VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ŘEŠENÍ INTERNÍCH HROZEB V MANAGEMENTU BEZPEČNOSTI INFORMACÍ

SOLUTION OF INTERNAL THREATS IN THE INFORMATION SECURITY MANAGEMENT SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN TRČKA
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR SEDLÁK
SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Trčka 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:

Řešení interních hrozeb v managementu bezpečnosti informací

v anglickém jazyce:

Solution of Internal Threats in the Information Security Management System

Pokyny pro vypracování:

Osnova zadání:
Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky. Praha: Český normalizační institut, 2006
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
HANÁČEK, P. a J. STAUDEK Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií. Praha: Úřad pro státní informační systém, 2000. ISBN 80-238-5400-3.
HAYDEN, L. IT security metrics: A practical framework for measuring security. New York: McGraw Hill, c2010. ISBN 00-717-1340-9.
MONSON, T., S. KAIP a J. ANTOON Loss prevention: threats and strategies : how people steal from your business and what you can do to stop it. Or.: Advantage Source, c2004. ISBN 09-743-8301-5.
POŽÁR, J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

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

V Brně, dne 21.05.2013

ABSTRAKT

Tato diplomová práce se zabývá problematikou interních hrozeb v organizaci a jejich omezení za pomocí implementace DLP systému. První část práce rozebírá systém řízení bezpečnosti informací a jeho náležitosti se zaváděním dle řady norem ISO/IEC 27000. Další kapitoly jsou věnovány interním hrozbám a technickému popisu DLP systému. Druhá část práce analyzuje organizaci a popisuje postup prováděné implementace DLP řešení, které má za úkol omezit interní hrozby. Závěr práce je věnován akceptačnímu řízení a finančnímu vyhodnocení implementace.

KLÍČOVÁ SLOVA

ISMS, DLP, management, organizace, bezpečnost informací, zabezpečení, data, norma, opatření, aktivum, interní hrozby, riziko, monitorování, ISO/IEC 27000.

ABSTRACT

This diploma thesis deals with internal threats in the organization and their restriction with the assistance of DLP system. The first part of the thesis discusses the information security management system and describes requirements for the introduction of the ISO/IEC 27000 standards series. Next chapters detail internal threats and technical description of the DLP system. The second part of the thesis analyzes the organization and describes the process of implementation of DLP solution, which aims to reduce internal threats. The conclusion of the thesis describes acceptance agreement and financial evaluation of the implementation.

KEYWORDS

ISMS, DLP, management, organization, information security, safety, data, standard, measure, asset, internal threats, risk, monitoring, ISO/IEC 27000.

BIBLIOGRAFICKÁ CITACE

TRČKA, M. *Řešení interních hrozeb v managementu bezpečnosti informací.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 91 s. Vedoucí diplomové práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

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

V Brně 21.5.2013

……

Martin Trčka

PODĚKOVÁNÍ

Rád bych na tomto místě srdečně poděkoval Ing. Petru Sedlákovi, který si vždy našel čas na potřebnou konzultaci a poskytoval cenné a odborné rady při vypracování této práce. Dále bych chtěl poděkovat rodině a přátelům za podporu.

OBSAH

ÚVOD 10
1 VYMEZENÍ PROBLÉMU A CÍL PRÁCE 12
2 TEORETICKÁ VÝCHODISKA PRÁCE 13
2.1 Bezpečnost informací 13
2.1.1 Informační bezpečnost organizace 13
2.1.2 Systémové vymezení bezpečnosti informací 16
2.1.3 Normy v oblasti bezpečnosti IT 17
2.2 Systém managementu bezpečnosti informací 19
2.2.1 Model PDCA 19
2.2.2 Ustanovení ISMS 20
2.2.3 Zavádění a provozování ISMS 22
2.2.4 Monitorování a přezkoumávání ISMS 23
2.2.5 Udržování a zlepšování ISMS 23
2.2.6 Zahájení bezpečnostních opatření 23
2.3 Analýza rizik 24
2.3.1 Pojmy z analýzy rizik 26
2.3.2 Analýza a identifikace hrozeb 27
2.4 Interní hrozby 28
2.4.1 Způsob ohrožení organizace zaměstnanci 29
2.4.2 Finanční dopad interních hrozeb 31
2.4.3 Náklady spojené s únikem dat 31
2.4.4 Snížení rizika ztráty 32
2.5 Omezení interních rizik 34
2.5.1 Monitorování zaměstnanců 34
2.5.2 Blokování uživatelské činnosti 36
2.6 Ochrana před ztrátou dat 37
2.6.1 Bezpečnostní politika a události DLP systému 38
2.6.2 Klasifikace dat 39
2.6.3 Způsob monitorování DLP systému 41
2.7 Prevence proti interním hrozbám 44
3 ANALÝZA PROBLÉMU A SOUČASNÁ SITUACE 45
3.1 Informace o společnosti 45
3.1.1 Organizační struktura společnosti 45
3.2 Bezpečnostní problémy společnosti 47
3.3 Postup pro řešení problémů 48
4 NÁVRH ŘEŠENÍ 49
4.1 Obchodní navázání kontaktu 49
4.2 Cíle a záměry implementace DLP 50

4.3 Základní studie proveditelnosti 51
4.3.1 Zdůvodnění realizace projektu a jeho potřebnost 51
4.3.2 Management projektu a řízení lidských zdrojů 52
4.3.3 Technické a technologické aspekty projektu 52
4.3.4 Legislativní aspekty projektu 54
4.3.5 Časový harmonogram projektu 54
4.3.6 Finanční a ekonomické aspekty projektu 56
4.4 Implementační analýza 58
4.4.1 Technický audit prostředí 58
4.4.2 Identifikace a ohodnocení aktiv 59
4.4.3 Identifikace a pravděpodobnost hrozeb 61
4.4.4 Vyhodnocení míry rizik 62
4.4.5 Návrh a princip bezpečnostních opatření 63
4.4.6 Návrh technického řešení 70
4.4.7 Návrh školení zaměstnanců 75
4.4.8 Implementační smlouva 75
4.5 Implementace 76
4.5.1 Testování na vzorové stanici 77
4.5.2 Školení uživatelů 77
4.5.3 Pilotní nasazení 78
4.5.4 Plné nasazení 79
4.5.5 Akceptační řízení a předání implementace 80
4.6 Posouzení a vylepšení DLP řešení 81
4.7 Finanční zhodnocení 81
ZÁVĚR 83
SEZNAM POUŽITÉ LITERATURY 85
SEZNAM POUŽITÝCH ZKRATEK 88
SEZNAM OBRÁZKŮ 89
SEZNAM TABULEK 90
PŘÍLOHY 91

ÚVOD

Současný moderní ekonomicko-technologický svět vytváří denně mnoho nových informací a dat, které mají určitou úroveň hodnoty bohatství a patří mezi klíčové prvky pro úspěšné podnikání a ekonomický růst každé organizace. Při pravidelném zvětšování objemu dat a informací je zapotřebí zavést mechanismy pro jejich ukládání. Jsou používány informační systémy organizace, lokální datová uložiště, nebo síťové, případně paměťová média, jako jsou pevné disky v pracovních stanicích, externí disky, flash paměti a jiné. Takto uložená data jsou dostupná velkému počtu uživatelů, což má za následek vysoké bezpečnostní nároky. Někteří zaměstnanci si velmi dobře uvědomují, že při práci manipulují s citlivými informacemi, mající danou úroveň bohatství a snaží se je různými metodami a častými útoky získat pro vlastní prospěch a finanční zisk. Mezi časté cíle těchto útoků patří informace o technologických postupech, obchodní informace, zdrojové kódy programů, tajné informace o produktech a strategii svého zaměstnavatele. Vždyť je tak jednoduché uložit tajný dokument na přenosné médium nebo vypálit databázi na CD. Dostanou-li se k těmto informacím neoprávněné osoby, může to vést od ztráty dobré pověsti společnosti přes soudní spor až ke krachu a ukončení podnikání. Z toho důvodu se začínají dnešní společnosti zajímat o možné způsoby zabezpečení svého bohatství ve formě informací před interními útoky, které přicházejí nejčastěji ze strany vlastních zaměstnanců a investují finanční prostředky do bezpečnosti informací.

Informační bezpečnost v oblasti interních hrozeb znamená komplexní pohled na vnitřní fungování společnosti. Pro účinnou ochranu je třeba pochopit mezilidské vztahy na pracovišti a porozumět problémům svých zaměstnanců, kteří jsou hlavní hrozbou pro vznik mimořádných událostí. Zaměstnanci mohou společnost ať už úmyslně, nebo neúmyslně poškozovat. Když si zaměstnanec odnese tužku nebo kancelářské potřeby, nejedná se o závažný problém. Pokud si ale odnese například přenosný disk plný nejdůležitějších firemních dat nebo odešle email na špatnou adresu, je již pozdě ptát se, co šlo udělat pro to, aby se data nedostala ke konkurenci nebo na veřejnost.

Práce je rozdělena logicky na dvě části, teoretická a praktická. V teoretické části jsou rozebírány problémy informační bezpečnosti a nutné náležitosti potřebné k plnohodnotnému zavedení podle řady norem ČSN ISO/IEC 27000. Další část je věnována interním hrozbám, které se vyskytují v dnešních společnostech a velikosti ekonomického dopadu. Na toto téma plynule navazuje možná ochrana před interními hrozbami ve formě DLP systému (data loss prevention).

V praktické části je rozebrána metodika postupu při implementaci DLP řešení do společnosti z důvodu nutnosti omezení interních hrozeb a úniku dat. Je zde popis analyzovaného subjektu a rozebrány objevené problémy na pracovišti. Posléze je v několika podkapitolách popsán postup celé implementace DLP řešení od navázání obchodního kontaktu, přes provedené analýzy společnosti až po finální implementaci

DLP softwaru do společnosti. Závěr diplomové práce je věnován vyhodnocení implementace za pomocí akceptačního řízení a akceptačního protokolu. Následně je rozebrána celková finanční zátěž projektu a návratnost investic v rozmezí jednoho roku.

1 VYMEZENÍ PROBLÉMU A CÍL PRÁCE

Práce se zabývá problematikou spojenou s únikem citlivých dat a výskytem interních hrozeb ve společnosti, pro kterou jsou data a informace základním ekonomickým kamenem. Hlavním cílem úniku dat už nejsou totiž osobní informace zaměstnanců nebo partnerů, ale duševní bohatství společnosti, mezi které patří informace a znalosti. Pokud společnosti uniknou čísla platebních karet partnerů, je to ostuda a výsledkem bude negativní publicita a nutnost složitě dodržet legislativní požadavky, které tyto případy ošetřují. Společnost se proto pochopitelně snaží incidentům tohoto typu předcházet. Důležité je ale uvědomit si, že pro útočníky dnes má větší cenu duševní vlastnictví firmy, které je mnohdy chráněno naopak nedostatečně. Povědomí o možnosti úniků dat, zapříčiněných zaměstnanci zevnitř společnosti, je na rozdíl od hrozby útoku zvenčí malé nebo přinejmenším podceňované. Navíc zaměstnanci často riskují na pracovišti tím, že provádějí nebezpečné činnosti, jako je používání nezašifrovaných USB disků, přeposílají emaily na osobní adresy a jiné nezodpovědné úkony. Z toho důvodu je důležité věnovat se omezením těchto incidentů za pomocí managementu bezpečnosti informací.

Hlavním cílem diplomové práce je popsat a identifikovat interní hrozby vyskytující se ve vybrané společnosti a vyhodnotit jejich ekonomický dopad. Na základě provedených analýz prostředí společnosti se provede postupná implementace DLP řešení za pomocí systému managementu bezpečnosti informací podpořenou technickými normami z řady ČSN ISO/IEC 27000. Tato práce si klade za cíl popsat a vytvořit metodiku pro zavádění DLP řešení, která spočívá od navazování obchodních kontaktů až po akceptační kritéria implementace.

Pro vytvoření diplomové práce jsem čerpal z dostupných veřejných zdrojů a technických dokumentů, které jsou reprezentovány ISO normami. Při tvorbě praktické části byly použity výsledky provedených analýz ve vybrané společnosti a vlastní pracovní zkušenosti s vývojem a implementací DLP řešením.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V dnešní době, plné moderních technologií, je více než důležité se zajímat o bezpečnost v oblasti informačních technologií, protože informace představuje velmi cenné aktivum[1], které je potřeba chránit. Mnoho organizací přistupuje k ochraně informací a dat nezodpovědně, případně vůbec. Z toho důvodu je nutné, aby se systematická ochrana informací a dat stala součástí řídících klíčových procesů ve společnosti a díky tomu se snížil výskyt rizik, případně obchodní dopad ze ztráty. Veškeré informace uchované a zpracovávané organizací jsou ohroženy útokem[2], chybou, přírodními vlivy (jako jsou požáry, záplavy) a jsou vystaveny zranitelnosti související s jejich používáním. Termín bezpečnost informací[3] je obecně založen na informacích považovaných za aktivum, které má hodnotu vyžadující příslušnou ochranu.

2.1 Bezpečnost informací

Bezpečnost informací je velmi často používaný pojem, jehož důležitost má rostoucí trend s ohledem na rostoucí hodnotu informací v organizaci. Informace, které jsou potřeba chránit, mají rozličnou podobu (elektronickou, tištěnou nebo informace vycházející z procesů v organizaci). Rizika úniku a zneužití informací hrozí nejen z vnějšího prostředí, ale zejména z vnitřního. Jedná se o komplexní pohled, který pomáhá organizaci poznat a chránit své cenné informace a také vede praktickými opatřeními k eliminaci, či výraznému sníženi dopadu v případě mimořádné události.

2.1.1 Informační bezpečnost organizace

Samotná správa a řízení bezpečnosti informací je v odpovědnosti statutárních orgánů a hlavního vedení organizace a měla by být součástí Enterprise Governance[4], kde se musí objevovat vazby na IT Governance. Vedení organizace poté zodpovídá za to, aby správa bezpečnosti byla součásti jimi prováděných procesů řízení kritických zdrojů v organizaci. Následně vedení organizace má za úkol reagovat na události vyvolané požadavky na bezpečnost informací. Je potřeba si v organizaci vymezit názory na to, co očekávat od programu bezpečnosti informací, jakým postupem jej implementovat a zavádět, princip hodnocení stavu současné bezpečnosti informací a formulovat základy

[1] Aktivum je cokoliv, co má pro organizaci hodnotu (2).

[2] Útok je pokus o zničení, vystavení hrozbě, změně, vyřazení z činnosti, zcizení nebo získání neautorizovaného použití čehokoliv, co má pro organizaci hodnotu (1).

[3] Bezpečnost informací je zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost, hodnověrnost (3).

[4] Enterprise Governance je souhrn odpovědností a praktik realizovaných vlastníky a vedením organizací, jejichž cílem je realizace strategického vývoje, dosahování cílů, zajištění přiměřeného řízení rizik a ověřování zodpovědné spotřeby zdrojů organizace (21).

pro budoucí vývoj. Na základě těchto poznatků se v ISG klade důraz na žádoucí vstupy, znalosti a ochranu informačních aktiv, přínos pro organizaci a také na integraci procesů (6).

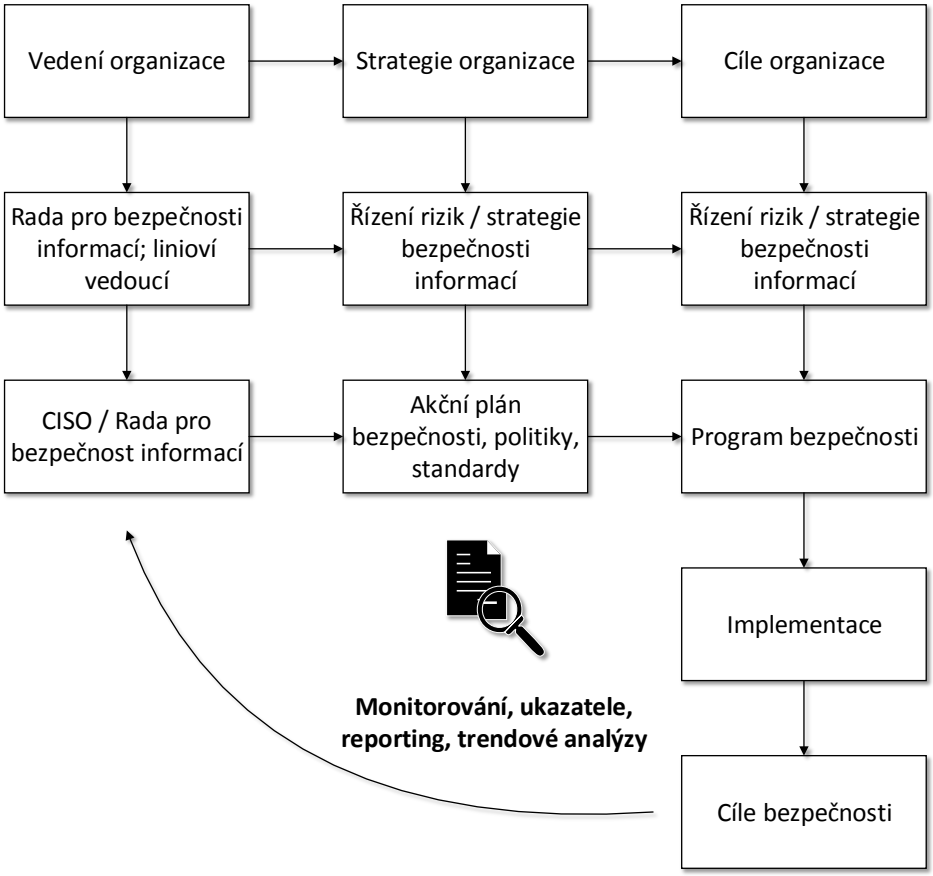
Informační bezpečnost organizace, neboli ISG je kompletní souhrn schopností vedení lidí, organizační struktury a procesů, kde hlavním cílem je ochrana informací. Hlavní předpoklad úspěchu mezi organizační strukturou a procesy je efektivní komunikace všech zúčastněných stran, která je založena na konstruktivních vztazích a sdílené podpoře definovaných cílů. Z toho důvodu je důležité definovat pět hlavních výstupů ISG, které na sebe plynule navazují:

a) Podpora strategických cílů za pomoci propojení bezpečnosti informací se strategií organizace.
b) Řízení rizik založené na ukazatelích, umožňujících snížit dopad případných hrozeb na přijatelnou úroveň.
c) Řízení zdrojů, opírající se o využívání znalostí z oblasti řízení bezpečnosti informací.
d) Hodnocení realizace cílů ISG pomocí měření, monitorování a reportingu.
e) Vykazování dosažených hodnot pomocí optimalizace investic do bezpečnosti informací (6).

Pro dosažení výše jmenovaných výstupů se také definují praktiky na úrovni hlavního vedení organizace, kterými se dosáhne optimální fungování ISG. Základní praktikou je zařazení a přidělení odpovědnosti za bezpečnost informací na úroveň statutárních orgánů v dané organizaci. S tím je spojené také zajištění efektivnosti bezpečnostní politiky formou její kontroly a schvalování. Na základě těchto praktik je důležité vytvořit zvláštní organizační jednotku pro bezpečnost informací a její adekvátní podporu ve vedení organizace.

V každé organizaci bývají základním zdrojem informací data. Data sama o sobě nejsou použitelná, pokud se neorganizují nebo se s nimi nezachází tak, aby se stala informacemi. Díky seskupení informací takovým způsobem, které umožňuje vytvářet smysluplné operace a aktivity, vznikají znalosti. Znalost se tvoří z dostupných informací a naopak, znalost je ukládána a přenášena jako organizovaná informace. V této souvislosti se o informacích a znalostech hovoří jako o informačních aktivech, bez kterých není organizace schopna fungovat a proto je potřeba zavést jejich adekvátní ochranu a uspořádání. Organizace musí stanovit odpovědnost za bezpečnost informací jako samostatnou část řízení, a nikoliv jako součást jiných rolí, které postrádají pravomoci, odpovědnost a zdroje k jejímu prosazování. Bohužel se tak často děje, neboť se činnosti spojené s řízením bezpečnosti informací mnohdy realizují oddělené v jednotlivých funkčních útvarech organizace, což vede k její neefektivnosti (různá terminologie, procesy, technologie). Důsledkem nízké integrace bezpečnostních procesů v rámci organizace vzniká duplicita nebo naopak bezpečnostní mezery, které mohou vést k incidentům a úniku informací (6).

Informační bezpečnost organizace generuje významné přínosy (sdílení hodnot mezi organizacemi praktikujícími ISG, větší předvídavost a omezení nejistot spojených s činnosti organizace, zajištění souladu s veřejnými a právními požadavky na správnost informací a jejich ochranu, zajištění účinné bezpečnostní politiky a jejího dodržování, základ pro účelné a účinné řízení rizika, zajištění, aby se kritická rozhodnutí neopírala o chybné informace), které mají vliv na zvyšování hodnoty organizace a zvyšují důvěru zákazníka, obchodního partnera, případně investora. Díky tomu se mohou zavádět nové technologie a snižují se provozní náklady omezením rizikových faktorů procesu organizace (6).



Obr. 1: Princip ISG (Zdroj: (11))

V organizaci jsou základní bezpečnostní cíle splněny tehdy, když je informace dostupná a použitelná v případě potřeby a systémy, které ji zpracovávají, jsou schopny je podle potřeby obnovit (dostupnost[5] informací), dále když informace jsou dostupné

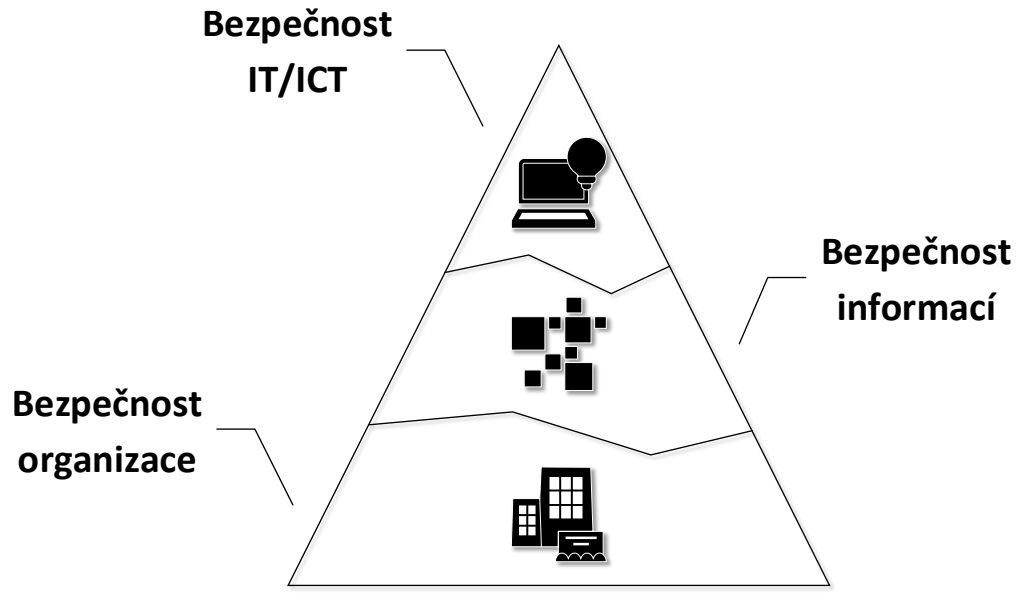
[5] Dostupnost je zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby (2).

pouze těm, kteří je potřebují (důvěrnost[6] informací) a informace jsou chráněné proti neoprávněným změnám (integrace[7] informací) (11).

Úroveň bezpečnosti se správně stanovuje a zabezpečuje komplexně, tedy v rovině administrativní, komunikační, fyzické a personální bezpečnosti, jak je například uvedeno v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, jak by na základě analýzy rizik a návrhu bezpečnostní politiky mělo být stanoveno i v jakékoli jiné organizaci, která chce chránit svá data (informace). Zajištění bezpečnosti organizace a jejich informací by mělo vycházet ze základních fází, jakými jsou prevence, zvládnutí rizika, respektive havarijního stavu a zajištění obnovy. Kromě podpůrných procesů je jejich smyslem chránit elementární a životně důležité procesy. Jsou to preventivní procesy, s jejichž pomocí snižujeme riziko porušení hlavních procesů (11).

2.1.2 Systémové vymezení bezpečnosti informací

Se samotným termínem bezpečnost informací jsou spojeny i další dva pojmy a to bezpečnost organizace a bezpečnost IT/ICT, které jsou vůči sobě ve vztahu. Bezpečnost organizace se týká zajištění bezpečnosti objektů, majetku organizace, jako je ostraha přístupu do objektu nebo organizace, strážní služby apod. Některé prvky, které jsou součástí bezpečnosti organizace, napomáhají a zvyšují bezpečnost ostatních pojmů (bezpečnost informace, bezpečnost IT/ICT) (6).



Obr. 2: Vztah úrovně bezpečnosti (Zdroj: (6))

[6] Důvěrnost je zajištění, že informace jsou přístupné nebo sdělený pouze těm, kteří jsou k tomu oprávnění (2).

[7] Integrita je zajištění správnosti a úplnosti informací (2).

Úkolem řízení bezpečnosti informací je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů, tedy nejen s informacemi v digitální formě, ale i například v papírové formě. Bezpečnost informací zahrnuje navíc proti bezpečnosti IT/ICT například způsob zpracování dat, jejich uložení a správu archivu nedigitálních dat, zásady skartace materiálů, nakládání s informacemi během jejich transportu na jiná místa, zásady pro poskytování informací novinářům a případně zásady spojené s veřejným vystupováním zaměstnanců organizace v rozhlase nebo v televizi.

Bezpečnost IT/ICT má hlavní úkol chránit aktiva, která jsou nedílnou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi, z toho důvodu je bezpečnost IT/ICT relativně nejužší oblastí řízení bezpečnosti. Jedná se o velmi komplikovaný problém, jelikož se zde pracuje s neviditelnými daty, informacemi a službami (nehmotná aktiva), které mají vysokou finanční hodnotu pro organizaci.

2.1.3 Normy v oblasti bezpečnosti IT

Důležitým krokem v bezpečnosti informací se staly normy, které vznikly ve Velké Británii, a první norma nesoucí označení BS 7799 byla uveřejněna roku 1995, kde se autoři snažili zformulovat nejlepší vžitou praxi související s bezpečností informací. Vznikl tak efektivní nástroj k hodnocení a aplikování bezpečnosti informací, který se rychle rozšířil po celém světě a dnes je k dostání v mnoha jazycích. Postupem času byla norma modernizována, kde v roce 1999 vznikla revize obsahující dva samostatné díly a v roce 2000 byla schválena jako mezinárodní standard ISO a uvedena pod označením ISO/IEC 17799:2000.

V roce 2005 byla uvedena mezinárodní organizaci pro normalizaci řada norem pod značením ISO/IEC 27000, které zahrnují nejaktuálnější poznatky z oblasti komplexní informační bezpečnosti a jsou postaveny na základech normy ISO/IEC 17799 a BS 7799 (6).

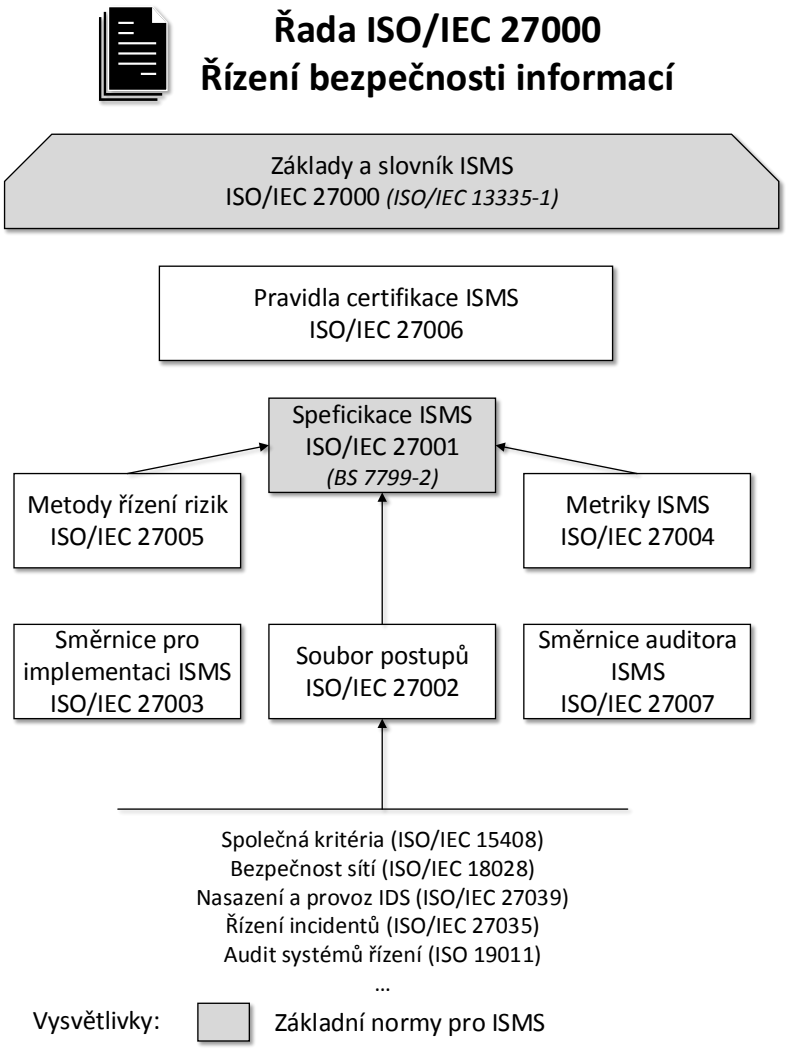
2.1.3.1 Řada ČSN ISO/IEC 27000 – Řízení bezpečnosti informací

Nová řada norem pro řízení bezpečnosti informací má pomoci organizacím všech typů a velikosti zavést a provozovat ISMS[8]. Normy řady ČSN ISO/IEC 27000 obsahuje následující dokumenty (6):

a) ČSN ISO/IEC 27000:2009, Systém řízení bezpečnosti informací – Přehled a slovník.
b) ČSN ISO/IEC 27001:2005, Systém řízení bezpečnosti informací – Požadavky.

