který vynalezl W. Edwards Deming (Humphreys, c2007).

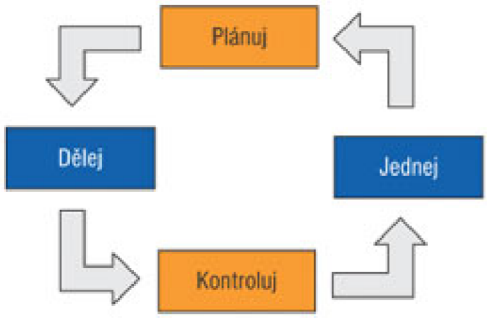
1.2.1 Demingův model

Demingův model, nebo také PDCA cyklus, je metoda postupného zlepšování uplatnitelná ve všech možných procesech, postupech, službách, aplikacích, implementacích apod. Jedná se o jednoduchý cyklus s těmito fázemi:

- P (*plan*) – plánuj
- D (*do*) – dělej
- C (*check*) – kontroluj

- A (*act*) – jednej

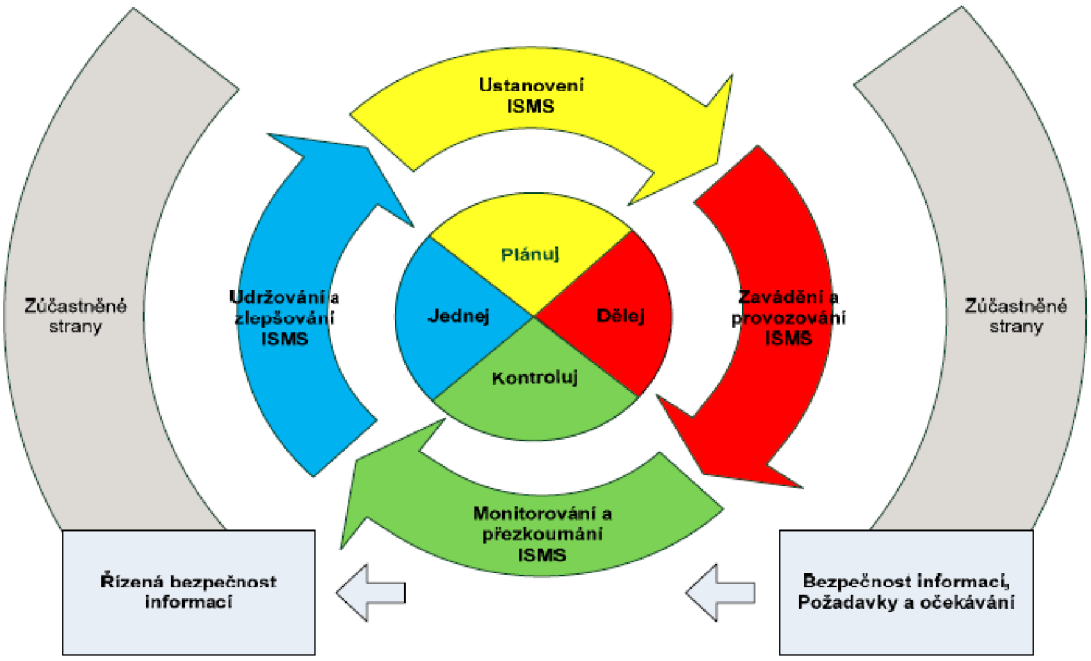
V podstatě první fáze nám říká: Naplánuj potřebné změny, zlepšení, záměr, cokoli co povede ke zlepšení problému, který řeším. Druhá fáze již vyzývá k realizaci plánu z fáze první. Ve třetí fázi probíhá kontrola výsledků a porovnává se s očekávaným výsledkem. V poslední fázi se jedná o úpravy všeho, co může ještě více zlepšit samotný plán na základě výstupů z předešlé fáze. Toto zlepšení je zavedeno do praxe a celý cyklus začíná od začátku. Cyklus je zobrazen na následujícím obrázku:



Obrázek 2 Znázornění cyklu PDCA (Zdroj: (Sedláček, 2011)).

1.2.2 Ustanovení ISMS

Ustanovení ISMS je první etapou při budování ISMS. Základním kamenem při ustavení ISMS je určení rozsahu a vazeb ISMS na základě činnosti organizace, struktury organizace, velikosti, umístění či používaného informačního systému.



Obrázek 3 Navázání ISMS na model PDCA (Zdroj: (Ondrák, 2013))

Jak je vidět na obrázku 3, ISMS se nese v duchu PDCA modelu. První etapa Ustanovení ISMS je tedy v rámci fáze Plánuj. V první etapě je nutné definovat politiku ISMS. Politika by měla obsahovat cíle zavedení ISMS a směr, kterým by se měl ubírat. Mělo by se také počítat s údržbou do budoucnosti. Velmi důležitým prvním krokem je vůbec souhlas a podpora managementu. Zavádění ISMS by mělo jít seshora. Také musí být definována kritéria, podle kterých jsou popisována a hodnocena rizika v organizaci (Doucek, 2008).

Součástí ustanovení ISMS je také identifikace aktiv, jejich ocenění a vypracování celkové analýzy rizik. Tento krok je kritický pro další etapy ISMS. Na základě výsledků řízení rizik by pak mělo vedení společnosti odsouhlasit návrhy opatření a současně by mělo souhlasit se zbytkovými riziky. Poslední krok v této etapě je pak prohlášení o aplikovatelnosti, což je povinný dokument pro organizaci v případě, kdy usiluje o shodu s normou ISO/EIC rodiny 27000. Tento dokument obsahuje cíle opatření a jednotlivá bezpečnostní opatření, která byla vybrána (Doucek, 2008).

1.2.3 Zavádění a provoz ISMS

Tato etapa je fází D (*do*), tedy dělej. Zde se soustředíme na prosazení a zavedení všech bezpečnostních opatření, jak byla navržena v předešlé etapě. Důležité je především naplánování konkrétního harmonogramu pro dílčí úkony a také alokace lidských zdrojů. Zde se také musí definovat a začít zavádět plán zvládání rizik. Po definování plánu zvládání rizik se může přejit na zavádění bezpečnostních opatření, která se plánovala v etapě první. Důležité také je určení, jakým způsobem se bude měřit účinnost zavedených opatření a jak budou měření použita k vyhodnocení pro příští možné zlepšení (ČSN ISO/IEC 27001, 2006).

Nedílnou součástí zavádění ISMS je také školení uživatelů. Organizaci musí zajistit školení pro všechny uživatele, kterých se bude týkat zavedení ISMS. Nezaškolený uživatel je pro bezpečnost informací problém, proto musíme v této části všechny uživatele zaškolit na bezpečnost, vhodné chování na internetu, vhodnou práci s daty a vůbec na ISMS (ČSN ISO/IEC 27001, 2006).

Posledním krokem v této etapě je zavedení systému pro řízení a sbírání informací o incidentech a také systém pro řízení zdrojů (Doucek, 2008).

1.2.4 Monitorování a přezkoumávání ISMS

Třetí etapa je fází C (*check*), tedy kontroluj. Při zavádění kteréhokoliv systému či produktu, je důležité také zavést systém zpětné vazby. V rámci ISMS by společnost měla projít všechny zavedené bezpečnostní opatření a přezkoumat, jak fungují a jak jsou účinná. Kontrola může být provedena interně, ale také externě. Externí audit pak poskytuje nový pohled, nezatížený „pracovní slepotou“. Externí audit má i své nevýhody, protože auditor nezná, jak to chodí uvnitř firmy, ale může přinést nové myšlenky. Na základě přezkoumání je pak nutné provést navržené úpravy, ať již vzešly z auditu interního nebo externího (ČSN ISO/IEC 27001, 2006).

1.2.5 Údržba a zlepšování ISMS

Poslední etapou ISMS je údržba a zlepšování aktuálního stavu ISMS. V této fázi bychom měli implementovat změny, které vznikly především zpětnou vazbou z předešlé etapy. Měli bychom zlepšit všechny aspekty, které figurují v celém ISMS v dané organizaci. Celý model by se tímto také měl postupně zjednodušovat pro správu a další existenci (ČSN ISO/IEC 27001, 2006).

1.2.6 Normy související s ISMS

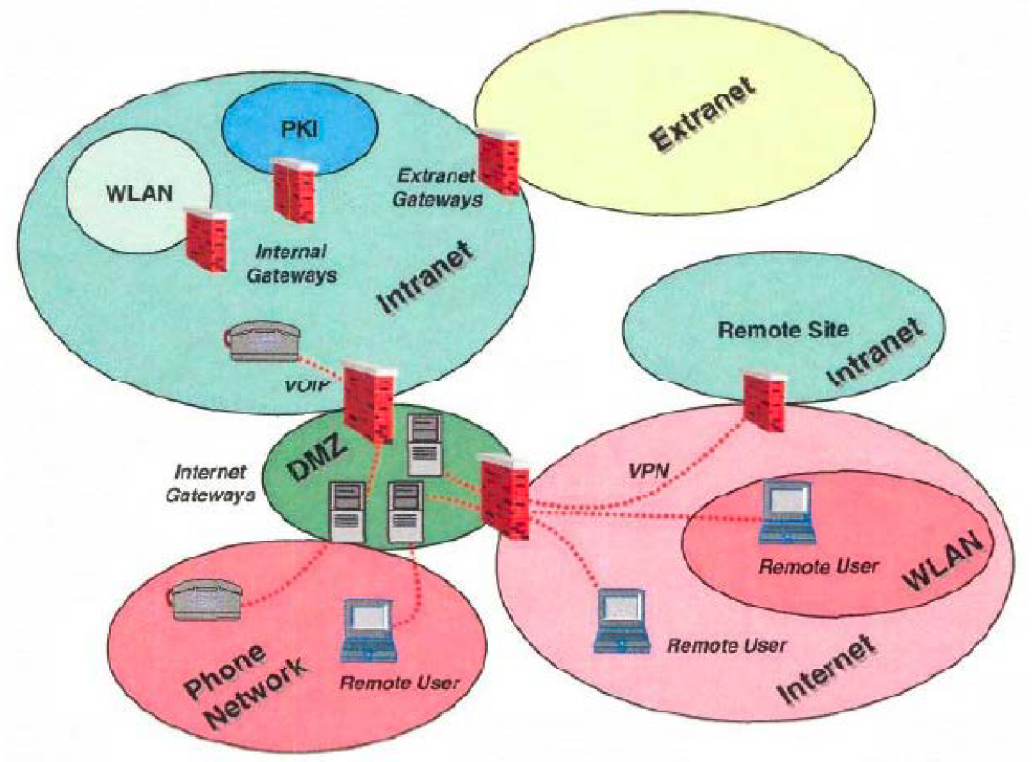
Norem souvisejících s ISMS je celá řada. Já zde uvedu pouze ty nejdůležitější, které se týkají ISMS či úzce souvisí s bezpečností informací.

Bezesporu nejdůležitější normou, která souvisí s ISMS, je norma ISO/IEC řady 27k. Norma nesla původně název BS 7799, poté ISO 17799 a v současnosti má již název ISO/IEC 27xxx. Tato norma specifikuje systém managementu bezpečnosti informací, tedy ISMS. Uvedu zde nejdůležitější části této normy dle (Ondrák, 2013):

- ISO/IEC 27000 – Základy a slovník
- ISO/IEC 27001 – Požadavky
- ISO/IEC 27002 – Soubor postupů
- ISO/IEC 27003 – Návod pro implementaci
- ISO/IEC 27004 – Metriky a měření účinnosti opatření
- ISO/IEC 27005 – Management rizik
- ISO/IEC 27006 – Požadavky na místa provádějící audit a certifikaci
- ISO/IEC 27007 – Směrnice pro audit

- ISO/IEC 27008 – Doporučení auditorům ISMS
- ISO/IEC 27xxx – specifikace pro obory činnost organizace (oborové)

Další normou, která se zabývá bezpečností je ISO/IEC 18028. Tato norma se zabývá bezpečností sítí a návrh takové síťové architektury může dle normy vypadat následovně:



Obrázek 4 Správná síťová architektura dle normy ISO 18028 (Zdroj: (ISO/IEC 18028-4:2005, 2005))

Mezi další vybrané normu ještě můžu uvést např. ISO 15408, také známou pod pojmem CC – Common Criteria, nebo normu ISO 19011, což je audit systémů řízení.

1.3 DLP systémy

DLP (Data Loss Prevention) systémy jsou systémy sloužící k ochraně před únikem citlivých informací. Mohou to být softwarová či hardwarová řešení, nebo kombinace obou přístupů. Zkratka DLP nemá standardizovaný výklad, v literatuře se můžeme setkat s pojmy Data Loss Prevention, Data Leak Prevetion, Data Loss Protection či Data Leak Protection. Význam těchto výkladů zkratek se může trochu lišit, neboť Data Loss Prevention v překladu znamená prevence před ztrátou dat, kdežto Data Leak Prevention znamená prevence před únikem dat. Ztrátu dat zde totiž chápu jako neúmyslnou hrozbu, ale u úniku dat se již můžeme bavit i o úmyslné hrozbě, kdy o data může zaměstnavatele připravit i jeho vlastní zaměstnanec (Data loss prevention complete certification kit - core series for it, 2013).

Další rozdíl můžeme chápat v interpretaci slova Prevention vs. Protection. Překlad slova Prevention je prevence, překlad slova Protection je ochrana. Tedy opět můžeme cítit lehký významový rozdíl, kdy u interpretace Protection se jedná pouze o statickou ochranu před ztrátou dat (ať před úmyslnou či neúmyslnou), ale u interpretace Prevention se může jednat i o systém, který dokáže predikovat, neboli předvídat, onu hrozbu úniku citlivých informací.

Kterýkoliv význam překladu této zkratky vede k jednomu cíli a tím je ochrana dat. Cílem DLP je tedy ochránit citlivá data společnosti před ztrátou, zcizením či zneužitím.

1.3.1 Srovnání síťových DLP a DLP koncových bodů

Síťová DLP jsou často hardwarová řešení, která většinou fungují jako výchozí brána na konci perimetru sítě. Jedná se většinou o dedikované síťové zařízení, které sleduje výstupní komunikaci a vyhodnocuje, zda se ven z perimetru posílá citlivý dokument, který se ven dostat nemá. Typicky se sleduje emailová komunikace, přenos FTP, HTTP či HTTPS komunikace (Monson, c2004).

Síťová DLP mívají pro větší podniky nižší náklady na vlastnictví než řešení DLP koncových bodů, ale vyžadují často složitou integraci do prostředí a sama o sobě se jsou nedostatečnou ochranou. Uživatel může data odnést z koncové stanice přes USB disk, vypálit na CD/DVD nebo poslat na mobilní telefon přes Bluetooth.

Na druhou stranu DLP koncových bodů představují softwarové řešení, kdy se na koncové stanice instaluje agent, který se stará o ochranu systému. Stejně jako síťová DLP dokáží DLP koncových bodů kontrolovat interní komunikaci, také kontrolovat email, FTP, HTTP či HTTPS spojení. Navíc dokáží ochránit i fyzické porty a např. blokovat připojování USB zařízení, mobilních telefonů či bluetooth. V případě DLP koncových bodů se ovšem jedná řádově o mnohem více klientů, které musí správce spravovat. V případě síťových DLP to mohou být ve větší síti maximálně desítky, v případě DLP koncových bodů to mohou být tisíce agentů. Proto je zde nutná přehledná centrální správa.

DLP koncových bodů tedy netrpí problém s únikem dat na koncové stanici, ale zase může mít jiné problémy. Např. si uživatel může nabootovat nový systém, kde není agent nainstalován a tak systém obejít. Nebo si přinese jiné zařízení bez nainstalovaného agenta. Toto se dá však řešit správným nastavením doménových politik.

1.3.2 Srovnání obsahově-orientovaných a kontextově-orientovaných DLP

Chtěl bych v této práci zavést nové rozdělení DLP systémů na obsahově-orientovaná (Content) DLP a konxtetově-orientovaná (Context) DLP. Na Content DLP můžeme dnes narazit na každém rohu. Jedná se o běžnou technologii, kterou používá snad každý DLP výrobce. Content DLP systémy se zaměřují na obsah dokumentu. Chránit ho na základě definovaného obsahu. Např. chce společnost chránit dokumenty, ve kterých je slovo „tajné“ nebo obsahuje číslo kreditní karty. Následně pokud takový dokument se uživatel snaží poslat ven z perimetru např. pomocí emailu, tak v případě síťového DLP proběhne na výstupu z perimetru prohledání tohoto dokumentu s definovanými výrazy. Obsah dokumentu se porovná s databází, a pokud se tam vyskytuje slovo „tajné“ nebo číslo kreditní karty, tak se email vrátí a dokument se neodešle.

Problém nastane v případě, když chce společnost chránit dokumenty, které nemají obsah, který by se dal číst. Např. výkresy v AutoCADu. Takový výkres je nějaký model, ale nemá text, kterým by se dalo jednoduše definovat, jak ho chceme chránit. K takovým případům většinou DLP výrobci reagují zákazem odesílání přes příponu, kdy bych si musel definovat, že nechci, aby se mi ze sítě dostali dokumenty s příponou .dwg. Jenže to je globální pravidlo a kdyby zákazník chtěl povolit odesílání určitých typů .dwg a určité ne, tak má smůlu.

Další problém nastane v případě, kdy uživatel toho nastavení zjistí a daný výraz pozmění. Např. vloží mezi číslo kreditní karty nějaký znak a systém tak obejde. Stejně by mohl systém obejít zašifrováním či zaheslováním souboru, protože takový soubor by contentový systém nemohl přečíst.

Kontextové DLP takové problémy nemá. Kontextové DLP se zaměřuje spíše na situace, při kterých data vznikají a kde se nacházejí. Zaměřuje se na kontext, v jakém s těmi daty uživatelé pracují. A následně po specifikování tohoto kontextu dokáže data selektivně chránit. Tedy určit tak, že v dané chvíli uživatel pracuje se svým soukromým dokumentem, takže systém tento dokument nijak omezovat nebude. Naopak když systém zjistí, že uživatel pracuje v kontextu citlivého dokumentu společnosti, např. prohlíží si vývojový kód, omezí uživatele tak, aby se tato citlivá data nedostala ven z definovaného perimetru. Výhoda této schopnosti rozlišit kontext spočívá i v tom, že dokáže selektivně řídit operace nad daným dokumentem právě na základě kontextu. Opět když bude pracovat se svým soukromým dokumentem ve Wordu, tak mu systém povolí kopírovat obsah do schránky. Pokud si ale otevře citlivý dokument s nabídkou, tak mu systém kopírování do schránky zakáže. Contentová DLP většinou také dokáží zakázat kopírování obsahu do schránky, ale pouze globálně, tedy nad všemi dokumenty ať pracuje uživatel se svým soukromým dokumentem, nebo s firemním citlivým – tedy omezí uživatele v jeho běžné práci. Příkladem contentového DLP je Symantec, Websense, RSA, Sophos. Kontextové DLP je např. Safetica od českého výrobce Safetica Technologies.

Nevýhodou kontextového DLP je fakt, že mu chybí obsahová kontrola. Dokonalým DLP se tedy jeví systém, který přebere výhodou obou přístupů – kombinace contentového a kontextového DLP.

Pozn. Při psaní této části teoretického východiska jsem vycházel především z vlastní několikaleté zkušenosti ve společnosti, která vyvíjí DLP řešení. Proto zde neuvádím žádné zdroje.

2 ANALÝZA SOUČASNÉHO STAVU

V této kapitole se budu věnovat analýze současného stavu společnosti. Představím vybranou společnost a sepíšu problém, který daná společnost řeší. Následně provedu technickou a bezpečnostní analýzu přímo v prostředí společnosti za účasti klíčových stakeholderů. Po této analýze bude následovat identifikace a ohodnocení aktiv a pak bude následovat analýza rizik. Kapitolu zakončím ekonomickým zhodnocením.

2.1 Popis vybrané společnosti

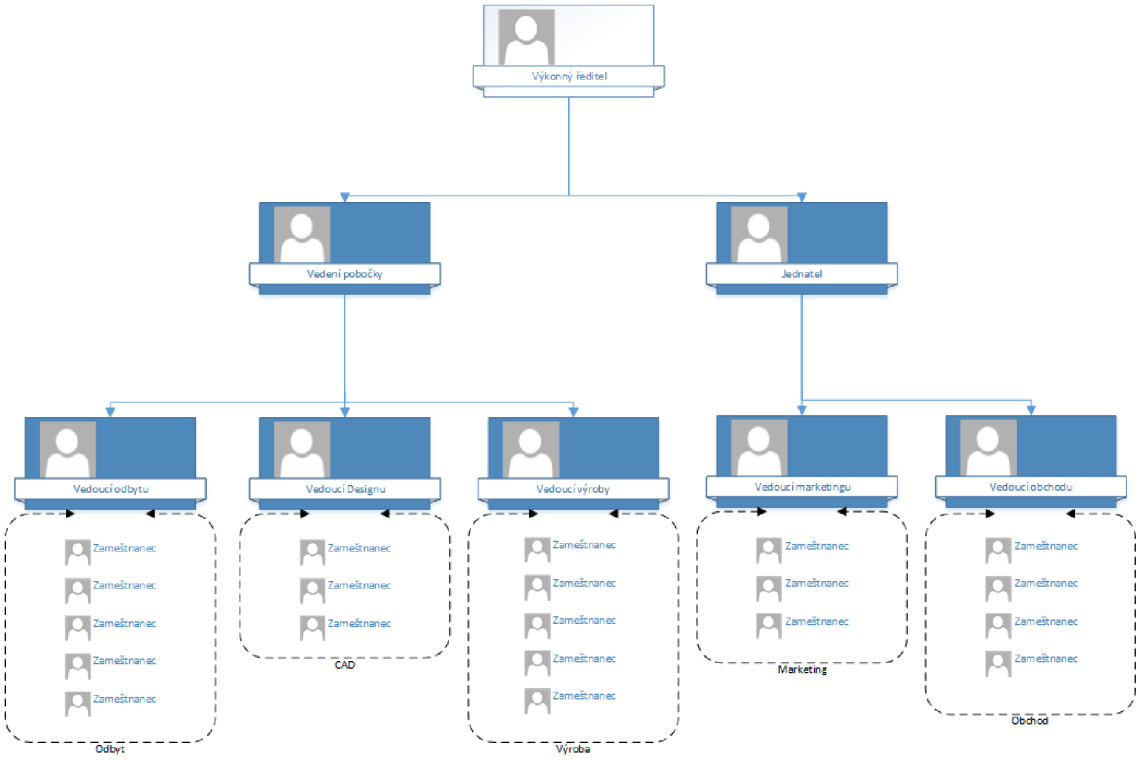
Pozn. Z bezpečnostních důvodů a vzájemně podepsanému NDA nemůžu v této práci uvést název analyzované společnosti. Pracovně ji v této práci budu tedy uvádět pouze jako Společnost.

Společnost se zabývá polygrafickou a kartonážní výrobou. Společnost byla založena v roce 1992, sídlí v České republice a zaměstnává kolem 100 zaměstnanců. Z celkového počtu 100 zaměstnanců je celkem 40 uživatelů počítačů, zbytek spadá do výroby. Společnost má stabilní odběratele a mezi její zákazníky patří i největší dodavatelé léčiv v České republice. Mezi know-how společnosti patří právě návrh a výroba obalů pro léky.

Společnost postupně zavádí ISMS a systémem DLP chce řešit právě vnitřní bezpečnost a auditní záležitosti. Mezi základní požadavek patří ochrana know-how společnosti, tedy ochrana výrobních nákresů.

2.1.1 Organizační struktura

Pro správně provedenou bezpečnostní analýzu a následně realizovanou implementaci DLP řešení musíme znát organizační strukturu analyzované společnosti. V této společnosti je organizační struktura liniová a má 3 stupně řízení.



Obrázek 5 Organizační struktura společnosti (Zdroj: Vlastní zpracování pro DP).

Velikost oddělení neodpovídá přesné velikosti, jde pouze o názorné zobrazení. Pod výkonného ředitele spadají přímo Vedení pobočky – ředitelka, a jednatel společnosti, který má kancelář v Praze. Pod ředitelku pobočky pak spadají oddělení odbytu, designu a výroby. Jednatel má v kanceláři v Praze oddělení marketingu a obchod. Obchodníci jsou většinu času na cestách po České republice i v zahraničí. IT oddělení má společnost outsourcované. Společnosti mají na starosti 2 zástupci z této externí IT společnosti.

2.2 Popis problému

Vedení společnosti na přelomu roku 2013/2014 zjistilo, že se jí rapidně snížily zisky. Dlouhou dobu trvalo zjistit příčinu, až vedení narazilo na nově vzniklou konkurenci v blízkosti dané společnosti. Konkurenci vedl bývalý zaměstnanec, který si přeposílal know-how společnosti na soukromý email a nabízel levnější služby. Bral tak společnosti zakázky, která přicházela o zisky a zákazníky. Společnost o počínání svého zaměstnance neměla v tu dobu ani tušení a se svými prostředky na to ani neměla jak přijít.

Společnost tak prodělala únik dat, který ji poškodil v řádu stotisíců Kč ve formě ztráty zisku. Únik dat nemusí způsobit pouze přímé finanční ztráty, ale může také způsobit ztrátu reputace, která v konečném důsledku také vede ke ztrátě finančních prostředků. Únik dat tak může kompletně zlikvidovat kteroukoliv společnost.

Analyzovaná společnost má perfektně zajištěnou fyzickou bezpečnost. Vstup do podniku je možný pouze skrz vrátnici, kde se o ochranu stará externí bezpečnostní služba. Zaměstnanci i externí návštěvníci jsou při vstupu i výstupu z objektu kontrolování a evidováni. Po celém areálu jsou rozmístěny bezpečnostní kamery, které monitorují pohyb a práci zaměstnanců. Zaměstnanci navíc absolvují v pravidelných intervalech školení BOZP a další nutná školení pro jejich pracovní náplň.

Na druhou stranu bezpečnost informací je zde řešena velmi málo nebo spíše vůbec. Společnost nemá zavedenou bezpečnostní směrnici, která by určovala, jak mají zaměstnanci nakládat s aktivy, aby společnost neohrozili. Nijak zvlášť nejsou ani řešena přístupová práva uživatelů v systému, tak mají uživatelé přístup kamkoli a kdokoliv si může stáhnout firemní citlivá data na USB disk nebo zaslat na email, a společnost nemá ani důkaz, kdo takový čin udělal.

Jediná ochrana, kterou má společnost zavedenou, tak je ochrana proti vnějším hrozbám. Společnost má plošně nasazen antivirový systém a firewall, který chrání počítače proti útokům hackerů a virů. Proti vnitřním hrozbám však chráněna společnost není vůbec.

Tento únik dat a zjištění, že společnost nemá možnost těmto útokům předejít, ani je dohledat, vedly k poptávce po řešení. Společnost tedy usiluje o zavedení ISMS a po nástroji, který dokáže ochránit citlivá data a zaznamenat veškerou činnost uživatelů firemních počítačů.

2.3 Technická analýza prostředí

Pro lepší zmapování současné situace této společnosti jsem naplánoval 2 workshopy, na kterých jsem s klíčovými stakeholdery prošel připravené dotazníky a následně vyhodnotil tyto odpovědi. První workshop byl zaměřen na technickou analýzu pro lepší představu o systémech, síti a vůbec fungování společnosti na technické úrovni. Workshop proběhl v místě sídla společnosti a jako klíčové osoby jsem vybral jednatele

společnosti, což je garant za projekt nasazení DLP systému, a pak zástupce IT, který spravuje společnosti IT a má tedy nejlepší přehled o technické úrovni.

Dotazník s odpověďmi vypadal následovně:

A. Cíle

1. Jaký je hlavní cíl projektu nasazení DLP?
   (konkrétní scénář nebo typ dat)
   Hlavním cílem projektu je ochrana know-how společnosti, zlepšení úrovni bezpečnosti za účelem zavedení ISMS. Dalším cílem pak sledování činnosti zaměstnanců a kontrola produktivity.

2. Jaké jsou časové požadavky na projekt?
   (konkrétní termíny, které je nutno dodržet, např. projekt musí být úspěšně zakončen do dalšího auditu)
   Časový požadavek ani konkrétní termíny, které je nutno dodržet, nejsou.

3. Jaké je plánované využití monitorování?
   (úroveň monitorování podle podrobnosti; využití snímků obrazovky)
   Je zájem o kompletní monitoring všech aktivit včetně snímků obrazovky do budoucna.

B. Architektura IT infrastruktury

4. Kolik je stanic v jednotlivých pobočkách organizace?
   (počet stanic organizace včetně notebooků)
   Celkem je 40 stanic, o nasazení DLP se uvažuje na 17 stanic.

5. Je využívána Active Directory?
   (ano/ne, případně upřesnění)
   Ano.

6. Jaká je struktura IT oddělení?
   (interní / outsourcované, popř. rozdělení kompetencí v IT oddělení vzhledem k Safetica)
   IT oddělení je outsourcované. O IT se starají 2 správci.

C. Síť

7. Jaké jsou kapacity linek využívaných v organizaci?
   (Rozděleno na jednotlivé pobočky)
   100 MB/s.

8. Jaký je volný datový tok mezi klienty a serverem?
   (Odhad v závislosti od kapacity linek a průměrného využití aplikacemi)
   Cca 80 %.

9. Jsou všechny stanice v jedné podsíti?
   Ano, jedná se o lokální síť.

D. Databáze

10. Jakou používáte verze databáze?
    (MS SQL, MS SQL Express, PostgreSQL, MySQL, ..)
    Aktuálně se používá pouze MS SQL Express.

11. Jaký je volný diskový prostor na serveru s databází?
    (případně dalších disků, které je možné využít na zálohy)
    200 GB.

E. Hardware

12. Jaké je minimální hardwarové vybavení počítačů?
    (RAM, Procesor)
    2 GB RAM, 1.6 GHz procesor.

F. Software

13. Jaký bezpečnostní software/hardware je využíván ve společnosti?
    (firewall, antivir, SIEM, VPN klient; cokoliv jiného)
    Firewall a antivir od Esetu.

14. Jsou k některým systémům vyžadovány certifikáty na straně klienta?
    (pro webové aplikace a jiné klienty)
    Ne.

15. Jací e-mailoví klienti jsou využíváni ve společnosti?
    (názvy a verze, použité protokoly a porty)
    MS Outlook 2007 a vyšší verze, Mozilla Thunderbird.

16. Jaký je jiný software používaný na stanicích?
    (CRM, Office, jiný software..)
    AutoCAD 2015, Helios, MS Office, Adobe Acrobat, Adobe Reader, Mozilla Firefox, Chrome.

17. Jaké jsou použité operační systémy na stanicích?
    (také pokud jsou ve společnosti UNIX systémy)
    Windows XP, Windows 7, Windows 8. UNIX žádné.

Z technické analýzy nevyplynuly žádné potenciální problémy. Prostředí je standardní na platformě Windows, stanice mají dostatečný výkon, síť má dobrou propustnost a společnost má nasazenou ochranu od Esetu. Z dotazníku vyplynulo, že hlavním cílem je ochrana know-how společnosti a sekundárním pak monitorování aktivit uživatelů za účelem auditu akcí.

2.4 Bezpečnostní analýza

Bezpečnostní analýza byla druhá část naplánovaných workshopů s klíčovými stakeholdery společnosti. V bezpečnostní analýze jsem se detailněji zaměřil na práci

uživatelů s daty, jak pracují uživatelé se systémy a také na procesy. Realizace byla obdobná, tedy interview se zodpovědnými osobami.

Otázky v tomto dotazníku vypadaly následovně:

0. Jaké jsou Vaše potřeby, se kterými má DLP systém pomoci?
   (např. konkrétní požadavky na monitoring, reporting, restrikce, konkrétní scénář, …)
   Ochránit know-how společnosti – výkresy v AutoCADu, monitorování aktivit, zákaz připojování externích zařízení, zákaz přístupu na vybrané servery, reportování managementu.

A. DATA

1. Jaké jsou hlavní kategorie dat, se kterými zaměstnanci pracují?
   (např. data o zákaznících, zaměstnancích, finanční data, …)
   Dokumenty PDF, Word a Excel – nabídky, smlouvy, ceníky, výnosy, data o zákaznících, data o zaměstnancích.
   Informace z výrobního a účetního systému – účetní data.
   Výstupy/výkresy z AutoCADu – know-how.

2. Kdo jsou autorizované osoby, které mají k datům přístup?
   (všichni nebo vybraní zaměstnanci, management, IT, externí subjekty, dodavatelé, zákazníci, …)
   K výstupům z AutoCADu pouze designéři. K účetním datům pouze vedení společnosti a účetní. K nabídkám pak oddělení odbytu a vedení.

3. Co by se stalo v případě, že by se k těmto datům dostala neautorizovaná osoba?
   (finanční ztráty, negativní PR, pokuty, vznik nových rizik, …)
   Finanční ztráty, ztráta reputace, vznik nových rizik.

4. Můžete popsat životní cyklus dat?
   (kde vznikají; kde zanikají; kde jsou uložena; kdy, kam a jak jsou zasílána; jak se s nimi pracuje, formát dat a jeho změny)

Data vznikají v jednom ze systémů. Data si pak uživatelé ukládají na plochu nebo na sdílený síťový disk. Data pak přeposílají zákazníkovi, dodavateli, řediteli. Buď interně, nebo externě. Je chtěné, aby uživatelé ukládali citlivá data pouze na síťový disk. Finální výstup z AutoCADu je uložen na síťový disk. Rozpracovaný výstup spíše lokálně.

5. Jaká jsou již zavedena opatření pro ochranu dat?
   (dodatky smluv, produkty třetích stran, procesy, zda a jak jsou tato opatření vynucována)
   Zaměstnanci mají podepsán protokol o pokutě při prozrazení informací.

B. SYSTÉMY

6. Jaký software je běžně používán pro práci s daty?
   (intranetové aplikace, ale také FTP klienti, aj.)
   Helios, AutoCAD, MS Office.

7. Která data jsou tímto systémem zpracovávána?
   (konkrétní kategorie dat viz výše)
   Uvedeno výše.

8. Kde a jak má tento software data uložena?
   (dotaz je cílen primárně na IT oddělení)
   Data jsou na serveru, kde běží aplikace.

9. Kteří zaměstnanci mají k systému přístup?
   (kteří mají systém nainstalován a zřízeny přístupové údaje, případně informace o právech uživatele)
   Všichni zaměstnanci, ale uvnitř aplikace je to řešeno přístupovými právy.

C. ZAMĚSTNANCI

10. Jsou zavedeny a vynuceny politiky pro hesla?

(např. použití správce hesel, školení uživatelů, vynucení úrovně hesla do systémů a také jejich změny)
Ne.

11. Mají zaměstnanci přístup k systémům a datům i mimo firmu?
(mobily, tablety, domácí stanice, …)
Jeden uživatel ano. Přistupuje přes RDP s notebookem.

12. Mají zaměstnanci povoleno využívat externí média pro přenos dat?
(USB flash disky, mobily, tablety, externí disky, …; informaci o BYOD politikách a povolení soukromých zařízení pro pracovní potřeby)
Ano, to chceme zakázat.

Po dokončení dotazníků jsem ještě s garantem projektu prodiskutoval další potřeby, které budou chtít systémem DLP řešit. Nastínil mi jeho představy následovně:

- Zakázat připojování USB zařízení a veškeré další porty.
- CD a DVD pouze pro čtení.
- Zakázat připojování mobilních zařízení, fotoaparátů a kamer k počítači.
- Zakázat přístupy na webmaily a server Facebook.
- Zakázat tisk mimo lokální síť.
- Označit všechny citlivé dokumenty.
- Tyto dokumenty se pak nesmí nahrávat na internet (kromě FTP serverů od zákazníků a dodavatelů), nahrávat na USB disky, mohou být odeslány pouze na emailové adresy definované v seznamu, nesmí být povoleno vytvoření snímku obrazovky nad tímto dokumentem, tisk povolen pouze v prostředí společnosti, zákaz pohybu po lokálních discích.
- Všechny výstupy reportovat na vedení.

2.5 Identifikace a ohodnocení aktiv

Z provedených dotazníků jsme se dozvěděli více informací o prostředí, a také jak s daty pracují uživatelé. Hlavní aktiva společnosti jsme idenfitikovali v dotazníku Bezpečnostní analýza v části A.1. V případě řešení problematiky DLP a bezpečnosti

informací má cenu řešit pouze informační aktiva. Z dotazníku tedy idenfitikuji nejdůležitější informační aktiva a zapíši do přehlednější tabulky:

Aktivum	Popis	Vlastník
Nabídky	Citlivé dokumenty obsahující nabídky společnosti.	Vedoucí obchodu
Smlouvy	Smlouvy s dodavateli a zákazníky.	Jednatel
Ceníky	Citlivé ceníky společnosti.	Výkonný ředitel
Výnosy	Údaje o ziscích a výnosech společnosti.	Výkonný ředitel
Data o zákaznících	Informace o zákaznících.	Jednatel
Data o zaměstnancích	Informace o zaměstnancích.	Jednatel
Účetní data	Účetní data z účetního systému.	Vedoucí pobočky
Výkresy	Know-how společnosti, výstupy z programu AutoCAD.	Výkonný ředitel

Tabulka 1 Identifikace aktiv (Zdroj: vlastní zpracování pro DP).

Nyní stanovím stupnici a hodnotící kritéria:

Dopad	Číselné vyjádření
Žádný dopad	1
Zanedbatelný dopad	2
Potíže a finanční ztráty	3
Vážné potíže a velké ztráty	4
Existenční potíže	5

Tabulka 2 Stupnice pro hodnotící kritéria (Zdroj: Vlastní zpracování pro DP).

Uvedená aktiva mají pro společnost určitou cenu a vlastníci společnosti je chtějí chránit. Pro účely analýzy nyní daná aktiva ohodnotím dle hlavních kritérií bezpečnosti informací, která jsem uvedl v první kapitole. Jedná se o ohodnocení z pohledu:

a) Dostupnosti - zajištění přístupnosti informace v požadovaný okamžik,
b) Důvěrnosti - zajištění přístupnosti k informaci pouze uživateli pro něj určené,
c) Integrity - zajištění správnosti a úplnosti informace.

Výslednou váhu aktiva budu počítat součtovým algoritmem, tedy jako zaokrouhlený průměr 3 kritérií (dostupnost, důvěrnost, integrita).

Aktivum	**Zdroj**	**Dostupnost**	**Důvěrnost**	**Integrita**	**Váha**
Nabídky	IS	4	4	4	4
	Síťový disk	2	4	4	3
	Uživatelská stanice	4	4	4	4
Smlouvy	IS	2	5	3	3
	Síťový disk	2	5	3	3
	Uživatelská stanice	2	5	3	3
Ceníky	IS	3	5	4	4
	Síťový disk	2	5	4	4
	Uživatelská stanice	3	5	4	4
Výnosy	IS	2	3	3	3
	Síťový disk	1	3	3	2
	Uživatelská stanice	1	3	3	2
Data o zákaznících	IS	3	4	3	3
	Síťový disk	2	4	3	3
	Uživatelská stanice	3	4	3	3
Data o zaměstnancích	IS	2	3	3	3
	Síťový disk	2	3	3	3
	Uživatelská stanice	2	3	3	3
Účetní data	IS	3	4	4	4
	Síťový disk	2	4	4	3

	Uživatelská stanice	3	4	4	4
Výkresy	IS	3	5	5	4
	Síťový disk	5	5	5	5
	Uživatelská stanice	5	5	5	5

Tabulka 3 Ohodnocení aktiv z pohledu 3 základních kritérií bezpečnosti informací (Zdroj: Vlastní tvorba pro DP).