[8] Systém managementu bezpečnosti informací ISMS je část celkového systému managementu organizace založena na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací (2).

c) ČSN ISO/IEC 27002:2005, Soubor postupů pro management bezpečnosti informací.
d) ČSN ISO/IEC 27003, Směrnice pro implementaci systému řízení bezpečnosti informací.
e) ČSN ISO/IEC 27004, Řízení bezpečnosti informací – Měření.
f) ČSN ISO/IEC 27005:2008, Řízení rizik bezpečnosti informací.
g) ČSN ISO/IEC 27006:2007, Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
h) ČSN ISO/IEC 27007, Směrnice pro auditování systémů řízení bezpečnosti informací.



Obr. 3: Koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací (Zdroj: (6))

2.2 Systém managementu bezpečnosti informací

V dnešní současné situaci se žádná organizace nemůže obejít bez kompletního a systematického řízení informací. Bezpečnost se stala nedílnou součástí každodenního řízení a vnitřní kultury organizace a řada těchto organizací se snaží přistupovat k ochraně informací systematicky na základě pravidel systému řízení bezpečnosti informací. Systém ISMS poskytuje zabezpečení informačních aktiv, aby byly plně dosaženy cíle organizace s ohledem na možná rizika. Požadavky na ISMS jsou sepsány v normě ČSN ISO/IEC 27001. Úspěšná implementace ISMS v organizaci vede ke zvyšování hodnot aktiv, lepší koordinaci práce s interními dokumenty, rychlé zotavení z incidentu, snížení rizik a neopakování chyb (6).

Systém řízení bezpečnosti informací je základem pro efektivní a účinné řízení bezpečnosti informací. Systém řízení se opírá o čtyři hlavní systémové etapy. Při první etapě, ustanovení ISMS, je snahou vše správně naplánovat. Počátkem je určení rozsahu řízení a stanovení základního rámce bezpečnostní politiky. Plánování pokračuje identifikací a ohodnocením rizikových scénářů, které vedou k výběru vhodných bezpečnostních opatření[9]. Výstupem z první etapy je formulace prohlášení o aplikovatelnosti a získání souhlasu vedení organizace se zavedením ISMS.

Druhá etapa se věnuje prosazováním ISMS, zde je velmi důležité stanovit dílčí (roční) plány na zvládání rizik, definovat dlouhodobě platná bezpečnostní pravidla a tato pravidla vysvětlit účastníkům a sledovat účinnost s jakou je bezpečnost prosazována.

Třetí etapa obsahuje zpětnou vazbu, která má základ v pravidelné kontrole pověřených osob. Dalším důležitým prvkem jsou interní audity ISMS. Všechny získané poznatky o ISMS jsou pak vedením organizace vyhodnoceny a vedou ke zpřesnění cílů pro další období.

V poslední etapě je dán prostor pro soustavné zlepšování ISMS. Mimo odstraňování nedostatků je hlavní výzvou využít všechny nápady, které dovolují zjednodušit a zkvalitnit systém řízení (1).

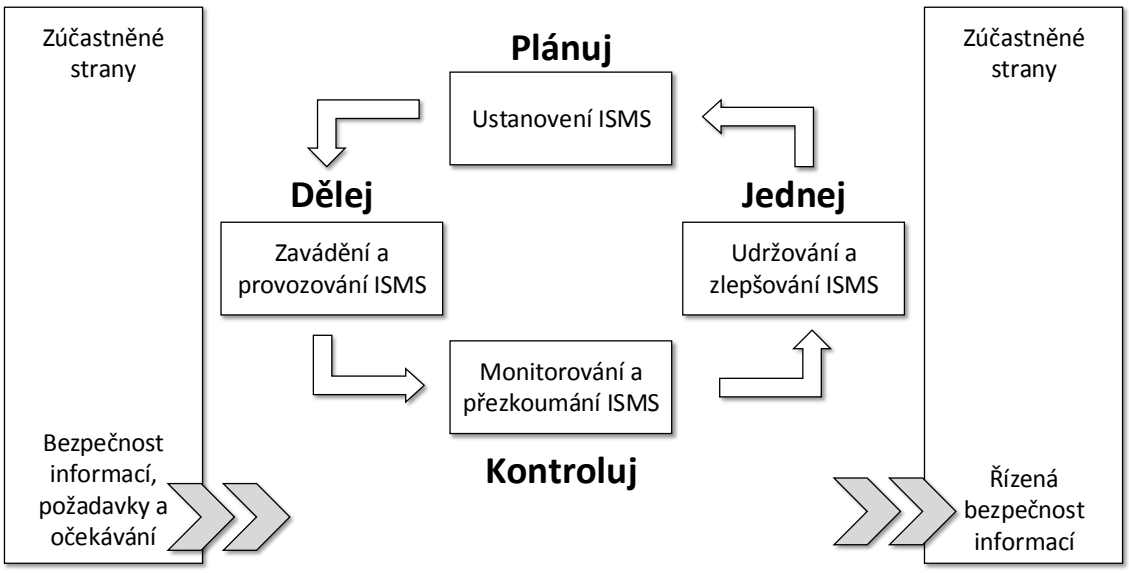
2.2.1 Model PDCA

ISMS je, podobně jako ostatní systémy řízení, založen na modelu PDCA. Koncept modelu PDCA poskytuje schematické vyjádření životního cyklu celého integrovaného systému řízení a zároveň zajišťuje kompletní zpětnou vazbu. Tento přístup umožňuje používat shodné metody, metodiky a postupy pro řízení každé komponenty integrovaného řízení a IMS jako celku. Tyto postupy jsou systémovým návodem jak dělat věci správně, případně podle nejlepších zkušeností, které vznikly v různých částech světa a které se prosadily již v zavedených společnostech. Ovšem každá

[9] Opatření je považována jakákoliv aktivita, zařízení, technika či jiný postup, který umožní snížit sílu hrozby, která na informační systém působí, nebo úplně zabránit v jejím účinku (6).

organizace má svoje vlastní specifika, která nutí odpovědného tvůrce integrovaného sytému řízení modifikovat a měnit doporučené mezinárodní normy. Samostatná metoda se skládá ze čtyř po sobě jdoucích částí (1):

a) Plánuj - začínají se získávat informace a popis řešeného problému, který slouží pro přípravu základních materiálů. Plán by měl obsahovat jednotlivé činnosti, které je třeba udělat k odstranění problému. Mělo by proběhnout ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby výsledky byly v souladu s celkovou politikou a cíli organizace.
b) Dělej - na základě vytvořeného plánu se postupuje a zavádí jednotlivé požadavky pro využívání politiky ISMS.
c) Kontroluj - souvisí s posuzováním, případně i měřením výkonu procesu vůči politice ISMS. Stanovují se výchozí hodnoty sledovaných ukazatelů, které určují kvalitu procesu a také postupné monitorování nadefinovaných ukazatelů a porovnávání stanovených hodnot s hodnotami naměřenými.
d) Jednej - má za úkol provádění nápravných opatření a preventivních činností, založených na základě vyhodnocení provedených vedením organizace a postupné stále zlepšování ISMS (1).



Obr. 4: PDCA model aplikovaný na procesy ISMS (Zdroj: (2))

2.2.2 Ustanovení ISMS

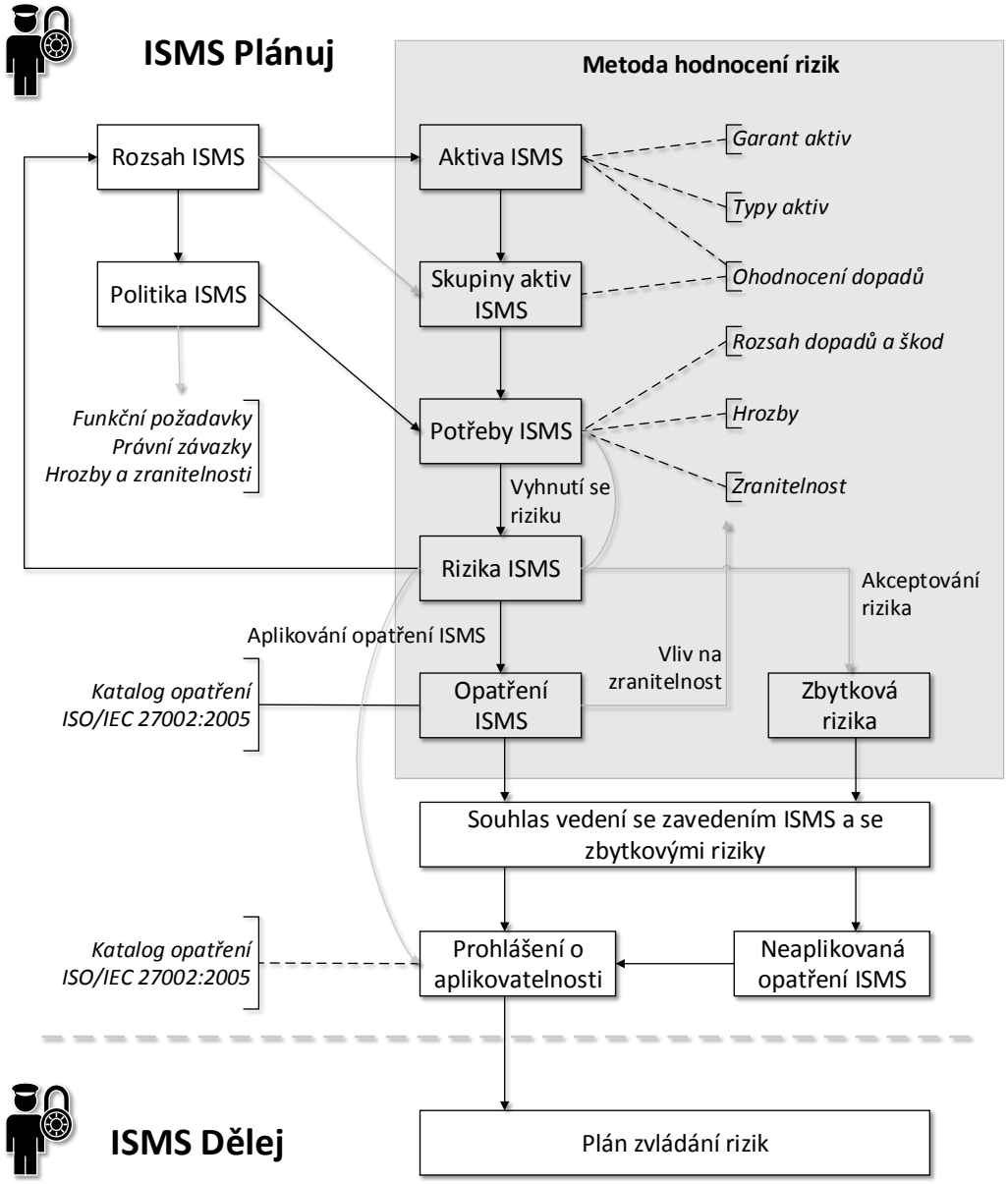
První etapou budování ISMS je ustanovení systému, při kterém jsou upřesněny správné formy bezpečnosti informací. Základní položkou je určení rozsahu hranic a vazeb ISMS na základě posouzení činnosti organizace, její organizační struktury, umístění, neboli lokality a používané technologie.

Za pomocí specifických potřeb organizace je nutné definovat politiku ISMS. Z praktického hlediska je důležité, aby politika[10] obsahovala upřesnění cílů a definovala základní směr a rámec pro řízení bezpečnosti informací s následující údržbou do budoucnosti. Definované cíle by měla politika zohlednit s požadavky organizace a souvisejícími zákonnými a smluvními předpisy. Rovněž musí být stanovena kritéria, podle kterých jsou popisována a hodnocena rizika v organizaci a vše schválené ze strany vedení organizace. Politika ISMS je rozsahem krátký, ale významem velmi důležitý dokument, protože prezentuje zájem vedení organizace o řízení bezpečnosti informací a definuje klíčové podmínky pro ohodnocení rizik, což je základem pro celý ISMS. Správně definovaná politika ISMS může hodně usnadnit budoucí prosazování pravidel a požadavků informací v organizaci (6).

Řízení a analýza rizik[11] je součástí ustanovení ISMS v organizaci a je klíčovým nástrojem pro systematické řízení bezpečnosti informací. Přesná znalost skutečných rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření schopných snížit negativní dopady těchto rizik. Dobrá, přesná znalost bezpečnostních rizik vede k účinnému vynakládání úsilí při prosazování bezpečnostních opatření, které tak přinášejí větší efektivitu. Analýze rizik je věnovaná kapitola 3.3.

Na základě výsledků řízení rizik by měly být připraveny dva formální kroky, ve kterých vedení organizace odsouhlasí zjištěné skutečnosti. Zde je potřeba, aby vedení organizace odsouhlasilo bezpečnostní opatření, která jsou nutná pro snížení bezpečnostních rizik. Současně s tím, by se vedení mělo vyjádřit, zda existují zbytková rizika pro chod organizace či nikoli. Posledním krokem je prohlášení o aplikovatelnosti, což je povinný dokument pro organizaci, která usiluje o shody svého ISMS s normou ČSN ISO/EIC 27001. Tento dokument musí obsahovat cíle opatření a jednotlivá bezpečnostní opatření, která byla pro daný ISMS vybrána na pokrytí existujících rizik. V praxi je prohlášení o aplikovatelnosti nejdůležitějším dokumentem, který postihuje systémové vazby ISMS (6).

[10] Politika je záměr a směr formálně vyjádřený vedením organizace (3).
[11] Analýza rizik je systematické používání informací k odhadu rizika a k identifikaci jeho zdrojů (2).



Obr. 5: Přehled činností při ustanovení ISMS (Zdroj: (6))

2.2.3 Zavádění a provozování ISMS

Tato etapa životního cyklu ISMS se soustředí na prosazení všech bezpečnostních opatření tak, jak byla navržena v předchozí etapě při ustanovení ISMS. Důležité je především připravit dílčí plány, kde jsou upřesněny termíny a odpovědní lidé. Všechna bezpečnostní opatření by měla být zdokumentována a mělo by dojít k vysvětlení bezpečnostních principů všem uživatelům a manažerům.

V této etapě organizace musí formulovat a vytvořit plán zvládání rizik[12] a započít s jeho postupným zaváděním. Ovšem musí se brát v úvahu finanční zdroje a přiřazení

[12] Zvládání rizik je proces výběru a přijímání opatření ke změně rizika (2).

rolí a odpovědnosti v organizaci. Je-li zaveden plán rizik, může se přejít k zavádění bezpečnostních opatření, které byly definovány v první etapě a určit, jakým způsobem se bude měřit účinnost zavedených opatření a stanovit, jak budou měření použita k vyhodnocení účinnosti opatření tak, aby se později daly závěry z hodnocení porovnávat a opakovat. Všechny výstupy, mezi které patří dokumentace a záznamy musí být správně řízeny a organizovány.

Dalším krokem je definovat a budovat program školení, kde organizace musí zajistit, aby zaměstnanci, kterých se týkají povinnosti definované v ISMS, byli odborně způsobilí k vykonávání požadovaných úkolů. A je potřeba zajistit, aby si samotní zaměstnanci byli vědomi svých činností v rámci bezpečnosti informací a svého přínosu k dosažení cílů ISMS.

Poslední částí je zavádění postupů a dalších opatření pro rychlou detekci a reakci na bezpečnostní incidenty a řízení zdrojů, kde je potřeba sledovat, zda jsou všechny náležitosti ISMS pokryty odpovídajícím množstvím odborných zdrojů (lidských, finančních, technických) a účinně řídit použití těchto zdrojů pro správné fungování (6).

2.2.4 Monitorování a přezkoumávání ISMS

Důležitým bodem třetí etapy je zajistit účinné zpětné vazby při zavádění ISMS. V souvislosti s tímto požadavkem by proto mělo dojít k prověřování všech aplikovaných bezpečnostních opatření a jejich důsledků na ISMS. Ověřování začíná u přímé kontroly odpovědných osob ze strany jejich nadřízených či bezpečnostním manažerem. Významnou roli též sehrává nezávislé posouzení fungování a účinnost ISMS pomocí interních auditů. Základní cíl všech použitých zpětných vazeb je připravit dostatek podkladů o skutečném fungování ISMS, které budou předloženy vedení organizace za účelem přezkoumání, zda celá realizace bezpečnosti informací je v souladu s předem danými principy a obecnými potřebami organizace. V této části je nezbytné monitorovat a ověřit účinnost prosazených bezpečnostních opatření, provádět interní audity ISMS a připravit zprávu o stavu ISMS a na jejím základě přehodnotit nebo upravit celý systém bezpečnosti (1).

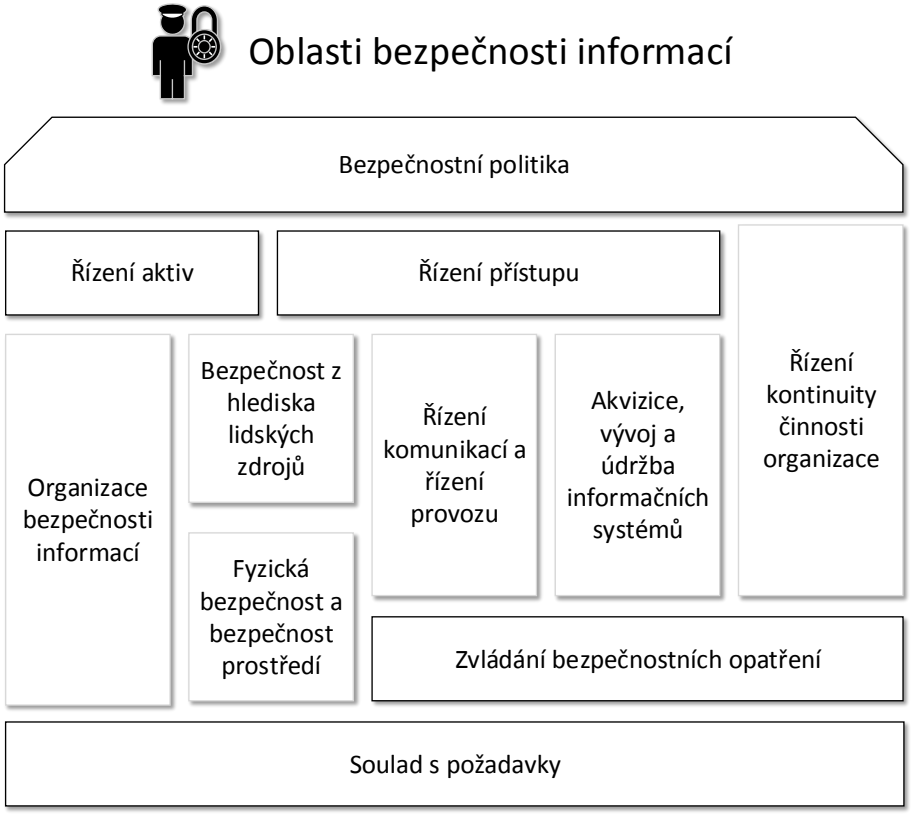
2.2.5 Udržování a zlepšování ISMS

Poslední etapou celého cyklu zavádění ISMS je jeho údržba a zlepšování. V této fázi by mělo docházet ke sběru podnětů k celkovému zlepšení ISMS a provádět odpovídající opatření k nápravě nedostatků (neshod), které se v průběhu provozu objevují. Z toho důvodu se postupně upravuje a zjednodušuje celý model bezpečnosti informací (1).

2.2.6 Zahájení bezpečnostních opatření

Pro plnou realizaci ISMS je potřeba vycházet z normy ČSN ISO/IEC 27002, Soubor postupů pro řízení bezpečnosti informací. Samotná norma obsahuje téměř 133 bezpečnostních opatření, která jsou rozděleny logicky do 11 oblastí. Doporučení, která

norma obsahuje, poskytuje většině bezpečnostních techniků základní východisko pro řízení bezpečnosti informací.



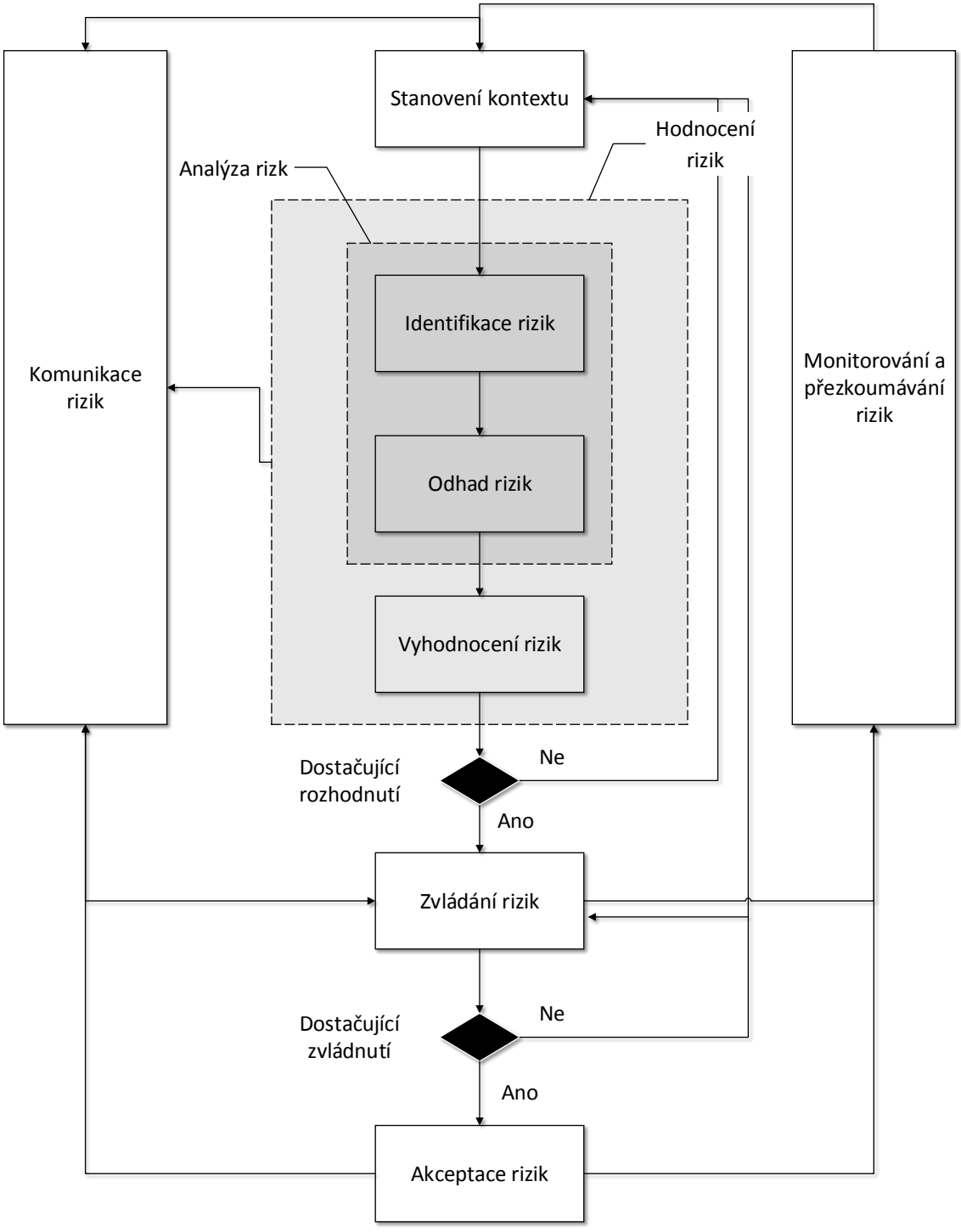
Obr. 6: Rozdělení oblasti bezpečnosti informací (Zdroj: (6))

2.3 Analýza rizik

Rizikem se obecně rozumí možnost nebezpečí vzniku škody, poškození, případně vzniku ztráty, například finanční, při podnikání a z toho důvodu je řízení a analýza rizik klíčovým nástrojem pro systematické řízení bezpečnosti informací. Přesná znalost skutečných rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření schopných snížit negativní dopady těchto rizik. Prvním krokem procesu snižování rizik je jejich analýza, která je chápana jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti. Analýza rizik obsahuje několik kroků:

a) Identifikace aktiv má za úkol vymezit posuzovanou organizaci a vytvořit popis aktiv.
b) Stanovení hodnoty aktiv určuje hodnotu a význam aktiv pro organizaci, ohodnocuje možný dopad jejich ztráty, změny či poškození.
c) Identifikace hrozeb a slabin určí druh událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv a určí slabá místa v organizaci, která mohou umožnit působení hrozeb.

d) Stanovení závažnosti hrozeb a míry zranitelnosti obstarává pravděpodobnost výskytu hrozby a míry zranitelnosti organizace vůči dané hrozbě (11).



Obr. 7: Proces řízení rizik ISMS (Zdroj: (11))

2.3.1 Pojmy z analýzy rizik

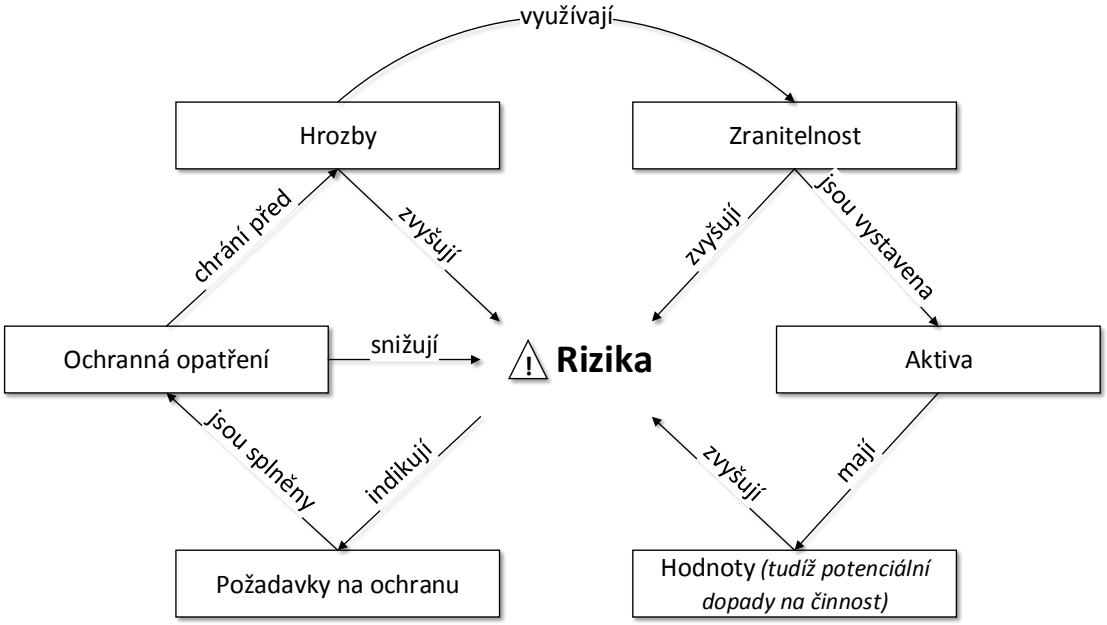
Aktivum je všechno, co má pro organizaci hodnotu, která může být zmenšena působením hrozby. Aktiva můžou být hmotná (nemovitosti, cenné papíry, peníze) a nehmotná (informace, kvalita a morálka zaměstnanců, autorská práva), ale aktivem může být i samotná organizace, jelikož hrozby mohou působit na celou její existenci. Základní charakteristikou aktiva je hodnota, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti aktiva pro danou organizaci.

Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu. Dělí se na přírodní a fyzické (živelné pohromy, výpadky elektrického proudu), technické a technologické (poruchy počítačů, porucha v síti) a na lidské, které se dále dělí na interní a externí. Lidským hrozbám je věnována kapitola 3.4. Škoda, kterou způsobí hrozba při jednom působení na určité aktivum, se nazývá dopad hrozby. Dopad hrozby může být odvozen od absolutní hodnoty ztrát, do které jsou zahrnuty náklady na znovuobnovení činnosti aktiva nebo náklady na odstranění následků škod. Základní charakteristikou hrozby je její úroveň, která se hodnotí podle nebezpečnosti, přístupu a motivace (6).

Zranitelností rozumíme nedostatek, slabinu nebo stav analyzovaného aktiva, který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Zranitelnost vznikne tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou pro zranitelnost je její úroveň. Úroveň zranitelnosti aktiva se hodnotí podle citlivosti a kritičnosti (4).

Protiopatření je postup, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby, snížení zranitelnosti nebo dopadu. Protiopatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následku vzniklé škody. Z pohledu analýzy rizik je protiopatření charakterizováno efektivitou a náklady, kde efektivita vyjadřuje, nakolik protiopatření sníží účinek hrozby. Mezi cíle protiopatření patří prevence, detekce a korekce.

Samotné riziko vzniká vzájemným působením hrozby a aktiva. Hrozba, která nepůsobí na žádné aktivum, nemusí být při analýze rizik brána v úvahu. Aktivum, na které nepůsobí žádná hrozba, není předmětem analýzy rizik. Úroveň rizika je určena hodnotou aktiva, zranitelnosti aktiva a velikostí hrozby. Tyto položky se také projevují na růstu rizika a jedině protiopatření snižuje vzniklou úroveň (6).



Obr. 8: Vztah pojmů při řízení rizik (Zdroj: (5))

2.3.2 Analýza a identifikace hrozeb

Aby se mohlo hrozbám v organizaci čelit, je nezbytné možné hrozby identifikovat. Identifikace hrozeb může být charakterizována jako pravidelné a kontinuální monitorování všech probíhajících interních a externích událostí, které ovlivňují plnění cílů organizace. U těchto událostí lze rozlišovat negativní a pozitivní dopad. Ty události, které mají negativní dopad, jsou vnímány jako hrozby.

K identifikaci hrozeb by se mělo přistupovat metodicky, aby bylo zajištěno, že byly identifikovány všechny důležité činnosti organizace, a tedy definována všechna rizika z nich vyplývající. Nejistota vyplývající z těchto aktiv by měla být identifikována a kategorizována. Úspěšná a efektivní identifikace vyžaduje rovněž dobrou znalost anatomii hrozeb vyskytujících se v okolí organizace, znalost trhu (prostředí), na kterých organizace operuje. Užitečnou pomůckou může být sestavení diagramů a schémat, která mohou jednoduše a názorně zachytit procesy a činnosti v organizaci, čímž se získá lepší přehled.

Pro identifikaci hrozeb lze vycházet se seznamu hrozeb, sestavených podle literatury, vlastních zkušeností, průzkumů nebo dříve provedených analýz. Hrozby se mohou odvozovat také od postavení organizace na trhu, hospodářských výsledků, případně záměru vedení organizace. Pro získání vlastního seznamu hrozeb organizace je vhodné použít některou z metod jako brainstorming[13], identifikace na základě minulých záznamů nebo metodu Delphi.

[13] Brainstorming je skupinová technika zaměřena na tvorbu co nejvíce nápadu a myšlenek na dané téma.

Každá hrozba se hodnotí vůči každému aktivu. U těch aktiv, na něž se hrozba může uplatnit, se určí úroveň hrozby vůči tomuto aktivu a úroveň zranitelnosti aktiva vůči této hrozbě. Výsledným stavem je seznam dvojic (hrozba - aktivum) se stanovenou úrovní hrozby a zranitelnosti (5).

Tab. 1: Příklady hrozeb z ČSN ISO/IEC 27005 (Zdroj: (4))

Typ	Hrozby	Zdroj
Ohrožení informací	Zachycení kompromitujících interferenčních signálů	Úmyslný
	Vzdálená špionáž	Úmyslný
	Odposlech	Úmyslný
	Krádež médií nebo dokumentů	Úmyslný
	Krádež zařízení	Úmyslný
	Zprovoznění recyklovaných nebo vyřazených médií	Úmyslný
	Vyzrazení	Náhodný, úmyslný
	Data pocházející z nedůvěrných zdrojů	Náhodný, úmyslný
	Falšování pomocí technických vybavení	Úmyslný
	Falšování pomocí aplikačního technického vybavení	Náhodný, úmyslný
	Odhalení pozice	Úmyslný

2.4 Interní hrozby

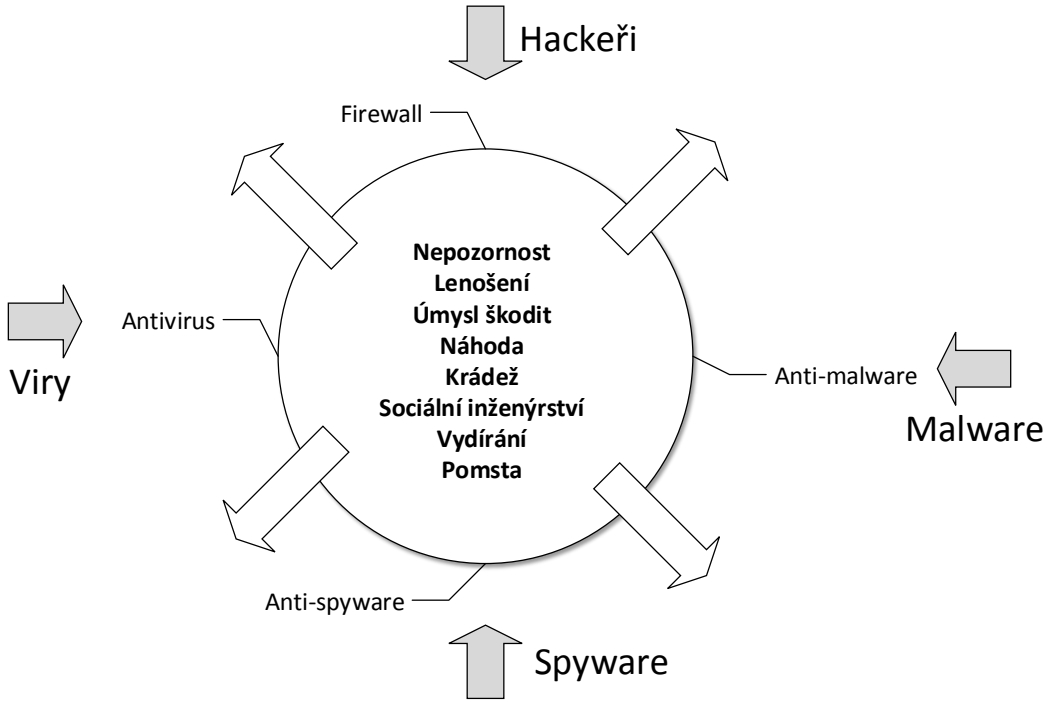
Organizace již více než dvacet let chrání svá citlivá data a IT techniku před útoky hackerů, počítačových virů a mnoha dalšími hrozbami, které útočí a přichází do společnosti z vnějšího prostředí, jako je například internet. I když zodpovědné osoby ve svém životě nepotkají žádného hackera nebo případně autora viru, dokážou investovat do ochrany proti těmto vnějším hrozbám podstatnou část rozpočtu společnosti na IT bezpečnost. Velmi často ignorují druhou skupinu hrozeb, kterou představují samotní zaměstnanci organizace a lidé pohybující se uvnitř. Z toho důvodu se začíná vyvíjet významný tlak na ochranu citlivých dat a informací proti interním hrozbám.

Každá organizace má určený svůj bezpečností perimetr a nelze se spoléhat na to, že veškerá možná nebezpečí leží za tímto perimetrem. Kombinace ochranných prvků a systému tvořených firewallem, antiviry a různými podobnými nástroji vznikal v odlišné situaci a potřebě, než jaká panuje v dnešních společnostech. Ochrana tohoto perimetru získává významné trhliny zevnitř, protože výše jmenované standartní nástroje nedokáží chránit únik a ochranu dat před chybami samotných zaměstnanců, z toho důvodu je bezpečnost velmi omezena.

Mezi pojem interní hrozby se řadí aktivita, případně nedostatek aktivity osoby pohybující se uvnitř společnosti, která vede k úmyslnému poškození společnosti, jak už zhoršení jména, tak zhoršení finanční stránky. Původcem interních hrozeb se může kromě zaměstnanců stát i personál třetích stran, mezi které lze zařadit například

uklízečky, opraváři, kteří mají přímý přístup do kanceláří a pohybují se v bezpečnostním perimetru společnosti.

Přímým hrozbám pocházejícím od vlastních zaměstnanců lze zamezit mnoha možnostmi, ale primární nebezpečí spočívá v postupné ignoraci bezpečnostních opatření ze strany vedení organizace. Management se často spoléhá a opírá o kvalitu svých zaměstnanců a nepřipouští si, že by někteří z nich mohli chtít vědomě poškodit organizaci, ve které jsou zaměstnáni. Manažeři společností často oponují tím, že znají své lidi, se kterými pracují. Může se jednat i o dlouholeté známosti a osobní vztah. Ani to ale nezaručuje, že takový zaměstnanec nemůže být zdrojem rizika. I osoba na zodpovědné pozici s dobrými vztahy s okolím může selhat. Původů nebezpečného chování může být celá řada od neúmyslných až po plně úmyslné. Toto nebezpečné chování při prováděném opakování může vést v budoucnu až ke krachu organizace (16).



Obr. 9: Ukázka porovnání interních a externích hrozeb (Zdroj: Vlastní tvorba pro DP)

2.4.1 Způsob ohrožení organizace zaměstnanci

Existuje mnoho způsobů, jak zaměstnanci můžou poškodit společnost, ať už neúmyslně, nebo v horším případě úmyslně s vidinou případného finančního zisku pro sebe. S dnešním postavením IT v procesech organizace stačí k velkým škodám i několik málo akcí, případně kliknutí. Zaměstnanci za počítačem často nabývají dojem anonymity a neuvědomují si zodpovědnost za své počínání. Email odeslaný omylem na špatnou adresu, externí disk zapomenutý v městské dopravě nebo nedostatečná obezřetnost při dodržování firemních bezpečnostních předpisů jsou jen několik málo věcí, které můžou

způsobit škodu z nepozornosti. Za těmito typy chyb mohou stát problémy s nízkou motivací zaměstnance, příznak vyhoření nebo jen únava a vyčerpání.

Špatná ochrana proti krádeži může zapříčinit ztrátu citlivých dat a údajů. Pachatelé drobných trestných činů si neuvědomují, k jakým datům se mohou dostat při zcizení notebooku nebo přenosných zařízení, mezi které můžeme považovat externí disk a jiné. Podle Výzkumného ústavu Ponemon Institute bylo zjištěno, že během jednoho týdne se pouze na amerických letištích ztratí více než 12 000 notebooků, což dělá téměř 660 000 notebooků ročně s citlivými daty (18). Z toho důvodu se začíná považovat šifrování dat při přenosu na přenosná média a šifrování dat na osobních počítačích za standard.

Úmysl poškodit zaměstnavatele vzniká při rozdílné představě společnosti a zaměstnance při jeho budoucím rozvoji a ohodnocení. Pracovník je méně motivovaný a klesá jeho zapálení a pozornost nebo začíná přemýšlet, jakým způsobem opustit společnost a nejvíce z tohoto kroku vytěžit. Jednotliví zaměstnanci mohou mít podle významnosti a povahy své pozice během pracovní doby k dispozici citlivá data, která mohou zcizit pro začátek vlastního podnikání nebo jako možnost lepší pozice u konkurenční společnosti. Ani okamžité zamezení přístupu k citlivým datům po doručení výpovědi není správným řešením, jelikož zaměstnanec si mohl vytvořit zálohu citlivých dat dříve.

Potřeba řešit nenadálou životní situaci nebo cílené vydírání mohou extrémně rychle zvýšit bezpečností riziko a být spouštěčem nežádoucích aktivit zaměstnance. V takových situacích může chování pracovníka zkratovat a z dříve bezproblémového jedince, se stane bezpečnostní riziko, které se bude aktivně snažit překonat zabezpečení dat společnosti a sabotovat práci svých kolegů ve snaze organizaci poškodit.

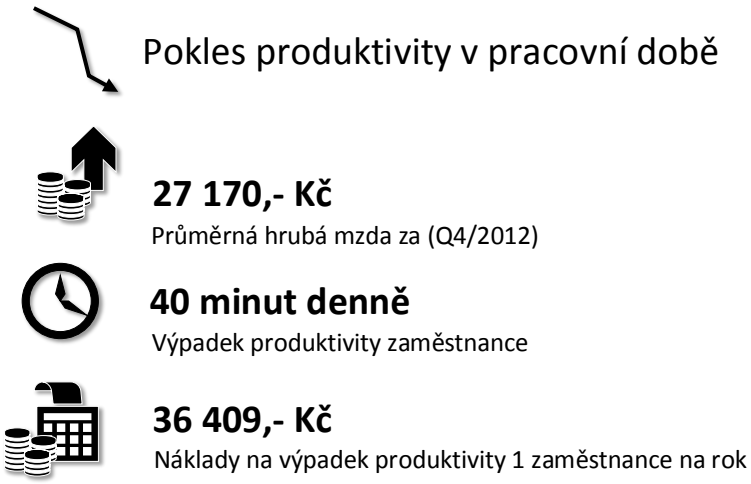
Mezi nejnovější bezpečnostní rizika patří sociální inženýrství. Schopný pachatel je schopen získat v podobě zaměstnance prodlouženou ruku do nitra společnosti a může si dělat cokoliv, k čemu má přístup zneužitý pracovník. Bohužel napadená osoba si není plně vědoma tohoto typu problému, že se stala oběti útočníka.

Loajalitu a spolehlivost zaměstnanců zkoumala mezinárodní společnost Gallup, která se zabývá výzkumem a poradenstvím v oblastech psychologie, managementu a dalších. Studie vycházející z dotazníku Gallup Management Journal Survey (17) ukazuje, že představy vedení společnosti o angažovanosti pracovníků mohou být realitě vzdálené. Pouze 27% zaměstnanců pracuje se zájmem a nadšením pro danou věc a přináší společnosti rozvoj a inovaci. Druhou skupinu (59%) tvoří pracovníci, kteří se necítí být spoluzodpovědní za úspěch podniku. Soustředí se na plnění předepsaných úkolů, avšak nemusí plně využívat svůj potencionál. Poslední a rizikovou skupinu tvoří 14% pracovníků, kteří chodí do práce negativně naladění a svou aktivitou se snaží společnosti spíše škodit než prospívat. Mohou záměrně zdržovat a sabotovat práci kolegů.

2.4.2 Finanční dopad interních hrozeb

Řada společností v současné době optimalizuje náklady, ale často se zaměřují na redukci financí směřujících z firmy k externím subjektům a nevšímají si finančních ztrát, jejichž původ se skrývá uvnitř společnosti. Nízká produktivita zaměstnanců nebo následky úniku citlivých údajů mohou mít přitom na postiženou firmu až zničující efekt.

Zaměstnavatel nemá potřebu bránit v občasném vyhledávání dopravního spoje nebo kontrole menu restaurace. Pokud však míra využívání internetu nebo například tiskáren překročí tolerovanou hranici, znamená každá minuta nebo vytištěná stránka navíc zbytečné náklady pro společnost. Neproduktivní zaměstnanec může mít nepříjemný dopad i na další kolegy, kteří pod dojmem neproduktivity ztrácejí motivaci pracovat. Nežádoucí chování se pak firmou šíří velmi rychle a skutečné ztráty rostou.



Obr. 10: Výpadek produktivity (Zdroj: (26))

Následky ztráty citlivých dat nebo osobních záznamů se sice neprojevují ihned, ale pozvolna a o to horší mohou být případné následky. Vedení každé společnosti by si mělo položit otázku, jakou hodnotu mají informace, které ve společnosti uchováváme a jaké ztráty nám způsobí, pokud se k těmto informacím dostane konkurence.

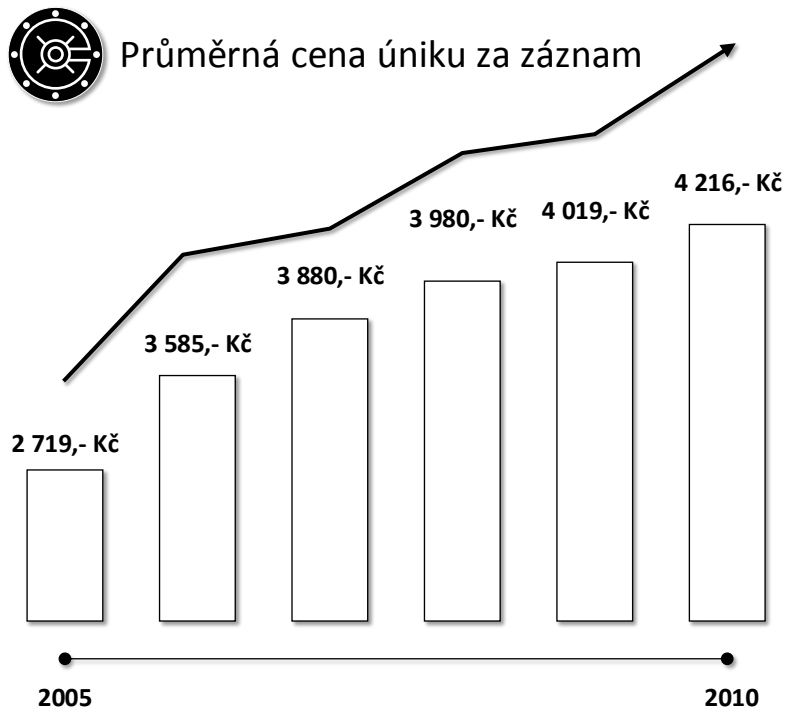
Bohužel si většina společností tyto otázky klade až v době, kdy k bezpečnostnímu incidentu dojde a data uniknou, ať už záměrně (úmyslem zaměstnance) nebo vlivem nepozornosti (ztráta přenosného zařízení, nedostatek zabezpečení).

2.4.3 Náklady spojené s únikem dat

Vyčíslení nákladů spojených s únikem dat je náročný proces, který je závislý na oboru dané firmy, její geografické i tržní pozici. Jasným faktem však je, že škody mohou dosahovat i mnoha desítek procent hodnoty společnosti, zvláště v odvětví, kde hrají informace a záznamy klíčovou roli. Pokud společnost investuje do vývoje nového

produktu a vlivem úniku dat jej konkurence uvede o týden dříve, nelze očekávat návrat investice původnímu autorovi.

Existují i zákonem chráněné osobní údaje, do jejichž kontroly vstupují navíc úřady, které dohlíží na dodržování tohoto zákona (v České republice je to Úřad pro ochranu osobních údajů - ÚOOÚ). Ten může při shledání nedostatečné ochrany osobních údajů uložit subjektu porušujícímu zákon citelnou pokutu (ÚOOÚ v případě právnických osob uděluje pokutu až 10 milionů Kč). Nepřímým dopadem úniku dat je většinou narušená důvěra zákazníků ve společnost a poškození dobrého jména značky. V zahraničí ukládají zákony společnostem povinnost informovat o odhalených únicích dat, tyto případy lze tedy poměrně přesně analyzovat. Výzkumný ústav Ponemon Institute (19) analyzoval jakou cenu má únik dat v různých státech a různých odvětvích. Podíl nákladů na jeden uniklý záznam v roce 2010 dosahoval hodnoty $214 (cca 4216,- Kč). Nejnáchylnější k úniku citlivých informací je veřejná správa (25% všech případů úniků dat) následována zdravotnictvím (15%), školstvím (14%), maloobchodními sítěmi (10%) a finančním sektorem (8%).



Obr. 11: Průměrná cena úniku za záznam (Zdroj: (19))

2.4.4 Snížení rizika ztráty

Problémy, jejichž původ je skryt uvnitř společnosti, mají často odlišný charakter, jejich dopad na firmu však může být ve finále vždy katastrofální. Přitom pro zlepšení situace stačí i bez dalších investic udělat málo. Vedení firem má k dispozici několik postupů,

kterými může nastolit alespoň základní stupeň zabezpečení proti finančním ztrátám způsobeným zaměstnanci.

V otázce bezpečnosti citlivých dat je důležité uvědomit si, že ve společnosti se pracuje citlivými daty a že tato data je potřeba chránit. Nutné je zejména zaměstnancům představit dopady úniku citlivých dat, možné finanční ztráty firmy a s tím např. související potřeba omezení pracovních míst. Rámec povinnosti ochraňovat utajované informace může být podchycen ve smlouvě nebo v dodatku smlouvy nazývané často dohoda o důvěrnosti (nebo o utajení, v anglicky mluvících zemích často Non-Disclosure Agreement). V tomto dokumentu si obě strany definují rozsah citlivých dat a své povinnosti při jejich ochraně a při případném prozrazení. Povinnost zaměstnance chránit zpracovávané osobní údaje je mu dána také zákonem (zde 101/2000 Sb., o ochraně osobních údajů), speciálně sepsaná dohoda však může pokrýt daleko širší rámec než jen zpracovávání osobních údajů. Obě strany si navíc mohou být jisty srozumitelností a rozsahem ochrany bez nutnosti studia paragrafů.

Další formou úmluvy mezi zaměstnancem a zaměstnavatelem je tzv. dohoda o přijatelném využívání zdrojů (Acceptable Use Policy), která vymezuje používání zdrojů zaměstnavatele pro pracovní i nepracovní využití ze strany zaměstnance. V ní je možné definovat, jaké chování zaměstnance je ještě přípustné při využívání firemních počítačů, programové výbavy, internetu a dalších zdrojů zaměstnavatele. Nejčastěji se dokument vyhraňuje proti využívání internetu a emailové komunikace. V dohodě bývají typicky uvedeny časy pro zákaz používání internetu a emailu k osobním účelům. Dále může dokument zakazovat stahování a instalování neautorizovaného softwaru, který by mohl ohrozit chod počítačové sítě a může stanovit zákaz uchovávání materiálů podléhajících autorským právům třetích stran na firemních počítačích. V případě porušení této dohody jsou definovány konkrétní postihy takového jednání (typicky omezení daného zdroje či vyšší kontrola, v případě závažného porušení i rozvázání spolupráce). Odsouhlasením podobné dohody dojde k vytvoření jasného mantinelu, ve kterém se budou zaměstnanci pohybovat.

Nelze se domnívat, že samotné zavedení represivních pravidel zajistí neprůstřelnou bezpečnost dat a maximální produktivitu zaměstnanců. Se zaměstnanci je potřeba o provedených opatřeních diskutovat, vysvětlit jim jejich důvod a odhalit ve spolupráci s nimi problémy, které již ve firmě existují nebo se aktuálně vytvářejí. Je třeba personálu vysvětlit, že nejde jen o obtěžování lidí, ale zaváděné změny budou mít v dlouhodobém horizontu pozitivní efekt na všechny zúčastněné. Dalším krokem po zavedení nových pravidel je sledování jejich naplňování a vyhodnocování efektivity zvoleného řešení. Každá změna je zaváděna s určitým cílem a očekáváním, proto je potřeba zjistit, jestli zvolené řešení k naplňování cíle směřuje.

2.5 Omezení interních rizik

Management společnosti není často schopný v rámci svého pracovního nasazení a denní agendy věnovat čas vynucování pravidel stanovených ve smlouvách a dohodách se zaměstnanci a předcházet tak problémům. S každodenním vynucováním může pomoci několik typů bezpečnostního softwaru, určených ke sledování produktivity zaměstnanců, blokování nevhodných aktivit či poskytujících ochranu před únikem dat (DLP - Data Loss Prevention software). Navíc mohou být popsané typy softwaru jediným způsobem pro získávání důvěryhodných důkazů o porušování podepsaných smluv v případě právních sporů.

2.5.1 Monitorování zaměstnanců

Praxe ukazuje, že zaměstnanci, kteří mají v pracovní době přístup k internetu, se často věnují vedle plnění pracovních úkolů i činnostem, které s programováním, analytickou činností či servisní činností příliš nesouvisí. Je tím na mysli oblíbené surfování po internetu, chatování či trávení času na sociální síti. Každý zaměstnavatel si jistě položil otázku, jak tyto aktivity vyloučit, respektive minimalizovat na přijatelnou míru. Z pohledu zaměstnavatele jakákoliv delší aktivita mimo plnění pracovních úkolů znamená kromě zbytečně vynaložených mzdových nákladů i ztrátu zisku.

Monitorovací software umožňuje vedení společnosti získat informace o skutečném pracovním nasazení jednotlivých zaměstnanců i celých pracovních skupin nebo oddělení. Podle způsobu nasazení softwaru do firemní infrastruktury rozlišujeme monitoring síťový a na koncové stanici. První typ sleduje provoz v síti, druhý pomocí agenta na každé stanici monitoruje i aktivitu, která se neděje na síti (hraní her apod.). Nevýhodou monitoringu je jeho bezzubost. Sám sice poskytuje cenné údaje o chování zaměstnanců, při napravování problematického chování však nechává všechnu práci na managementu společnosti. Přirovnání ke sledování výtržníků na bezpečnostních kamerách je sice příliš hrubé k zaměstnancům, nejlépe však demonstruje vztah mezi monitoringem a škodou, před kterou sice může varovat, ale sám jí nezabrání.

2.5.1.1 Právní stránka monitorování zaměstnanců

V případě nasazení monitorovacích prostředků na ochranu před interními hrozbami je potřebné brát ohled na více okolností. Z právní stránky dochází totiž na pracovišti ke střetu práv zaměstnavatele a zaměstnance. Tento střet je tedy třeba vhodně vymezit a vést monitorování tak, aby bylo v souladu s platnou legislativou a bylo transparentní oběma stranám.

Zaměstnanci jsou povinni dle zákoníků práce pracovní dobu a výrobní prostředky (tedy i počítač) využívat k pracovní činnosti a tu vykonávat kvalitně a včas. Krom toho je povinností každého zaměstnance řádně hospodařit s prostředky svěřenými ze strany

zaměstnavatele a užívat je pouze v souvislosti s vykonávanou prací. Užívat k osobním účelům počítač a telefon, případně další pracovní prostředky, je oprávněn zaměstnanec pouze s předchozím souhlasem zaměstnavatele. Tomu zákon umožňuje přiměřeným způsobem kontrolovat, zda zaměstnanec nezneužívá svěřené prostředky. Cílem kontroly je i zjištění, zda zaměstnanec všechny uložené pracovní úkoly plní řádně a včas (8).

Naproti tomu stojí zákonné právo zaměstnance na ochranu jeho soukromí. Zaměstnavatel tak nesmí bez závažných důvodů narušovat soukromí zaměstnance na pracovištích a ve společenských prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci (8).

Určení mantinelů dovolené a zakázané kontroly zaměstnance používajícího internet je z právního hlediska někdy sporné. Přesto lze najít v zákoně a jeho výkladu vodítko, které by mělo vyváženým způsobem říci, co se smí a co už není z pohledu zaměstnavatele dovoleno. Způsoby monitoringu zaměstnance jsou podmíněny předchozí informací o zavedení takového způsobu kontroly. Zákoník práce v tomto stanoví: *„Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.* ‘‘ (8, str. 85). Zaměstnanec musí být předem upozorněn o kontrolních mechanizmech. Závažný důvod pro kontrolu zaměstnanců je dán v případě, že zaměstnanec pracuje s finančními prostředky zaměstnavatele nebo má přístup a přímo pracuje s obchodním tajemstvím, případně citlivými firemními informacemi.

O monitoringu pouhých přístupů na internet (navštívených stránek, délky přístupů) a práce s počítačem na druhou stranu zaměstnavatel informovat nemusí. V praxi lze jen doporučit, aby společnost informovala své zaměstnance o monitorování přístupu na internet a práce s počítačem.

Zákoník práce a jeho výklad vymezuje dovolené a zakázané způsoby monitoringu práce zaměstnance, včetně nutnosti splnění podmínek předchozího informování zaměstnance o způsobu kontroly (8).

Obr. 12: Kontroly zaměstnanců (Zdroj: (8))

2.5.2 Blokování uživatelské činnosti

Blokování nežádoucích aktivit uživatelů omezuje rušivé faktory a rozptýlení, kterému pracovníci čelí. Nejedná se však pouze o nástroj pro zvýšení produktivity, ale i o důležitou součást bezpečnostních procesů. Podobně jako nástroje proti úniku dat, se kterými blokování tvoří klíčové prvky informační bezpečnosti firem.