Z tabulky vidíme, že společnost se musí nejvíce zaměřit na ochranu výkresů, tedy své know-how. Zároveň nalezneme velké množství aktiv, které jsou ohodnoceny jako Vážné potíže a velké ztráty, takže ty se také musí řešit co nejdříve. Pouze u jednoho aktiva má porušení kritérií bezpečnosti zanedbatelný dopad, a to v případě výnosů společnosti.

2.6 Analýza rizik

V předchozí podkapitole jsme identifikovali a ohodnotili aktiva společnosti. Tato aktiva jsou pro společnost cenným majetkem, který chce chránit. Jako další krok jsem tedy provedl analýzu rizik, kde jsem nejdříve idenfitikoval hrozby, které hrozí daným aktivům, a poté vytvořil matici zranitelnosti a matici rizik.

2.6.1 Identifikace hrozeb a zranitelností

V této části jsem provedl identifikaci hrozeb a zranitelností. Věnoval jsem se pouze hrozbám informačním aktivům z pohledu vnitřních hrozeb, tedy pro situace, které může řešit DLP systém. Kompletní výčet hrozeb by byl velmi rozsáhlý a zasahoval by nad rámec této práce.

Prvně jsem vytvořil hodnotící kritérium:

Pravděpodobnost (v %)	Slovní vyjádření	Číselné vyjádření
0 - 19	Zanedbatelná	1
20 - 39	Nízká	2
40 - 59	Střední	3
60 - 79	Vysoká	4
80 - 100	Velmi vysoká	5

Tabulka 4 Hodnotící kritérium pro pravděpodobnost hrozby (Zdroj: Vlastní zpracování pro DP).

Následně jsem sestavil tabulku identifikovaných hrozeb a zranitelností:

Hrozba	Pravděpodobnost	Příklad zranitelnosti
1. Ztráta USB disku s aktivem	3	Lidský faktor, nepozornost
2. Neúmyslné zaslání aktiva na špatnou emailovou adresu	2	Lidský faktor, nepozornost
3. Úmyslné zaslání aktiva konkurenci	2	Lidský faktor
4. Špatně natavená oprávnění k aktivu	3	Nedostatečná kontrola správců IT
5. Nahrání aktiva na veřejně přístupný server	3	Nezaškolení uživatelé
6. Úmyslná krádež aktiva	1	Chybí audit, či systém na zabezpečení
7. Vytištění aktiva a uložení na nechráněné místo	2	Nezaškolení uživatelé, lidská chyba
8. Špatně nastavená oprávnění k systému, ve kterém jsou aktiva	2	Nedostatečná kontrola správců IT
9. Odeslání aktiva nezašifrovaně přes email	5	Chybí systém pro šifrování, nezaškolení uživatelé

Tabulka 5 Identifikace hrozeb a zranitelností aktiv (Zdroj: Vlastní zpracování pro DP).

2.6.2 Matice zranitelnosti

Po identifikaci hrozeb a zranitelností jsem vytvořil matici zranitelnosti, kde jsem dal do matice hrozby a aktiva, a určil jsem, jak jsou aktiva náchylná na uvedené hrozby. Pokud daná hrozba nemá vliv na aktivum, bude buňka prázdná.

Zranitelnost (V)		**Číslo hrozby**	1.	2.	3.	4.	5.	6.	7.	8.	9.
		Pst.[1] hrozby (T)	3	2	2	3	3	1	2	2	5
Aktivum	**Zdroj**	**Váha (A)**									
Nabídky	IS	4	1	3	2		1	1	3	3	4
	Síťový disk	3	2	1	1	3	1	1	2		2

[1] Pravděpodobnost

	Uživatelská stanice	4	4	3	2	3	1	1	3		4
Smlouvy	IS	3	1	3	2		1	1	3	3	4
	Síťový disk	3	2	1	1	3	1	1	2		2
	Uživatelská stanice	3	4	3	2	3	1	1	3		4
Ceníky	IS	4	1	2	3		2	3	3	3	3
	Síťový disk	4	1	1	1	3	1	1	2		2
	Uživatelská stanice	4	3	2	3	3	2	3	3		3
Výnosy	IS	3	2	3	3		2	1	2	3	3
	Síťový disk	2	2	1	1	3	1	1	1		2
	Uživatelská stanice	2	3	3	3	3	2	1	2		3
Data o zákaznících	IS	3	3	3	3		3	3	2	3	3
	Síťový disk	3	3	2	1	3	1	1	1		2
	Uživatelská stanice	3	4	4	3	3	3	3	2		3
Data o zaměstnancích	IS	3	3	3	3		2	1	3	3	3
	Síťový disk	3	3	2	1	3	1	1	2		2
	Uživatelská stanice	3	4	4	3	3	2	1	3		3
Účetní data	IS	4	3	3	3		2	2	2	2	3
	Síťový disk	3	3	1	1	3	1	1	1		2
	Uživatelská stanice	4	4	3	3	3	2	2	2		3
Výkresy	IS	4	2	2	4		3	4	3	2	4
	Síťový disk	5	4	1	2	3	1	3	2		2
	Uživatelská stanice	5	4	3	4	3	3	4	3		4

Tabulka 6 Matice zranitelnosti (Zdroj: Vlastní zpracování pro DP).

Nevyplněné buňky tedy znamenají, že daná hrozba nemá vliv na aktivum. V tom případě se jedná o dvě doplňkové hrozby, kdy hrozba č. 4 má vliv pouze na dokumenty, takže není spojena s žádným aktivem který má zdroj IS, a naopak hrozba č. 8 má zase vliv pouze na systém, tedy pouze na aktiva, která pochází ze zdroje IS.

2.6.3 Matice rizik

Jako poslední krok jsem určil matici rizik. Hodnota rizika se počítá dle vzorce:

$$R = T * A * V$$

kde R je míra rizika, T je pravděpodobnost hrozby, A je váha aktiva a V zranitelnost vypočítaná v tabulce 6 (Steiner, 2007). Pro matici rizik jsem si ještě vytvořil hodnotící kritéria míry rizika:

Riziko	Číselné vyjádření
Bezvýznamné riziko	1 - 24
Akceptovatelné riziko	25 - 49
Nízké riziko	50 - 74
Nežádoucí riziko	75 - 99
Nepřijatelné riziko	100 - 125

Tabulka 7 Hodnotící kritéria míry rizika (Zdroj: Vlastní zpracování pro DP).

Následně jsem sestavil výslednou matici rizik:

Míra rizika (R)		**Číslo hrozby**	1.	2.	3.	4.	5.	6.	7.	8.	9.
		Pst.[2] hrozby (T)	3	2	2	3	3	1	2	2	5
Aktivum	**Zdroj**	**Váha (A)**									
Nabídky	IS	4	12	24	16		12	4	24	24	80
	Síťový disk	3	18	6	6	27	9	3	12		30
	Uživatelská stanice	4	48	24	16	36	12	4	24		80
Smlouvy	IS	3	9	18	12		9	3	18	18	60
	Síťový disk	3	18	6	6	27	9	3	12		30
	Uživatelská stanice	3	36	18	12	27	9	3	18		60
Ceníky	IS	4	12	16	24		24	12	24	24	60
	Síťový disk	4	12	8	8	36	12	4	16		40
	Uživatelská stanice	4	36	16	24	36	24	12	24		60
Výnosy	IS	3	18	18	18		18	3	12	18	45

[2] Pravděpodobnost

	Síťový disk	2	12	4	4	18	6	2	4		20
	Uživatelská stanice	2	18	12	12	18	12	2	8		30
Data o zákaznících	IS	3	27	18	18		27	9	12	18	45
	Síťový disk	3	27	12	6	27	9	3	6		30
	Uživatelská stanice	3	36	24	18	27	27	9	12		45
Data o zaměstnancích	IS	3	27	18	18		18	3	18	18	45
	Síťový disk	3	27	12	6	27	9	3	12		30
	Uživatelská stanice	3	36	24	18	27	18	3	18		45
Účetní data	IS	4	36	24	24		24	8	16	16	60
	Síťový disk	3	27	6	6	27	9	3	6		30
	Uživatelská stanice	4	48	24	24	36	24	8	16		60
Výkresy	IS	4	12	24	16		12	4	24	24	80
	Síťový disk	5	18	6	6	27	9	3	12		30
	Uživatelská stanice	5	48	24	16	36	12	4	24		80

Tabulka 8 Míra rizika (Zdroj: Vlastní zpracování pro DP).

Jak vidíme z tabulky, většina rizik spadá do kategorie bezvýznamných. Na druhou stranu nalezneme i nežádoucí rizika, která je nutné co nejdříve řešit.

2.7 Dostupné DLP systémy

V České republice existuje pouze jeden výrobce DLP systému. Na druhou stranu ve světě je takových výrobců celá řada a i tito výrobci mají zde v České republice své obchodní zastoupení. Můžeme se tedy setkat s několika nabízenými řešeními a vybrat to nejvhodnější, je často těžký úkol.

V České republice existuje pouze jeden výrobce DLP systému. Toto DLP se nazývá Safetica a je vyvíjeno společností Safetica Technologies s.r.o. Na českém trhu existuje ještě řešení od společnosti SODATSW spol. s r.o., které však není plnohodnotné DLP. Ve světě pak mezi největší výrobce patří např. společnost McAfee,

kterou koupil Intel[3], či Symantec. Další DLP systémy, se kterými se můžeme setkat, jsou GFI, RSA, Websense, Trend Micro či CoSoSys Endpoint Protector.

Všechny uvedené DLP systémy jsou založeny na analýze obsahu, tedy contentová DLP. SODATSW se zaměřuje spíše na monitorování aktivit a šifrování. Safetica je jediným zástupcem kontextového DLP.

2.8 Dopady úniku dat

Dle studie Cost of Data Breach, kterou provedla společnost Ponemon Institude v květnu roku 2014, stojí průměrně 1 zcizený záznam společnost €140[4]. Průměrný počet záznamů obsažených v jednom bezpečnostním incidentu je 24 371 (2014 Cost of Data Breach Study: Germany, 2014). Z těchto čísel tedy můžu vyčíslit průměrné náklady na jeden bezpečnostní incident:

$$140 * 24371 = €3\ 411\ 940$$

Jeden únik dat v důsledku bezpečnostního incident tedy stojí společnost v průměru €3 411 940, což je při aktuálním kurzu[5] 93 487 156 Kč. Studie bere v úvahu jak přímé, tak nepřímé náklady, které mohou mít povahu ztráty reputace a tím ztráty zákazníků, dodavatelů apod.

[3] http://www.mcafee.com/us/about/intel-mcafee.aspx
[4] Platí pro Německo. Česká republika nebyla součástí studie.
[5] 27,4 Kč za 1 euro.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole se zaměřím na vlastní návrhy řešení problému, který jsem analyzoval v předcházející kapitole. Definuji rozhodovací kritéria a vyberu vhodné řešení, které bude nejvíce odpovídat požadavkům dané společnosti a problému.

V další části se pak budu zabývat samotnou implementací vybraného řešení do prostředí zákazníka. Implementace DLP systému není triviální a je nutná důkladná příprava s naplánováním všech fází projektu. Řešení je nutné nasazovat do prostředí postupně po vlnách, abychom neomezili BCM organizace. V první části se budu zabývat nastavením a konfigurací produktu, následně pilotní implementací a analýzou namonitorovaných dat. Z analýzy identifikuji hlavní rizika, provedu ohodnocení těchto rizik a navrhnu a realizuji opatření, která sníží tato rizika. Nakonec provedu ekonomické zhodnocení celého projektu.

3.1 Rozhodovací kritéria

Pro výběr správného řešení je nutné definovat správná rozhodovací kritéria. Pro tento projekt jsou především důležité požadavky na požadovanou funkčnost. Dále je zajisté kritérium cena řešení a spolehlivost. Rozhodovací kritéria a váhy zapíši do přehlednější tabulky:

Rozhodovací kritérium	Váha
Monitorování aplikací	4
Monitorování webových stránek	4
Monitorování souborů	4
DLP – ochrana souborů	5
DLP – ochrana není založena na obsahu	4
DLP – ochrana aplikací	5
Řízení přístupu na webové stránky	3
Řízení spouštění aplikací	3
Device Control – řízení externích zařízená	3

Cena	3
Reference	2
Prostředí v češtině	2
Reporty	3

Tabulka 9 Rozhodovací kritéria pro výběr DLP systému (Zdroj: Vlastní zpracování pro DP).

Definovaná kritéria vychází z provedených dotazníků a požadavků od zákazníka. Váha je určena subjektivně dle chápání důležitosti těchto požadavků z provedených analýz a dotazníků.

3.2 Výběr DLP systému

Na základě definovaných rozhodovacích kritérií nyní provedu porovnání dostupných řešení a vyberu to nejvhodnější.

Rozhodovací kritérium	Safetica	Symantec	McAfee	GFI	RSA	Websense	Trend Micro	SodatSW	CoSoSys
Monitorování aplikací	2	0	0	0	0	0	0	2	0
Monitorování webových stránek	2	2	0	0	0	2	0	2	0
Monitorování souborů	2	2	2	0	0	2	0	2	2
DLP – ochrana souborů	2	2	2	2	2	2	2	0	2
DLP – ochrana není založena na obsahu	2	0	0	0	0	0	0	0	0
DLP – ochrana aplikací	2	1	2	0	0	2	0	0	0
Řízení přístupu na webové stránky	2	2	2	0	2	2	0	0	0
Řízení spouštění aplikací	2	2	2	0	0	0	0	0	0
Device Control – řízení externích zařízení	2	2	2	2	2	2	2	2	2
Cena	0	2	1	2		1	0	2	2
Reference	1	2	2	2	2	2	2	1	2
Prostředí v češtině	2	0	0	0	0	0	0	2	0

Reporty	2	2	2	2	2	2	2	2	2

Tabulka 10 Porovnání dostupných řešení dle kritérií (Zdroj: Vlastní zpracování pro DP).[6]

Legenda k tabulce 10:

- Hodnota 0 – dané řešení neposkytuje danou funkčnost vůbec
- Hodnota 1 – dané řešení poskytuje danou funkčnost částečně
- Hodnota 2 – daná řešení poskytuje danou funkčnost

V případě ceny byla kritéria nastavena následovně:

- Hodnota 0 – Cena je větší než 2000 Kč za perpertuální licenci
- Hodnota 1 – Cena je mezi 1500 Kč a 2000 Kč za perpertuální licenci
- Hodnota 2 – Cena je menší než 1500 Kč za perpetuální licenci

Pokud buňka není vyplněna, údaje se mi nepodařilo dohledat. Při porovnávání jednotlivých DLP systémů jsem vycházel z informací uvedených výrobcem na webových stránkách daného řešení, a pokud byla možnost stažení demoverze, vyzkoušel jsem funkčnost v mém testovacím prostředí.

Jako další krok ohodnotím výsledná kritéria dle váhy uvedené v tabulce 9. Výsledné skóre pro dané řešení bude součet výsledných hodnot vynásobených váhou.

Rozhodovací kritérium	Váha	Safetica	Symantec	McAfee	GFI	RSA	Websense	Trend Micro	SodatSW	CoSoSys
Monitorování aplikací	4	8	0	0	0	0	0	0	8	0
Monitorování webových stránek	4	8	8	0	0	0	8	0	8	0
Monitorování souborů	4	8	8	8	0	0	8	0	8	8
DLP – ochrana souborů	5	10	10	10	10	10	10	10	0	10
DLP – ochrana není založena na obsahu	4	8	0	0	0	0	0	0	0	0

[6] Při porovnání jednotlivých řešení jsem vycházel z těchto zdrojů: (Symantec Data Loss Prevention, 2015), (McAfee Total Protection for Data Loss Prevention, 2015), (GFI Software, 2015), (EMC, 2015), (Websense, 2015), (Tend Micro, 2015), (SODATSW, 2015) a (CoSoSys, 2015).

DLP – ochrana aplikací	5	10	5	10	0	0	10	0	0	0
Řízení přístupu na webové stránky	3	6	6	6	0	6	6	0	0	0
Řízení spouštění aplikací	3	6	6	6	0	0	0	0	0	0
Device Control – řízení externích zařízení	3	6	6	6	6	6	6	6	6	6
Cena	3	0	6	3	6		3	0	6	6
Reference	2	2	4	4	4	4	4	4	2	4
Prostředí v češtině	2	4	0	0	0	0	0	0	4	0
Reporty	3	6	6	6	6	6	6	6	6	6
Celkem		**82**	**65**	**59**	**32**	**32**	**61**	**26**	**48**	**40**

Tabulka 11 Ohodnocení řešení na základě kritérií a váhy (Zdroj: Vlastní zpracování pro DP).

Dle výsledků pro definovaná kritéria a váhy vychází nejlépe řešení Safetica od českého výrobce Safetica Technologies s.r.o. Na druhém místě skončilo řešení od společnosti Symantec a na třetím řešení Websense. Řešení Safetica jsem tedy vybral jako nejvhodnější pro tento projekt a nadále se budu v práci věnovat nasazení právě tohoto řešení.

3.2.1 Popis vybraného DLP řešení

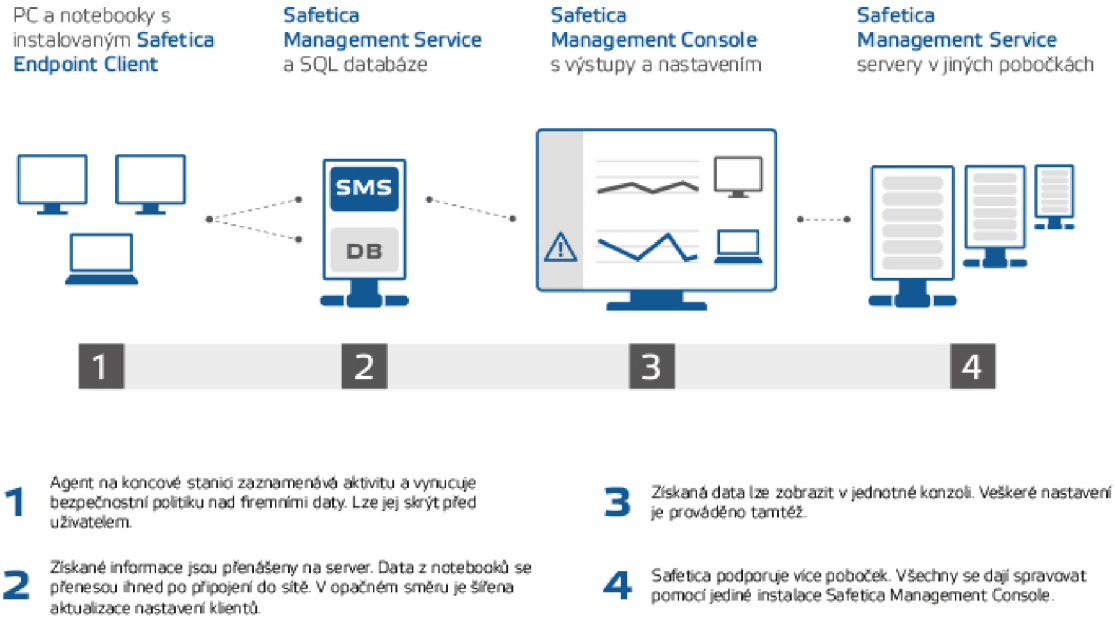
Jako vhodné DLP řešení k vyřešení problému zvýšení ochrany citlivých informací před únikem ve vybrané společnosti jsem si vybral řešení české technologické firmy Safetica Technologies s.r.o., jejíž produkt se jmenuje Safetica.

Safetica patří do kategorie řešení DLP koncových bodů postaveného na kontextově-orientované ochraně. Tento inovativní způsob ochrany dat zavedla jako první a v oblasti ochrany bezpečnosti informací se touto filozofií snaží porazit giganty na trhu DLP uvedené v předchozí části.