Aby blokování mohlo efektivně fungovat a přinášet zamýšlený efekt, není vhodné podceňovat úvodní fázi nasazení a nastavení pravidel. Důležité je správně určit, co a pro jakou skupinu bude blokováno. Nejlépe, pokud se v úvodní fázi nejdříve nasadí monitorovací software, který poskytne přehled, jaké aktivity uživatelé na počítači provádějí – přístupy na webové stránky, využití aplikací, tisk apod., a až následně pomocí blacklistingu[14] či whitelistingu[15] se provede dané blokování. U blacklistingu může být komplikované nastavit správně seznam položek, aby obsáhl všechny nežádoucí aktivity. Často se stává, že jich zůstane řada povolena, protože při určování pravidel není možné pamatovat na vše. Tato starost s dobrým programem, který obsahuje kvalitní klasifikaci webových stránek a aplikací, odpadne.

[14] Blacklisting obsahuje seznam položek, které jsou zakázané využívat. Ostatní položky neuvedené v seznamu se smí používat.

[15] Whitelisting obsahuje seznam povolených položek, vše co není obsaženo je považováno za zakázané.

2.6 Ochrana před ztrátou dat

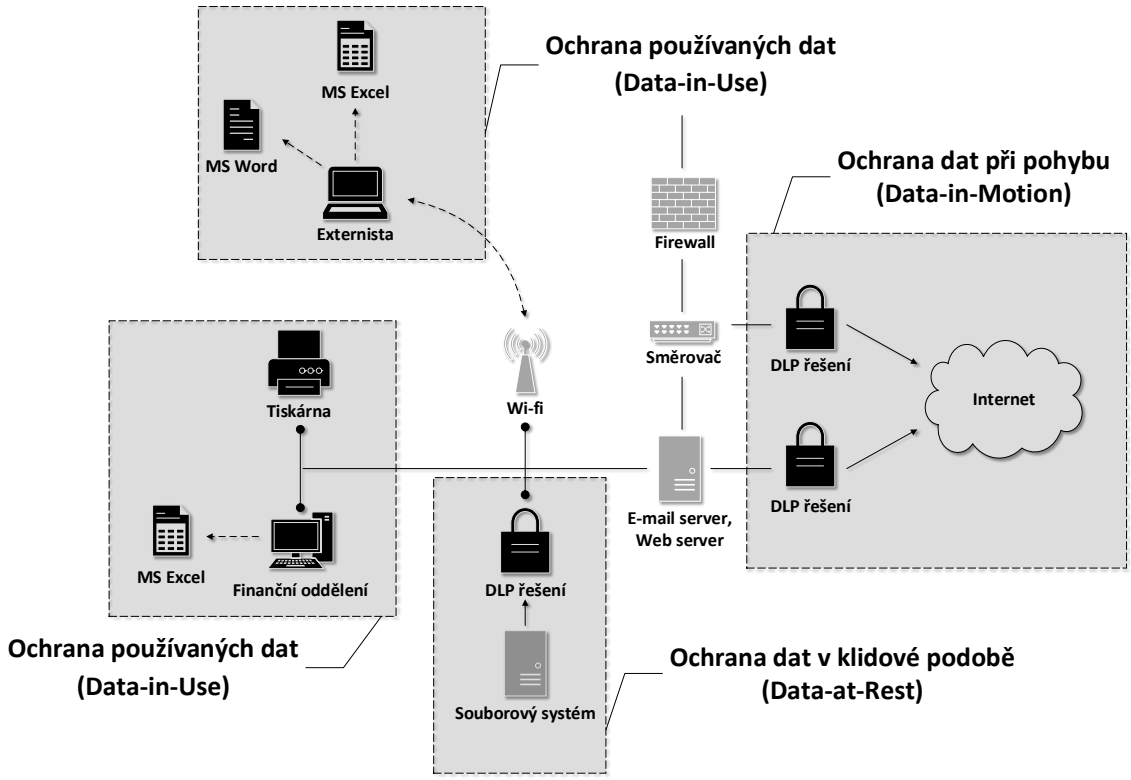
Současné trendy informační a komunikační bezpečnosti pomalu opouštějí od pasivního pohledu na práci s daty. Dříve stačilo jasně vymezit, kdo má k datům jaký přístup a odkud, ale s masivním rozvojem informačních technologií tento pohled není úplný. Problém nastává, pokud chce společnost kontrolovat, co se s daty děje poté, co byla zpřístupněna autorizované osobě a jak správně zaručit, že se tato osoba bude řídit interní bezpečnostní politikou. Kromě toho, že data mohou být vynesena zcela úmyslně, je důležité se také zaměřit na úniky z nepozornosti.

Ochrana před ztrátou dat (data loss prevention, neboli DLP) je termín z oblasti informační bezpečnosti, který představuje systémy schopné identifikovat, monitorovat a chránit data společnosti. Zajišťuje, aby k citlivým datům (informacím) měly přístup pouze autorizované osoby a aby tyto osoby manipulovaly se svěřenými daty pouze povoleným způsobem na základě interních bezpečnostních politik a nařízení. Pojem DLP jakožto ochrana před ztrátou dat je někdy nahrazován výrazy ILDP (Information Leak Detection and Prevention – prevence proti úniku dat) nebo CMF (Content Monitoring and filtering – monitorování a sledování obsahu) (20).

Hlavním cílem DLP systému[16] je na základě bezpečnostní politiky společnosti analyzovat (klasifikovat), monitorovat a chránit důvěrná data. Z toho důvodu lze DLP rozdělit na 3 základní části:

a) Ochrana používaných dat (data in use) se zaměřuje na každodenní interakci zaměstnanců s daty na koncových stanicích a dohlíží, jak je s daty nakládáno, kam se kopírují, jestli jsou upravovány a kdo je otvírá.
b) Ochrana dat při pohybu (data in motion) zabezpečuje ochranu dat a datový tok po síti nebo z koncové stanice na externí zařízení. Díky tomu chrání data proti náhodným nálezcům i zlodějům, případně posílání dat po síti.
c) Ochrana dat v klidové podobě (data at rest) znamená zabezpečení datových uložišť (center), kde se nachází citlivé informace. Používají se různé šifrovací algoritmy nebo virtuální disky pro větší úroveň bezpečnosti (13).

[16] Pojem DLP systém značí pouze samotnou aplikaci (produkt), která je naistalována ve firemním prostředí. Naproti tomu DLP řešení zahrňuje centralizovanou správu pro vytvořenou bezpečnostní politiky a prosazuje tuto politiku ve firemních procesech za pomocí monitoringu a ochrany dat. Dostupné uživatelské rozhraní řeší ekonomicko-technické problémy, které nastaly na základě úniku dat.



Obr. 13: Pohyb dat ve společnosti (Zdroj: Vlastní tvorba pro DP)

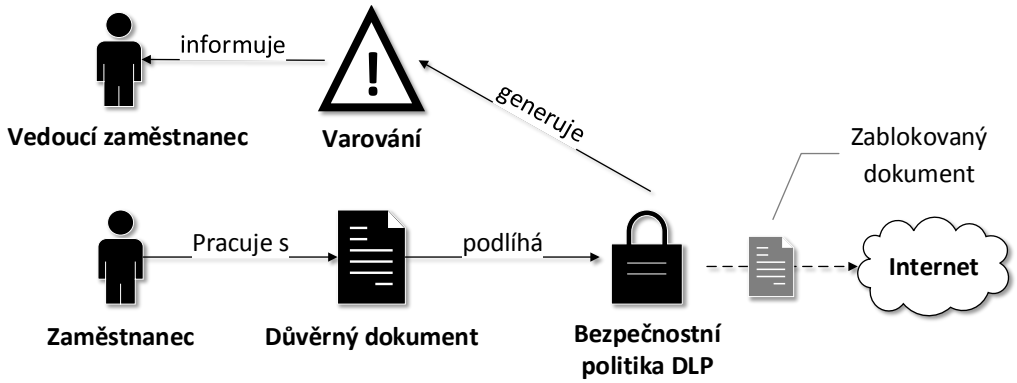
2.6.1 Bezpečnostní politika a události DLP systému

Aby celý systém DLP fungoval správně a dobře reagoval na vzniklé bezpečnostní události[17], je důležité, aby si společnost určila, co chce chránit a před čím. K tomu slouží bezpečnostní politika DLP definující, kteří zaměstnanci a jaké operace mohou a nemohou provádět s důvěrnými daty.

Zaměstnanec společnosti má v náplni své práce vytváření a upravování finančních dokumentů (faktury, výplatní pásky), kde tyto dokumenty obsahují důvěrná interní data (rodná čísla, bankovní účty) a bezpečnostní politika[18] DLP je nastavena tak, že omezuje posílání těchto dokumentů na internetovou síť. Pokusí-li se i přes to zaměstnanec dokument zaslat, vzniká bezpečnostní událost, na kterou je upozorněn příslušný vedoucí (bezpečnostní technik) a celá událost je díky správné bezpečnostní politice DLP zaznamenána.

[17] Bezpečnostní událost je identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací (2).

[18] Bezpečnostní politika jsou pravidla, směrnice a zvyklosti určující způsoby, pomocí kterých jsou v dané organizaci a jejich systémech řízena, chráněna a distribuována aktiva, včetně citlivých informací (2).



Obr. 14: Bezpečnostní událost DLP (Zdroj: Vlastní tvorba pro DP)

Spolehlivost zabránění úniku důvěrných informací pomocí DLP systému plně závisí od kvality specifikace bezpečnostní politiky. Nekvalitní a nekoncepční návrh bezpečnostní politiky může způsobit nefunkčnost systému DLP a podpořit tak únik důvěrných informací.

2.6.2 Klasifikace dat

Základním předpokladem pro spolehlivost DLP systému je také, že se dostane ke správným a relevantním datům. Je zřejmé, že veškerá data nebudou uložena v čistě textovém formátu, aby je mohl software bez problému zpracovat, a proto je nezbytnou funkcí DLP znalost formátu různých souborů a datových struktur, jako jsou dokumenty MS Office, aplikací CAD a mnoho jiných. Má-li se nástroj dostat správně k citlivým datům, je potřeba, aby uměl provést vhodnou a inteligentní klasifikaci dat[19] (analýzu dat), díky tomu lze následně určit, která data jsou pro společnost důležitá a předmětem aplikování bezpečnostní politiky. DLP systém dokáže data klasifikovat podle dvou hlavních principů, a to klasifikace podle kontextu a podle obsahu (například kontext znamená obálku s informacemi o příjemci a obsah je list papíru, který je vložen v obálce) (13).

Základní způsob klasifikace dat je za pomocí kontextu, kdy DLP systém dokáže data najít a identifikovat podle těchto pravidel:

a) Podle lokality uložení dat, zda se data nachází na databázovém serveru nebo v adresáři lokálního počítače.
b) Podle používané aplikace jako je například MS Office (.xlsx, .docx a jiné), z tohoto důvodu DLP systémy obsahují předdefinovaný katalog přípon a aplikací.
c) Podle přesného, nebo podobného názvu souboru za pomocí klíčového slova.
d) Podle uživatele, který data používá.

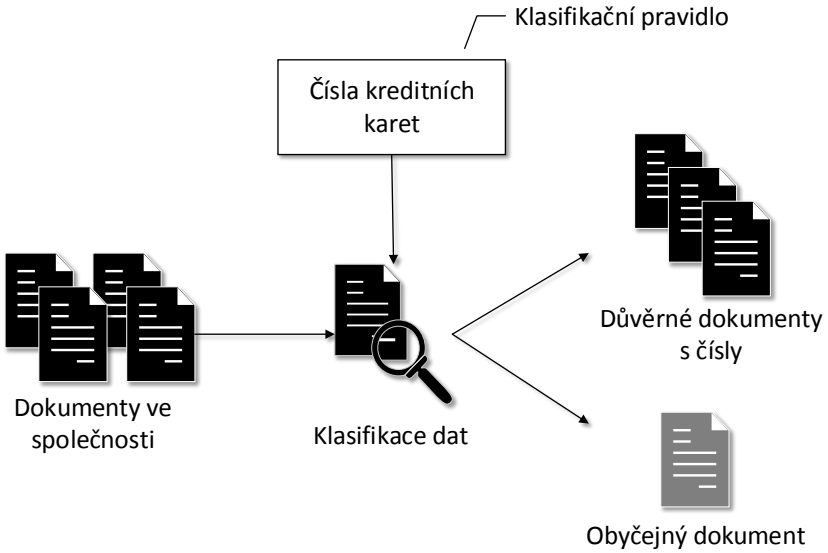
[19] Klasifikace dat je rozdělení datových souborů na základě definovaných pravidel do předem daných tříd (23).

Kontextová klasifikace má nevýhodu, že nedokáže pracovat s obsahem binárních souborů a nedokáže zjistit, zda soubor obsahuje v sobě důvěrné informace, které jsou předmětem bezpečnostní politiky. Z toho důvodu dává větší smysl používat i klasifikaci na základě obsahu dat.

Klasifikace podle obsahu není náročná pro obyčejný textový dokument, jakým je například obsah emailu. Problém se velice komplikuje při binárních souborech, kde dostat se k samotnému obsahu je velmi komplikované. Systémy DLP tento problém řeší pomocí metody nazývané cracking souborů. Cracking souborů je technologie, která se používá ke čtení obsahu souboru, i když je obsah uložený v několika vrstvách (například Excel tabulka vložena do dokumentu Word a ten je ještě komprimovaný – první se musí dekomprimovat soubor, analyzovat dokument Word a v něm najít zmiňovanou tabulku a až následně provést analýzu tabulky). Tento problém dokáže být ještě komplikovanější například při použití CAD souboru a následné uložení do dokumentu PDF. Na takto objevený obsah lze použit již několik metod analýz nebo technik, jakými jsou (13):

a) Analýzy pomocí regulárních výrazů (čísla kreditních karet, rodná čísla a jiné).
b) Databázový otisk (exact data matching) je technika, kdy se hledá přesná shoda mezi používanými daty a daty uloženými v databázi.
c) Částečná shoda dokumentů (partial document matching) je analýza, která v dokumentu hledá kompletní nebo částečnou shodu (pouze věty) s předdefinovaným obsahem.
d) Statická analýza, která využívá strojové učení a jiné statistické metody pro analýzu dokumentu.
e) Analýza za pomocí kategorií a slovníku je nejméně účinná technika, kdy dochází k velkým chybám. Dokumenty analyzuje na základě předdefinovaných klíčových slov, případně kategorií.

Takto nalezená a klasifikovaná data se mohou označit (pomocí speciálního označení, kterému rozumí DLP systém) za důvěrné a mohou se seskupovat do datových kategorií (jako jsou finanční data, obchodní data, smlouvy s partnery, procesy společnosti), na které lze aplikovat bezpečnostní politiku, definovanou za pomocí DLP systému (15).



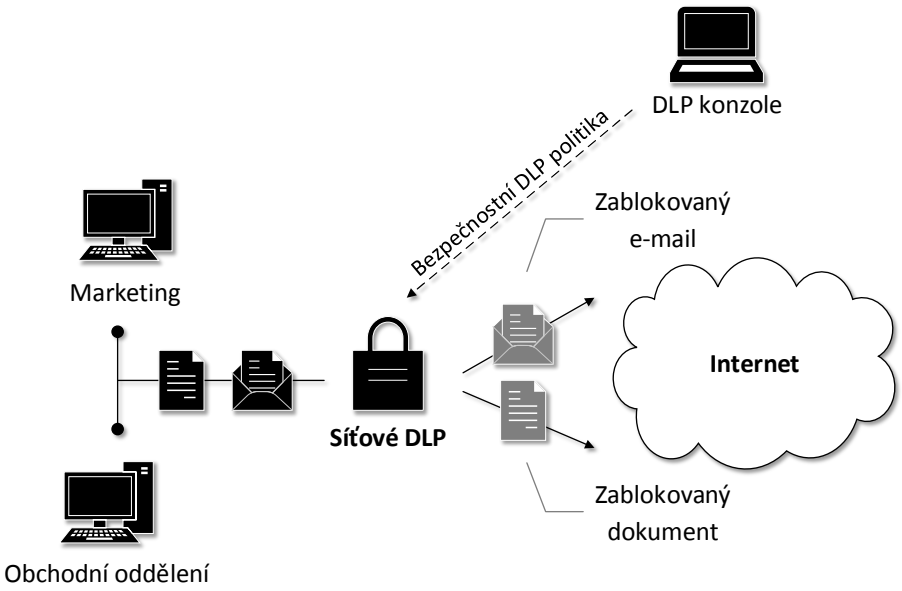
Obr. 15: Ukázka principu klasifikace dat (Zdroj: Vlastní tvorba pro DP)

2.6.3 Způsob monitorování DLP systému

V úvodu kapitoly 3.6 je zmíněno, že DLP systém lze rozdělit na 3 základní části (ochrana používaných dat, dat při pohybu a dat v klidové podobě). Aby mohl DLP systém plnit tyto funkce, musí být implementován do firemní sítě (Network DLP) nebo přímo na koncové stanice (Endpoint DLP, někdy označované jako Host-based DLP).

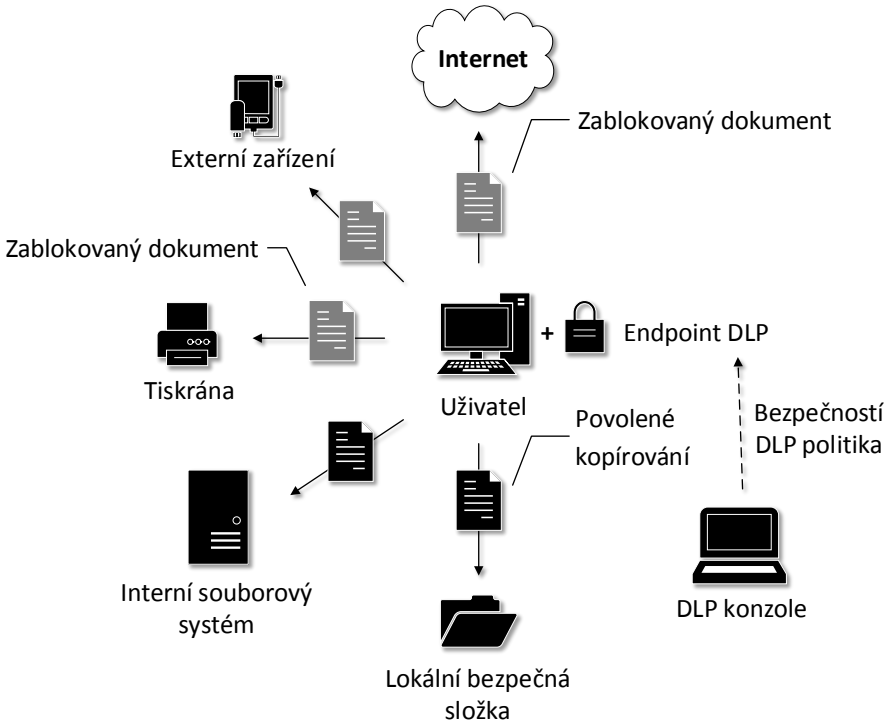
Síťové DLP pomáhá společnosti chránit data na úrovni síťového perimetru a dokáže zabránit pokusům o únik citlivých dat na úrovni vnější komunikace, tedy hlídá, která data opouštějí firmu po síti. Často se jedná o samostatné zařízení, instalované do sítě společnosti, nejlépe u připojení k internetu. Díky tomu se skenují data uložena na všech dostupných síťových uložištích a identifikují, kde se citlivá data nachází a kdo je jejich majitelem. Využívají k tomu výše zmiňované principy klasifikace dat. Nejčastěji sledovanou komunikací je elektronická pošta, popřípadě komunikace prostřednictvím protokolů FTP, http nebo dokonce i HTTP. Celkově se jedná o jednodušší řešení, které je méně náročné na implementaci a nabízí nižší TCO[20] (celkové náklady vlastnictví) než koncové DLP systémy (13).

[20] TCO jsou celkové náklady vlastnictví a počítající se jako pořizovací náklady aktiva + provozní náklady aktiva nebo produktu (25).



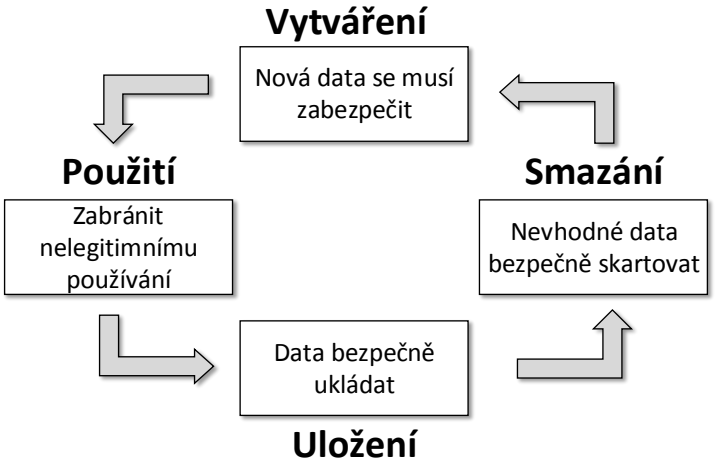
Obr. 16: Princip fungování síťového DLP (Zdroj: Vlastní tvorba pro DP)

V případě koncového systému DLP jsou hlídány přímo aktivity uživatele, které provádí na koncové stanici, jako je například monitorování aplikací, které pracují s důvěrnými soubory. Stejně jako síťové DLP, kontrolují komunikaci mezi interními skupinami uživatelů a mezi interními a externími subjekty. Rovněž mohou kontrolovat emailovou komunikaci a také používání komunikačních programů, ovšem v rozmezí zákona (kapitola 2.5.1). Hlavní výhodou koncového DLP systému je schopnost kontroly přístupu na fyzická zařízení (externí disky, DVD mechaniky, mobilní komunikační zařízení), stejně jako schopnost kontrolovat fyzické komunikační porty stanic, kde mezi ně patří také řešení pro šifrování disků (FDE – Full Disk Encryption) či souborů a složek na pevných discích (FFE – File and Folder Encryption). Nevýhodou zde jsou větší finanční náklady i náročnost na implementaci, jelikož bezpečnostní technici spravují stovky až tisíce počítačů. Naprostou nutností je mít systém, který obsahuje efektivní centralizovanou správu, díky níž lze ušetřit jak náklady, tak i čas pro plné nasazení (14).



Obr. 17: Princip fungování endpoint DLP (Zdroj: Vlastní tvorba pro DP)

Při ochraně dat je potřeba pamatovat i na nebezpečí plynoucí z možnosti obnovení smazaných dat a pro citlivé údaje používat datové skartovačky, které daný sektor disku opakovaně přepíší množstvím náhodných údajů. Na tento proces je nutné pamatovat vždy před prodejem firemního hardwaru, přesunu zařízení od jednoho pracovníka k jinému apod.



Obr. 18: Životní cyklus dat (Zdroj: Vlastní tvorba pro DP)

2.7 Prevence proti interním hrozbám

Jako DLP (Data Loss Prevention) systémy bývají často označovány i různé programy, které obsahují málo nebo vůbec žádné preventivní prvky. V případě, že dojde k neautorizovanému přístupu k citlivým informacím či pokusu o jejich vynesení nepovoleným způsobem, DLP software zasáhne a danou operaci znemožní, v lepším případě zašle také upozornění bezpečnostnímu manažerovi nebo nadřízenému zaměstnanci. V podstatě však reaguje až na právě probíhající nebezpečí, kterému data zrovna čelí a tomu se snaží zabránit. Co bylo příčinou pokusu o únik dat a proč k němu došlo, již základní DLP systém neřeší. Důležité je však zjistit i skutečnou příčinu incidentu, jinak společnost riskuje další a další pokusy zneužití citlivých informací. V případě, že za pokusem o únik dat stojí snahy konkurence, nic jí nebrání zkoušet své praktiky znovu a znovu také na dalších zaměstnancích. Dalšími zdroji nebezpečí může být nespokojený zaměstnanec, nabídka lepší práce od konkurence, akutní potřeba peněz nebo nepozornost způsobená ztrátou motivace.

Jistý preventivní prvek je obsažen v již samotném nasazení DLP softwaru, jehož přítomnost může skutečně preventivně odradit zaměstnance od vynášení dat. DLP je potřeba vnímat jako poslední instanci před tím, než je společnost skutečně poškozena. Jde o nezastupitelný prvek informační bezpečnosti firmy, nejde však o prvek jediný, proto je potřeba skutečnou prevenci úniku dat doplnit o další bezpečnostní řešení nejen softwarové, ale i administrativní.

Z hlediska organizačního má smysl, aby každý zaměstnanec měl přístup pouze k informacím, které potřebuje ke své práci. Jednou z častých příčin úniků dat je i prostá lidská zvědavost, kdy zaměstnanci zkoumají data, která bezprostředně nepotřebují. Administrativně je vhodné chránit se před selháním zaměstnanců dohodou o důvěrnosti (NDA – Non-disclosure Agreement) a směrnicemi[21] definujícími povinnosti pracovníků v oblasti práce s citlivými daty.

Softwarově je možné se chránit správně zvoleným DLP systémem spojeným s monitorovacími funkcemi, které sledují aktivity jednotlivých uživatelů nakládajících s citlivými údaji společnosti. Chování každého zaměstnance není nějakou konstantou, v čase se mění a může mít různé tendence (ať již pozitivní či negativní). Je proto užitečné mít software, který všechna zaznamenaná data umí zpracovat a vyhodnotit krátkodobé i dlouhodobé odchylky a trendy. Lze tak odhalit zaměstnance, kteří ztratili motivaci k práci či vykazují kritické odchylky od vlastního normálu, což může naznačovat nekalé úmysly a potencionální hrozbu pro citlivá data společnosti. Rizikové chování zaměstnanců je zjištěno již v jeho počátku, než dojde ke vzniku škod. V takovémto případě je možné mluvit o skutečné prevenci úniku dat.

[21] Směrnice je doporučení toho, co se očekává, že má být provedeno, aby byl dosažen určitý cíl (1).

3 ANALÝZA PROBLÉMU A SOUČASNÁ SITUACE

V praktické části diplomové práce je popsána metodologie zavádění DLP řešení do organizace na základě ISMS principů a poznatků z reálných obchodních styků. První část se zabývá popisem společnosti a seznamem problémů, kterým v současné době čelí a musí je vyřešit, případně minimalizovat.

3.1 Informace o společnosti

Společnost <*utajená*> působí na trhu od roku 2004 a aktivně spolupracuje se svými zákazníky a partnery na profesionálních řešeních jejich požadavků ve všech oblastech své činnosti, mezi které patří hlavně implementace a vývoj bezpečnostního softwarového produktu. Rovněž poskytuje společnost <*utajená*> náročná projektová, technická, technologická a systémová řešení spojená s kompletními dodávkami a implementacemi softwarového produktu k cílovému zákazníku.

Za pomocí aktivní spolupráce, odborných znalostí a kvalitní práce zaměstnanců společnosti, bylo vybudováno mnoho dlouhodobých a trvalých vztahů s významnými koncovými zákazníky a partnery působícími na světovém trhu. Mezi hlavní zákazníky se řadí nadnárodní společnosti, stejné jako společnosti s několika málo zaměstnanci působící pouze na lokálním trhu. I tyto malé společnosti mají plnou podporu a přístup k informacím a znalostem.

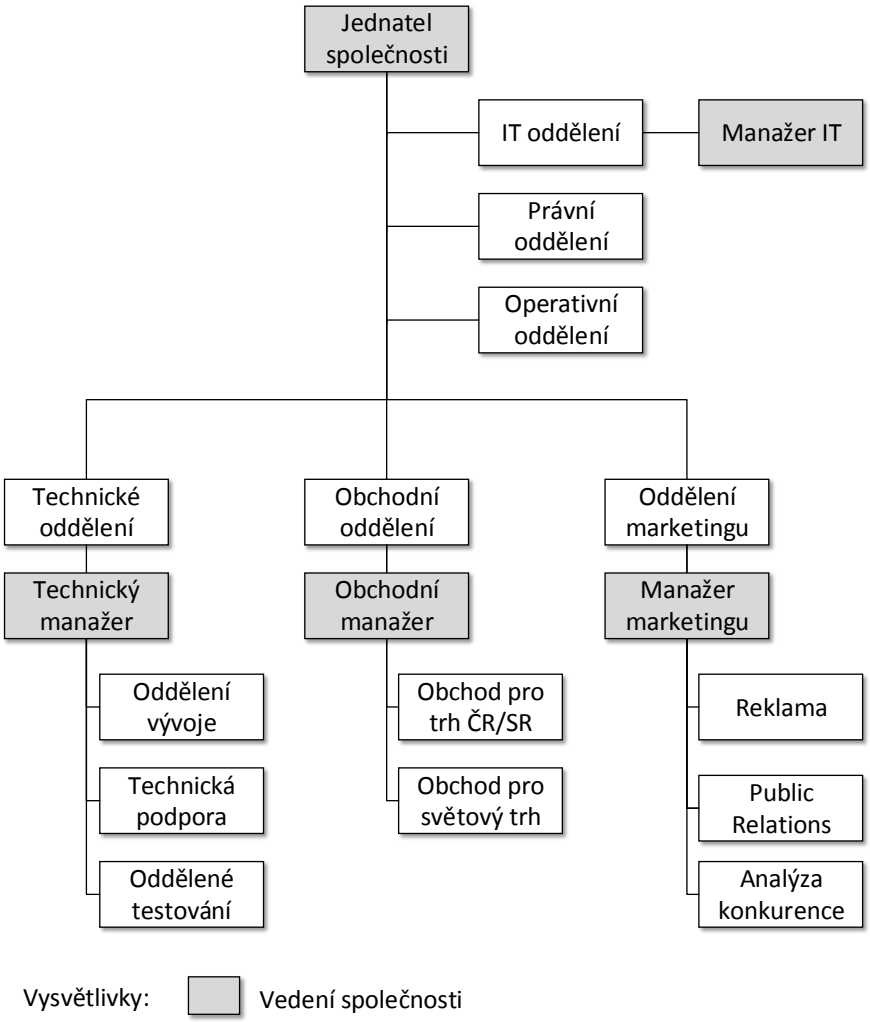
V současné situaci a za pomoci aktivního rozvoje je ve společnosti zaměstnáváno přes 50 stálých zaměstnanců a také společnost úzce spolupracuje i s řadou dalších externích specialistů, kteří se věnují specifickým problémům při vývoji softwarového produktu a dodávce služeb. Politika neustálého zvyšování odbornosti zaměstnanců je zárukou vysoké kvality produktu a poskytovaných služeb. Sídlo společnost <*utajená*> se nachází v Brně a od roku 2010 s obchodní pobočkou v Praze.

Hlavní myšlenkou je být prospěšným článkem lidské společnosti respektující svět kolem sebe, přinášející druhým svou prací služby a produkty, které budou užitečné. Každá činnost pro zákazníka musí být přínosem pro obě strany, kde výsledkem takové činnosti bude kvalitní základna dlouhodobého, rovného obchodního vztahu. Společnost stále přináší svým zákazníkům nová, moderní a perspektivní řešení. Chce být u vznikání těchto řešení a podílet se na jejich realizaci. Mezi hlavní hodnoty, kterými se naplňuje pracovní nasazení je profesionalita, spolehlivost, slušnost, sensitivita a sofistikovanost.

3.1.1 Organizační struktura společnosti

Analyzovaná společnost <*utajená*> obsahuje několik hlavních oddělení (IT, právní, operativní, technické, obchodní a marketing), které jsou organizovány do liniové

organizační struktury[22], kde hlavní zodpovědnost za vedení společnosti přejímá jednatel (majitel). Další pravomoci jsou delegovány na nižší subjekty a jednotliví manažeři se aktivně podílí na vedení společnosti.



Obr. 19: Organizační struktura společnosti <*utajená*> (Zdroj: Vlastní tvorba pro DP)

Ředitel společnosti odpovídá za celkový chod společnosti, za řádné hospodaření se svěřeným majetkem a za jeho ochranu, za dodržování právních předpisů společnosti. Zastupuje společnost navenek ve věcech, které se týkají její činnosti. K zajištění činnosti společnosti vydává příkazy, které jsou závazné pro všechny zaměstnance. Deleguje své pravomoci na další pracovníky v souladu s organizačním řádem. Jsou mu podřízeny všechny organizační útvary společnosti.

[22] Liniová organizační struktura je jedním z typů formální organizační struktury. Jde o jedno ze základních organizačních uspořádání. Pozice a vztahy nadřízenosti a podřízenosti jsou uspořádány a orientovány vertikálně. Každý nadřízený má jasně přidělené podřízené a každý podřízený má jasně přiděleného nadřízeného (22).

Hlavním cílem IT oddělení je zabezpečit a podporovat chod podnikové strategie, kde funguje jako technologický garant zavádění nových inovací a řešení (webové a produktové stránky, CRM systémy, datové sklady, zavádění DLP řešení v rámci ISMS a mnoho dalších). Musí tedy aktivně spolupracovat s iniciátory těchto inovací a podílet se na porovnání přínosů a nákladů zavádění a údržbě těchto inovací.

V právním a operativním oddělení je řešena problematika lidských zdrojů, mzdy, účetnictví a smluvní položky se zákazníky (partnery) nebo zaměstnanci. Podporuje všechna oddělení společnosti v právních záležitostech, ale také včas předchází sporům. Pomáhá managementu v obchodních rozhodnutích pro zajištění rychlého a efektivního uzavření obchodu. Oddělení má přístup ke všem právním dokumentům společnosti, které jsou považovány na vysoce interní (obchodní smlouvy, pracovní smlouvy) a neměly by se dostat z bezpečnostního perimetru společnosti.

Technické oddělení má na starosti kompletní vývoj, testování a nasazení softwarového produktu u zákazníků. Poskytuje rozsáhlá technická školení pro partnery a poskytuje zákaznickou podporu a služby s tím spojené. Zaměstnanci v tomto oddělení pracují a využívají firemní znalosti a informace, které transformují do finální podoby produktu. Jedná se z pohledu bezpečnosti o klíčové oddělení, kde je nutné zabezpečit informace proti šířením, případně vyzrazením mimo společnost.

Obchodní oddělení odpovídá za kvalitní a úplné služby zákazníkům v oblasti realizace zakázky a spolupráci s partnery. Vytváří obchodní strategii (realizace cenové a obchodní politiky) a vyhledává nové možnosti na trhu. Velice důležitá úloha je získávání zpětných vazeb od zákazníků, které se dostávají až do technického oddělení, které na ně reaguje. Oddělení pracuje s interními informacemi a má přístup k finančním dokumentům společnosti.

Práce oddělení marketingu je primárně zaměřena na styk s veřejností, zajištění propagačních aktivit společnosti a řízení marketingové komunikace (hromadná korespondence, internet, public relations a jiné). Díky tomu buduje povědomí o značce a vztahů se zákazníky. Důležitou aktivitou pro ostatní oddělení je tvorba konkurenčního zpravodajství (competitive intelligence[23]). Materiály kolující v oddělení marketingu se rozdělují na interní a externí. Zaměstnanci musí být velmi obezřetní při manipulaci, z důvodu nechtěného vyzrazení interních dokumentů veřejnosti, případně konkurenci.

3.2 Bezpečnostní problémy společnosti

Společnost <*utajená*> se personálně dynamicky rozrůstá a na celém pracovišti vládne neformální a přátelská atmosféra. Tato neformálnost a příjemné vztahy spolu s odhodláním zaměstnanců pozitivně nahlížet na firemní cíle, vede k dobrým

[23] Competitive intelligence je zjišťování, sledování a vyhodnocování konkurenčního prostředí (firmy, organizace) s cílem odhalit slabé a silné stránky konkurence, rozpoznat její strategické záměry (9).

obchodním výsledkům společnosti. Bohužel vzájemná důvěru, přátelské vztahy a zvýšené fluktuace[24] zaměstnanců (zaměstnanec opouštějící perimetr společnosti zvyšuje riziko, že se citlivá data mohou dostat do rukou konkurence ať už úmyslně nebo neúmyslně) vede k neřešení bezpečnosti informací ve společnosti, což může mít v budoucnu následky ve formě ztráty důvěry zákazníků, partnerů, případně i ukončení podnikání z důvodu ztráty interních dat, případně soudních sporů.

Ve společnosti neexistují směrnice, stanovení odpovědnosti a principy, určující správné nakládání s citlivými informacemi, případně metodiky pro zvládání bezpečnostních incidentů. Je zde poměrně vysoké riziko spojené se zavlečením škodlivých softwarů do prostředí společnosti a naopak možnost úniku citlivých informací (dat), z důvodu zmiňované fluktuace zaměstnanců, na veřejnost nebo do rukou konkurence. S tím souvisí i nedostatečné řešení přístupu k citlivým datům a jejich klasifikace, jelikož každý zaměstnanec se může k těmto datům dostat a pracovat s nimi, i když je přímo ke své práci nepotřebuje.

Mezi další problém patří také nekvalitní úroveň dokumentace pracovních procesů. Jsou pouze známy odpovědné osoby, které provádí, případně dohlíží na danou aktivitu. Špatná úroveň dokumentace je odraz přátelského prostředí společnosti, kde se klade důraz na osobní přístup a odpovědnost zaměstnance.

3.3 Postup pro řešení problémů

Z výše popsaných globálních problémů lze zjistit, že se zde klade velký důraz na lidský faktor a důvěru v něm. Nepředpokládá se lidské selhání nebo lidská chyba, což při stálém rozvoji společnosti může mít fatální následky a negativní finanční dopad jak na celou společnost, tak i na zákazníky a partnery.

Pro zvýšení bezpečnosti informací a snížení rizik spojené s únikem citlivých dat se společnost rozhodla investovat finanční náklady do vybraného DLP řešení. Při postupné implementaci DLP řešení se bude vycházet z norem řady ISO 27000, jelikož do budoucna je plánovaná certifikace ISMS, která otevře společnosti nové trhy s jejich partnery a potencionální zvýšení zakázek na českém a světovém trhu.

[24] Fluktuace zaměstnanců je odchod pracovníků z organizace (24).

4 NÁVRH ŘEŠENÍ

Na základě výše analyzovaných problémů se společnost rozhodla pro implementaci DLP řešení z důvodu získání ISMS certifikace. Vybraná společnost <*utajená*>, ve které bude prováděna implementace DLP, nemá doposud zaveden management jakosti a management řízení interních procesů, založených na normách řady ISO 9000. Z toho důvodu celý implementační proces bude vycházet z doporučení a zkušeností dodavatele DLP řešení. K hlavním požadavkům patří přiblížit se k získání ISMS certifikace, z toho důvodu je zavádění DLP řešení založeno na PDCA modelu a obchodních zkušenostech dodavatele.

Pro společnosti, které mají už certifikaci ČSN ISO/IEC 9001, často vlastní i certifikaci bezpečnosti informací ČSN ISO/IEC 27001. Jelikož při zavádění se obě normy navzájem doplňují a při provádění certifikace se zavádí společně. V tomto případě je implementace DLP řešení individuální záležitostí, z důvodu splnění posloupnosti kroků a postupů definovaných v interních směrnicích. Návrh a postup celého řešení je prováděn ve společnosti, která nemá ČSN ISO/IEC 9001 certifikaci pro lepší pochopení logiky postupné implementace.

4.1 Obchodní navázání kontaktu

Vytvoření dobrého vztahu s obchodním partnerem (společnost dodávající DLP řešení) je jeden z nejdůležitějších faktorů úspěchu obchodního jednání a celé postupné implementace DLP řešení. Celý obchodní vztah je navazován již od prvního kontaktu a je budován po celou dobu jednání a trvání partnerství. Pro výběr vhodného kandidáta na dodavatele DLP řešení, je důležité uskutečnit interní výběrové řízení, kde vedení společnosti na základě prvotní analýzy trhu (za pomocí sledování referencí, marketingových materiálů) s bezpečnostními produkty, vybere dodavatele, který bude řešit implementaci DLP softwaru.

Po výběru kandidáta je nezbytně nutné se připravit na osobní schůzku s dodavatelem, kde společnost <*utajená*> bude zastupovat obchodní manažer a manažer IT.

Obr. 20: Základní postup přípravy na obchodní schůzku s dodavatelem DLP (Zdroj: Vlastní tvorba pro DP)

4.2 Cíle a záměry implementace DLP

Vhodně zvolené cíle a záměry jsou důležitým předpokladem pro úspěšný začátek jednání o postupu implementace DLP řešení a omezení interních rizik ve společnosti. Určující je rozeznat základní rozdíl mezi cílem projektu a jeho záměrem, jelikož v tomto kroku probíhá analýza cílů společnosti a definují se záměry k jejímu dosažení.

Cíle jsou dlouhodobé plány nebo vize, které chce společnost splnit. Bývají často definovány obecně (tudíž jsou neměřitelné), jsou v souladu s interní politikou, obchodní strategií společnosti a pomáhají určit celkový rámec pro efektivní implementaci. Na základě cílů projektu se definují už konkrétní záměry, které určují směr celého postupu zavádění DLP řešení a komplexně popisují, jakým stylem se splní cíle projektu. Záměry jsou psané realisticky a jejich základní vlastnost je měřitelnost za pomocí různých ukazatelů. Pro správné na lezení cílů v oblasti bezpečnosti informací je vhodné, aby byly položeny následující otázky:

a) Co má být ve společnosti <*utajená*> zlepšeno?
   Cíl: Zvýšit bezpečnost informací ve společnosti.
   Cíl: Zlepšit pracovní morálku zaměstnanců na pracovišti.
   Cíl: Ochrana před lidským selháním.
b) Čeho má být ve společnosti <*utajená*> dosaženo?
   Cíl: Vyřešit problémy, které brání ISMS certifikaci.
   Cíl: Hlídat manipulaci s interními informacemi a daty.
   Cíl: Kvalifikace interních a externích informací a dat.
c) Co má být ve společnosti <*utajená*> odstraněno?
   Cíl: Únik interních dat přes přenosná zařízení.

Při definování záměrů se vychází s výše popsaných cílů. Záměry definuje společnost <*utajená*> spolu s dodavatelem DLP řešení, jelikož se orientuje v technologické problematice, která je potřeba pro tvorbu konkrétních záměrů, aby jim zákazník porozuměl. Nejčastěji se vychází z otázky, jak daného cíle dosáhnout za pomocí DLP řešení.

Tab. 2: Ukázka cílů a záměru pro implementaci DLP (Zdroj: Vlastní tvorba pro DP)

Cíle *(Co má být dosaženo, zlepšeno, odstraněno?)*	**Záměry** *(Jak daného cíle dosáhnout?)*
Ochrana před lidským selháním	Nastavit bezpečnostní DLP politiku
Vyřešit problémy, které brání ISMS certifikaci	Implementace DLP řešení během 2 měsíců
Kvalifikace interních a externích dat	Nastavit klasifikační pravidla pro klasifikaci dat
Únik interních dat přes přenosná zařízení	Používat endpoint DLP systém

Výstupem jednání o cílech a záměrech je dokument, který definuje problematiku a cíle v bezpečnosti informací ve společnost <*utajená*> Na základě definovaných cílů dodavatel DLP řešení sestavuje záměry dopomáhajíc odstranit objevené problémy a

dosáhnout definované cíle. Dále dokument obsahuje základní dohodu o vytvoření studie proveditelnosti, která je založena na výše sepsaných informacích.

4.3 Základní studie proveditelnosti

Studie proveditelnosti, případně také označovaná jako technickoekonomická studie, je dokument, který souhrnně a ze všech realizačně významných hledisek popisuje záměr projektu. Jeho účelem je zhodnotit všechny realizační alternativy a posoudit technickou realizovatelnost a finanční náročnost implementace DLP řešení do společnosti <*utajená*> Poskytuje základní podklady pro vedení společnosti ohledně rozhodnutí o investici a zavádění DLP řešení. Cílem studie proveditelnosti je získat podklady pro implementační analýzu, která je stěžejním krokem pro úspěšné zavedení DLP řešení ve společnosti.

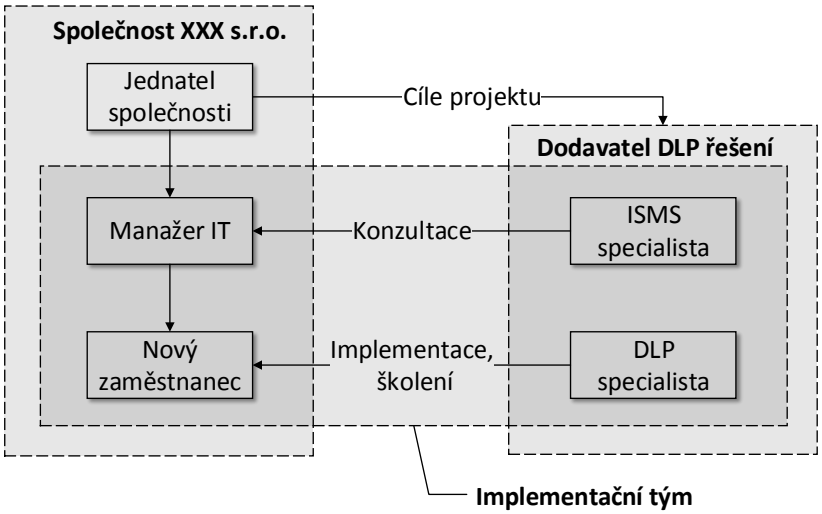
4.3.1 Zdůvodnění realizace projektu a jeho potřebnost

Z důvodu ekonomického a personálního růstu společnosti <*utajená*> se objevují nové problémy spojené s fluktuací zaměstnanců. Interním auditem bylo zjištěno, že se zvyšuje počet úniků dat, které způsobují samotní legitimní zaměstnanci. Za mnohými úniky dat stojí nepozornost zaměstnanců (lze spekulovat, zda se v nějakých případech nejedná o úmyslné krádeže dat za cílem vlastního obohacení a prospěchu). S růstem společnosti vstupují do této problematiky i další technologické trendy. Data se různě sdílí (napříč intranetem), masově se rozšířila externí paměťová média a disky, uživatelé často pracují nikoliv na desktopech, ale na noteboocích, které si nosí domů. Přibývají mobilní telefony, tablety pro manažery a další podobná zařízení. Zaměstnanci se z domova mnohdy připojují do firemní sítě nezabezpečeným způsobem. K vyřizování pracovních záležitostí používají webové emaily, své soukromé mobilní telefony používají k práci s podnikovými daty a naopak firemní notebooky s nimi sdílejí jejich rodinní příslušníci. S tím souvisí i přístup zaměstnanců ke všem firemním datům (i ty, které nejsou potřebné pro práci zaměstnance) a neexistující směrnice pro řízení přístupu.

Dalším důležitým aspektem je přiblížit se k ISMS certifikaci, která umožní společnosti <*utajená*> vstoupit na různé trhy (především ruský trh) a získávat nové partnery a zákazníky. Realizace projektu (implementace DLP řešení) je nezbytná z důvodů:

a) Únik dat kvůli nepozornosti.
b) Prevence proti úmyslným únikům dat.
c) Klasifikovat firemní data.
d) Řídit přístup k firemním datům a informacím.
e) Přiblížit se k získání ISMS certifikace.

4.3.2 Management projektu a řízení lidských zdrojů



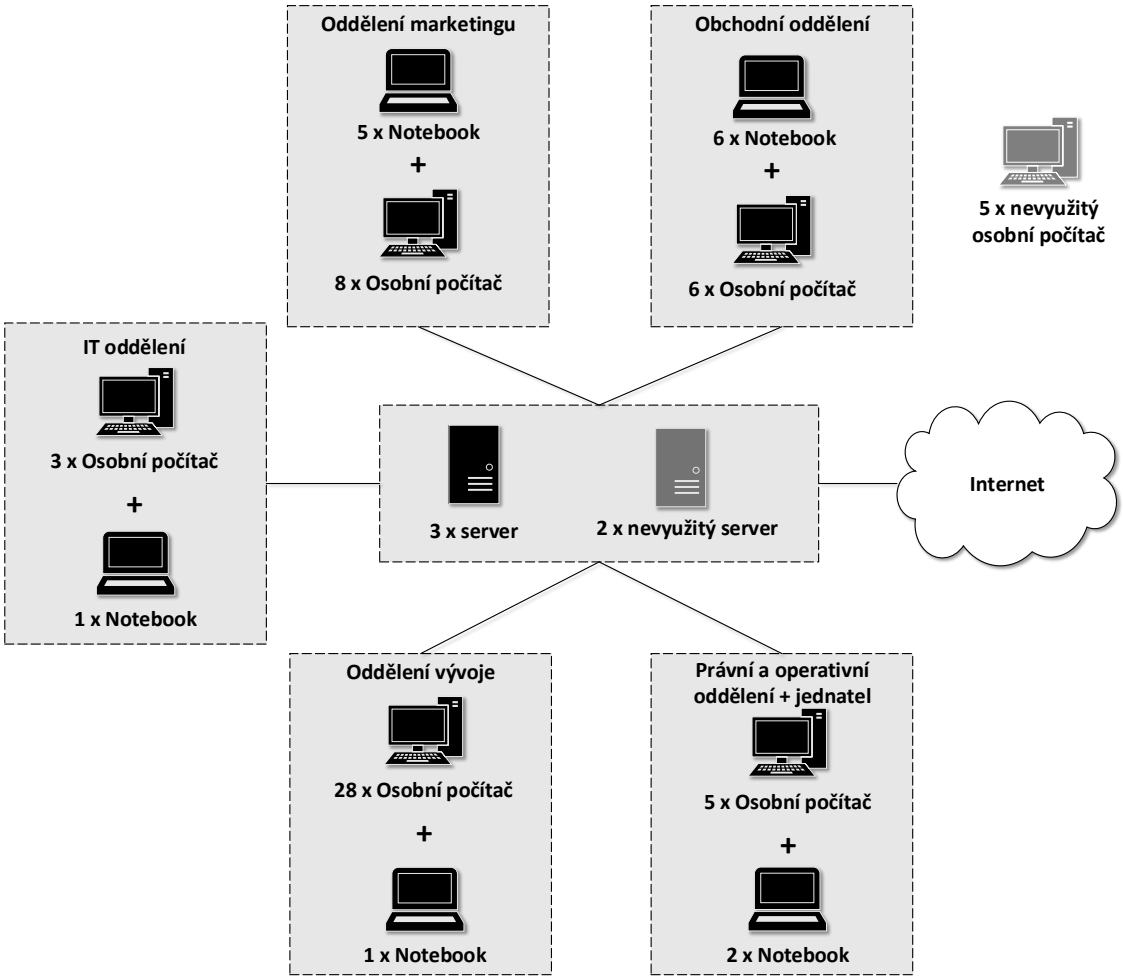
Obr. 21: Lidské zdroje potřebné pro implementaci DLP řešení (Zdroj: Vlastní tvorba pro DP)

Celý projekt není příliš náročný na lidské zdroje. Většina nároků na lidské zdroje je pokryta s vlastních zdrojů a ve fázi implementační analýzy se počítá s přijetím jednoho nového zaměstnance. Implementační tým se skládá ze 4 členů. Dva členi jsou ze strany společnosti <*utajená*> a další dva ze strany dodavatele DLP řešení:

a) Manažer IT – je vedoucím celého projektu a osobou zodpovědnou za realizaci.
b) Nový zaměstnanec (DLP technik) – je přímý podřízený manažerovi IT. Úzce spolupracuje s DLP specialistou a řeší otázku implementace, testování a budoucí správu dodaného softwaru napříč společnosti. Školí interní zaměstnance ohledně práce s citlivými informacemi a daty.
c) ISMS specialista - řídí a koordinuje správnost implementace dle norem řady ČSN ISO/IEC 27000. Má na starosti analýzu aktiv, rizik, hrozeb a tvorbu základních bezpečnostních politik dle ISMS.
d) DLP specialista – stará se o technickou realizaci DLP řešení, provádění školení, jak správně probíhá správa dodaného bezpečnostního softwaru.

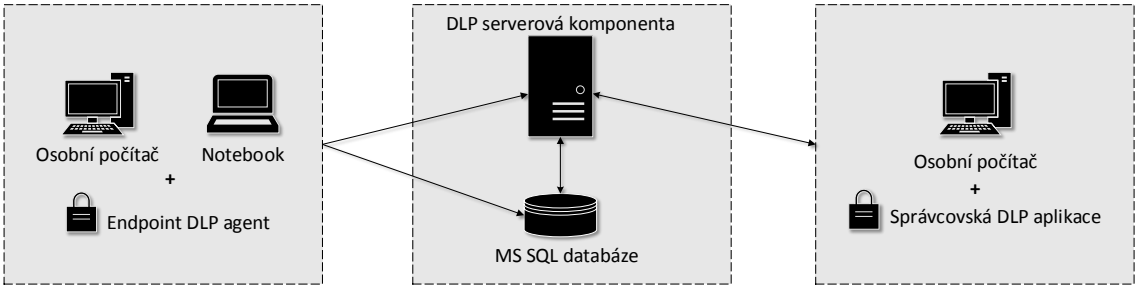
4.3.3 Technické a technologické aspekty projektu

Důležitým aspektem pro implementaci DLP řešení je prozkoumat vhodné technické a technologické možnosti společnosti. Jelikož se jedná o implementaci komplexního softwarového řešení, je velmi důležité zaměřit základní topologii sítě a hardwarové možnosti. Ve společnosti pracuje celkem 50 zaměstnanců využívající přidělené osobní počítače, dále je aktivních 15 notebooků, které jsou využívány vedením společnosti, celým obchodním oddělením a části marketingu (dalších 5 osobních počítačů je volně k dispozici). Dále se zde nachází 5 serverů, kde 3 servery jsou aktivně zapojeny do firemní sítě, ostatní dva nejsou využity.



Obr. 22: Základní topologie společnosti (Zdroj: Vlastní tvorba pro DP)

Na základě těchto poznatků a předem definovaných požadavků na implementaci DLP řešení, dodavatel zvolil přistoupit na endpoint DLP, které dokáže zabezpečit data i mimo perimetr společnosti. S tím souvisí i náročnost na IT architekturu, která je potřeba pro bezproblémový chod celého bezpečnostního systému. Řešení se skládá z endpoint DLP agenta nainstalovaného na všechny koncové stanice (osobní počítače, notebooky), serverové komponenty s MS SQL databází obsluhující koncové stanice a správcovské DLP aplikace.



Obr. 23: DLP architektura (Zdroj: Vlastní tvorba pro DP)

Tab. 3: Technické požadavky pro DLP architekturu (Zdroj: Vlastní tvorba pro DP)

Endpoint DLP agent	DLP serverová komponenta	MS SQL databáze
1,8 GHz dvou jádrový procesor *32-bit (x86) nebo 64-bit (x64)*	1,6 GHz dvou jádrový procesor *32-bit (x86) nebo 64-bit (x64)*	1,6 GHz dvou jádrový procesor *32-bit (x86) nebo 64-bit (x64)*
2 GB paměti RAM	4 GB paměti RAM	4 GB paměti RAM
2 GB volného místa na disku	2 GB volného místa na disku	500 GB volného místa na disku
MS Windows XP SP3, Vista, 7	Sdílený nebo dedikovaný server	Sdílený nebo dedikovaný server
Instalační balík MSI	Vyžaduje propojení s MS SQL 2008 serverem	MS Windows Server 2003 SP2, 2008, 2008 R2, *32-bit a 64-bit*
	Podpora Active Directory	

Na základě požadavků DLP architektury nebude potřeba investovat do nového hardwarového zařízení a softwarového řešení (kromě licence na DLP produkt).

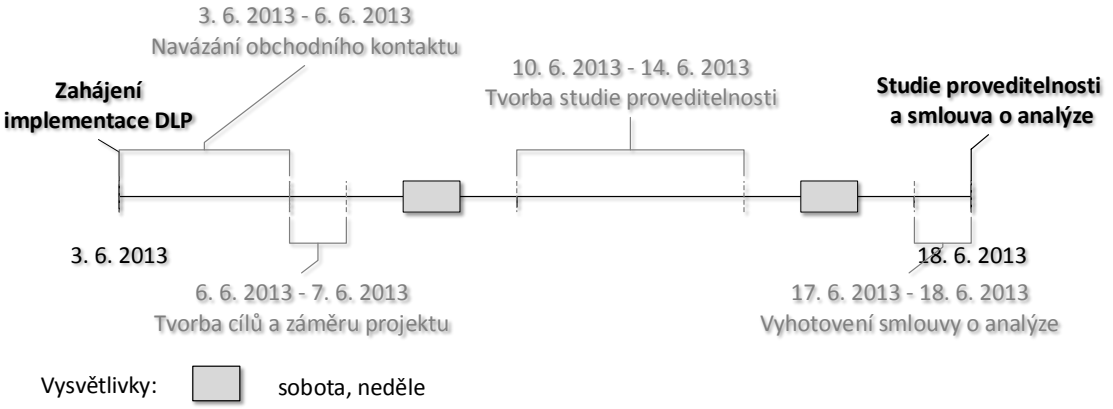
4.3.4 Legislativní aspekty projektu

Ochrana dat není jen legitimním zájmem vedení společnosti, ale v České republice také zákonnou povinností, pokud společnost disponuje s osobními údaji ať již zákazníků nebo zaměstnanců (101/2000 Sb., o ochraně osobních údajů). Data pocházející z monitoringu rovněž podléhají ochraně a je nutné u nich detailně nastavit přístupová práva.

Dalším důležitým směrem je tvorba ISMS ve shodě s normami ČSN ISO/IEC 27000 pro budoucí certifikaci.