Bezpečnostní software Safetica nabízí kompletní řešení pro ochranu dat (DLP – Data Leak Prevention). Pokrývá širokou oblast bezpečnostních hrozeb majících společného jmenovatele – lidský faktor. Safetica chrání proti úmyslným i náhodným únikům dat, škodlivým aktivitám, poklesu produktivity i rizikům spojeným s trendem BYOD (Bring Your Own Device). Filosofie produktu Safetica je postavena na třech pilířích: flexibilita, úplnost a jednoduchost používání. Safetica nabízí společnostem

plnohodnotnou ochranu před únikem dat, poskytuje jejich managementu detailní přehled o aktivitách uživatelů a efektivně vynucuje bezpečnostní pravidla a politiky v rámci organizace. Safetica v jednom balíčku nabízí rozsáhlý soubor nástrojů, které by jinak vyžadovali více bezpečnostních programů od různých dodavatelů (Safetica Technologies s.r.o., 2015).

Architektura řešení je založena na bázi klient-server. Klient se instaluje přímo na koncové stanice a pak komunikuje se serverovou komponentou. V první fázi se připojí na server a zjistí IP adresu databáze, se kterou poté komunikuji napřímo. Do databáze klient ukládá záznamy a stahuje si z ní nastavení, které je uloženo lokálně, takže funguje i offline. Server se spravuje přes centrální správcovskou konzoli, jako je zobrazeno na obrázku 5.



Obrázek 6 Architektura produktu Safetica. Zdroj: (Safetica Technologies s.r.o., 2015)

Seznam klíčových funkcí a vlastností si shrneme v následující tabulce:

Kompletní prevence úniků dat	I přes snadnou instalaci a použití hlídá Safetica všechny cesty pro únik dat.
Trendy a produktivita	Software varuje vedení společnosti v případě náhlých změn v chování zaměstnanců nebo při dlouhodobém poklesu produktivity.
Přehled o aktivitách	Safetica odhalí porušení bezpečnostních nařízení a upozorní na možné hrozby dříve, než způsobí ohrožení citlivých informací.
Ochrana dat přenášených e-mailem	Safetica zajistí, aby se chráněná data neocitla ve špatné e-mailové schránce. Software také zaznamená, kam byla jaká data zaslána a kým.
Blokování aplikací s časovými pravidly	Software omezí dostupné aplikace pouze na ty pracovní. Aplikace mohou být povoleny nebo zakázány i pro konkrétní časový úsek.
Omezení navštěvovaných webů	Můžete jednoduše vybrat, která skupina má přístup ke kterým webovým portálům či jejich podstránkám. Blokovat můžete konkrétní servery nebo vytvářet pravidla na základě vybraných slov nebo kategorií.
Kontrola tisku	Safetica kontroluje, kdo může tisknout jaké dokumenty. Můžete také nastavit limity pro tisk oddělení nebo jednotlivců.

Tabulka 12 Základní funkce a vlastnosti produktu Safetica 1. část. Zdroj: (Safetica Technologies s.r.o., 2015)

Správa přenosných zařízení	Safetica zamezí uživatelům v připojování zařízení, která nejsou schválena pro provoz ve firemní síti.
Šifrování	Software umožní šifrovat celé oddíly nebo vytvářet zabezpečené síťové disky. Pro přenosná média lze vynutit zašifrování vynášeného obsahu, když data opouští zabezpečenou oblast.
Testovací a informativní DLP režimy	Se softwarem Safetica urychlíte nasazení ochrany dat díky testovacímu režimu, informativní režim naopak umožňuje vzdělávat uživatele o nově nasazené ochraně informací.
Klasifikace dat za chodu	Citlivá data jsou chráněna ihned po jejich vytvoření.
Jednotná konzole pro správu	Safetica Management Console umožnuje centrální správu celé bezpečnosti z jednoho místa. Obsahuje veškeré přehledy i nastavení.
Inspekce šifrovaných spojení SSL/HTTPS	Safetica kontroluje také zabezpečená spojení k webovým stránkám, šifrované IM spojení a zabezpečené e-mailové přenosy.
Minimální náklady na implementaci a provoz (nízké TCO)	Není třeba nakupovat specializovaná bezpečnostní zařízení. Klienti instalovaní na všech koncových stanicích zajišťují také prvky síťového DLP.
Univerzální přístup	Díky unikátnímu přístupu k ochraně dat není software Safetica závislý na konkrétních aplikacích nebo protokolech.

Tabulka 13 Základní vlastnosti a funkce produktu Safetica 2. část. Zdroj: (Safetica Technologies s.r.o., 2015)

3.3 Plán projektu nasazení vybraného DLP systému

Projekt implementace DLP systému je velmi komplexní a časově náročná činnost. Je tedy nutné vytvořit plnohodnotnou dokumentaci ke každému projektu a detailně naplánovat jednotlivé fáze a činnosti.

3.3.1 Cíle projektu

Celkovým cílem projektu je zvýšit úroveň bezpečnosti ve společnosti. Konkrétní definované cíle v rámci dokumentu Smlouva o dílo:

- Nainstalovat software Safetica pro celou organizaci
- Nastavit software Safetica pro celou organizaci
- Zlepšit úroveň bezpečnosti v organizaci

Projekt se týká rozsahu definovaného zákazníkem, tedy 17 stanic.

3.3.2 Činnosti v projektu

K vytvoření harmonogramu sepíši nejdříve jednotlivé činnosti a k nim následně vytvořím časovou analýzu.

A. Kick-off se zákazníkem

Oficiální zahájení projektu za přítomnosti klíčových stakeholderů a realizátorů projektu.

B. Technická analýza

Technická analýza obsahuje ověření kompatibility s prostředím a zajištěním případných problému při implementaci. Analýza zahrnuje mj. používané aplikace a specifikaci prostředí. Pro technickou analýzu využiji dotazníku a interview se zákazníkem.

C. Bezpečnostní analýza

Bezpečnostní analýza obsahuje specifikaci scénářů, procesů a definice požadavků na produkt. Cílem je identifikovat scénáře, které se budou implementovat, a na ně identifikovat možné nastavení. Zároveň je nutné zjistit uživatelské role a přístupová práva jednotlivých uživatelů.

D. Pilotní nasazení

Tato činnost obsahuje pilotní nasazení produktu do společnosti na pár vybraných stanic. Při implementaci se postupuje postupně, aby se neomezilo tzv. BCM[7]. Tato činnost obsahuje instalaci serverové části řešení, správcovské konzole a instalace klientské části na pár vybraných koncových stanic.

[7] Business continuity management neboli řízení kontinuity organizace je aktivita úzce spojená a podřízená podnikání, která může poskytnout strategický a provozní rámec pro pohled na způsob, jakým organizace poskytuje svoje produkty a služby a jak je při tom odolná proti jejich zničení, narušení nebo ztrátě. (Ondrák, 2013)

E. Školení

Správci produktu Safetica budou proškoleni na používání, administraci a údržbu produktu.

F. Konfigurace a základní nastavení

Tato činnost obsahuje základní nastavení produktu včetně ověření funkčnosti a zapnutí monitorovacích funkcí pro potřeby činnosti následující. Základní konfigurace obsahuje připojení serveru, nastavení spojení na databázi, SMTP serveru a další správcovské nastavení.

G. Rozšíření implementace

Rozšíření pilotní implementace po ověření funkčnosti na finální počet stanic.

H. Analýza namonitorovaných dat

Analýza namonitorovaných dat je základním stavebním kamenem pro nasazení DLP modulu softwaru Safetica. Z analýzy zjistíme základní bezpečnostní rizika, scénáře jak se pracuje s daty a aplikacemi, a následně na to můžeme nastavit bezpečnostní politiky.

I. Pokročilé nastavení

Tato činnost navazuje na analýzu namonitorovaných dat. Díky ní totiž můžeme provést pokročilejší nastavení DLP a již zavést bezpečnostní politiky.

J. Testování bezpečnostních politik

V této fázi testujeme bezpečnostní politiky, jestli blokují správné incidenty.

K. Optimalizace

Optimalizace pracuje s výstupy testování politik a volitelně poskytuje možnost upravit nastavení.

L. Akceptace

Oficiální ukončení projektu.

3.3.3 Časová analýza projektu

Pro vytvoření časové analýzy použiji metodu PERT[8], protože jednotlivé činnosti mají stochastickou povahu, neznáme jejich přesné trvání.

Činnost	Doba trvání [hodiny]				
	a_{ij}	m_{ij}	b_{ij}	t_{ij}	σ^2_{ij}
A. Kick-off se zákazníkem	1	2	4	2	0,25
B. Technická analýza	1	2	5	2	0,44
C. Bezpečnostní analýza	1	2	5	2	0,44
D. Pilotní nasazení	3	8	16	9	4,69
E. Školení	4	8	16	9	4,00
F. Konfigurace a základní nastavení	3	5	8	5	0,69
G. Rozšíření implementace	2	4	8	4	1,00
H. Analýza namonitorovaných dat	4	8	16	9	4,00
I. Pokročilé nastavení	4	8	16	9	4,00
J. Testování bezpečnostních politik	8	16	24	16	7,11
K. Optimalizace	4	8	16	9	4,00
L. Akceptace	1	2	4	2	0,25
Celkem	**36**	**73**	**138**	**78**	

Tabulka 14 Doba trvání jednotlivých činností projektu.

V tabulce jsou uvedeny jednotlivé činnosti a dle metody PERT také doba trvání. Jednotlivé sloupce znamenají následující:

- a_{ij} – nejkratší předpokládanou dobu trvání činnosti – optimistický odhad,
- b_{ij} – nejdelší uvažovanou dobu trvání činnosti – pesimistický odhad,
- m_{ij} – nejpravděpodobnější dobu realizace činnosti – modální (normální) odhad.
- t_{ij} – střední hodnota (zaokrouhlena na celá čísla)
- σ^2_{ij} – rozptyl (zaokrouhlen na dvě desetinná místa)

[8] Program Evaluation and Review Technique je Je zobecněním metody kritické cesty(CPM). Tato metoda se používá k řízení složitých akcí majících stochastickou povahu. Zde se doba trvání každé dílčí činnosti chápe jako náhodná proměnná mající určité rozložení pravděpodobnosti. (Metoda PERT, 2014)

V realizaci tohoto projektu jsou práce účtovány na tzv. člověkohodiny, kde jeden člověkoden znamená 8 hodin práce jednoho technika. Z tabulky tedy můžeme vyčíst, že projekt je možné realizovat nejdříve za 36 hodin (4,5 člověkodne), nejpozději za 138 hodin (17,25 člověkodne) a nejpravděpodobněji za 73 hodin (9,125 člověkodne).

Střední hodnotu t_{ij} jsem pak spočítal váženým průměrem dle následujícího vzorce (Metoda PERT, 2014):

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

a rozptyl:

$$t_{ij} = \frac{(b_{ij} - a_{ij})^2}{36}$$

Pro přesnější plán projektu vytvořím ještě časovou analýzu pomocí CPM[9] metody a určím tak dobu trvání projektu na základě výpočtu kritické cesty.

Činnost	Následující činnost	t_{ij}	ZM	KM	ZP	KP	CR
A. Kick-off se zákazníkem	B, C	2	0	2	0	2	0
B. Technická analýza	D	2	2	4	2	4	0
C. Bezpečnostní analýza	D	2	2	4	2	4	0
D. Pilotní nasazení	E, F	9	4	13	4	13	0
E. Školení	G	9	13	22	13	22	0
F. Konfigurace a základní nastavení	G	5	13	18	17	22	4
G. Rozšíření implementace	H	4	22	26	22	26	0
H. Analýza namonitorovaných dat	I	9	26	35	26	35	0
I. Pokročilé nastavení	J	9	35	44	35	44	0
J. Testování bezpečnostních politik	K	16	44	60	44	60	0
K. Optimalizace	L	9	60	69	60	69	0
L. Akceptace	-	2	69	71	69	71	0

Tabulka 15 Časová analýza pomocí metody CPM.

Vysvětlivky k tabulce:

- t_{ij} – střední hodnota (zaokrouhlena na celá čísla)
- ZM – začátek možný
- KM – konec možný
- ZP – začátek přípustný

[9] Critical Path Metod

- KP – konec přípustný
- CR – celková rezerva

Činnosti jsou v tomto projektu naplánovány v návaznosti jedné na druhou. Proto v tabulce 15 nenalezneme příliš časových rezerv v tomto plánu. Nicméně můžeme z tabulky vypočítat kritickou cestu a určit tak dobu trvání celého projektu:

$$2 + 2 + 9 + 9 + 4 + 9 + 9 + 16 + 9 + 2 = 71$$

Kritická cesta tohoto projektu vyšla 71 hodin (8,875 člověkodne), což je zároveň reálně odhadovaná doba trvání tohoto projektu. Pro upřesnění je to doba aktivně strávená na tomto projektu v prostředí zákazníka, nezapočítávám do ní práci interní a také prodlevy mezi jednotlivými činnostmi. Jedná se o dobu, která se bude účtovat zákazníkovi jako práce na implementaci.

Obrázek 7 PERT diagram činností projektu

Na obrázku 7 ještě vidíme jednotlivé činnosti projektu znázorněny do přehledného diagramu.

3.3.4 Komunikační platforma (realizační tým)

Komunikační platforma je určena na definování rolí a odpovědností v rámci dodávky díla a způsoby komunikace v jednotlivých případech.

Komunikační matice uvádí přehled rolí a odpovědností v rámci projektu:

Za společnost	**Zákazník**		
Kontaktní osoba za management	Jméno	Email	Telefon
Ve spolupráci s Key Account Managerem zpracovává smlouvy a průvodní dokumenty; s Project Managerem komunikuje o plánování a realizaci projektu.			
Kontaktní osoba za IT oddělení	Jméno	Email	Telefon
Osoba odpovědná za realizaci plnění na straně zákazníka; zajišťuje připravenost prostředí pro testovací i reálné nasazení produktu; slouží jako primární kontakt pro Technical Consultanta za společnost zákazníka.			

Tabulka 16 Komunikační matice – zákazník

Za společnost	**Safetica Technologies s.r.o.**		
Key Account Manager	Jméno	Email	Telefon
Slouží jako primární kontakt objednatelovi za společnost Safetica Technologies s.r.o.; připravuje a realizuje podepsání smluv a průvodních dokumentů.			
Project Manager	Jméno	Email	Telefon
Osoba odpovědná za plánování a realizaci projektu.			
Technical Consultant	Jméno	Email	Telefon
V spolupráci s IT oddělením objednatele realizuje testovací i plné nasazení produktu; odpovídá za řešení případných technických dotazů a problémů.			

Tabulka 17 Komunikační matice – dodavatel

V tabulce 16 a 17 jsou sepsány role za zákazníka a za dodavatele. Neuvádím zde žádné kontaktní údaje z důvodu utajení.

Komunikační pravidla jsou ve zkratce znázorněna v následující tabulce:

Typ komunikace	**Safetica Technologies**	**Zákazník**
Technický dotaz/problém	Technical Consultant	Kontaktní osoba za IT oddělení
Analytický dotaz/požadavek	Technical Consultant	Kontaktní osoba za IT oddělení, Kontaktní osoba za management
Obchodní dotaz	Key Account Manager	Kontaktní osoba za IT oddělení, Kontaktní osoba za management

Obchodní dotaz k plnění	Project Manager, Key Account Manager	Kontaktní osoba za IT oddělení, Kontaktní osoba za management

Tabulka 18 Komunikační pravidla ve zkratce

Pravidla pro obecnou komunikaci jsou pak nastavena následovně:

- V případě obchodních dotazů komunikuje se zákazníkem primárně KeyAccount Manager;
- V případě formální stránky projektu, plánování, domlouvání termínů komunikuje s objednatelem primárně Project Manager;
- Pro případ dotazů k realizaci projektu komunikuje s objednatelem primárně Technical Consultant;
- Pro případ řešení problémů komunikuje s objednatelem primárně Technical Consultant. Postupuje se v těchto případech podle standardních procesů komunikace se zákaznickou podporou Safetica Technologies s.r.o., a podle eskalačního procesu popsaného níže.

Pravidla postupu při eskalaci incidentu ze strany zákazníka:

1. Primárním kontaktem zákazníka je Technical Consultant;
2. V případě nutnosti eskalace osloví zákazník Project Managera s popisem situace;
3. Poslední úroveň eskalace představují KeyAccount Manager s Project Managerem v emailové kopii.

3.4 Návrh nastavení a zlepšení

Z provedené analýzy z druhé kapitoly si můžeme udělat obrázek o aktuální situaci ve společnosti a potřebách, které chce daná organizace řešit a zlepšit. Na základě sesbíraných a zanalyzovaných informací tak mohu navrhnout základní plán nastavení, který bude přílohou dokumentu Smlouva o dílo a konzultován se zákazníkem. Jde o návrh, který se bude měnit během implementace po diskuzi se zákazníkem. Z provedených analýz také vyplývá pár rizik, které musíme zohlednit při samotném projektu a redukovat je.

Plán nastavení produktu vypadá následovně:

3.4.1 Nastavení monitorovacích funkcí

Níže uvedené funkce budou zapnuty pro všechny uživatele:

- Monitorování aplikací
- Monitorování webových stránek
- Monitorování emailů bez monitorování obsahu
- Monitorování tisku
- Monitorování pohybu souborů
- Monitorování síťového toku
- Vyhledávané řetězce
- Aktivita uživatelů – využití pracovních stanic zaměstnanců

3.4.2 Nastavení restriktivních funkcí

Restriktivní funkce budou nastaveny následovně:

1. Restrikce pro přístup na webové stránky
    - Pomocí seznamu zakázaných stránek
    - Zakázaná kategorie stránek: Webmails – email.cz, gmail.com, atd.
    - Zakázaná kategorie stránek: Social networks
    - Zakázaný vybraný server: www.facebook.com, www.youtube.com
2. Restrikce pro spouštění aplikací
    - Pomocí seznamu zakázaných aplikací na kategorii torrentů
    - Zakázané aplikace: Aplikace na externích médiích

3.4.3 Nastavení pro ochranu dat

Ochrana dat bude nastavena následovně:

1. Restrikce pro přístup externích médií do systému
    - Zákaz USB disků
    - Zákaz Bluetooth portu
    - Zákaz FireWire
    - Zákaz IrDA
    - Zákaz LPT
    - Zákaz COM
    - Pro čtení CD/DVD

- Zákaz přenosných zařízení systému Windows (fotoaparáty, mobilní telefony, kamery)

2. Označení citlivých dat
    - Budou zavedeny kategorie citlivých dat, které se definují se zákazníkem v rámci Analýzy.
    - Podle normalizované struktury dokumentů budou označeny dokumenty ve sdíleném úložišti, a to následovným způsobem:
        - Jednorázově budou označeny data podle filtrovacích pravidel a odpovídající datovou kategorií.
        - Bude nastaveno průběžné značení dat podle filtrovacích pravidel v rámci celého rozsahu organizace.
    - Budou označeny všechny PDF, MS Excel a MS Word dokumenty.
    - Bude nastaveno defaultní označení z vybraných aplikací a při specifikovaných situacích zákazníkem.

3. Budou definovány datové bezpečnostní politiky pro ochranu citlivých dat. Politiky budou mít následovné parametry:
    - Přístup na lokální disky: Zákaz
    - Přístup na externí média: Zákaz
    - Přístup na tiskárny: Tisk povolen pouze pro tiskárny využívané v dané organizační jednotce
    - Přístup na síť: Zákaz s výjimkou na FTP server využívaný v dané organizační jednotce
    - Snímky obrazovky, vypalování: Zakázáno
    - Kopírování do schránky: Povoleno
    - Může být definováno více politik na základě požadavků zákazníka.

4. Budou nastaveny DLP pravidla pro celou organizaci a všechny kategorie citlivých dat definovaných výše. Bude také nastaveno aplikační DLP pravidlo pro aplikaci AutoCAD. DLP pravidla budou nastaveny v testovacím režimu (vše

je monitorováno, nic není restriktivně zakázáno. Uživatelé nejsou notifikováni o omezení práce s daty a aplikacemi.).