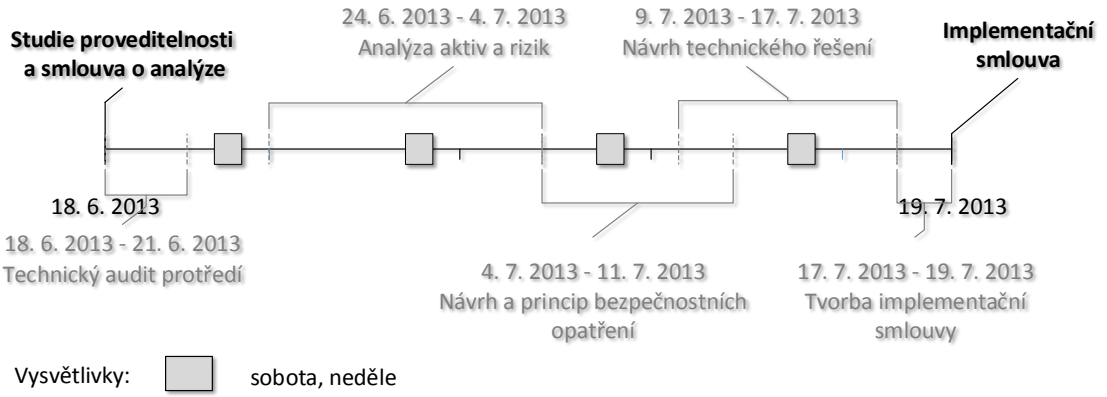
4.3.5 Časový harmonogram projektu

Časový harmonogram projektu je rozdělen na 4 fáze, které jsou založeny na PDCA modelu. Celý postup předchází komunikační fáze, kdy se vyhotovují základní smlouvy a určí se základní stanoviska pro zavádění DLP řešení. Výstupem první fáze je studie proveditelnosti a smlouva o analýze (tj. seznam potřebných analýz).



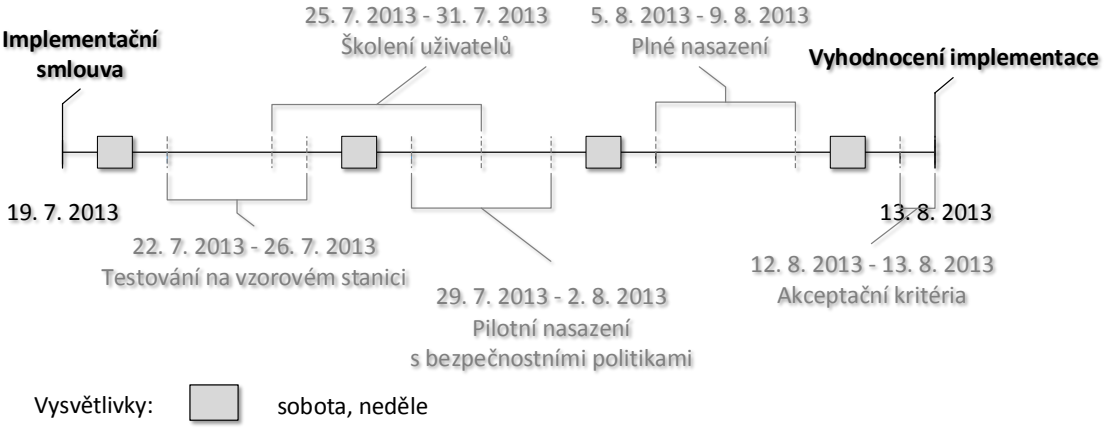
Obr. 24: Časový harmonogram komunikační fáze (Zdroj: Vlastní tvorba pro DP)

Druhá fáze se zaobírá základním ustanovením zavádění DLP řešení. Obsahuje několik analýz a výstupem je implementační smlouva.



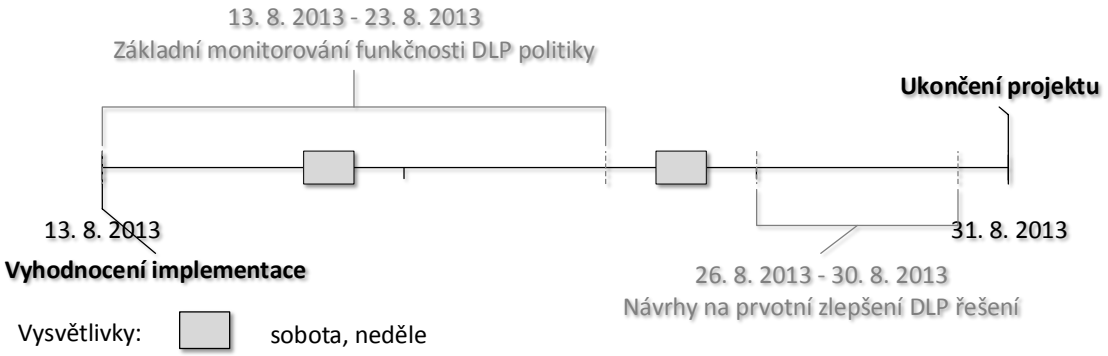
Obr. 25: Časový harmonogram pro ustanovení implementace DLP řešení (Zdroj: Vlastní tvorba pro DP)

Třetí fáze popisuje postup při instalaci DLP softwaru, přes pilotní nasazení až po akceptační kritéria. Výstupem je vyhodnocení implementace.



Obr. 26: Časový harmonogram pro zavádění a provozování DLP řešení (Zdroj: Vlastní tvorba pro DP)

V poslední, čtvrté fázi, se uskutečňuje monitorování funkčnosti DLP řešení a jeho postupné udržování, případně zlepšování.



Obr. 27: Časový harmonogram pro monitorování a zlepšování DLP řešení (Zdroj: Vlastní tvorba pro DP)

Z výsledného časového diagramu vyplývá, že celý projekt implementace DLP řešení ve společnosti <*utajená*> bude trvat od 3.6.2013 do 31.8.2013. Do této doby jsou zahrnuta všechna obchodní jednání, analýzy, postupná implementace za pomocí pilotní strategie, školení uživatelů, vyhodnocení a postupné zlepšování fungování celého DLP řešení.

4.3.6 Finanční a ekonomické aspekty projektu

Důležitým aspektem je finanční náročnost projektu a jeho návratnost při ochraně informačních aktiv. Zavádění DLP technologie si vyžaduje najmout nového zaměstnance do IT oddělení, který se aktivně podílí na všech částech projektu, posléze bude pokračovat na udržování a zlepšování DLP řešení.

Tab. 4: Náklady na nového zaměstnance - DLP technik (Zdroj: Vlastní tvorba pro DP)

Pozice	Podíl na projektu	Forma	Počet měsíců	Vztah ke společnosti	Super-hrubá mzda
DLP technik[25]	100%	HPP	3	Nový zaměstnanec	41 200 Kč

Velkou finanční zátěží je placení služeb ze strany dodavatele, které jsou poskytovány pro efektivnější implementaci. V následující tabulce je uveden základní rozpočet všech potřebných služeb.

[25] DLP technik je zaměstnanec, který má na starosti práci s DLP produktem. Nastavuje bezpečností politiku, vytváří klasifikační pravidla a pracuje se správcovskou aplikací na základě pokynu svého přímého nadřízeného a tím je manažer IT.

Tab. 5: Rozpis a ceník vykonaných služeb (Zdroj: Vlastní tvorba pro DP)

Název služby	Celková doba trvání	Dodavatel	Počet dnů dodavatele	Náklady na 1 den práce	Celková cena
Tvorba cílů a záměrů projektu	2 dny	ISMS specialista	1	6 000 Kč	6 000 Kč
Studie proveditelnosti	5 dnů	DLP specialista	3	5 000 Kč	15 000 Kč
Smlouva o analýze	2 dny	ISMS specialista	1	Zdarma	Zdarma
Technický audit prostředí	4 dny	DLP specialista	4	5 000 Kč	20 000 Kč
Analýza aktiv a rizik	9 dnů	ISMS specialista	5	6 000 Kč	30 000 Kč
Zvládání rizik a tvorba politik	6 dnů	ISMS specialista	3	6 000 Kč	18 000 Kč
Návrh technického řešení	3 dny	DLP specialista	3	5 000 Kč	15 000 Kč
Návrh pilotního nasazení	3 dny	DLP specialista	2	5 000 Kč	10 000 Kč
Testování na vzorové stanici	5 dnů	DLP specialista	3	5 000 Kč	15 000 Kč
Školení uživatelů	5 dnů	DLP specialista	2	5 000 Kč	15 000 Kč
Pilotní nasazení	5 dnů	DLP specialista	3	5 000 Kč	15 000 Kč
Plné nasazení	5 dnů	DLP specialista	4	5 000 Kč	20 000 Kč
Akceptační kritéria	2 dny	ISMS, DLP specialista	2	Zdarma	Zdarma

Pozn.: Ceník služeb vychází z reálných hodnot.

Za poskytnuté služby si v tomto projektu dodavatel naúčtuje 179 000 Kč. Technická podpora je poskytována zdarma, jelikož je v ceně licence produktu, která je účtována za jeden kalendářní rok. Po uplynutí této doby je potřeba opět zakoupit nové licence.

Tab. 6: Cena za licence (Zdroj: Vlastní tvorba pro DP)

Licence	Cena 1 licence	Počet licencí	Celková cena
DLP software	2 999 Kč	70	209 930 Kč

Pozn.: Ceník produktu vychází z reálné hodnoty.

Do celkových nákladů pro implementaci DLP řešení je nutné započítat plat nového zaměstnance po dobu 3 měsíců, služby poskytované dodavatelem DLP řešení a nákup samotných licencí softwaru. **Celková cena činí 512 530 Kč** (3 x 41 200 Kč + 179 000 Kč + 209 930 Kč).

4.4 Implementační analýza

Implementační analýza vychází ze studie proveditelnosti a zabývá se zkoumáním struktury prostředí společnosti. Důležité je zjistit detailní architekturu IT společnosti (předběžný rámec se nachází ve studii proveditelnosti), do které má být nasazen DLP systém.

Pro přiblížení se k ISMS certifikaci je vhodné provést identifikaci aktiv společnosti a analyzovat působící možná rizika. Na základě těchto poznatků se vytvoří doporučení pro tvorbu bezpečnostní politiky a seznam opatření, které lze vyřešit dodaným DLP systémem. Poslední částí implementační analýzy je vytvoření postupu pro samotnou implementaci, jedná se o popis pilotního nasazení, akceptační testy a popis plného nasazení. Z těchto všech poznatků vznikne implementační smlouva, ve které se určují role zodpovědnosti.

4.4.1 Technický audit prostředí

Síťové prostředí společnosti je rozděleno na jednotlivé oblasti podle oddělení (vývoj, obchod, marketing, operativně právní, IT oddělení) a využívá hvězdicovou topologii sítě. Centrálním místem pro komunikaci je serverovna, kde se nachází aktivní prvky sítě, jako je webový, databázový a aplikační server. Každé oddělení má vlastní switch pro kabelové připojení počítače do sítě a access point, využívaný pro bezdrátové připojení. Jednotlivé počítače jsou vždy přímo napojeny na příslušný switch podle toho, ve kterém oddělení se vyskytují. Z toho důvodu nehrozí při náhodném výpadku více počítačů kolaps celofiremní sítě. Síťová architektura využívá také bezdrátové přístupové body pro připojení externích zaměstnanců do firemní sítě a vnitřní přístupový bod pro potřeby návštěv. K dispozici je také pro zaměstnance VPN pro případnou práci z domova. Stáří pracovních stanic odpovídá horizontu 1 – 3 let, což je pro zavádění DLP softwaru dostačující. Veškeré pracovní stanice obsahují USB výstupy, vypalovací mechaniky, firewire a u notebooků se objevuje ještě bluetooth.

Tab. 7: Běžná konfigurace osobního počítače a notebooku ve společnosti *<utajená>* (Zdroj: Vlastní tvorba pro DP)

Konfigurace osobního počítače	Konfigurace notebooku
2,5 GHz čtyř-jádrový procesor	2 GHz dvou-jádrový procesor
6 GB paměti RAM	4 GB paměti RAM
500 GB volného místa na disku	320 GB volného místa na disku
MS Windows 7	MS Windows 7

Ve společnosti je používán na pracovních stanicích výhradně operační systém Microsoft Windows 7 Pro a servery běží na nové platformě Microsoft Windows Server 2012. Mezi další serverové služby patří Microsoft SQL Server 2012 a Team Foundation Server 2012 pro lepší podporu vývoje a správu zdrojových kódů.

Z aplikačního pohledu se ve společnosti vyskytuje několik druhů softwaru, rozdělených na základě jednotlivých oddělení. Základem je interní informační systém, postavený na produktu YYY, využíván celou společností, kde jednotlivé oddělení mají přiřazené odlišné moduly pro jejich potřebu a pro potřebu technické podpory je zde helpdesk s databází všech zákazníků a partnerů. Do tohoto systému má přístup celá společnost. Pro zákaznickou spokojenost používá obchodní oddělení a část technické podpory vlastní partnerský systém s podporou CRM.

Rovněž byla provedena z důvodu kompatibility analýza softwaru třetí strany, které jsou fyzicky nainstalovány na pracovních stanicích, jelikož se k nim bude přidávat i endpoint DLP agent.

Tab. 8: Kompatibilita endpoint DLP agenta s používaným softwarem (Zdroj: Vlastní tvorba pro DP)

Software třetí strany	Kompatibilita s endpoint DLP agentem
Adobe Illustrator CS6	Ano
Adobe Photoshop CS6	Ano
Adobe Reader XI	Ano
Balsamiq Mockups	Zatím ne (v nové verzi ano)
DEAMON Tools	Ano
Microsoft Internet Explorer 10	Ano
Microsoft Office Professional Plus 2010	Ano
Microsoft Visual Studio 2012	Ano

Pozn.: Kompatibilita endpoint DLP agenta se softwarem vychází z reálných prostředí

V podrobnější analýze bylo zjištěno, že mnoho zaměstnanců a vedoucích týmů používá pro dočasné ukládání informací cloudové řešení Google Apps, což nebylo v původní specifikaci popsáno. Jedná se o nejslabší a nejvíce nebezpečnou oblast pro únik dat. Proto bylo dodatečně domluveno, že se omezí sdílení a posílání dat na Google uložiště za pomocí endpoint DLP agenta. Hlavním autorem technického auditu je DLP specialista ze strany dodavatele a manažer IT (+ nový zaměstnanec z důvodu zaškolení).

4.4.2 Identifikace a ohodnocení aktiv

Identifikace a ohodnocení aktiv společnosti je základní krok v celkovém procesu analýzy rizik, z toho důvodu pro identifikaci aktiv je pověřený ISMS specialista ze strany dodavatele DLP řešení, který za pomocí manažera IT a vedení společnosti vytvoří seznam aktiv, které jsou potřeba chránit před únikem. Předmětem identifikace aktiv budou informační aktiva, jelikož pouze ty dokáže implementované DLP řešení bezpečně ochránit. Hlavním principem při ohodnocení aktiv jsou náklady vzniklé v důsledku porušení:

a) Důvěrnosti - informace jsou přístupny nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
b) Integrity - zajištění správnosti a úplnosti informací.

c) Dostupnosti - informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

Tab. 9: Schéma pro hodnocení dopadu (Zdroj: Vlastní tvorba pro DP)

	Stupeň	**Popis dopadu při narušení bezpečnosti**
1	Nízký	Nízký dopad na společnost - jedná se dopad, který je zanedbatelný a nezpůsobí ztrátu
2	Střední	Střední dopad na společnost - vzniknou interní potíže a malá finanční ztráta
3	Vysoký	Vysoký dopad na společnost - vzniknou vážné potíže a velká finanční ztráta
4	Kritický	Kritický dopad na společnost - velké finanční a veřejné problémy spojené s negativním dopadem na budoucnost společnosti

Tab. 10: Přehled informačních aktiv ve společnosti *<utajená>* a jejich váha (Zdroj: Vlastní tvorba pro DP)

Název aktiva	**Popis aktiva**	**Garant aktiva**	**Váha**
Zdrojové kódy	Jsou nositelem hlavních znalostí produktu	Manažer vývoje	4[26]
Tech. dokumentace	Technický popis produktu určený pro vývoj	Manažer vývoje	3
Marketingové plány	Plány budoucích reklamních kampaní	Manažer marketingu	3
Obchodní plány	Popisují plány na expanzi společnosti	Obchodní manažer	4
Pracovní smlouvy	Obsahují informace o zaměstnancích	Vedoucí operativy	3
Obchodní smlouvy	Obsahují informace o zákaznících	Právní oddělení	3
Účetnictví a faktury	Dokumenty nesoucí finanční stránku obchodních jednání a mzdové politiky	Vedoucí operativy	3
Data zákazníků	Osobní kontakty a důvěrné informace o zákaznících	Manažer vývoje	3
Licenční klíče	Licence k prodávanému softwaru	Manažer vývoje	4
Finanční hospodaření	Informace o investicích a hospodaření společnosti	Jednatel společnosti	2

Z provedené analýzy vyplývá, že společnost se nejvíce bude snažit zabezpečit zdrojové kódy a licenční klíče, jelikož se jedná o nejcennější aktiva, která společnost vlastní. Mezi kritická aktiva se řadí i obchodní plány, určující metodiku prodeje a velmi důvěrné informace o expanzi společnosti.

[26] Váha pro zdrojové kódy se vypočítá jako hodnota aktiva z hlediska důvěrnosti (4), dostupnosti (4) a integrity (4) = (4+4+4) / 3 = 4.

4.4.3 Identifikace a pravděpodobnost hrozeb

Po identifikaci informačních aktiv je nutné nalézt možné interní hrozby a definovat jejích pravděpodobnost výskytu. U tohoto kroku je důležité aktivní zapojení manažera IT s vedením společnosti, kteří společně s ISMS specialistou ze strany dodavatele DLP řešení vytvoří odpovídající schéma. Identifikace se bude týkat pouze interních hrozeb, které přímo souvisí s DLP řešením.

Tab. 11: Schéma pro hodnocení úrovně hrozby (Zdroj: Vlastní tvorba pro DP)

	Stupeň	**% výskyt za rok**	
1	Nízká	0 – 20 %	Málo pravděpodobné
2	Střední	20 – 50 %	Příležitostné
3	Vysoká	50 – 70 %	Pravděpodobné až časté
4	Kritická	70 – 100 %	Velmi časté

Tab. 12: Seznam interních hrozeb se stupněm výskytu (Zdroj: Vlastní tvorba pro DP)

Název hrozby	**Stupeň výskytu**
Nepozornost zaměstnanců	
Ztráta externích zařízení s dokumenty	3
Ztráta notebooku s dokumenty	2
Neúmyslné odeslání dokumentu pomocí sítě	4
Nepozorné vytisknutí dokumentů	3
Úmyslné poškození dokumentů	
Neoprávněný přístup k informacím	4
Neoprávněný přístup k aplikacím	3
Neoprávněné používání externích zařízení	4
Změna struktury a informací v dokumentu	3
Krádež dokumentů	
Krádež externích zařízení s dokumenty	2
Krádež medií s dokumenty	2
Úmyslné odeslání dokumentů pomocí sítě	3
Krádež interních dokumentů za pomocí tisku	1
Úmyslné vykopírování části dokumentů	4
Zprovoznění vyřazených medií	2

Z provedené analýzy vyplývá, že díky neřízenému přístupu k informacím si mohou za pomocí soukromých zařízení vykopírovat libovolné dokumenty a přistupovat například ke zdrojovým kódům, které jsou považovány za největší aktivum společnosti. Vhodné je se také zaměřit na chyby zaměstnanců při používání Google Apps.

4.4.4 Vyhodnocení míry rizik

Nejvýznamnějším krokem pro řízení rizik je výpočet míry rizik. Vyhodnocení rizika závisí na velikosti ztráty a zjištění pravděpodobnosti výskytu případné ztráty. Pro určení velikosti míry je použita součtová matice rizik.

Tab. 13: Princip hodnocení rizik (Zdroj: Vlastní tvorba pro DP)

		Pravděpodobnost			
		Nízká (1)	Střední (2)	Vysoká (3)	Kritická (4)
Dopad	Nízký (1)	2	3	4	5
	Střední (2)	3	4	5	6
	Vysoký (3)	4	5	6	7
	Kritický (4)	5	6	7	8

Tab. 14: Hodnocení rizik vůči informačnímu aktivu (Zdroj: Vlastní tvorba pro DP)

	Aktiva	Zdrojové kódy	Tech. dokumentace	Marketingové plány	Obchodní plány	Pracovní smlouvy	Obchodní smlouvy	Účetnictví a faktury	Data zákazníků	Licenční klíče	Finanční hospodaření
Hrozby		*4*	*3*	*3*	*4*	*3*	*3*	*3*	*3*	*4*	*2*
Nepozornost zaměstnanců											
Ztráta externích zařízení s dokumenty	*3*	7	6	6	7	6	6	6	6	7	5
Ztráta notebooku s dokumenty	*2*	6	5	5	6	5	5	5	5	6	4
Neúmyslné odeslání dokumentu pomocí sítě	*4*	8	7	7	8	7	7	7	7	8	6
Nepozorné vytisknutí dokumentů	*3*	7	6	6	7	6	6	6	6	7	5
Úmyslné poškození dokumentů											
Neoprávněný přístup k informacím	*4*	8	7	7	8	7	7	7	7	8	6
Neoprávněný přístup k aplikacím	*3*	7	6	6	7	6	6	6	6	7	5
Neoprávněné používání externích zařízení	*4*	8	7	7	8	7	7	7	7	8	6
Změna struktury a informací v dokumentu	*3*	7	6	6	7	6	6	6	6	7	5
Krádež dokumentů											
Krádež externích zařízení s dokumenty	*2*	6	5	5	6	5	5	5	5	6	4
Krádež medií s dokumenty	*2*	6	5	5	6	5	5	5	5	6	4
Úmyslné odeslání dokumentů pomocí sítě	*3*	7	6	6	7	6	6	6	6	7	5
Krádež interních dokumentů za pomocí tisku	*1*	5	4	4	5	4	4	4	4	5	3
Úmyslné vykopírování části dokumentů	*4*	8	7	7	8	7	7	7	7	8	6
Zprovoznění vyřazených medií	*2*	6	5	5	6	5	5	5	5	6	4

4.4.5 Návrh a princip bezpečnostních opatření

Pro eliminaci všech identifikovaných rizik je potřeba definovat opatření a bezpečnostní politiku, kterou je nutné zavést, aby byl dopad na informační aktiva minimalizován. Při definování bezpečnostních politik se vychází z funkčnosti DLP systému a normy ČSN ISO/IEC 27001:2006. Vzhledem k tomu, že společnost se chce přiblížit k ISMS certifikaci, budou uvedena opatření pouze oblastí, které dokáže ovlivnit implementovaný DLP systém. Celý proces provádí DLP specialista a ISMS specialista ze strany dodavatele, kteří nesou plnou zodpovědnost.

Tab. 15: Seznam opatření normy ČSN ISO/IEC 27001, které se týkají DLP systému (Zdroj: Vlastní tvorba pro DP)

	Opatření normy ČSN ISO/IEC 27001	**Funkčnost DLP**	**Požadavek**
7.2	**Klasifikace informací**		
7.2.1	Doporučení pro klasifikaci	Klasifikace dat	Kritický
7.2.2	Označování a nakládání s informacemi	Označování dat	Kritický
9.2	**Bezpečnost zařízení**		
9.2.5	Bezpečnost zařízení mimo prostory organizace	Šifrování dat	Vysoký
9.2.6	Bezpečnost likvidace nebo opakované použití zařízení	Skartace dat	Nízký
10.7	**Bezpečnost při zacházení s médii**		
10.7.4	Bezpečnost systémové dokumentace	Zabezpečení dat	Kritický
10.8	**Výměna informací**		
10.8.3	Bezpečnost médií při přepravě	Šifrování dat	Kritický
10.8.4	Elektronické zasílání zpráv	Šifrování zpráv	Střední
10.10	**Monitorování**		
10.10.1	Pořizování auditních záznamů	Protokol DLP	Nízký
10.10.2	Monitorování používání systému	Protokol DLP	Nízký
10.10.3	Ochrana vytvořených záznamů	Protokol DLP	Nízký
10.10.4	Administrátorský a operátorský deník	Systémový přístup	Nízký
10.10.5	Záznam selhání	Protokol DLP	Nízký
10.10.6	Synchronizace hodin	Synchronizace	Nízký
11.6	**Řízení přístupu k aplikacím a informacím**		
11.6.1	Omezení přístupu k informacím	Zabezpečení dat	Kritický
12.3	**Kryptografická opatření**		
12.3.1	Politika pro použití kryptografických opatření	Šifrování dat	Nízký
12.3.2	Správa klíčů	Šifrovací klíče	Nízký
12.5	**Bezpečnost procesů vývoje a podpory**		
12.5.4	Únik informací	Zabezpečení dat	Kritický
15.1	**Soulad s právními normami**		
15.1.3	Ochrana záznamů organizace	Zabezpečení dat	Kritický
15.1.4	Ochrana dat a soukromí osobních informací	Zabezpečení dat	Kritický

Dle požadavků společnosti jsou určena opatření, která mají kritický požadavek. Tato opatření by měla mít při zavádění maximální prioritu.

4.4.5.1 A.7.2 Klasifikace informací

Cílem klasifikace informací za pomocí DLP systému je mít přehled o datech, která se nachází na koncových stanicích, s nimiž zaměstnanci pracují a denně přichází do styku. Informace mohou mít různý stupeň citlivosti a mohou být různě kritické, některé mohou vyžadovat vyšší úroveň bezpečnosti nebo zvláštní způsob zacházení. Systém pro klasifikaci informací by měl určovat adekvátní stupeň ochrany dokumentů (3). Toto opatření zajišťuje odpovídající úroveň zabezpečení informací i pro další oblasti.

A.7.2.1 Doporučení pro klasifikaci (kritické):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Společnosti <*utajená*> na základě klasifikace dat určí, jaké typy informací se nachází na koncových stanicích, ke kterým mají uživatelé přístup. S největší pravděpodobností to jsou zdrojové kódy, obchodní a marketingové materiály, případně smlouvy a data o zákaznících. Po aktivování funkce klasifikace dat v DLP produktu lze na základě principů popsaných v kapitole 3.6.2 automaticky roztřídit nalezená data do skupin, které mají být předmětem ochrany.
Zdroje opatření: Pravidelná klasifikace informací (1 den / měsíčně), první spuštěna klasifikace napříč společnosti (24 hodin)

A.7.2.1 Označování a nakládání s informacemi (kritické):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Každá klasifikovaná skupina dat z předchozího opatření je ze strany DLP produktu (za pomocí funkce označování dat) programově označena, díky čemuž lze identifikovat úroveň zabezpečení pro tisk, kopírování, mazání a úpravu dat.
Zdroje opatření: Nastavení označování dat (1 den / měsíčně)

4.4.5.2 A.9.2 Bezpečnost zařízení

Za pomocí vhodné bezpečnosti zařízení lze předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv. Ochrana zařízení (včetně těch, která se používají mimo hlavní perimetr) je nezbytná jak pro snížení rizika neautorizovaného přístupu k datům, tak k zajištění ochrany proti ztrátě nebo poškození (3).

A.9.2.5 Bezpečnost zařízení mimo prostory organizace (vysoké):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)

Opatření: Data na zařízeních používané mimo prostory organizace musí být zabezpečeny šifrovacími algoritmy, kterými disponuje DLP produkt. Předchází se zneužití dat při náhodné ztrátě nebo krádeži zařízení. Šifrování může probíhat automaticky při kopírování označených dat na externí zařízení nebo manuálně podle nastavené bezpečnostní politiky.
Zdroje opatření: Nastavení šifrování (1 hodina / týdně)

A.9.2.6 Bezpečná likvidace nebo opakované použití zařízení (kritické):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Všechna paměťová zařízení, která obsahují interní informace (označené informace) a jsou předmětem vyřazení, případně mají být předány k trvalému používání do rukou jiné osoby, musí být na ně aplikována funkce skartace dat, která je součástí DLP produktu. Tato funkce dle definovaných algoritmů několikanásobně bezpečně smaže a přepíše původní informace.
Zdroje opatření: Nastavení skartace při likvidaci paměťového zařízení (1 hodina / týdně)

4.4.5.3 A.10.7 Bezpečnost při zacházení s médii

Bezpečnost médii předchází neoprávněnému vyzrazení informací, které může vést k poškození aktiv společnosti. Dané média by měla být kontrolována a stanoveny náležité provozní postupy týkající se zabezpečení dokumentů, počítačových medií, vstupních a výstupních dat a systémové dokumentace před neoprávněným vyzrazením, modifikací nebo odstraněním (3).

A.10.7.4 Bezpečnost systémové dokumentace (kritické):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Systémové dokumentace mají technický popis, který je určen pouze pro definované zaměstnance bezpečnostní politikou. Ostatní zaměstnanci mají k těmto dokumentům zakázaný přístup. Mohou do dokumentací náhlednou pouze po předchozím požádání odpovědné osoby. Neoprávněný přístup zajišťuje funkce zabezpečení dat, kde se definují zaměstnanci, kteří mají právo se systémovými dokumentacemi manipulovat.
Zdroje opatření: Nastavení zabezpečení systémových dokumentů (1 hodina / týdně)

4.4.5.4 A.10.8 Výměna informací

Při pohybu zaměstnanců je důležité si vyměňovat informace prostřednictvím přenosných zařízení nebo emailové komunikace, jenže tyto kanály často bývají nezabezpečené a zdrojem úniků dat. Výměna informací a programů mezi organizacemi nebo zaměstnanci by měla být založena na formální politice, prováděna v souladu s platnými dohodami a měla by být ve shodě s platnou legislativou (3).