3.4.4 Administrativní nastavení

Bude provedeno následující administrativní nastavení:

1. Nastavení klienta na koncových stanicích
    - Normální režim klienta s notifikacemi
    - Zakázána odinstalace a aktualizace software Safetica

2. Nastavení připojení k serveru, aktualizace
    - Bude nastaveno připojení k SMTP serveru a propojení s Active Directory strukturou

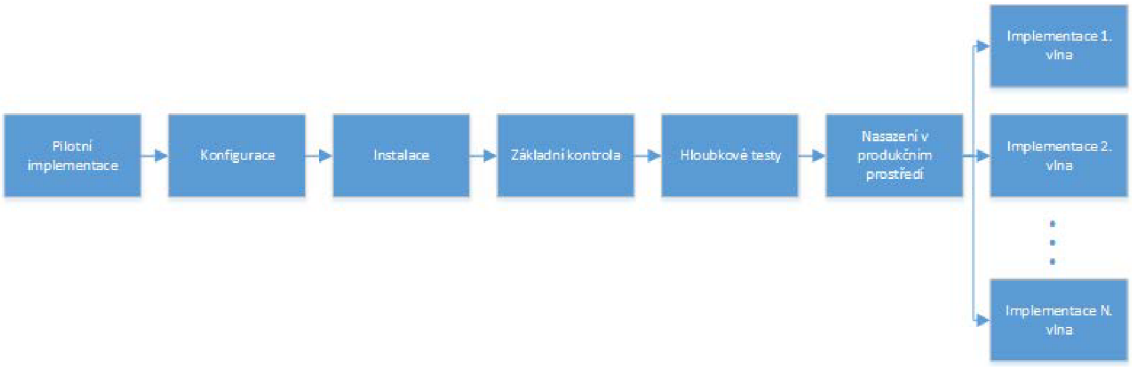
3. Reporty
    - Budou nastaveny týdenní reporty, které budou obsahovat kompletní přehled v rámci celé organizace. Reporty budou chodit na emailové adresy definované zákazníkem.

4. Archivy
    - Bude nastavená pravidelná archivace všech záznamů specifikována zákazníkem.

5. Varování, se budou spouštět v následujících případech:
    - Safetica služba byla neočekávaně ukončena, na serveru není dostatek místa (databáze), Komponenty byly poškozeny, licence vypršela, uživatel se snaží prolomit ochrany Safetica;
    - Uživatel se pokouší přistoupit na zakázanou aplikaci nebo web, Uživatel se snaží připojit zakázané externí zařízení.

3.5 Implementační plán DLP systému

Nasazení DLP systému není triviální proces, a proto je k úspěšné realizaci potřeba implementační plán. Implementace DLP se skládá z několika jednotlivých činností, které zde popíši. Implementační plán pro tuto společnost jsem navrhl následovně:



Obrázek 8 Implementační plán

V této implementaci se tedy budu zabývat následujícími fázemi:

- Pilotní implementace
- Konfigurace
- Instalace
- Základní kontrola
- Hloubkové tesy
- Nasazení v produkčním prostředí

Implementační plán jsem sestavil na základě principů PDCA. Samotná implementace je takto navržena z důvodu zachování BCM, protože nasazení do celého rozsahu implementace v jeden moment by mohla mít fatální následky. Řešení Safetica totiž využívá invazivní technologie v systému a zároveň se integruje do síťové vrstvy. Často využívá podobné technologie jako antiviry a jiné bezpečnostní produkty, může tedy docházet ke kolizím s těmito produktu. Proto jsem zvolil opatrnější strategii, kde nasazení probíhá od nejméně kritických jednotek organizace a jde postupně po vlnách. V první vlně je nasazení klientské stanice pouze na 2 stanice, probíhá ověření prostředí, poté se pokračuje v instalaci dále a iterativně probíhá kontrola a instalaci s další každou vlnou. Po prvním větším množství nasazených počítačů probíhají hloubkové testy, které kontrolují, zda je vše na koncových stanicích v pořádku. Končí se potom nasazením do produkčního prostředí v celém rozsahu a nasazením DLP politik, které se také musím

testovat a ladit. Po dokončení těchto iterativních cyklů je nasazení kompletní a proběhne akceptace.

3.6 Pilotní implementace

Pilotní implementace je prvním kontaktem řešení s daným prostředím zákazníka. V případě nasazení DLP řešení, ostatně jako jakéhokoliv jiného softwaru, do celého prostředí je nutné jednat rozvážně a nasazovat postupně. K tomuto účelu slouží pilotní implementace, což v tomto případě považuji nasazení na 2 vybrané testovací stroje z produkčního prostředí.

V případě nasazení DLP postupuji od nejméně kritických jednotek organizace. Se zákazníkem tedy proběhla domluva, kde mi vyhradil 2 stanice k nasazení pilotní implementace.

Pilotní implementace obsahuje následující fáze:

- Ověření připravených prerekvizit
- Ověření prostředí zákazníka
- Instalace serverové komponenty Safetica Management Service (dále SMS)
- Instalace správcovské konzole Safetica Management Console (dále SMC)
- Instalace 2 klientských testovacích stanic Safetica Endpoint Client (dále SEC)
- Základní ověření funkčnosti

3.6.1 Ověření připravených prerekvizit

V prvním kontaktu IT oddělení za stranu zákazníka s technickým konzultantem za stranu Safetica Technologies probíhá výměna dokumentu, který zmiňuje zákazníkovi minimální softwarové a hardwarové požadavky a dále také požaduje přípravu některých prerekvizit. Prerekvizity jsou připravovány dopředu z důvodu úspory času. Zákazník má připravit následující:

- Možnost lokálního nebo vzdáleného přístupu k serveru a klientským stanicím (např. pomocí produktu TeamViewer).
- Připravenou databázi v podporované verzi (případně je možné použít MS SQL Express, která je součástí instalátoru Safetica).
- Koncové stanice musí mít dostupné síťové spojení na serverovou službu a databázi.

- Serverová služba musí mít na firewallu výjimku pro porty: 1433 (SMS – DB), 4438 (SMS – SEC) a 4441 (SMS – SMC).
- V případě zájmu o zasílání automatických upozornění je nutno vytvořit poštovní účet pro tyto účely.
- Strukturu v Microsoft® Active Directory® (preference bez duplicit ve více skupinách).
- Zajistit možnost restartu koncových stanic.
- Mít možnost lokálně deaktivovat antivir pro instalaci, čí ladění kompatibility.
- Nutná je instalace .NET framework 3.5 a dostupných aktualizací operačního systému.

Většina prerekvizit je nastavována z důvodu základní funkčnosti produktu. Pokud jsou tedy tyto prerekvizity připraveny v pořádku, ušetří to v projektu čas v případě případného ladění problémů. V tomto projektu byly prerekvizity v pořádku připraveny, můžeme tedy postupovat na další fázi.

3.6.2 Ověření prostředí

Ověření prostředí obsahuje kontrolu a prevenci před případnou nekompatibilitou. Do tohoto ověření patří kontrola softwaru, hardwaru i sítě. V prvním kroku jsou ověřovány minimální hardwarové a softwarové požadavky.

Zákazník má prostředí pouze na systému Microsoft Windows od edice XP, tedy kompatibilní. Stanice také splňují minimální hardwarové požadavky. Databázi budeme instalovat MS SQL Express. Síťová architektura je standardní a nedochází k větším výpadkům, prostředí je tedy v pořádku pro nasazení.

3.7 Konfigurace a základní nastavení

Po pilotní implementaci nám již produkt v pořádku funguje a tak můžeme začít s konfigurací. V této fázi projektu se bavíme o základním nastavení produktu, které je nutné pro samotné fungování produktu a také jako příprava pro následující fáze.

3.7.1 Správcovské nastavení

Nastavení serveru je první nastavení, které se ve správcovské konzoli dělá. Jedná se o připojení této konzole na serverovou komponentu. Ve stejném pohledu je nutné ještě

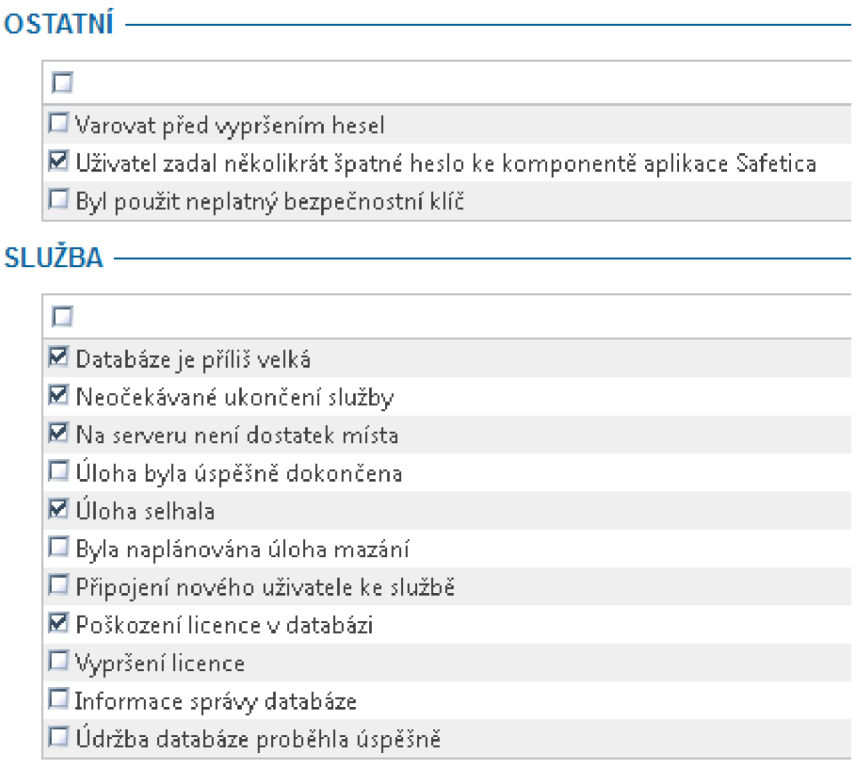
nastavit připojení na databázi a nastavit SMTP server pro zasílání reportů. Po úspěšném nastavení jsme připojeni na server a můžeme dělat další nastavení v produktu.

Dle požadavků zákazníka je nutno také nastavit zálohu a archivaci databáze. Nastavil jsem 2 úlohy – jednu pravidelnou čtvrtletní zálohu a archivaci databáze se záznamy, druhou měsíční zálohu databáze nastavení.

Dalším požadavkem bylo nastavení pravidelných reportů, které budou chodit jednou týdně na email managementu, a také varování, která budou dostávat zástupci IT oddělení v případě nějakého bezpečnostního či správcovského incidentu. Reporty jsem nastavil následovně:

Obrázek 9 Nastavení reportu

Report bude tedy chodit s obsahem definovaným na obrázku 9. Varování jsme zatím nastavili pouze servisní, hlídání bezpečnostních incidentů bude mít smysl až v pozdější fázi nastavení DLP. Servisní varování budou chodit v následujících situacích:

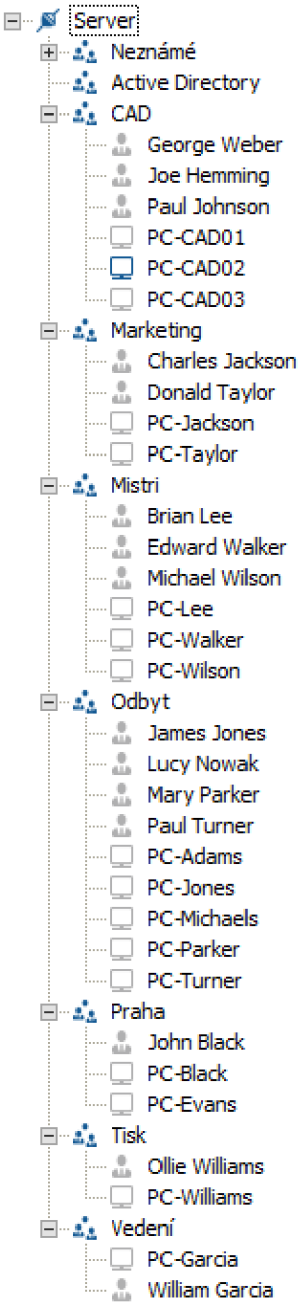


Obrázek 10 Nastavení varování

3.7.2 Vytvoření struktury uživatelů

Struktura uživatelů je v systému DLP, a konkrétně v produktu Safetica, velmi důležitá. Pro dobře definovanou strukturu je pak totiž jednodušší aplikovat bezpečnostní politiky např. po odděleních. V jednom oddělení totiž většinou pracovníci pracují podobně, využívají podobné aplikaci a přistupují k podobným datům. Jedná se tedy o homogenní prostředí, pro které je jednodušší nastavit bezpečnostní politiku. Bezpečnostní politika je pak tedy většinou vytvořena pro každé oddělení zvlášť. Můžou být ale takové případy, kde se nastaví jedna globální politika pro celou firmu a pak již jen pár upřesňujících na vybrané uživatele či skupinky uživatelů. Výhodou je, pokud má společnost dobře definovanou strukturu v AD. Tuto strukturu pak můžeme synchronizovat pomocí produktu Safetica a bude tak zajištěno, že struktura je vždy aktuální a správce nemusí spravovat strukturu na více místech v případě fluktuace zaměstnanců.

Analyzovaná společnost však neměla vhodně utvořenou strukturu AD, tak jsem ji definoval dle organizační struktury a přiřadil do ní vybrané uživatele. Výsledek v produktu je vidět na následujícím obrázku:



Obrázek 11 Strom uživatelů

Uživatelům jsem přiřadil pseudonymy z důvodu utajení. Do kategorie Neznámé se přidávají nově nainstalovaní klienti, kteří by se připojili k serveru. Zbytek skupin je dle oddělení v dané společnosti, kam se nasazoval produkt Safetica. V uživatelském stromu pak mohu nastavovat funkce na celý server, vybrané skupiny, jednotlivé uživatele či stanice. Ve stromu funguje klasické dědění seshora dolů, tedy co nastavím na nejvyšším uzlu, zdědí se od této nadřazené úrovně až na úroveň nejnižší.

3.7.3 Základní nastavení funkcí

V této fázi nastavím pouze základní monitoring, abychom si ověřili, že komunikace mezi klienty a serverem je v pořádku a klienti nám tak sbírají data. Zároveň data poté využiji pro analýzu namonitorovaných dat.

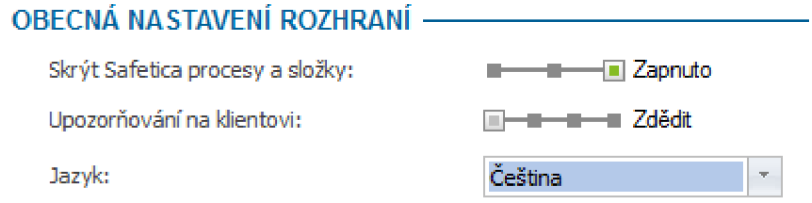
Nastavil jsem tedy následující funkce:

- Weby – monitorování aktivního času navštívených webových stránek.
- Aplikace – monitorování aktivního času stráveného v aplikacích.
- Emaily (bez obsahu) – monitorování emailové komunikace, tedy monitorování odesílatele, příjemce, předmětu, přílohy a časového razítka.
- Tisk – monitorování počtu stran, názvu dokumentu, režim tisku, na jaké tiskárně apod.
- Soubory – monitorování pohybu souborů, tedy monitorování operací otevření, kopírování, přesunutí, přejmenování, odstranění, vytvoření, FTP přenos, stažení z webu. Nastavil jsem filtr, aby se nezaznamenávaly lokální souborové operace. Zajímá mě především pohyb souborů mimo perimetr koncové stanice. Lokální souborové operace totiž významně znepřehlední výsledky v samotné vizualizaci dat.
- Síťový provoz – monitorování staženého a nahrávaného objemu dat na síť.
- Správce zařízení – monitorování připojovaných externích zařízení.
- Aktivita uživatelů – počítání aktivního využití koncové stanice.

3.7.4 Nastavení skrytého režimu

Vedení společnosti si v první fázi nasazení produktu přeje, aby o tomto produktu uživatelé nevěděli. Safetica díky svým technologiím dokáže kompletně skrývat běh i instalaci před uživatelem. V tomto případě tedy také zároveň musím nastavit zapnutí skrývání procesů a složek, abychom předešli odhalení uživateli.

Takto tedy vypadá nastavení skrytého režimu:



Obrázek 12 Nastavení skrytého režimu

3.8 Instalace produktu do prostředí

V této první fázi již rozšiřuji implementaci dále do prostředí. Vyberu vzorek stanic z více oddělení, abych neměl zavádějící výsledky. Každé oddělení totiž využívá různé aplikace a zaměstnanci pracují jinak. V každém oddělení se tedy mohou vyskytnout různé problémy. Těmto problémům chci předejít vyzkoušením instalaci již na širší heterogenní prostředí a ověřit tak základní funkčnost.

Celkem se zákazníkem vybereme 5 stanic a po instalaci bude následovat základní kontrola a také hloubkové testy.

3.8.1 Instalací pomocí GPO

GPO[10] je ideálním způsobem, jak většího prostředí v doméně instalovat software. Pro moje využití je to také vhodný způsob, jak zvolit instalaci pouze na vybrané koncové stanice. GPO tedy slouží k vzdálené instalaci v případě, kdy např. nemáme ke koncové stanici přístup nebo nechceme rušit uživatele v práci. Pro naše účely je to tedy nutné využití této technologie, protože vedení si nepřeje, aby uživatelé v první fázi věděli o nasazování tohoto produktu.

Instalace tedy probíhá v tzv. silent módu na pozadí při restartování stanice. V případě instalace přes GPO jsou tedy vyžadovány 2 restarty koncových stanic – první pro uplatnění GPO politiky, druhý pro instalaci klientské komponenty SEC. Instalaci jsem prováděl ve spolupráci s IT technikem externí společnosti, který přidal GPO pravidlo pro vybranou skupinu počítačů v doméně.

3.9 Základní kontrola a hloubkové testy

Fázi základní kontroly a hloubkových testů jsem spojil do jedné, protože spolu úzce souvisí. Nemůžeme pokračovat v další fázi bez předešlé kontroly prostředí a stavu instalace. Tato část je tedy stěžejní pro další pokračování implementace.

Ke kontrole prostředí se využívají monitorovací nástroje na síti a sledování vytížení prostředků na koncových stanicích. Je to z důvodu odhalení nadměrného vytěžování[11] koncových stanic či zahlcení sítě.

Pro hloubkové testy jsem vytvořil následující scénář:

[10] Group Policy Object

[11] Jako nadměrné zpomalení považuji 20 a více % oproti normálu. Výrobce produktu uvádí zpomalení 10 %.

Oblast	Provedený test	Výsledek	Kontrola záznamu v konzoli
Zabezpečené webové servery	Navštívení webové adresy https//ib24.csob.cz v Google Chrome	OK	OK
	Navštívení webové adresy https//ib24.csob.cz ve Firefoxu	OK	OK
	Navštívení webové adresy https//ib24.csob.cz v Internet Explorer	OK	OK
Intranetové stránky	Navštívení stránky používané ve vnitřní síti Intranet	OK	OK
Emaily	Odeslání emailu z Outlooku	OK	OK
	Přijetí emailu z Outlooku	OK	OK
Soubory	Zkopírování souboru přes exploer.exe	OK	OK
	Přesunutí souboru přes explorer.exe	OK	OK
	Smazání souboru přes explorer.exe	OK	OK
	Otevření souboru přes Total Commander	OK	OK
	Zkopírování souboru přes Total Commander	OK	OK
	Smazání souboru přes Total Commander	OK	OK
Blokování webu	Blokování přístupu na www.facebook.com v Google Chrome	NOT OK	NOT OK
	Blokování přístupu na www.facebook.com ve Firefoxu	NOT OK	NOT OK
	Blokování přístupu na www.facebook.com v Internet Exploreru	NOT OK	NOT OK
Blokování aplikací	Blokování spuštění Opera.exe	OK	OK

Správce zařízení	Blokování připojení USB zařízení	OK	OK
DLP	Blokování kopírování souboru	OK	OK
	Šifrování souboru	OK	OK
	Zakázání vytvoření snímku obrazovky nad souborem	OK	OK
	Zakázaní kopírování obsahu do schránky	OK	OK
	Omezení aplikace – vynucení ukládání pouze na síť	OK	OK

Tabulka 19 Testovací skript

Při testování tedy proběhla většina testů v pořádku. Jediný problém se vyskytl při blokování webů. Po následné analýze se objevil problém v komponentě SEC, kde se nezaregistrovala služba STProxy a tedy nefungovala síťová vrstva, která právě zajišťuje funkci blokování webů. Po přeinstalaci této vrstvy na koncové stanici se problém odstranil.

3.10 Analýza namonitorovaných dat

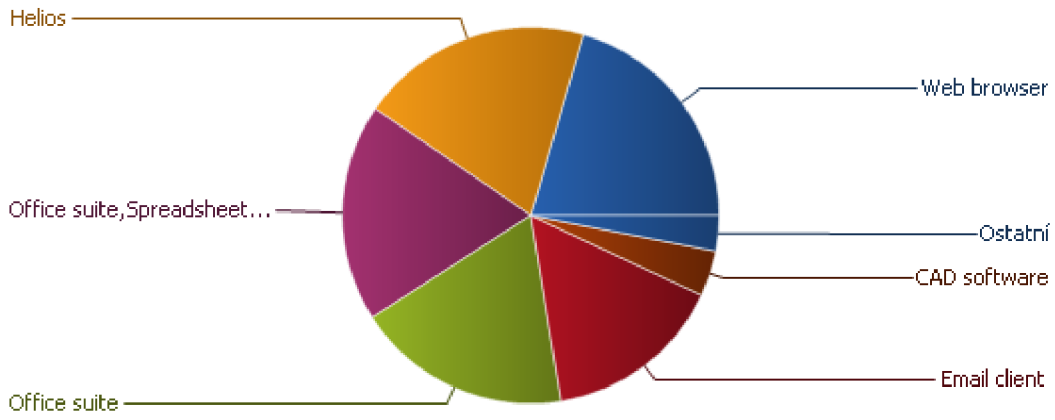
Analýza namonitorovaných dat je první pohled do prostředí zákazníka, kdy můžeme zjistit potenciální bezpečnostní rizika a zároveň si udělat obrázek o tom, jak fungují uživatelé, jaké aplikace používají a jak pracují se soubory. Analýza se provede z namonitorovaných dat v období 1 měsíce a v kompletním rozsahu, tedy 17 stanic. V analýze se zaměřím na 3 základní oblasti: Produktivita, práce s daty a využití IT prostředků. Výstupem analýzy je pak přehled rizik a návrh opatření.

3.10.1 Produktivita

Oblast produktivity se týká analýzy z monitoringu, kde produktivitu dokážeme určit z využití aplikací a navštívených webových stránek uživateli.

Využití aplikací

Následující graf zobrazuje aktivní práci uživatelů v různých kategoriích aplikací.



Graf 1 Nejpoužívanější kategorie aplikací

Z grafu lze vyčíst, že převažuje práce v produktivních aplikacích. Nejpoužívanější aplikace patří do kategorie kancelářského software, která je v grafu znázorněna jako Office suite, případně i Spreadsheet. Mezi další produktivní kategorie řadíme kategorii Helios, Email client a CAD software.

Druhou nejpoužívanější kategorií je však kategorie Web browser, u které nedokážeme rozlišit, zda spadá do produktivní či neproduktivní skupiny. Celkem tráví zaměstnanci 22 % své pracovní doby ve webovém prohlížeči. Záznamy navštívených stránek budu rozebírat v další části této analýzy.

Zcela jistě však můžeme jako neproduktivní označit kategorii Games. Jeden uživatel strávil přibližně hodinu hraním hry Diablo III.

Aplikace	Aktivní čas
Helios Orange (helios.exe)	1317:29:35
Autodesk® Inventor® 2014 (inventor.exe)	56:34:01
AutoCAD LT Application (acadlt.exe)	45:36:59
AutoCAD Application (acad.exe)	39:49:56
Skype (skype.exe)	26:37:36
Adobe Photoshop CS6 (photoshop.exe)	10:20:53
MarkWare (markware.exe)	5:36:40
Diablo III Retail (diablo iii.exe)	0:58:02

Tabulka 20 Aktivní čas ve vybraných aplikacích

Do tabulky jsem vybral některé aplikace a aktivní čas v nich strávený. AutoCAD programy jsou aktivně využívané. Na druhou stranu Adobe Photoshop CS6 byl tento měsíc využíván pouze 10 hodin, což je na zvážení vedení společnosti.

Dále upozorňuji na aktivní využívání aplikace Skype, která může sloužit k neproduktivním činnostem, ale také jako potenciální kanál úniku dat.

Navštěvované weby

Následující graf zobrazuje aktivní čas uživatelů strávený na různých kategoriích webů.

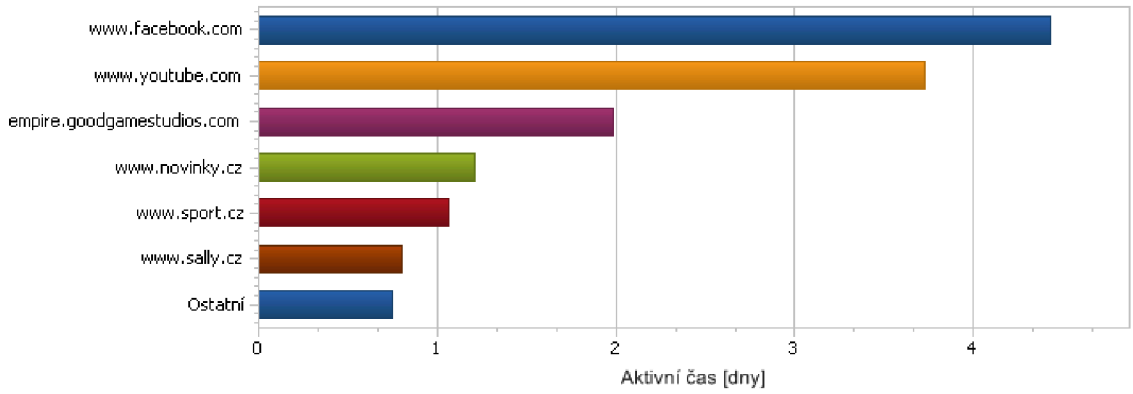
Graf 2 Nejnavštěvovanější kategorie webů

V grafu 2 nalezneme nejnavštěvovanější kategorie neproduktivních webů. Nejvíce času zaměstnanci tráví na serverech věnovaným volnému času, pak na sociálních sítích a čtením zpráv. Mezi neproduktivní patří také kategorie Shopping a Games.

Dále bych chtěl upozornit na výskyt kritické kategorie Pornography, kde je velmi vysoké riziko infekce počítače škodlivým software.

Celkově z analýzy navštěvovaných webů vyplývá, že zaměstnanci tráví z celkového času na Internetu až 90 % neproduktivní činností.

Mezi nejnavštěvovanější neproduktivní weby patří následující:



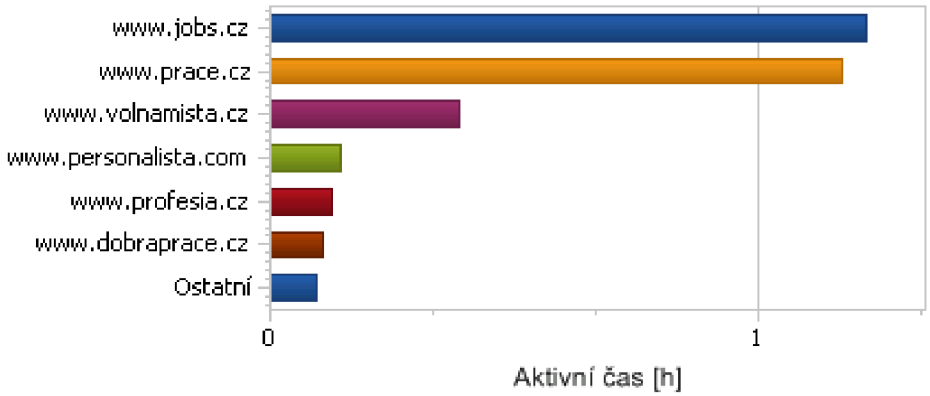
Graf 3 Nejnavštěvovanější neproduktivní weby

Nejvíce času tedy uživatelé tráví na serveru www.facebook.com, na druhém místě pak na www.youtube.com.

Vyhledávání práce

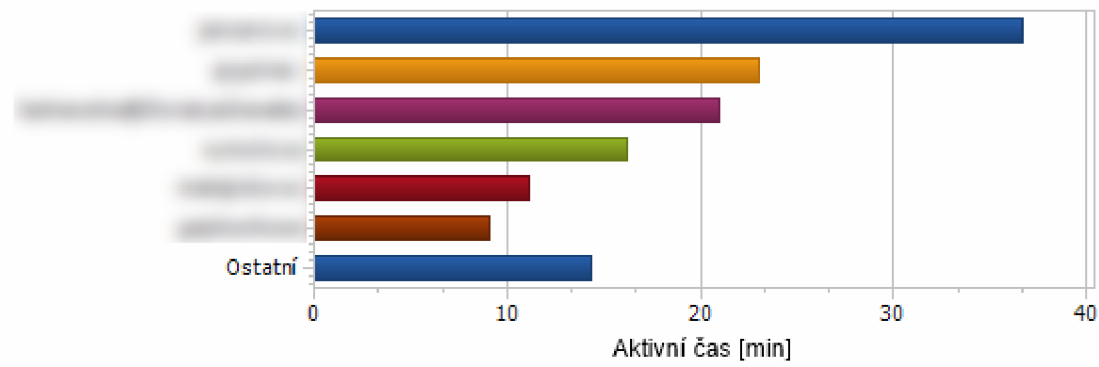
Jako samostatnou kategorii navštívených serverů pak chápeme weby pro vyhledávání práce. Z naší zkušenosti vyplývá, že zaměstnanci, kteří aktivně tráví čas na webech této kategorie, obvykle ze společnosti do několika měsíců odcházejí.

Následující graf zobrazuje servery z této kategorie, kde strávili uživatelé nejvíce času.



Graf 4 Nejnavštěvovanější servery z kategorie vyhledávání práce

Záznamy si můžeme vyfiltrovat dle této kategorie a uvidíme, kteří uživatelé zde tráví nejvíce času.



Graf 5 Nejaktivnější uživatelé v kategorii vyhledávání práce

Doporučuji zaměřit se na detaily a případně se zamyslet nad řešením této situace. Mezi dobré postupy patří diskuze ohledně spokojenosti s prací a s kolektivem, změna pracovní náplně nebo pracovních podmínek.

Celkový neproduktivní čas

Už z funkcí Aplikace a Weby jsem schopný vyčíslit celkové množství neproduktivního času. V aplikacích jsem zjistil, že 22 % pracovní doby je tráveno ve webových prohlížečích. Celkový čas strávený používáním webových prohlížečů je podle zjištění z 90 % tráven neproduktivně.

Z těchto čísel vyplývá, že zhruba 20 % veškeré činnosti je neproduktivní. To odpovídá průměru 1,5 hodiny neproduktivní činnosti za pracovní den. Tato hodnota je průměr všech uživatelů a jediným pohledem do správcovské konzole je možné odhalit nejméně produktivní uživatele a naopak ty s vysokým nasazením. Doporučuji tedy tento čas částečně omezit např. interní směrnicí a poté vynutit její dodržování produktem Safetica.

Náklady na neproduktivní čas

Jednoduchým výpočtem můžu zjistit, kolik společnost platí ve formě mzdy za tuto neproduktivní činnost. Hrubá měsíční mzda se v tomto kraji aktuálně pohybuje okolo 23 072 Kč (Český statistický úřad, 2015). Když vezmu v úvahu 100 zaměstnanců, tak na mzdách společnost za rok vyplatí 23,072 mil. Kč. 20 % neproduktivního času tedy znamená 4,61 mil. Kč za rok vynaložených na činnosti nesouvisející s výkonem práce. S produktem Safetica dokážeme zvýšit produktivitu zaměstnanců a ušetřit tak společnosti nemalé náklady.

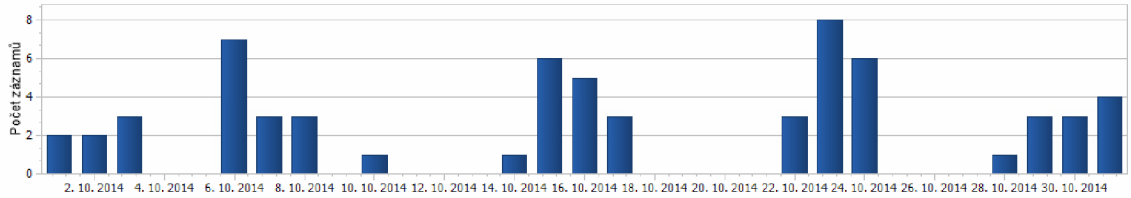
3.10.2 Práce s daty

V této části se zaměřím na analýzu možných bezpečnostních rizik úniku citlivých informací. Budu analyzovat, jak uživatelé pracují s firemními daty.

Vynášení dat ze společnosti

V této části jsem se zaměřil na analýzu souborů odesílaných přes emailové klienty. Zaměřil jsem se především na ochranu know-how společnosti, tedy na soubory CAD softwaru.

Celkem bylo za toto období odesláno 64 emailů, které obsahovaly CADovské soubory. Rozvržení v čase je rovnoměrné, nejedná se tedy o nějakou výjimečnou situaci, kdy by zaměstnanec chtěl odeslat všechny soubory např. konkurenci nebo na soukromý mail pro využití v budoucím zaměstnání:



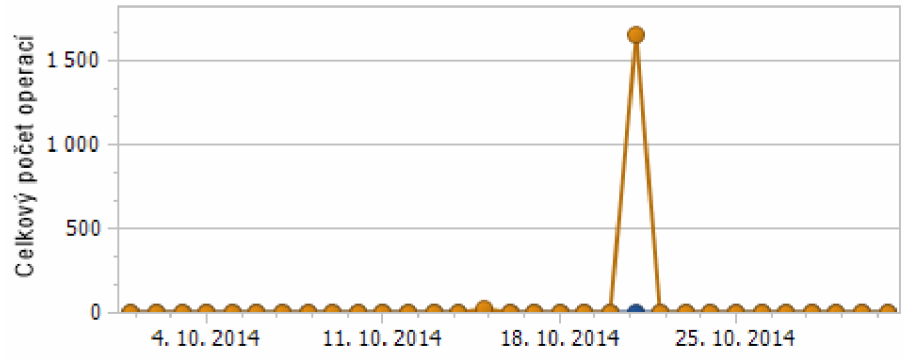
Graf 6 Rozvržení odeslaných CAD souborů mailem v čase

Dále jsem sledoval emailové domény, kam se soubory odesílaly. Objevil jsem několik CADových souborů, které byly odeslány na doménu konkurence. Doporučuji prošetřit tuto událost na možný únik dat ke konkurenci.

Mezi dalšími adresami jsem nalezl domény seznam.cz a quick.cz. Doporučuji zamezit odesílání citlivých dat na soukromé schránky zaměstnanců. Doporučuji také nastavit v produktu Safetica bezpečnostní politiku, která tuto ochranu zajistí.

Jako další potenciální kanál pro únik dat jsou USB disky a obecně externí zařízení. V další analýze jsem se zaměřil na nahrávání CAD souborů na tato média.

Obecně se tato média využívají pouze výjimečně, ale přesto jsem objevil jeden významný výkyv. Situace je znázorněna na následujícím grafu:



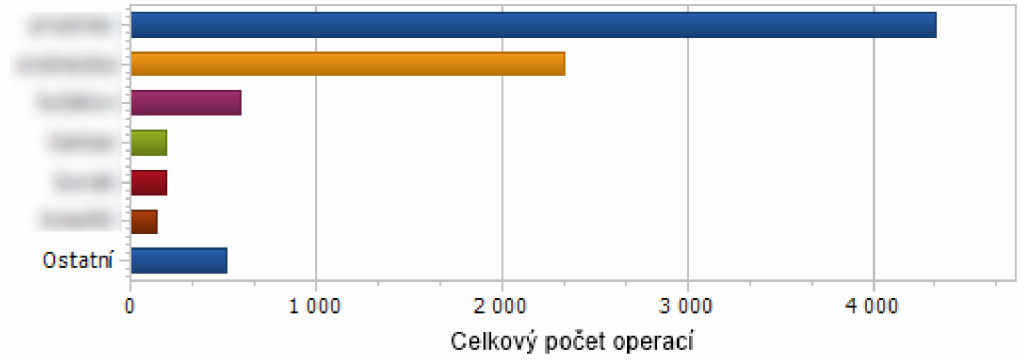
Graf 7 Časová osa nahrávání souborů na externí média

Jednalo se o jednoho uživatele, který jednorázově nahrál na externí zařízení převážně JPEG soubory, ale také značné množství CAD souborů. Doporučujeme prověřit tuto událost a poté nastavit bezpečnostní politiku – např. zakázat nahrávání citlivých firemních souborů na externí média.

Nekorektní práce s daty

Dle požadavku zákazníka jsem se zaměřil na sledování work-flow při práci s CAD soubory. Společnost si přeje, aby zaměstnanci ukládali tyto výstupy na síťové disky.

Následující graf zobrazuje uživatele a celkový počet operací s těmito soubory na lokálním disku:



Graf 8 Uživatelé a počet operací na lokálním disku

Při pohledu do detailu jsem zjistil, že až 80 % těchto lokálních operací je operace vytvoření souboru. Síťové disky jsou využívány ve výrazně menší míře. Doporučuji tedy nastavit bezpečnostní politiky v produktu Safetica tak, aby se toto nařízení o využívání síťového disku opravdu dodržovalo.

3.10.3 Využití IT prostředků

V této části se zaměřím na efektivní využití IT prostředků. K tomuto účelu mi slouží monitorování aktivity koncových stanic, tisku a aplikací.

Využití pracovních stanic

V této části se zaměřuji na využití IT prostředků. Konkrétně dokážeme touto funkcí zjistit aktivní využívání stanic. Jako příklad prezentuji souhrnnou tabulku nejméně využitých stanic:

Datum: 1. 10. 2014 - 31. 10. 2014

PC	Celková doba běhu	Celková doba nečinnosti	Využití
[redacted]	599 h 59 min 39 s	599 h 59 min 16 s	0.00 %
[redacted]	495 h 56 min 53 s	488 h 46 min 6 s	1.45 %
[redacted]	369 h 45 min 10 s	353 h 10 min 48 s	4.48 %
[redacted]	601 h 24 min 50 s	571 h 22 min 17 s	5.00 %
[redacted]	222 h 19 min 8 s	193 h 36 min 25 s	12.91 %
[redacted]	277 h 6 min 19 s	233 h 15 min 47 s	15.82 %
[redacted]	469 h 30 min 30 s	375 h 13 min 29 s	20.08 %
[redacted]	312 h 26 min 12 s	235 h 3 min 20 s	24.77 %
[redacted]	417 h 15 min 4 s	312 h 28 min 37 s	25.11 %

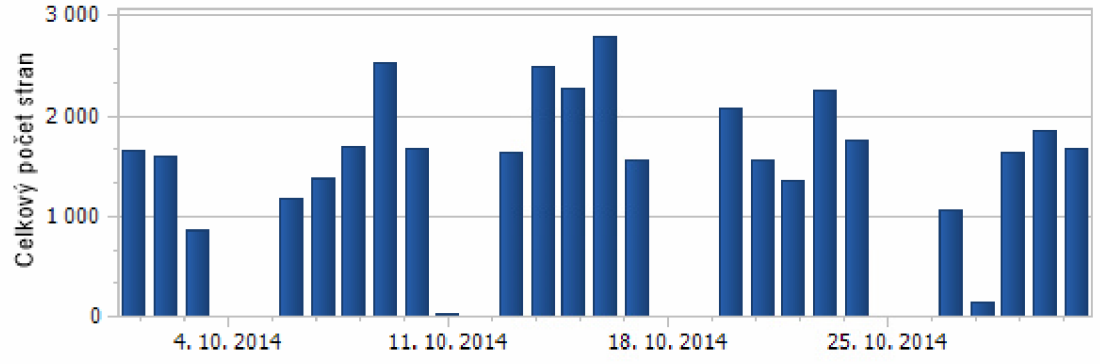
Tabulka 21 Využití pracovních stanic

Za zmínku stojí první počítač, kde je celková aktivní činnost v tomto měsíci 0 %. Na tomto počítači nebyla provedena žádná aktivní činnost a počítač běžel skoro 600 hodin nevyužit. I u dalších zobrazených počítačů je míra využití poměrně nízká.