A.10.8.3 Bezpečnost médií při přepravě (kritické):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Média obsahující informace během přepravy, musí být chráněna šifrovací funkcí DLP produktu proti neopravnému zneužití, dojde-li k odcizení nebo ztrátě.
Zdroje opatření: Nastavení šifrování (1 hodina / týdně)

A.10.8.4 Elektronické zasílání zpráv (střední):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Chráněné informace (označené dle opatření A.7.2.1), které si zaměstnanci posílají prostřednictvím emailové komunikace musí být při přenosu automaticky šifrovány, případně je-li příjemce neautorizován, odeslání email je zablokováno.
Zdroje opatření: Nastavení šifrování (1 hodina / týdně)

4.4.5.5 A.10.10 Monitorování

Hlavním cílem monitorování je detekovat neoprávněné zpracování informací. Každá nepovolená operace bude DLP systémem zaznamenána a posléze upozorněna odpovědná osoba. Veškeré aktivity související s monitorováním a zaznamenáváním událostí by měly být v souladu s relevantními zákonnými požadavky. Následné monitorování systému umožňuje kontrolování účinnosti přijatých opatření a ověření souladu s modelem politiky řízení přístupu.

A.10.10.1 Pořizování auditních záznamů (nízké):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Při práci s informacemi může docházet k bezpečnostním událostem z důvodu porušení přístupu, neoprávněného zkopírování, mazání a přesouvání dat. Tato aktivita musí být zaznamenána a uchována pro budoucí vyšetřování. Při výskytu bezpečnostně

významné události musí být varována odpovědná osoba. Veškerý monitoring v rámci chráněných informací obstarává funkce protokol DLP.
Zdroje opatření: Nastavení monitorování dle legislativy (24 hodin / ročně)

A.10.10.2 Monitorování používání systému (nízké):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Nutnost stanovit pravidla pro monitorování používání výpočetní techniky při práci s informacemi. Dále je potřeba definovat pravidelné vyhodnocování zaznamenaných výsledků a pokusů změn na systémovém nastavení z důvodu pokusu o zneužití dat. Tohle rovněž řeší funkce protokol DLP.
Zdroje opatření: Nastavení monitorování dle legislativy (24 hodin / ročně)

A.10.10.3 Ochrana vytvořených záznamů(nízké):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Je-li zapnutá funkce protokol DLP, vznikají záznamy, které podléhají utajení a spadají do chráněných aktiv. Kompletní správa monitorování probíhá ve správcovské aplikaci DLP produktu, do které má přístup pouze odpovědná osoba. Autentizace probíhá prostřednictvím přiděleného 8 – 16 znakového hesla.
Zdroje opatření: Nastavení přístupu do aplikace (1 hodina / měsíčně)

A.10.10.4 Administrátorský a operátorský deník (nízké):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Správcovská aplikace DLP produktu automaticky zaznamenává prováděné operace (zapínání funkcí, prohlížení si zaznamenaných výsledků) pro pozdější analýzu, případně dohledání problému.
Zdroje opatření: Zaznamenávání probíhá automaticky ihned po instalaci (0 hodin)

A.10.10.5 Záznam selhání (nízké):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Při výskytu technické chyby nebo selhání systému musí být vytvořený záznam, který je potřeba analyzovat s odpovědnou osobou nebo s technickou podporou dodávaného systému. Na základě výsledku analýzy je potřeba provést opatření minimalizující opětovný výskyt selhání.
Zdroje opatření: Analýza záznamu a tvorba nového opatření (12 hodin / měsíčně)

A.10.10.6 Synchronizace času (nízké):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Funkce synchronizace v produktu DLP má automatickou synchronizaci času klientských stanic, které jsou vzájemně propojeny v síti. Aktuální čas je získáván z časového serveru dodáván třetí stranou.
Zdroje opatření: Časová synchronizace probíhá automaticky (0 hodin)

4.4.5.6 A.11.6 Řízení přístupu k aplikacím a informacím

Na klientských stanicích a serverech společnosti se nachází mnoho důvěrných informací, které jsou předmětem bezpečnostní politiky. Je důležité předcházet neoprávněným přístupům k těmto informacím.

A.11.6.1 Omezení přístupu k informacím (kritické):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Každý zaměstnanec musí mít nastaven přístup k informacím, které potřebuje k vykonávání své činnosti. Ostatní informace musí být zabezpečeny před přístupem nepovolaných zaměstnanců. Pokus o neoprávněný přístup musí být zaznamenán a následně varována odpovědná osoba. Za pomocí DLP funkce zabezpečení dat lze rovněž řešit omezení přístupu k informacím na aplikační úrovni.
Zdroje opatření: Časová synchronizace probíhá automaticky (0 hodin)

4.4.5.7 A.12.3 Kryptografická opatření

Kryptografie a šifrování dokáže uchránit důvěrnost, autentičnost a integritu informací, díky tomu se aktivně zvyšuje bezpečnost.

A.12.3.1 Politika pro použití kryptografických opatření (nízké):

Odpovědná osoba: DLP technik (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Pro zabezpečení informací je vhodné definovat šifrovací algoritmy, případně šifrované virtuální disky, které budou sloužit jako uložiště informací. Výše pojmenované funkce jsou plně podporované ze strany DLP produktu.
Zdroje opatření: Tvorba šifrovaných disků a bezpečnostní politiky (3 dny / měsíčně)

A.12.3.2 Správa klíčů (nízké):

Odpovědná osoba: DLP technik (společnost <*utajená*>)

Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Pro podporu šifrování je potřeba definice a používání bezpečnostních klíčů pro jednotlivé koncové stanice. Klíče jsou DLP produktem generovány pro každou stanici, která je využívá například pro připojení šifrovaných virtuálních disků.
Zdroje opatření: Tvorba databáze klíčů (2 dny / měsíčně)

4.4.5.8 A.12.5 Bezpečnost procesů vývoje a podpory

Při modifikaci nebo instalaci softwarového vybavení může docházet k různým chybám, které mohou vést až k úniku dat. Z toho důvodu je vhodné udržovat bezpečnost programového vybavení společnosti.

A.12.5.4 Únik informací (kritické):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Při používání nového softwaru odpovědná osoba prověří, zda nedochází k nepovolenému úniku dat prostřednictvím sítě nebo externích zdrojů. Za pomocí DLP produktu lze chránit informace na aplikační úrovni a pravidelně monitorovat chod těchto aplikací.
Zdroje opatření: Monitorování chodu aplikací, zda nedochází k únikům dat (3 hodiny / týdně)

4.4.5.9 A.15.1 Soulad s právními normami

Společnost při zpracovávání záznamů a práce s osobními údaji (rodná čísla, čísla účtů a jiné), by se měla vyvarovat porušení norem trestního nebo občanského práva, zákonných nebo smluvních a bezpečnostních požadavků.

A.15.1.3 Ochrana záznamů organizace (kritické):

Odpovědná osoba: Manažer IT (společnost <*utajená*>)
Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Záznamy společnosti, které podléhají utajení, musí být zabezpečeny proti únikům a ztrátě. K tomu se doporučuje používat funkce zabezpečení dat spolu s klasifikací dat nacházející se v DLP produktu. Při ochraně musí být dodrženy všechny právní a smluvní náležitosti.
Zdroje opatření: Zabezpečení záznamů (2 dny / měsíčně)

A.15.1.4 Ochrana dat a soukromí osobních informací (kritické):

Odpovědná osoba: Manažer IT, právní oddělení (společnost <*utajená*>)

Školitel v rámci implementace: DLP specialista (dodavatel)
Opatření: Ochrana osobních údajů musí být založena na právních předpisech a smluvních závazcích společnosti. Za pomocí funkce zabezpečení dat a šifrování dat v DLP produktu jsou osobní údaje bezpečně uloženy a přístupny pouze odpovědným osobám.
Zdroje opatření: Zabezpečení záznamů (2 dny / měsíčně)

Při zavedení opatření se vycházelo z funkčnosti DLP produktu, který umožňoval řešit jednotlivé problémy různými způsoby. Jedná se pouze o základní doporučení, jež společnost <*utajená*> může využít, případně na základě pozdějších vlastních zkušeností může přejít na jiný přístup zabezpečení dat pomocí DLP řešení. Důležitým aspektem je stále vylepšování DLP politiky a s tím souvisí také lepší přístup k definovaným opatřením na základě vlastních nejlepších zkušeností.

4.4.6 Návrh technického řešení

Z technického pohledu je síťová architektura IT ve společnosti dostatečná pro nasazení kompletního DLP systému, rovněž i všechny koncové stanice a přenosné počítače splňují minimální požadavky definované v kapitole 5.3.3. Bylo zjištěno, že společnost vlastní 2 servery, které nejsou využívány pro činnost, takže zde se nachází i technická rezerva při problému s výkonostní celého řešení. Dalším podpůrným aspektem pro bezproblémovou implementaci je využívání Active Directory[27] a díky tomu proběhne plné nasazení rychleji, než se původně očekávalo.

DLP systém je založen na architektuře klient-server. Na koncových stanicích je spuštěna aplikace endpoint DLP agent, který komunikuje se serverovou komponentou DLP a centrální databází založenou na MS SQL serveru. Bezpečnostní manažer nebo odpovědná osoba využívají ke vzdálenému připojení správcovskou aplikaci. Data získaná monitoringem jednotlivých koncových stanic jsou ukládána na databázový server. Popis jednotlivých komponentů[28] je následující:

a) Endpoint DLP agent - reprezentuje klientskou komponentu, která běží na koncových stanicích zaměstnanců. Spouští se vždy při startu operačního systému jako služba a zajišťuje monitorování, vynucování bezpečnostních DLP politik. Komunikace probíhá s databází a serverovou komponentou.
b) Serverová komponenta DLP - reprezentuje serverovou část. Běží jako služba na serveru. V rámci jedné domény jich může běžet i více a to díky distribuci

[27] Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře.

[28] Možnost pro prvotní implementaci je nainstalovat všechny 3 komponenty na jednu stanici a sledovat jejích funkčnost, ale z důvodu objektivního testování funkcionalit se tento přístup nedoporučuje.

zátěže pomocí rozdělování stromu Active Directory. V rámci společnosti je dostačující jedna běžící serverová komponenta.

c) Správcovská aplikace DLP – je centrum celého řešení a slouží pro nastavení a správu endpoint DLP agentů, serverové komponenty, databáze a samozřejmě pro správu funkčnosti. Dále zobrazuje výstupy monitoringu, statistiky a grafy.

Instalace produktu je nenáročná, jelikož všechny komponenty jsou součástí speciálního univerzálního instalátoru (obsahuje také podrobného průvodce pro různé typy instalací a požadavků), který se spouští na dané stanici a odpovědná osoba volí instalaci požadované komponenty. Jako první část celé integrace je instalace služby serverové komponenty, která v rámci společnosti zajišťuje propojení mezi všemi částmi DLP produktu. Instalaci je nutné provádět na serverový operační systém s doménovou službou Active Directory. Služba se automaticky spouští ihned po instalaci. Správcovská aplikace se instaluje formou průvodce, kterému není potřeba věnovat větší pozornost. Záleží na odpovědné osobě, kde si přejete aplikaci nainstalovat. Lze ji provozovat jak na serverových, tak i klientských stanicích. Endpoint DLP agenta je potřeba instalovat na koncovou stanici zaměstnanců. Využít jde manuální instalace za pomocí průvodce instalátoru, kde se musí nadefinovat IP adresa serverové komponenty nebo za pomocí GPO[29] pravidel. Pro prvotní nasazení se doporučuje instalace přes průvodce, až ve fází plného nasazení je vhodné přejít na GPO pravidla.

Ve společnosti <*utajená*> se doporučuje DLP řešení implementovat postupně po jednotlivých fázích z důvodu ověření funkcionality a kompatibility s ostatními prvky infrastruktury ICT (síťová architektura, používané aplikace). V každé fázi je vytvořen seznam testů, který vychází z reálného použití.

4.4.6.1 První fáze implementace – testování na vzorové stanici

V první fázi proběhne instalace všech části DLP systému (skládající se ze tří komponent – serverová část, správcovská aplikace, endpoint DLP agent) na jednu vybranou koncovou stanici, která leží mimo síťovou architekturu společnosti z důvodu možných technických problémů. Ověří se základní kompatibilita a stabilita koncové stanice s nainstalovaným endpoint DLP agentem. Vybraná stanice má shodné aplikační vybavení jako je používáno v celé společnosti. Před instalací se doporučuje udělat bod obnovy operačního systému, ke kterému se lze vrátit při neočekávaných problémech a nejasnostech.

Dalším důležitým krokem je tvorba testovacích scénářů a akceptačních kritérií[30] na základě zkušenosti DLP specialisty a výstupech technického auditu prostředí

[29] Group Policy je nástroj pro hromadnou správu oprávnění a nastavení aplikovaných jak na celý počítač, tak na přihlášeného uživatele. Ve skupinách zásad je možné vytvářet kolekce nastavení, nazývané Group Policy Object - GPO, které dokáží měnit konkrétní parametry chování počítače nebo uživatele.

[30] Akceptační kritérium je stav, který má nastat po provedení testu, aby byl test označen za přijatelný. Jestliže se výsledek testu nevyhovuje akceptačnímu kritériu, test je označen za nepřijatelný.

společnosti. Při provádění testu jsou vyhodnocována akceptační kritéria, určující, zda může implementace postoupit do další fáze. Testovací scénáře musí obsahovat popis testu, odpovědnou osobu za test, akceptační kritérium a vyhodnocení. Při navrhování seznamu testů se vycházelo z reálného prostředí společnosti <*utajená*>.

Tab. 16: Návrh testů pro první fázi implementace (Zdroj: Vlastní tvorba pro DP)

	Popis testu	**Odpovědná osoba**	**Akceptační kritérium**
T1	Instalace serverové komponenty a kontrola spuštění služby	DLP technik	Bez problémů
T2	Kontrola funkce restartování serverové komponenty	DLP technik	Bez problémů
T3	Instalace správcovské aplikace a nastavení spojení se serverovou komponentou	DLP technik	Bez problémů
T4	Instalace endpoint DLP agent	DLP technik	Bez problémů
T5	Odinstalace endpoint DLP agenta	DLP technik	Bez problémů
T6	Rychlost koncové stanice	DLP technik	Zpomalení OS o max. 15%
T7	Uživatel se pokusí násilně vypínat službu endpoint DLP agenta, aby se zbavil ochrany	DLP technik	Nedovoleno
T8	Spouštění aplikací a základní pracovní činnosti s nimi (načítání dat, ukládání dat)	DLP technik	Bez problémů
T9	Spojení endpoint DLP agenta se serverovou komponentou	DLP technik	Bez problémů
T10	Ověření spojení všech komponent dohromady za pomocí správcovské aplikace	DLP technik	Bez problémů
T11	Přes správcovskou aplikaci nastavit klasifikaci dat a následná kontrola výsledků	DLP technik	Bez problémů

Při provádění testů se musí provádět zápis průběhu, který je následně předán dodavateli DLP řešení. Na základě zápisu a rozhovorech s DLP technikem společnosti se provede vyhodnocení akceptačních kritérií a posoudí se postup do další fáze implementace. DLP technik je také plně zodpovědný za průběh první fáze zavádění.

4.4.6.2 Druhá fáze implementace – pilotní nasazení

Druhá fáze implementace je časově a technicky náročnější, jelikož celý DLP systém se integruje do reálné infrastruktury společnosti. Pro ověření funkčnosti v reálném provozu se vybere nejméně rizikové oddělení, ve kterém probíhá důkladné testování všech potřebných funkcionalit. Vybraným oddělením je marketing, kde případné problémy s nefunkčností stanic nebudou mít takový velký dopad na fungování společnosti.

Implementace začíná serverovou komponentou a konfigurací MS SQL serveru, kde je nutné vytvořit databázi pro ukládání nastavení a záznamů z koncových stanic. Serverová komponenta se instaluje přímo na aplikační server společnosti. Následně za pomocí služby GPO jsou vybrány stanice, které mají být předmětem instalace endpoint

DLP agenta (oddělení marketingu). Konfigurace je o něco náročnější, ale celý proces je s větším počtem stanic rychlejší a flexibilnější. Poslední částí je instalace správcovské aplikace na libovolný počítač v síti. Doporučuje se použít počítač, na který mají přístup pouze odpovědné osoby (manažer IT, DLP technik nebo jednatel). Z této stanice bude probíhat kompletní správa DLP řešení a kontrola prováděného monitoringu koncových stanic.

Nezbytným krokem pro správné posouzení druhé fáze jsou rovněž testovací scénáře, které v této fázi vychází ze seznamu hrozeb definovaný v kapitole 5.4.3. I zde je nutné definovat akceptační kritéria, určující správnost testu.

Tab. 17: Návrh testů pro druhou fázi implementace (Zdroj: Vlastní tvorba pro DP)

	Popis testu	**Odpovědná osoba**	**Akceptační kritérium**
P1	Instalace serverové komponenty a konfigurace MS SQL serveru	DLP technik	Bez problémů
P2	Instalace správcovské aplikace a spojení se serverem	DLP technik	Bez problémů
P3	Instalace endpoint DLP agenta za pomocí GPO	DLP technik	Bez problémů
P4	Odinstalace endpoint DLP agenta za pomocí GPO	DLP technik	Bez problémů
P5	Ověření spojení všech komponent dohromady za pomocí správcovské aplikace	DLP technik	Bez problémů
P6	Klasifikace všech marketingových dokumentů	DLP technik	Minimálně 98% dokumentů
P7	Označení nalezených dokumentů a nastavení důvěrnosti	DLP technik	Všechny klasifikované dokumenty
P8	Manuální šifrovaní a dešifrování dokumentů	DLP technik	Bez problémů
P9	Odeslání důvěrného dokumentu na síť	DLP technik	Zakázáno a informovat
P10	Odeslání obyčejného dokumentu na síť	DLP technik	Bez problému
P11	Vytisknutí důvěrného dokumentu	DLP technik	Zakázáno a informovat
P12	Neoprávněné otevření souboru z aplikace MS Word	DLP technik	Zakázáno a informovat
P13	Použití vlastních zakázaného externího disku	DLP technik	Zakázáno a informovat
P14	Úprava důvěrných dokumentů a pokus o uložení	DLP technik	Zakázáno a informovat
P15	Skartování dat na externím zařízení	DLP technik	Nemožnost najít dokument

Pro plné nasazení musí vyhovovat všechna akceptační kritéria a při testování je nutné zapisovat chování DLP systému, aby bylo možné předejít problémům a vzniklým nejasnostem při plném nasazení, které se bude řídit výstupem z pilotního testování. Za pilotní nasazení je zodpovědný DLP technik, který předává všechny výstupy DLP specialistovi na analýzu a manažerovi IT na zhodnocení. Na základě jednání s vedením společnosti se rozhodne termín plánovaného plného nasazení. Původně odhadovaný termín je stanoven na 5. 8. 2013.

4.4.6.3 Třetí fáze implementace – plné nasazení

V poslední fázi implementace se na zbývající koncové stanice nainstaluje endpoint DLP agent rovněž za pomocí služby GPO. Důležitým upozorněním je, že nasazování probíhá po odděleních v následujícím pořadí[31]:

a) Oddělení marketing (už je vše připraveno z pilotního nasazení)
b) Oddělení obchodu
c) Oddělení vývoje
d) Operativní a právní oddělení
e) Oddělení IT

Serverová komponenta a správcovská aplikace zůstávají nainstalované z pilotního nasazení. Důležitou součástí poslední části je seznam provedených testů, vytvořený na základě seznamu opatření, který je definován v kapitole 5.4.5. Pokud jsou splněna všechna akceptační kritéria definovaných testů, lze považovat, že vybraná opatření z normy ČSN ISO/IEC 27001 jsou implementována.

Tab. 18: Návrh testů pro třetí fázi implementace (Zdroj: Vlastní tvorba pro DP)

	Popis testu	**Odpovědná osoba**	**Akceptační kritérium**
S1	Instalace všech endpoint DLP agenta za pomocí GPO	DLP technik	Bez problémů
S2	Odinstalace vybraného endpoint DLP agenta za pomocí GPO	DLP technik	Bez problémů
S3	Ověření spojení všech komponent dohromady za pomocí správcovské aplikace	DLP technik	Bez problémů
S4	Klasifikace všech interních dokumentů na základě vytvořených pravidel	DLP technik	Minimálně 99% dokumentů
S5	Označení nalezených dokumentů a nastavení důvěrnosti	DLP technik	Všechny klasifikované dokumenty
S6	Manuální i automatické šifrování / dešifrování označených dokumentů při kopírování mimo perimetr společnosti	DLP technik	Bez problému
S7	Skartování vybraných dat	DLP technik	Nemožnost najít skartovaný dokument
S8	Neoprávněné otevření souboru	DLP technik	Zakázáno a informovat
S9	Automatické šifrování dat při kopírování na externí zařízení	DLP technik	Bez problému
S10	Šifrování emailů s označenými informacemi	DLP technik	Bez problému
S11	Analýza záznamů z předešlých testů	IT manažer	Bez problému
S12	Analýza záznamů ohledně práce na koncové stanici (používané aplikace)	IT manažer	Bez problému

[31] Implementace dalšího oddělení smí pokračovat, až jakmile bude dokončena implementace na předchozím oddělení.

	Popis testu	Odpovědná osoba	Akceptační kritérium
S13	Nastavení uživatelských účtů pro přístup do správcovské aplikace a ověřit bezpečnost	IT manažer	Bez problému
S14	Kontrola záznamů spojených s manipulací správcovské aplikace	IT manažer	Bez problému
S15	Při technických problémech koncové stanice upozornit odpovědnou osobu	DLP technik	Bez problému
S16	Synchronizovat nastavení času na všech koncových stanicích	DLP technik	Bez problému
S17	Nepovolený přístup aplikace k vybraným označeným dokumentům	DLP technik	Zakázáno a informovat
S18	Vytvoření virtuálních zašifrovaných disků	DLP technik	Bez problému
S19	Pro každou koncovou stanici vygenerovat bezpečnostní klíč	DLP technik	Bez problému
S20	Zašifrovaná databáze záznamů	IT manažer	Bez problému
S21	Klasifikovat dokumenty obsahující osobní informace a aplikovat na ně speciální bezpečnostní politiku a přístupy	IT manažer	Bez problému

Úspěšné ukončení implementace a předání celého projektu vedení společnosti závisí na splnění všech výše definovaných akceptačních kritériích.

4.4.7 Návrh školení zaměstnanců

Pro zvládnutí logiky správy DLP produktu a nastavování bezpečnostní politiky na základě ISMS je důležité provést školení. Školení bude probíhat na dvou fázích, kdy v první fázi (25.7. – 26.7.2013) proběhne seznámení s normou ČSN ISO/IEC 27001, které bude mít na starosti ISMS specialista. Účast je povinná pro celé oddělení IT a vedení společnosti. Druhá část školení proběhne v termínech od 29.7. – 31.7.2013 a předmětem je technický popis DLP produktu, seznámení práce se správcovskou aplikací a popis jednotlivých funkcí. Školení je primárně určeno pro DLP technika a IT manažera.

4.4.8 Implementační smlouva

Implementační smlouva pojednává o postupu zavádění DLP řešení do společnosti. Podle časového rozsahu projektu je začátek plánován na 22.7.2013 a dokončení 13.8.2013 při schvalování všech akceptačních kritérií.

Jestliže je test neproveditelný nebo se u něho vyskytne chyba, která zabrání potvrzení akceptačního kritéria, je nutné ho maximálně 2x opakovat. Při posledním selhání musí být ihned kontaktován DLP technik, který se pokusí sjednat nápravu osobně nebo za pomocí technické podpory dodavatele DLP řešení.

Odpovědná osoba za celý proces implementace je manažer IT, který je součástí implementačního týmu, jehož složení je definováno v kapitole 5.3.2. Po dokončené implementaci odpovědnost převezme nový zaměstnanec společnosti (DLP technik), podílející se aktivně na všech částech zavádění.

Cena služeb v rámci implementace (testování na jedné stanici, pilotní nasazení, plné nasazení) je kalkulována na 65 000 Kč a cena za licence činí 209 930 Kč. Celková suma za implementaci DLP řešení je 274 930 Kč.

4.5 Implementace

Instalace DLP systému do společnosti <*utajená*> se řídí postupy dohodnuté v implementační smlouvě. Celá implementace je rozdělena na tři fáze, ve kterých se vždy instalují všechny potřebné komponenty a provádí povinné úkony:

1. Ověření splněných podmínek pro síťovou architekturu.
2. Na vybraný server (počítač) se nainstaluje serverová komponenta:
    a. Instalace probíhá z univerzálního instalátoru, kde je nutné zvolit cílovou složku (C:\DLP\Server\). Po úspěšné instalaci se služba ServerDLP.exe automatický spustí. Ověření spuštěné služby probíhá ve správci úloh poskytované operačním systémem. Poslední krok je nastavit výjimky pro firewall a antivirový program na daný proces a komunikační porty 4438 (slouží pro komunikace s endpoint DLP agentem) a 4441 (slouží pro komunikaci se správcovskou aplikací).
3. Na vybraný počítač sloužící pro správu DLP řešení se nainstaluje správcovská aplikace:
    a. Instalace probíhá také z univerzálního instalátoru, kde je nutné zvolit cílovou složku (C:\Program Files\Správcovská aplikace\). Na závěr je nutné nastavit příslušné výjimky na firewall a antivirový program. Správcovská aplikace běží jako proces s názvem DLPspravce.exe.
4. Za pomocí správcovské aplikace se provede napojení a konfigurace serverové komponenty:
    a. Po spuštění správcovské aplikace uživatel vytvoří dle integrovaného průvodce připojení na serverovou komponentu a vyplní všechny potřebné údaje (IP komponenty adresa, adresa databázového serveru, přístupové heslo).
5. Na koncové stanice proběhne instalace endpoint DLP agenta:
    a. Instalace koncové stanice probíhá buď přes univerzálního instalátora, kde se zvolí cílová složka (C:\Program Files\DLPagent\), adresa serverové komponenty a komunikační port (4438) nebo za pomocí služby GPO. Po instalaci se spustí ihned proces DLPagent.exe, který je pro běžného uživatele z bezpečnostních důvodů skrytý.

6. Konfigurace všech komponent a ověření vzájemné komunikace.

4.5.1 Testování na vzorové stanici

Podle popisu v implementační smlouvě se provádí instalace DLP produktu na jednu vybranou stanici, kde bude vyzkoušena funkcionalita a dojde k prvnímu seznámení s funkčností a logikou DLP produktu.

Tab. 19: Výsledky testu první fáze implementace (Zdroj: Vlastní tvorba pro DP)

	Popis testu	**Akceptační kritérium**	**Výsledky testu**
T1	Instalace serverové komponenty a kontrola spuštění služby	Bez problémů	V pořádku
T2	Kontrola funkce restartování serverové komponenty	Bez problémů	V pořádku
T3	Instalace správcovské aplikace a nastavení spojení se serverovou komponentou	Bez problémů	V pořádku
T4	Instalace endpoint DLP agent	Bez problémů	V pořádku
T5	Odinstalace endpoint DLP agenta	Bez problémů	V pořádku
T6	Rychlost koncové stanice	Zpomalení OS o max. 15%	Neprošlo (zpomalené OS o 20%)
T7	Uživatel se pokusí násilně vypínat službu endpoint DLP agenta, aby se zbavil ochrany	Nedovoleno	V pořádku
T8	Spouštění aplikací a základní pracovní činnosti s nimi (načítání dat, ukládání dat)	Bez problémů	Neprošlo (Adobe Phostoshop CS6)
T9	Spojení endpoint DLP agenta se serverovou komponentou	Bez problémů	V pořádku
T10	Ověření spojení všech komponent dohromady za pomocí správcovské aplikace	Bez problémů	V pořádku
T11	Přes správcovskou aplikaci nastavit klasifikaci dat a následná kontrola výsledků	Bez problémů	V pořádku

U výsledků lze pozorovat, že testy T6 a T8 neprošly akceptačním kritériem a byl kontaktován DLP specialista, který provedl analýzu záznamu z testování a vyhodnocení výsledků. Analýza testu T6 ukázala, že zpomalení operačního systému o 20% bylo způsobeno neprovedenou aktualizací koncové stanice, což mělo za následek i špatnou spolupráci endpoint DLP agenta s aplikací Adobe Photoshop CS6 (zde je garantována kompatibilita). Po provedené aktualizaci operačního systému bylo naměřené zpomalení pouze o 12% a problémy s Adobe Photoshop CS6 odezněly.

4.5.2 Školení uživatelů

Školení uživatelů probíhá formou prezentací a workshopů, které má připravené dodavatel DLP řešení. Povinnou účast mají členové implementačního týmu, jelikož ti

budou posléze proškolovat své zaměstnance ohledně práce s nainstalovaným DLP systémem.