Doporučuji zavedení politiky na vypínání počítačů po pracovní době kvůli šetření firemních nákladů. Míra aktivního využití by měla být alespoň 75 %.

Tisk

Následující graf zobrazuje počet vytištěných stran za den:



Graf 9 Počet vytištěných stran za den

Z analýzy vyplynulo, že většina tištěných dokumentů je pracovního charakteru. Pouze ve dvou případech se jednalo o tisk soukromých dokumentů. Soubory:

- AUTA: Velký obrazový průvodce (360 barevných stran)

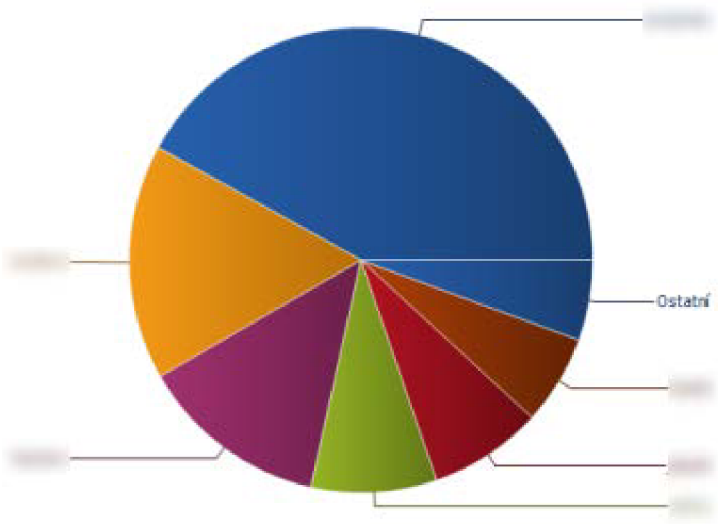
- Sbírka sudoku.pdf (104 černobílých stran)

Nechávám na uvážení společnosti, zda umožní zaměstnancům tisk soukromých dokumentů nebo zavede nějakou politiku. S produktem Safetica dokáží blokovat tisk globálně, vybraných souborů, případně nastavit kvótu, kolik stran mohou uživatelé tisknout.

Nákladné licence

V této části jsem se zaměřil na využití aplikací, na které společnost vynakládá poměrně vysoké částky a je v zájmu společnosti, aby tyto aplikace byly využívány co nejefektivněji.

Zaměřil jsem se především na využívání programu AutoCAD a příbuzný software. Následující graf zobrazuje uživatele, kteří tento software využívají nejvíce:



Graf 10 Nejaktivnější uživatelé v CAD aplikacích

U prvního uživatele, který je na grafu znázorněn tmavě modrou barvou, bylo zjištěno, že cca 25 % z pracovní doby tráví neproduktivně. Druhý nejaktivnější uživatel, znázorněn barvou oranžovou, tráví až 1/3 pracovní doby procházením webových stránek nesouvisejících s pracovní činností. Zde vidím prostor pro zefektivnění ve využívání těchto nákladných aplikací.

3.10.4 Závěr analýzy: Přehled rizik a opatření

Následující tabulka shrnuje zjištěná rizika a popisuje návrhy opatření:

Riziko	Opatření	Poznámka
Odesílání citlivých dat na email konkurence	• Zavedení DLP politik	Lze nastavit seznam povolených emailových adres či domén. Ostatní budou zakázané.
Nahrávání citlivých souborů na externí média	• Zavedení DLP politik	a) Lze nastavit seznam povolených pracovních USB disků. Zbytek bude zakázán. b) Lze nastavit úplný zákaz nahrávání citlivých souborů na externí média. c) Lze globálně zakázat používání externích zařízení.
Ukládání citlivých souborů na lokální disk	• Zavedení aplikační politiky	Lze nastavit aplikační politiku, která vynutí ukládat výstupy z vybraných aplikací např. do síťového umístění.
Využívání webmailů v pracovní době	• Blokování webových stránek	Lze blokovat webovou kategorii Webmails.
Přístup na stránky s pornografickým obsahem	• Blokování webových stránek	Lze blokovat webovou kategorii Pornography.
Vyhledávání práce	• Zvýšit motivaci zaměstnanců • Nastavení varování	Samozřejmě můžeme zakázat přístup na tyto servery, ale tím se riziko neodstraní. Lze nastavit varování, které na takovou situaci upozorní.
Neproduktivní činnost na Internetu	• Blokování webových stránek • Nastavení varování	Lze blokovat vybrané servery nebo webové kategorie, které nesouvisejí s pracovní činností. Doporučuji blokovat pouze servery, které nechceme dle politiky povolit. Menší odreagování např. pročtením novinek nemusí být na škodu. Lze nastavit varování, které přijde na email v případě překročení určitého času na dané kategorii webů.
Hraní her v pracovní době	• Blokování aplikací	Lze nastavit blokování aplikační kategorie Games v pracovní době.
Používání aplikace Skype	• Zavedení DLP politik	Lze zakázat přístup aplikace k citlivým datům.
Malé využití pracovních stanic	• Zavedení politiky	Politiku lze kontrolovat ve funkci Aktivita uživatelů.

	vypínaní strojů	
Tisk soukromých dokumentů	• Blokování tisku	a) Lze nastavit kompletní blokování tisku pro vybrané uživatele. b) Lze nastavit blokování některého typu dat. c) Lze nastavit kvótu pro povolený počet tištěných stran.
Nízké využití drahých licencí	• Reporty	Lze sledovat využití těchto aplikací.

Tabulka 22 Přehled rizik a návrh opatření

3.10.5 Ohodnocení rizik

Analyzovaná rizika nyní musíme ohodnotit, abychom věděli, která jsou pro společnost kritická a naopak která urgentně řešit nemusíme. Jako první si zavedeme hodnotící škálu pro pravděpodobnost a dopad rizika.

Pravděpodobnost (v %)	Slovní vyjádření	Číselné vyjádření
0 - 19	Zanedbatelná	1
20 - 39	Nízká	2
40 - 59	Střední	3
60 - 79	Vysoká	4
80 - 100	Velmi vysoká	5

Tabulka 23 Vyjádření pravděpodobnosti

Dopad	Číselné vyjádření
Žádný dopad	1
Zanedbatelný dopad	2
Potíže a finanční ztráty	3
Vážné potíže a velké ztráty	4
Existenční potíže	5

Tabulka 24 Vyjádření dopadu

Číselné vyjádření dopadu a pravděpodobnosti nyní zavedu do matice k jednotlivým rizikům a dopočítám tak významnost jednotlivých rizik.

Riziko	Pravděpodobnost	Dopad	Významnost
1. Odesílání citlivých dat na email konkurence	2	5	10
2. Nahrávání citlivých souborů na externí média	3	3	9
3. Ukládání citlivých souborů na lokální disk	3	2	6
4. Využívání webmailů v pracovní době	4	3	12
5. Přístup na stránky s pornografickým obsahem	2	3	6
6. Vyhledávání práce	1	4	8[12]
7. Neproduktivní činnost na Internetu	4	2	8
8. Hraní her v pracovní době	2	1	2
9. Používání aplikace Skype	3	3	6
10. Malé využití pracovních stanic	3	1	3
11. Tisk soukromých dokumentů	2	1	2
12. Nízké využití drahých licencí	3	1	3

Tabulka 25 Ohodnocení rizik

Nyní si můžeme ohodnocená rizika promítnout do mapy rizik:

Pravděpodobnost **Dopad**	**1**	**2**	**3**	**4**	**5**
1		8, 11	10, 12		
2			3	7	
3		5	2, 9	4	
4	6				
5		1			

Tabulka 26 Mapa rizik (inspirace z (Smejkal, 2010)).

Riziko přijatelné
Riziko podmínečně přijatelné
Riziko nepřijatelné

[12] Uměle jsem navýšil významnost tohoto rizika ze 4 na 8, protože sice samotné riziko vyhledávání nové práce není tak pravděpodobné a nenese tak velký dopad, ale ze zkušenosti vyplývá, že lidé, kteří opouštějí své zaměstnání, si také často s sebou berou firemní data. A únik těchto dat má největší dopad.

Z tabulky můžeme vyčíst nejdůležitější rizika a naopak ta, které aktuálně nevyžadují nejvyšší prioritu. Zcela nepochybně největším rizikem je přímý únik dat ke konkurenci, tedy riziko č. 1. Další rizika, např. 2,4, 6 nebo 9 také souvisí s potenciálním únikem dat a tudíž se řadí do druhé kategorie významnosti. Za rizika přijatelná považujeme neproduktivní činnost uživatelů či neefektivní využití zdrojů.

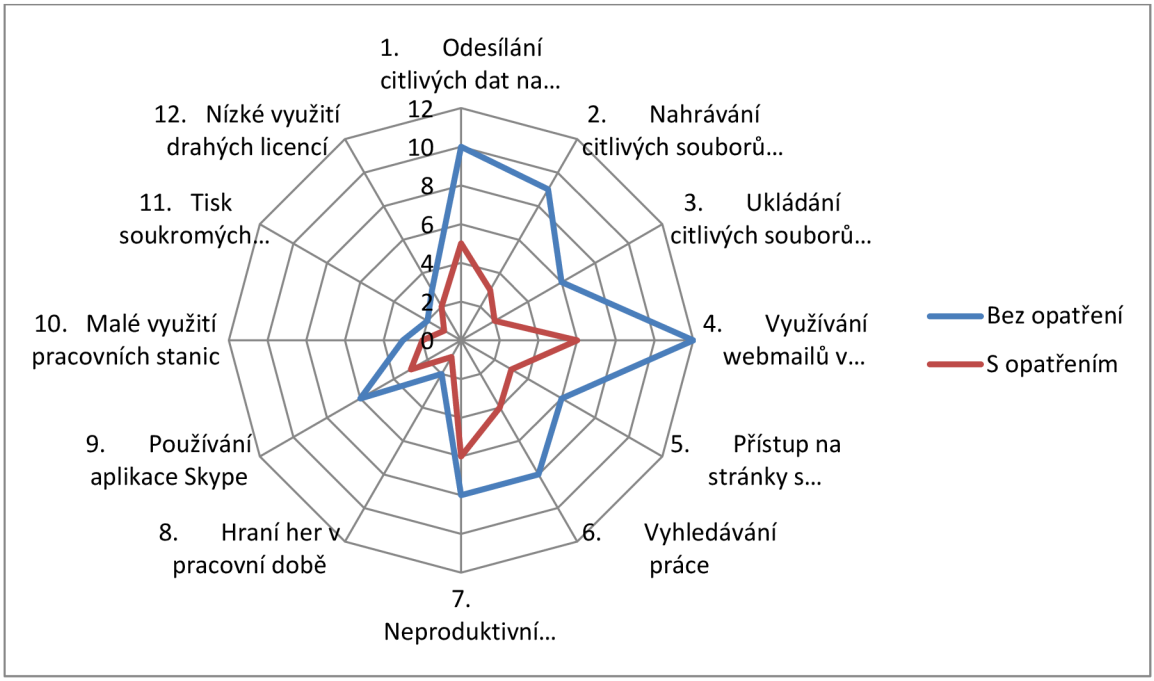
Po zavedení opatření se nám hodnoty zlepší. Podívejme se na novou tabulku:

Riziko	Pravděpodobnost	Dopad	Významnost	Opatření	Pravděpodobnost	Dopad	Výsledek
1. Odesílání citlivých dat na email konkurence	2	5	10	Zavedení DLP politik	1	5	5
2. Nahrávání citlivých souborů na externí média	3	3	9	Zavedení DLP politik	1	3	3
3. Ukládání citlivých souborů na lokální disk	3	2	6	Zavedení aplikační politiky	1	2	2
4. Využívání webmailů v pracovní době	4	3	12	Blokování webových stránek	2	3	6
5. Přístup na stránky s pornografickým obsahem	2	3	6	Blokování webových stránek	1	3	3
6. Vyhledávání práce	1	4	8	Zvýšit motivaci zaměstnanců Nastavení varování	1	4	4
7. Neproduktivní činnost na Internetu	4	2	8	Blokování webových stránek Nastavení varování	3	2	6
8. Hraní her v pracovní době	2	1	2	Blokování aplikací	1	1	1
9. Používání aplikace Skype	3	3	6	Zavedení DLP politik	1	3	3
10. Malé využití	3	1	3	Zavedení politiky	2	1	2

pracovních stanic				vypínaní strojů			
11. Tisk soukromých dokumentů	2	1	2	Blokování tisku	1	1	1
12. Nízké využití drahých licencí	3	1	3	Reporty	2	1	2

Tabulka 27 Přehodnocení rizika po zavedení opatření

Z tabulky vidíme, že bychom pomocí zavedeného opatření velmi významně snížili většinu zde uvedených rizik. Rozdíly ve významnosti rizik si můžeme prohlédnout na následujícím grafu:



Graf 11 Rozdíl ve významnosti rizika s opatřením a bez

Opatřením tedy můžeme dosáhnout výrazného snížení rizika. V další části této práce si ukážeme, jak budu toto opatření do společnosti zavádět.

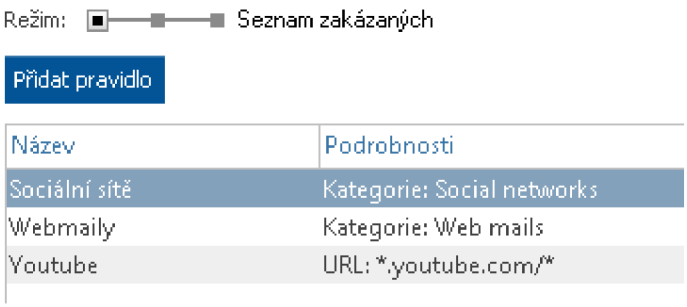
3.11 Nastavení restriktivních funkcí

V první části dalšího nastavení produktu se budu věnovat nastavení restriktivních funkcí, tedy těch globálních pro celou organizaci. Tyto restriktivní funkce jsou méně rizikové než funkce modulu DLP, proto začínám s nastavením dříve.

Nastavení restriktivních funkcí se bude týkat blokování přístupu na webové stránky a blokování spouštění aplikací. Jak bylo upřesněno dříve v Plánu nastavení.

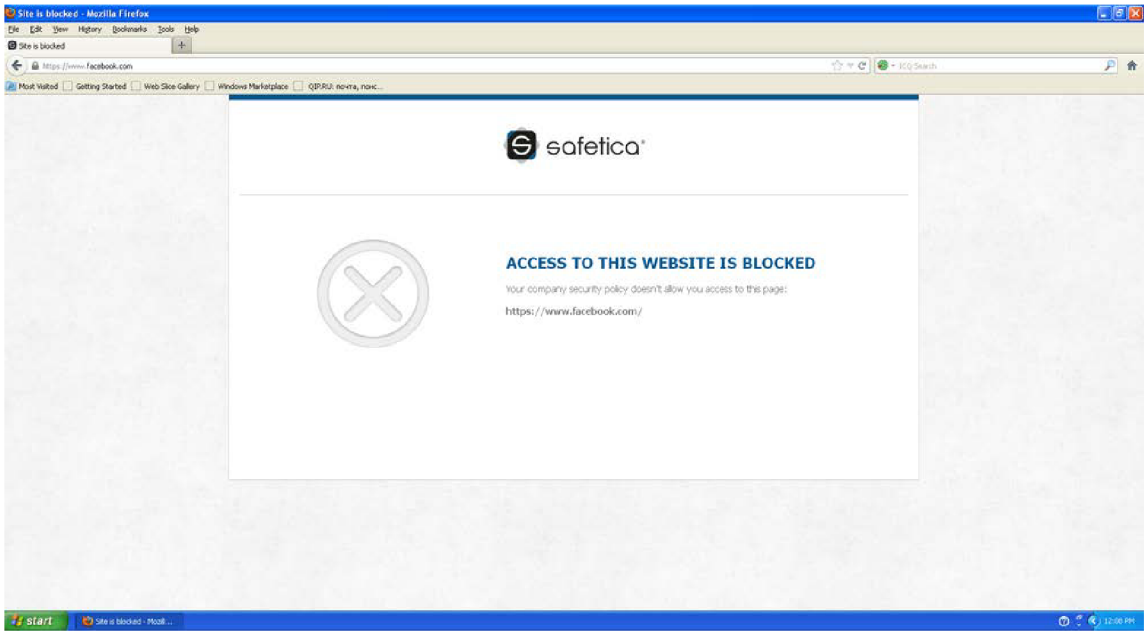
Prvně budeme nastavovat restrikce pro přístupy na webové stránky. Tyto restrikce nastavím pomocí seznamu zakázaných stránek, protože víme, které stránky chceme blokovat. Opačný přístup nastavení pomocí seznamu povolených stránek je sice bezpečnější, ale značně omezuje uživatele díky úzce specifikované množině pouze povolených webových serverů.

Na následujícím obrázku vidíme nastavení, které jsem v této fázi nastavil:



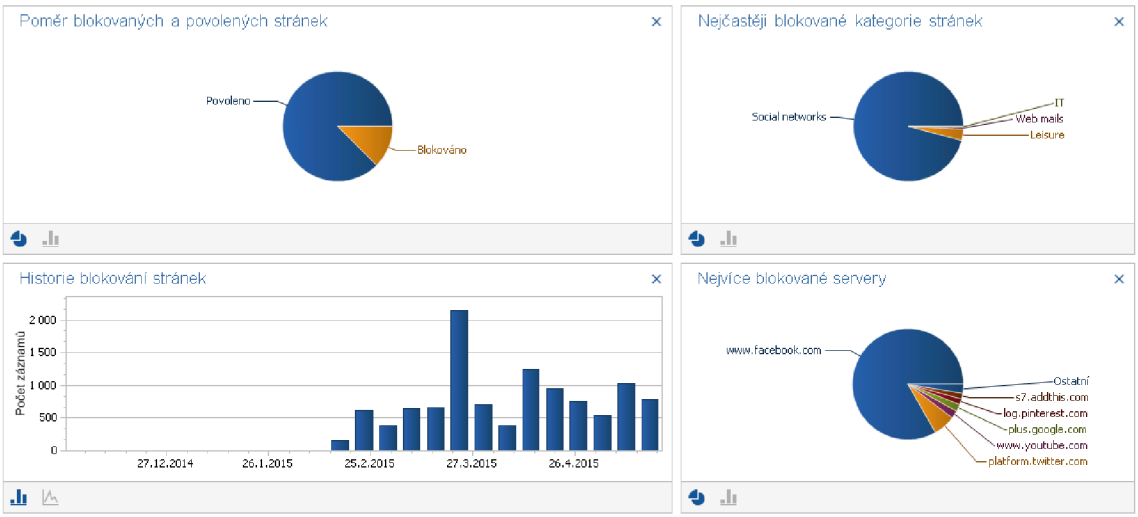
Obrázek 13 Ukázka nastavení blokování webů.

Jak vypadá blokovaná stránka, když na ni uživatelé přistoupí, můžeme vidět na následujícím obrázku:



Obrázek 14 Ukázka blokované stránky www.facebook.com.

A zde již máme výsledky blokovaných stránek za období prosinec 2014 až květen 2015:



Obrázek 15 Výsledky blokovaných stránek za období prosinec 2014 až květen 2015.

Nejvíce blokovanou stránkou je tedy www.faceook.com. Tak velký počet přístupů může být dán i blokováním různých pluginů vložených na jiných stránkách

Podobně proběhlo nastavení blokování aplikací, kdy jsem nastavil blokování spouštění aplikací z kategorie Torrent.

3.12 Nastavení DLP

Pro nastavení DLP v produktu Safetica je nutné provést několik kroků nastavení.