4.5.3 Pilotní nasazení

Po vyřešení problémů z první fáze se implementační tým rozhodl nainstalovat a otestovat DLP systém v reálném provozu. Serverová komponenta byla zapojena do síťového provozu a endpoint DLP agent byl nainstalován podle implementační smlouvy pouze na oddělení marketingu, kde také probíhaly všechny vyhodnocovací testy.

Tab. 20: Výsledky testů po druhé fázi implementace (Zdroj: Vlastní tvorba pro DP)

	Popis testu	**Akceptační kritérium**	**Výsledky testu**
P1	Instalace serverové komponenty a konfigurace MS SQL serveru	Bez problémů	V pořádku
P2	Instalace správcovské aplikace a spojení se serverem	Bez problémů	Neprošlo
P3	Instalace endpoint DLP agenta za pomocí GPO	Bez problémů	V pořádku
P4	Odinstalace endpoint DLP agenta za pomocí GPO	Bez problémů	V pořádku
P5	Ověření spojení všech komponent dohromady za pomocí správcovské aplikace	Bez problémů	V pořádku
P6	Klasifikace všech marketingových dokumentů	Minimálně 98% dokumentů	V pořádku
P7	Označení nalezených dokumentů a nastavení důvěrnosti	Všechny klasifikované dokumenty	Neprošlo (10% se špatně označilo)
P8	Manuální šifrovaní a dešifrování dokumentů	Bez problémů	V pořádku
P9	Odeslání důvěrného dokumentu na síť	Zakázáno a informovat	Neprošlo (chyběla informovanost)
P10	Odeslání obyčejného dokumentu na síť	Bez problému	V pořádku
P11	Vytisknutí důvěrného dokumentu	Zakázáno a informovat	V pořádku
P12	Neoprávněné otevření souboru z aplikace MS Word	Zakázáno a informovat	V pořádku
P13	Použití vlastního zakázaného externího disku	Zakázáno a informovat	V pořádku
P14	Úprava důvěrných dokumentů a pokus o uložení	Zakázáno a informovat	V pořádku
P15	Skartování dat na externím zařízení	Nemožnost najít dokument	V pořádku

U pilotní fáze se objevily celkem 3 problémy (test P2, P7 a P9). U testu P2 bylo objeveno, že chyba ve spojení nastala z důvodu špatně nastavených výjimek pro firewall (změna komunikačního portu, místo 4441 byl nastaven port 4438, sloužící pro komunikaci s endpoint DLP agentem). Po následné opravě test proběhl v pořádku.

Vážnější komplikace nastaly u testu P7 a P9. DLP specialista po analýze a komunikaci s oddělením podpory zjistil, že problém je na straně produktu, o kterém

dodavatel DLP řešení už ví a garantuje do nové aktualizace DLP produktu odstranit výše definované problémy.

4.5.4 Plné nasazení

I přes objevené problémy se společnost <*utajená*> rozhodla pokračovat v implementaci. Při instalování DLP produktu pro plné nasazení je k dispozici aktualizovaná verze, ve které jsou vyřešeny problémy z předchozí etapy a testování proběhlo úspěšně.

Podle plánu, který je definovaný v implementační smlouvě se instaluje endpoint DLP agent postupně po jednotlivých odděleních:

a) Oddělení marketingu – v pořádku
b) Oddělení obchodu – v pořádku
c) Oddělení vývoje – v pořádku
d) Operativní a právní oddělení – v pořádku
e) Oddělení IT – v pořádku

Výhodou tohoto typu implementace je dostupná modulárnost. Společnost <*utajená*> může zvolit libovolné pořadí oddělení, ve kterých si přeje nasazovat DLP systém. Díky tomu lze při implementaci ušetřit čas i peníze, pokud je zvolen vhodný postup, který je pro společnost dostatečně vyhovující.

Po dokončení kompletní instalace na všechny koncové stanice se přešlo k testování dle definovaného seznamu testů. Při postupném testování se neobjevily žádné zásadní problémy, které by nedovolily přijmutí akceptačního kritéria.

Také vytvořený seznam opatření z kapitoly 5.4.5 prošel po implementaci poslední fázi revizí a zhodnotily se jednotlivé položky spolu s provedenými testy a zjistilo se, jak velký význam mělo zavedení DLP systému do společnosti <*utajená*> na opatření.

Tab. 21: Výsledky testů po plném nasazení (Zdroj: Vlastní tvorba pro DP)

	Popis testu	**Akceptační kritérium**	**Výsledky testu**
S1	Instalace všech endpoint DLP agenta za pomocí GPO	Bez problémů	V pořádku (-)
S2	Odinstalace vybraného endpoint DLP agenta za pomocí GPO	Bez problémů	V pořádku (-)
S3	Ověření spojení všech komponent dohromady za pomocí správcovské aplikace	Bez problémů	V pořádku (-)
S4	Klasifikace všech interních dokumentů na základě vytvořených pravidel	Minimálně 99% dokumentů	V pořádku (7.2.1)
S5	Označení nalezených dokumentů a nastavení důvěrnosti	Všechny klasifikované dokumenty	V pořádku (7.2.2)
S6	Manuální i automatické šifrování / dešifrování označených dokumentů při kopírování mimo perimetr společnosti	Bez problému	V pořádku (9.2.5)

	Popis testu	Odpovědná osoba	Výsledky testu
S7	Skartování vybraných dat	Nemožnost najít skartovaný dokument	V pořádku (9.2.6)
S8	Neoprávněné otevření souboru	Zakázáno a informovat	V pořádku (10.7.4)
S9	Automatické šifrování dat při kopírování na externí zařízení	Bez problému	V pořádku (10.8.3)
S10	Šifrování emailů s označenými informacemi	Bez problému	V pořádku (10.8.4)
S11	Analýza záznamů z předešlých testů	Bez problému	V pořádku (10.10.1)
S12	Analýza záznamů ohledně práce na koncové stanici (používané aplikace)	Bez problému	V pořádku (10.10.2)
S13	Nastavení uživatelských účtů pro přístup do správcovské aplikace a ověřit jejich	Bez problému	V pořádku (10.10.3)
S14	Kontrola záznamů spojených s manipulací správcovské aplikace	Bez problému	V pořádku (10.10.4)
S15	Při technických problémech koncové stanice upozornit odpovědnou osobu	Bez problému	V pořádku (10.10.5)
S16	Synchronizovat nastavení času na všech koncových stanicích	Bez problému	V pořádku (10.10.6)
S17	Nepovolený přístup aplikace k vybraným označeným dokumentům	Zakázáno a informovat	V pořádku (11.6.1)
S18	Vytvoření virtuálních zašifrovaných disků	Bez problému	V pořádku (12.3.1)
S19	Pro každou koncovou stanici vygenerovat bezpečnostní klíč	Bez problému	V pořádku (12.3.2)
S20	Zašifrovaná databáze záznamů	Bez problému	V pořádku (15.1.3)
S21	Klasifikovat dokumenty obsahující osobní informace a aplikovat na ně speciální bezpečnostní politiku a přístupy	Bez problému	V pořádku (15.1.4)

4.5.5 Akceptační řízení a předání implementace

Celý proces implementace probíhal v pořádku a objevené problémy se řešily operativně. Dodavatel DLP předal společnosti *<utajená>* všechny dokumenty a doporučení na zlepšování bezpečnostní politiky a chodu celého systému. Hlavní odpovědnost v rámci implementace měl manažer IT, který je rovněž hlavní odpovědnou osobou za bezpečnost informací. Po předání akceptačního protokolu odpovědnost ve společnosti za samotnou funkčnost a stabilitu DLP systému převzal DLP technik. Posledním dokumentem, který utvrzuje správnost implementace a spokojenost společnosti s celým průběhem, je podepsání akceptačního protokolu.

Tab. 22: Akceptační protokol (Zdroj: Vlastní tvorba pro DP)

Akceptační protokol			
Název projektu:		Implementace DLP řešení	
Dodavatel:		*utajená informace*	
Zákazník:		*utajená informace*	
Akceptace			
Předmět akceptačního řízení:		Implementace DLP řešení na základě provedené studie proveditelnosti a implementační analýzy s definovanými akceptačními kritérii. Pro správnost implementace musí vyhovovat všechna akceptační kritéria bez výhrad.	
Seznam výhrad			
Výhrada		Termín a vyřešení výhrady	
Při pilotním nasazení nebyly přijaty testy P7 a P9.		Testy byly přijaty při aktualizaci nové verze produktu. Aktualizace proběhla 7.8.2013 ve fázi plného nasazení.	
Výsledek akceptace			
Akceptováno		~~Neakceptováno~~	
Podpisová část			
Místo:		*utajená informace*	
Datum a čas:		*utajená informace*	
Dodavatel		Zákazník	
Jméno:	*DLP specialista*	Jméno:	*Manažer IT*
Podpis:	*utajená informace*	Podpis:	*utajená informace*

4.6 Posouzení a vylepšení DLP řešení

Po technické implementaci a nasazení DLP systému do společnosti je nutné provádět jeho pravidelné monitorování a přezkoumání, zda všechna nastavení pracují správně a uživatelé se chovají k zabezpečeným informacím adekvátně. Na základě těchto výsledků je třeba upravovat nastavení DLP produktu tak, aby vedení společnosti bylo spokojeno a zaměstnanci neměli pocit omezování v pracovní době.

Rovněž se doporučuje jednou za 6 - 12 měsíců provést analýzu rizik, zda se objevila nová aktiva, případně nové hrozby, které budou potřeba omezit s pomocí implementovaného DLP řešení. Jedná se o nekonečný cyklus událostí vedoucí ke kvalitní bezpečnosti informací. Odpovědnou osobou za správné nastavení, fungování a vylepšování celého DLP systému má na starosti DLP technik a manažer IT zodpovídá za dodržování definované bezpečnostní politiky.

4.7 Finanční zhodnocení

Zavádění nové technologie do společnosti <*utajená*> byl finančně a časově velmi náročný proces. Celá finanční stránka se odvíjela od poskytovaných služeb ze strany

dodavatele DLP řešení. Společnost <*utajená*> měla na výběr ze dvou variant financování projektu. Jedna z možností byla zakoupení si pouze licencí DLP produktu a celou implementaci podle vlastních zkušeností s instalací softwaru provádět samostatně, bez nutnosti asistence ze strany DLP dodavatele. Druhá varianta spočívala v zakoupení licence DLP produktu a k němu poskytované služby v rámci celé implementace. Jelikož společnost nemá zaveden management jakosti a řízení (ČSN ISO/IEC 9001), byla na základě jednání vedení společnosti <*utajená*> dohodnuta druhá varianta financování (zakoupení licence a služeb pro implementaci).

Pro potřeby implementace a následně pro údržbu DLP řešení společnost <*utajená*> na doporučení dodavatele vypsala výběrové řízení na novou pozici s názvem DLP technik, kterého před implementací zaměstnala. Náklady spojené s jeho mzdou je nutné započítat v rámci nasazování DLP řešení, které trvá tři měsíce a super hrubá mzda byla stanovena na 41 200 Kč měsíčně.

Tab. 23: Náklady na implementaci DLP pro první rok (Zdroj: Vlastní tvorba pro DP)

Nákladová položka	**Poznámka**	**Částka**
Mzda pro DLP technika	Náklady na 3 měsíce	123 600 Kč
Licence DLP produktu na 1 rok	Bylo potřeba 70 licencí	209 930 Kč
Služby v rámci implementace	Celý projekt implementace DLP	179 000 Kč
Technická podpora na 1 rok	Technická podpora je v ceně licence produktu	0 Kč
Celková částka pro první rok		**512 530 Kč**

Jelikož se očekává, že společnost <*utajená*> bude chtít DLP systém provozovat i další rok, bude nutné provést opět investici do licencí. Nyní už odpadá nutnost investovat do služeb a případně mezd nových zaměstnanců, jelikož už budou zaběhlé procesy pro práci s DLP systémem. Je očekáván nárůst počtu licencí, jelikož společnost <*utajená*> se stále dynamicky rozvíjí a přicházejí noví zaměstnanci.

Tab. 24: Náklady provozu DLP systému na další rok (Zdroj: Vlastní tvorba pro DP)

Nákladová položka	**Poznámka**	**Částka**
Licence DLP produktu na další rok	Bude potřeba 80 licencí	239 920 Kč
Technická podpora na další rok	Technická podpora je v ceně licence produktu	0 Kč
Celková částka pro další rok		**239 920 Kč**

Celkové finanční náklady na implementaci a následný provoz DLP řešení po dobu dvou let byly vyčísleny na hodnotu **752 450 Kč**.

ZÁVĚR

Celá diplomová práce je koncipována na dvě hlavní části. V první teoretické části jsou rozebrány základní principy spojené s bezpečností organizace a se zaváděním systému řízení bezpečnosti informací, které jsou podpořeny řadou norem ČSN ISO/IEC 27000:2006. Další kapitoly se věnují analýze rizik a seznámením s interními hrozbami, kde jsou zmiňovány a řešeny současné problémy ochrany citlivých dat v organizacích a možné nežádoucí aktivity samotných zaměstnanců a jejich ekonomický dopad. Konec teoretické části ukazuje možné způsoby řešení interních hrozeb za pomocí monitorovacího softwaru a systému na ochranu dat před ztrátou, neboli DLP (data loss prevention).

Druhá část diplomové práce se věnuje reálné implementaci DLP řešení do vybrané společnosti <*utajená*>, která má zájem zvýšit ochranu svých citlivých dat a chce postupně usilovat o získání certifikace ISMS podle ČSN ISO/IEC 27001, jelikož podobné mechanismy nejsou ve společnosti vůbec zavedeny a při rostoucí expanzi se objevuje i větší riziko úniku dat a interních hrozeb. Při zavádění DLP řešení jsem vycházel primárně z vlastních znalostí a pracovních zkušeností, které jsou spojeny s několikaletým vývojem DLP softwaru a jeho nasazováním v reálném prostředí. Celá praktická část je psána ze strany dodavatele DLP řešení, který s vybranou společností <*utajená*> řeší všechny problémy spojené se vzniklou zakázkou.

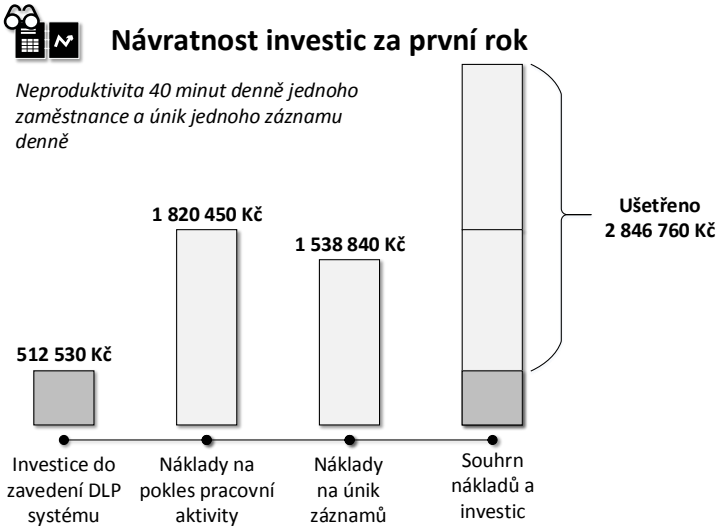
Základním bodem bylo navázání obchodního kontaktu se společností <*utajená*> a vytvořit dokument o cílech a záměrech, který reflektoval hlavní požadavky pro zavedení DLP systému. Z vytvořeného dokumentu se vycházelo při tvorbě studie proveditelnosti, která patřila mezi stěžejní pilíře celé implementace a určovala celý její směr. Studie proveditelnosti totiž reprezentovala hlavní kupní smlouvu mezi společnostní <*utajená*> a dodavatelem DLP, kde byly definované lidské, technické, legislativní, časové a finanční aspekty celého projektu a obsahovala také seznam požadovaných analýz, které se musely ve vybrané společnosti <*utajená*> uskutečnit pro následnou bezproblémovou implementaci. Po podepsání kupní smlouvy se začalo pracovat na implementační analýze, která obsahovala detailní audit prostředí společnosti, analýzu rizik a návrh bezpečnostních opatření dle ČSN ISO/IEC 27001, která šla vyřešit dodaným DLP systémem. Nutnou součástí bylo vytvořit i kompletní technický návrh pro celou implementaci a seznam nutných školení zaměstnanců. Implementační analýza sloužila jako odrazový můstek pro hlavní implementaci DLP řešení a výstupem byla vyhotovena implementační smlouva. Celá implementace, dle technického návrhu, byla rozdělena na tři fáze (testování na vzorové stanici, pilotní nasazení a plné nasazení), ve kterých byly prováděny předepsané a schválené testy a jejich akceptační kritéria. Výstupem z každé fáze byl protokol o provedených testovacích scénářích a výsledcích. Poslední fáze celé implementace bylo akceptační řízení, kde vybraná společnost <*utajená*> a dodavatel DLP řešení podepsali protokol o

přijetí, který potvrzoval správnost celé implementace podle všech výše dohodnutých náležitostí.

Celá implementace proběhla v pořádku a ukázala, jak náročné je zavádět novou technologii do společnosti, která má přes 50 zaměstnanců. Chod společnosti <*utajená*> nebyl omezen a implementace trvala od prvního plánování po finální ukončení téměř 3 měsíce a výstupem celého projektu bylo 7 dokumentů:

a) Dokument o cílech a záměrech.
b) Studie proveditelnosti – kupní smlouva.
c) Smlouva o implementaci.
d) Protokol o výsledcích testování z první fáze.
e) Protokol o výsledcích testování z druhé fáze.
f) Protokol o výsledcích testování z třetí fáze.
g) Akceptační protokol.

Jako každý projekt nebo zavádění nové technologie do společnosti je finančně náročné a mnohdy samotné finance a jejich velikost určují úspěch a neúspěch projektu. Společnost <*utajená*> v tomto směru důvěřovala dodavateli DLP řešení a investovala také do poskytovaných služeb a cena celkové implementace dosáhla hodnoty 512 530 Kč. Díky nákupu této technologie společnost <*utajená*> mohla omezit únik dat a neaktivitu svých zaměstnanců, což mělo za následek ušetření nákladů. V kapitolách 3.4.2 a 3.4.3 jsou uvedeny finanční náklady na zaměstnance při 40 minutách neaktivní práce denně s průměrnou mzdou a náklady na únik jednoho záznamu dle výzkumu, který provedl ústav Ponemon Institute. Stojí-li společnost výpadek aktivity jednoho zaměstnance ročně 36 409 Kč, při 50 zaměstnancích to činí 1 820 450 Kč a unikne-li denně jeden záznam v průměrné hodnotě 4 216 Kč, tak ročně uniknou záznamy v hodnotě 1 538 840 Kč. Při sečtení těchto částek a odečtení nákladů na implementaci DLP řešení, ušetří společnost <*utajená*> ročně **2 846 760 Kč**.



Obr. 28: Návratnost investic za první rok (Zdroj: Vlastní tvorba pro DP)

SEZNAM POUŽITÉ LITERATURY

1) ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27000:2009. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. 24 s. Třídící znak 36 9790.

2) ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27001:2006. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006. 35 s. Třídící znak 36 9790.

3) ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27002:2006. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006. 95 s. Třídící znak 36 9790.

4) ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27005:2009. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 52 s. Třídící znak 36 9790.

5) ANTUŠÁK, Emil. *Krizová připravenost firmy*. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2013, 182 s. ISBN 978-80-7357-983-8.

6) DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací*. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 978-80-86946-88-7.

7) HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.

8) JANSA, Lukáš a Petr OTEVŘEL. *Softwarové právo: praktický průvodce právní problematikou v IT*. Vyd. 1. Brno: Computer Press, 2011, 340 s. ISBN 978-80-251-3458-0.

9) NÁRODNÍ KNIHOVNA ČR. *Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. 2013 [cit. 2013-04-24]. Dostupné z: http://aleph.nkp.cz/F/?func=file&file_name=find-b&local_base=ktd.

10) POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, 219 s. ISBN 978-80-7251-250-8.

11) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010, 354 s. Expert (Grada). ISBN 978-80-247-3051-6.

12) HAYDEN, Lance. *IT security metrics: a practical framework for measuring security*. New York: McGraw Hill, c2010, xxvii, 368 p. ISBN 00-717-1340-9.

13) MOGULL, Rich. *Understanding and selecting a data loss prevention solution.* [online]. USA: The SANS Institute, 2007 [cit. 2013-04-06]. Dostupné z: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf.

14) MOGULL, Rich. *Best practices for endpoint data loss prevention* [online]. USA: Securosis, L.L.C, 2008 [cit. 2013-04-13]. Dostupné z: https://securosis.com/assets/library/reports/BestPracticesforEndpointDLP.pdf.

15) MOGULL, Rich. *DLP content discovery: Best practices for stored data discovery and protection* [online]. USA: Securosis, L.L.C, 2008 [cit. 2013-04-14]. Dostupné z: https://securosis.com/assets/library/reports/DLP-Content-Discovery-Best-Practices.pdf.

16) MONSON, Thomas N, Sarah KAIP a Jerry ANTOON. *Loss prevention: threats and strategies : how people steal from your business and what you can do to stop it*. Medford, Or.: Advantage Source, c2004, ii, 276 p. ISBN 09-743-8301-5.

17) GALLUP BUSINESS JOURNAL. *Gallup Study: Feeling Good Matters in the Workplace* [online]. 2006 [cit. 2013-04-26]. Dostupné z: http://businessjournal.gallup.com/content/20770/gallup-study-feeling-good-matters-in-the.aspx.

18) PENEMON INSTITUTE. *Airport Insecurity: The Case of Missing & Lost Laptops* [online]. 2008 [cit. 2013-04-26]. Dostupné z: http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf.

19) PENEMON INSTITUTE. *2011 Cost of Data Breach Study: United States* [online]. 2012 [cit. 2013-04-26]. Dostupné z: http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf.

20) CHEE, Wong. *Information leakage, detection, and prevention* [online]. 2007 [cit. 2013-04-28]. Dostupné z: http://www.infotectsecurity.com/resources/ISSA_Dec_2007.pdf.

21) DEVELOPMENT, Organisation for Economic Co-operation and. *OECD principles of corporate governance* [online]. [rev. ed.]. Paris: OECD, 2004, 111 s. [cit. 2013-05-10]. ISBN 92-640-1597-3. Dostupné z: http://www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf

22) MANAGEMENTMANIA. *Managementmania.com* [online]. 2011-2013 [cit. 2013-05-10]. Dostupné z: https://managementmania.com/cs/liniova-organizacni-struktura

23) HOLČÍK, Jiří. *Analýza a klasifikace dat* [online]. Vyd. 1. Brno: Akademické nakladatelství CERM, 2012 [cit. 2013-05-10]. ISBN 978-807-2047-932. Dostupné z: http://www.iba.muni.cz/res/file/ucebnice/holcik-analyza-klasifikace-dat.pdf

24) MILKOVICH, George T. *Řízení lidských zdrojů*. Praha: Grada, 1993. ISBN 80-856-2329-3.

25) BUSINESSCENTER. *BusinessCenter.cz* [online]. 1998-2013 [cit. 2013-05-10]. Dostupné z: http://business.center.cz/business/pojmy/pojem.aspx?PojemID=1970

26) ČESKÝ STATISTICKÝ ÚŘAD. *Průměrné mzdy – 4.čtvrletí 2012* [online]. 2013 [cit. 2013-05-10]. Dostupné z: http://www.czso.cz/csu/csu.nsf/informace/cpmz031113.doc

SEZNAM POUŽITÝCH ZKRATEK

AD (*Active Directory*, adresářová služba)
AUP (*Acceptable Use Policy*, dohoda o přijatelném využívání zdrojů)
CAD (*Computer Aided Design*, počítačem podporované navrhování)
CMF (*Content Monitoring and Filtering,* monitorování a sledování obsahu)
CRM (*Customer Relationship Management*, řízení vztahu se zákazníky)
ČSN (*Česká technická norma,* -)
DLP (*Data Loss Prevention,* ochrana před ztrátou dat)
FDE (*Full Disk Encryption*, šifrování celého disku)
FFE (*File and Folder Encryption*, šifrování souborů a složek)
FTP (*File Transfer Protocol*, protokol pro přenos souborů)
GPO (*Group Policy Object*, nastavení pro skupiny)
HTTP (*Hypertext Transfer Protocol*, protokol pro výměnu hypertextových dokumentů)
ILDP (*Information Leak Detection and Prevention*, prevence proti úniku dat)
IP (*Internet Protocol,* protokolem pracujícím na síťové vrstvě)
ISG (*Information Security Governance,* správa a řízení bezpečnosti informací)
ISMS (*Information Security Management* Systém, systém řízení bezpečnosti informací)
ISO (*International Organization for Standardization*, mezinárodní organizace pro standardizaci)
ICT (*Information and Communications Technology*, informační a komunikační technologie)
NDA (*Non-Disclosure Agreement*, dohoda o důvěrnosti)
PDCA (*Plan-Do-Check-Act*, plánuj-dělej-zkontroluj-jednej)
SQL (*Structured Query Language,* strukturovaný dotazovací jazyk)
TCO (*Total Cost of Ownership*, celkové náklady vlastnictví)
TFS (*Team Foundation Server,* -)
ÚOOÚ (*Úřad pro ochranu osobních údajů,* -)
USB (*Universal Serial Bus*, univerzální sériová sběrnice)
VPN (*Virtual Private Network*, virtuální privátní síť)

SEZNAM OBRÁZKŮ

Obr. 1: Princip ISG 15
Obr. 2: Vztah úrovně bezpečnosti 16
Obr. 3: Koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací 18
Obr. 4: PDCA model aplikovaný na procesy ISMS 20
Obr. 5: Přehled činností při ustanovení ISMS 22
Obr. 6: Rozdělení oblasti bezpečnosti informací 24
Obr. 7: Proces řízení rizik ISMS 25
Obr. 8: Vztah pojmů při řízení rizik 27
Obr. 9: Ukázka porovnání interních a externích hrozeb 29
Obr. 10: Výpadek produktivity 31
Obr. 11: Průměrná cena úniku za záznam 32
Obr. 12: Kontroly zaměstnanců 36
Obr. 13: Pohyb dat ve společnosti 38
Obr. 14: Bezpečnostní událost DLP 39
Obr. 15: Ukázka principu klasifikace dat 41
Obr. 16: Princip fungování síťového DLP 42
Obr. 17: Princip fungování endpoint DLP 43
Obr. 18: Životní cyklus dat 43
Obr. 19: Organizační struktura společnosti <*utajená*> 46
Obr. 20: Základní postup přípravy na obchodní schůzku s dodavatelem DLP 49
Obr. 21: Lidské zdroje potřebné pro implementaci DLP řešení 52
Obr. 22: Základní topologie společnosti 53
Obr. 23: DLP architektura 53
Obr. 24: Časový harmonogram komunikační fáze 54
Obr. 25: Časový harmonogram pro ustanovení implementace DLP řešení 55
Obr. 26: Časový harmonogram pro zavádění a provozování DLP řešení 55
Obr. 27: Časový harmonogram pro monitorování a zlepšování DLP řešení 56
Obr. 28: Návratnost investic za první rok 84

SEZNAM TABULEK

Tab. 1: Příklady hrozeb z ČSN ISO/IEC 27005 28
Tab. 2: Ukázka cílů a záměru pro implementaci DLP 50
Tab. 3: Technické požadavky pro DLP architekturu 54
Tab. 4: Náklady na nového zaměstnance - DLP technik 56
Tab. 5: Rozpis a ceník vykonaných služeb 57
Tab. 6: Cena za licence 57
Tab. 7: Běžná konfigurace osobního počítače a notebooku ve společnosti <*utajená*> . 58
Tab. 8: Kompatibilita endpoint DLP agenta s používaným softwarem 59
Tab. 9: Schéma pro hodnocení dopadu 60
Tab. 10: Přehled informačních aktiv ve společnosti <*utajená*> a jejich váha 60
Tab. 11: Schéma pro hodnocení úrovně hrozby 61
Tab. 12: Seznam interních hrozeb se stupněm výskytu 61
Tab. 13: Princip hodnocení rizik 62
Tab. 14: Hodnocení rizik vůči informačnímu aktivu 62
Tab. 15: Seznam opatření normy ČSN ISO/IEC 27001, které se týkají DLP systému .. 63
Tab. 16: Návrh testů pro první fázi implementace 72
Tab. 17: Návrh testů pro druhou fázi implementace 73
Tab. 18: Návrh testů pro třetí fázi implementace 74
Tab. 19: Výsledky testu první fáze implementace 77
Tab. 20: Výsledky testů po druhé fázi implementace 78
Tab. 21: Výsledky testů po plném nasazení 79
Tab. 22: Akceptační protokol 81
Tab. 23: Náklady na implementaci DLP pro první rok 82
Tab. 24: Náklady provozu DLP systému na další rok 82

PŘÍLOHY

Práce neobsahuje přílohy.