1. Vytvoření datové kategorie

V prvním kroku se jedná o vytvoření datové kategorie, kterou budou označena citlivá data. Pro tuto společnost jsem definoval dvě datové kategorie: know-how a citlivé.

2. Vytvoření filtrovacího pravidla

Filtrovací pravidlo nám vyhledá potřebné soubory k označení. Do filtrovacího pravidla můžu zadat název soubor, umístění, příponu nebo aplikaci, která daný soubor vytvoří. Vytvořil jsem dvě filtrovací pravidla dle plánu nastavení. První pravidlo, které obsahuje pouze přípony .pdf a soubory aplikací Word a Excel. Druhé pravidlo je určeno pro výstupy z aplikace AutoCAD.

3. Analýza dat

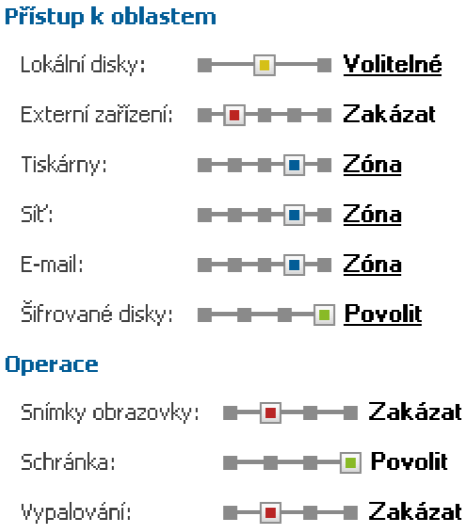
Před samotným označením citlivých dat je vhodné provést analýzu, jestli nám filtrovací pravidlo nalezne správné soubory k označení. Analýza nalezla pouze požadované soubory.

4. Označení dat

V tomto kroku proběhne již označení souborů danou datovou kategorií, pro kterou následně vytvořím bezpečnostní politiku. Označení jsem nastavil dvojího druhu. Jedno označení, které označí aktuálně existující soubory. A druhé, které označuje dynamicky nově vznikající soubory.

5. Vytvoření bezpečnostní politiky

Bezpečnostní politiku jsem navrhl dle plánu nastavení. K vidění na následujícím obrázku:



Obrázek 16 Nastavení DLP politiky.

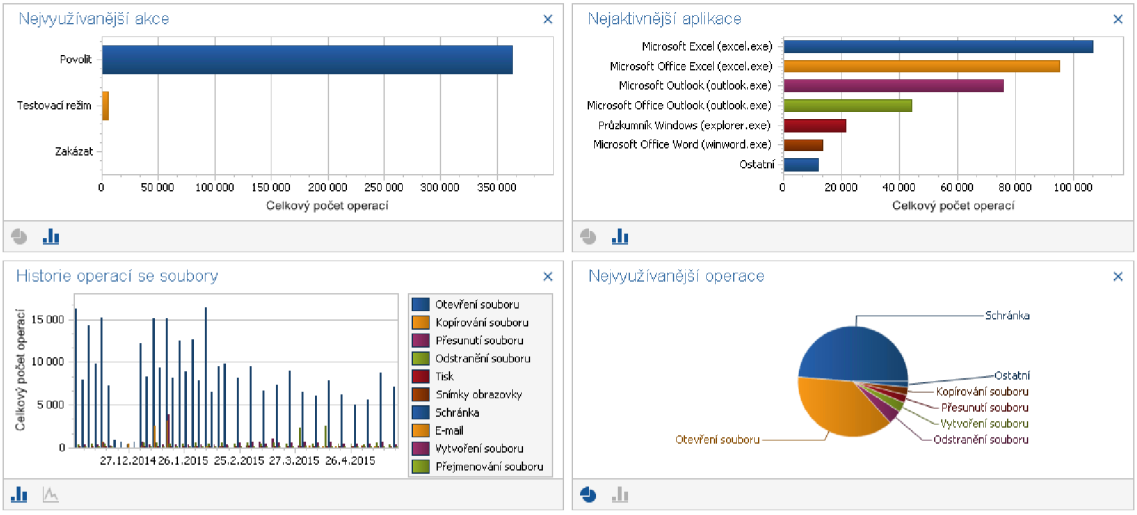
Politiku jsem nastavil zatím pouze v testovacím režimu, protože zatím nechceme uživatele omezovat, ale pouze si politiku testovat, jestli blokuje ty správné incidenty. V nastavení jsou vidět zóny. Tyto zóny představují bezpečnostní perimetr, který byl definován v Plánu nastavení. Do emailů jsem tedy přidal pouze domény společnosti a dodavatelů. Síť jsem definoval lokální rozsah a tiskárny jsem přidal také pouze existující tiskárny ve společnosti.

6. Spojení bezpečnostní politiky s datovou kategorií

Jako poslední krok zbývá spárovat bezpečnostní politiku s datovými kategoriemi. Po tomto uložení již platí nastavená testovací politika a po určitém období se můžeme podívat na výsledky, zda politika funguje správně.

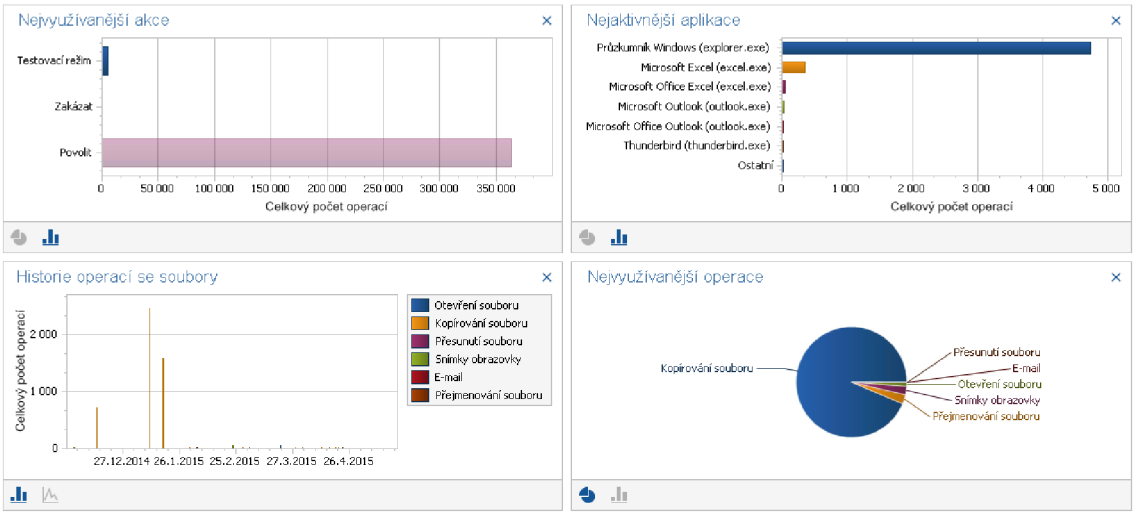
3.13 Sledování a vyhodnocení DLP politik

Pohledem do konzole a analyzováním blokovaných incidentů jsme zjistili, že politika blokuje požadované soubory dle přání společnosti. Na níže přiloženém obrázku jsou zobrazeny incidenty sesbírané za dané období:



Obrázek 17 DLP Protokol a o incidentech.

Většina akcí je kategorie Povolit, která nás v tuto chvíli nezajímá. Proto si vyfiltrujeme pouze akce Testovací režim a Zakázat, které nám dají představu o incidentech, které by blokovala bezpečnostní politika, kdyby byla nastavena v restriktivním režimu:



Obrázek 18 Blokované incidenty testovací politikou.

Zde již vidíme, že většina blokovaných akcí pochází z kopírování souboru přes aplikaci explorer.exe. Na časové ose je navíc znázorněn poměrně velký výkyv, tak se na něj zaměříme a časově si přiblížíme:

Akce | Agregace

Aplikace	Uživat...	Soubor	Typ operace	Zdroj	Cíl	Typ ...	Cílové zaříz...
Akce: Povolit							**5245 operací se soubory**
Akce: Testovací režim							**2443 operací se soubory**
Průzkumník Windows (explorer.exe)		NCHL aktual.březen ...	Kopírování souboru	C:\Users	Desktop\MOJE\BOZP\N...	I:\MOJE\BOZP\NCHL aktual...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		tel.čísla.xls	Kopírování souboru	C:\Users	Desktop\MOJE\BOZP\tel....	I:\MOJE\BOZP\tel.čísla.xls	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		CEDULKY.xls	Kopírování souboru	C:\Users	Desktop\MOJE\CEDULKY...	I:\MOJE\CEDULKY.xls	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		certifikat ISO 9001.200...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		Certifikát ISO 9001_20...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		Certifikát ISO 9001_20...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		Distribuční list.xls	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		Př.č.2 k Q1 Distribuční...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		př.č.1 Q13 Roční plán ...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		př.č.2 Q13 Týdenní pl...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		příloha č.1 k Q14.pdf	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		př.č.3-Protokol o před...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		příloha č.1 k Q2 Intern...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		příloha č.2 k Q2 Kontr...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		příloha č.1 k Q2 Intern...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		Seznam záznamů Zah...	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...
Průzkumník Windows (explorer.exe)		Organigram 1.3.2012.xls	Kopírování souboru	C:\Users	Desktop\MOJE\ISO 9001....	I:\MOJE\ISO 9001.2008\Archi...	USB	USB FLASH DRI...

Obrázek 19 Zakázané akce při kopírování souboru

V detailním logu vidíme, že šlo o kopírování citlivých souborů na USB disk. Toto chování bude blokováno, až se vedení domluví na přepnutí politiky do restriktivního režimu.

Politika je tedy nastavena správně a po přepnutí do restriktivního režimu, budou již citlivá data společnosti chráněna. Aktuálně je to nastaveno pouze pasivně.

3.14 Ekonomické zhodnocení

Na závěr realizace vlastního návrhu provedu ekonomické zhodnocení. Již v dřívější části této práce jsem provedl kalkulaci dopadů úniku dat. Průměrný únik dat tedy může

vyjít společnost až na 93 487 156 Kč (2014 Cost of Data Breach Study: Germany, 2014). Z analýzy namonitorovaných dat mi vyplynulo, že celková neproduktivní činnost uživatelů je 20 %. Na základě průměrného hrubé mzdy 23 072 Kč v tomto kraji (Český statistický úřad, 2015), společnost vyplácí těmto 17 zaměstnancům zhruba 392 224 Kč za rok. Za neproduktivní činnost tedy vynakládá 78 445 Kč za rok.

Položka	**Cena**
Cena 1 licence produktu Safetica 5	5000 Kč
17 licencí	85 000 Kč
Cena implementace za 1 MD[13]	16000 Kč
8 MD implementace	128 000 Kč
Celkem (bez DPH)	**213 000 Kč**
DPH (21 %)	44730 Kč
Celkem (s DPH)	**257 730 Kč**

Tabulka 28 Cenová kalkulace projektu

Cena implementace je zde dražší než samotné licence. Je to dáno tím, že se jedná o malý počet stanic, a oproti tomu o komplexní práce při nasazení DLP do této společnosti.

Společnost vyšel tento projekt na 257 730 Kč. Tato částka obsahuje trvalé licence produktu Safetica pro 17 stanice a cenu implementace. Pokud bychom tedy s produktem dokázali ochránit jeden únik dat, ušetříme společnosti náklady v řádech milionů Kč. Další náklady ušetříme zvýšením produktivity zaměstnanců.

[13] Man-Day (člověkoden)

ZÁVĚR

Cílem této práce byl výběr vhodného DLP systému pro řešení konkrétního problému společnosti. Vybraná společnost již totiž zažila únik dat, který vedl k výrazné finanční ztrátě. To byl hlavní důvod, proč se společnost začala zajímat o ISMS a DLP systém, jejímž nasazením chtěla dalším ztrátám předejít.

DLP systémů je však celá řada a vybrat to správné řešení od spolehlivého dodavatele je nelehký úkol. Stěžejní částí v mé práci byla provedená analýza, kde jsem za pomocí provedených interview klíčových stakeholderů zjistil nutné informace o společnosti a současném stavu zavedené bezpečnosti informací. Díky provedené analýze jsem tak mohl identifikovat rizika a navrhnout vhodné řešení jako opatření. Návrh řešení také vycházel z konkrétních potřeb, které jsem se dozvěděl právě při prováděných rozhovorech.

Klíčovým požadavkem společnosti bylo chránit své know-how, tedy výstupy z aplikace AutoCAD. Toto bylo nejdůležitějším kritériem pro výběr vhodného řešení. Jak jsem dokázal v této práci, většina dostupných DLP systémů tento požadavek nedokáže splnit. Převážná většina těchto systémů totiž využívá k ochraně citlivých souborů analýzu obsahu. Jenže ve výkresu z aplikace AutoCAD žádný textový obsah nenalezneme, je potřeba ochránit danou aplikaci a tyto konkrétní výstupy.

Vybral jsem tedy kontextové DLP řešení, které se nezaměřuje na obsah, ale na situace, při kterých citlivá data vznikají. Je to tedy ideální řešení pro problém, který daná společnost řeší. Toto vybrané řešení splnilo většinu definovaných kritérií, které jsem určil na základě analýzy potřeb a současné situace.

Jak se ukázalo v implementační části, řešení nejen perfektně splňuje klíčový požadavek na ochranu know-how společnosti, ale také poskytuje další funkce, které společnost náležitě ocenila. S řešením jsem dokázal provést analýzu přímo reálných dat společnosti a poukázat na další možná rizika spojená s potenciálním únikem dat. Pro tato rizika jsem opět navrhl opatření a následně po odsouhlasení garantů projektu také zavedl. Řešení je tedy implementováno a společnost má nástroj pro ochranu svých dat. Zároveň jsme dokázali zvýšit produktivitu zaměstnanců na základě blokování činností nesouvisejících s pracovní náplní. S řešením jsme tak dokázali vynutit bezpečnostní směrnici, kterou jsem společnosti doporučil a navrhl. Ve směrnici je pouze napsáno, jak

se mají uživatelé chovat a co mají dělat, ale s řešením, které jsem do společnosti implementoval, to může společnost vynutit. Při implementaci jsem postupoval dle principů PDCA a díky dodržením těchto zásad, jsem úspěšně implementoval řešení do produkčního prostředí při zachování BCM, tedy řízení kontinuity organizace.

Jako další pokračování tohoto projektu bych navrhoval rozšíření analýzy pro celou bezpečnost ICT a zavedení kompletního ISMS. S implementací DLP jsme vyřešili ochranu informací proti interním hrozbám, ale zavedení ISMS by bylo dalším vhodným krokem pro lepší ochranu informací. Po zavedení ISMS by společnost měla ochráněné informace a mohla by se tak v klidu věnovat rozvoji svého businessu.

SEZNAM POUŽITÉ LITERATURY

1. CoSoSys. 2015. *Data Loss Prevention* [online]. [cit. 2015-02-27]. Dostupné z: http://www.endpointprotector.com/
2. *Český statistický úřad* [online]. 2015. [cit. 2015-01-15]. Dostupné z: https://www.czso.cz/
3. *ČSN ISO/IEC 27001: Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. 2006. Praha: Český normalizační institut.
4. *Data loss prevention complete certification kit - core series for it*. 2013. S.l.: Emereo Publishing. ISBN 978-148-8501-227.
5. DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. 2008. *Řízení bezpečnosti informací*. 1. vyd. Praha: Professional Publishing, 239 s. ISBN 978-80-86946-88-7.
6. EMC. 2015. *RSA Data Loss Prevention* [online]. [cit. 2015-02-27]. Dostupné z: http://www.emc.com/security/rsa-data-loss-prevention.htm
7. GFI Software. 2015. *GFI EndpointSecurity Software* [online]. [cit. 2015-02-27]. Dostupné z: https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-endpointsecurity
8. HUMPHREYS, Ted. c2007. *Implementing the ISO/IEC 27001 information security management system standard*. Boston: Artech House, xix, 265 p. ISBN 978-159-6931-725.
9. *ISO/IEC 18028-4:2005*. 2005. 4. Ženeva: ISO.
10. *McAfee Total Protection for Data Loss Prevention* [online]. 2015. [cit. 2015-02-27]. Dostupné z: http://www.mcafee.com/in/products/total-protection-for-data-loss-prevention.aspx
11. Metoda PERT. 2014. In: *Vysoká škola báňská - Technická univerzita Ostrava* [online]. [cit. 2015-04-08]. Dostupné z: http://books.fs.vsb.cz/SystAnal/texty/26.htm
12. MONSON, Thomas N, Sarah KAIP a Jerry ANTOON. c2004. *Loss prevention: threats and strategies : how people steal from your business and what you can do to stop it*. Medford, Or.: Advantage Source, ii, 276 p. ISBN 09-743-8301-5.

13. ONDRÁK, Viktor. 2013. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 377 s. ISBN 978-80-7204-872-4.
14. 2014 Cost of Data Breach Study: Germany. In: *2014 Cost of Data Breach Study: Germany* [online]. 2014. [cit. 2015-02-23].
15. POŽÁR, Josef. 2005. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 309 s. ISBN 80-868-9838-5.
16. Safetica Technologies s.r.o.. 2015. *Safetica - Prevence úniku dat a kompletní ochrana lidského selhání* [online]. [cit. 2015-02-20]. Dostupné z: www.safetica.cz
17. SEDLÁČEK, Miroslav. 2011. Demingův cyklus PDCA: a norma ISO/IEC 20000-1:2011. *SystemOnLine* [online]. Roč. 2011, č. 12 [cit. 2015-02-20]. Dostupné z: http://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm
18. SMEJKAL, Vladimír. 2010. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 354 s. ISBN 978-80-247-3051-6.
19. SODATSW. 2015. *Šifrování dat, bezpečnost IT, prevence úniku dat* [online]. [cit. 2015-02-27]. Dostupné z: http://www.sodatsw.cz/
20. STEINER, František a Jiří TUPA. 2007. *Management rizik v systémech řízení bezpečnosti informací*. Plzeň: Západočeská univerzita. ISBN 978-807-0435-359.
21. *Symantec Data Loss Prevention* [online]. 2015. [cit. 2015-02-27]. Dostupné z: https://www.symantec.com/data-loss-prevention/
22. Tend Micro. 2015. *Integrated Data Loss Prevention* [online]. [cit. 2015-02-27]. Dostupné z: https://www.trendmicro.com/us/about-us/index.html
23. Websense. 2015. *Data Security - Triton* [online]. [cit. 2015-02-27]. Dostupné z: https://www.websense.com/content/triton-ap-data.aspx

SEZNAM POUŽITÝCH ZKRATEK

AD (Active Directory) = adresářová struktura

BCM (Business Continuity Management) = systém řízení kontinuity organizace

BOZP = Bezpečnost a ochrana zdraví při práci

BYOD (Bring Your Own Device) = trend, kdy si zaměstnanci nosí do práce vlastní zařízení a pracují na nich

CPM (Critical Path Method) = metoda kritické cesty

ČSN = označení českých technických norem

DLP (Data Loss Prevention) = systém pro ochranu před ztrátou citlivých dat

FTP (File Transfer Protocol) = protokol pro přenos souborů pomocí sítě

GPO (Group Policy) = skupinová politika pro nastavení chování systému

IEC (International Electrotechnical Commission) = mezinárodní elektrotechnická komise

ISMS (Information Security Management System) = systém řízení bezpečnosti informací

ISO (Internation Organisation for Standardization) = mezinárodní organizace pro normalizaci

NDA (Non-disclosure Agreement) = dohoda o mlčenlivosti

PDCA (Plan, Do,Check, Act) = Plánuj, udělej, zkontroluj, jednej

PERT (Program Evaluation and Review Technique) = metoda síťové analýzy

RDP (Remote Desktop Protocol) = síťový protokol umožňující ovládání vzdáleného počíta

SIEM (Security Information and Event Management) = systém pro sběr bezpečnostních incidentů z různých bezpečnostních nástrojů

SMTP (Simple Mail Transfer Protocol) = protokol využívaný pro odesílání elektronické pošty

VPN (Virtual Private Network) = technologie pro bezpečné tunelování spojení přes Internet

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

PŘÍLOHY

Práce neobsahuje žádné přílohy.