Zabezpečení firemní infrastruktury proti úniku dat

Bc. Petr Broschinski

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr Broschinski**
Osobní číslo:	**A15360**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Zabezpečení firemní infrastruktury proti úniku dat**
Téma anglicky:	**Securing Corporate Infrastructures Against Data Leakage**

Zásady pro vypracování:

1. **Popište používané prvky pro zabezpečení firemní infrastruktury proti úniku dat (Data Leakage Prevention)**
2. **Specifikujte využití systémů DLP ve firemní infrastruktuře**
3. **Identifikujte slabá místa systémů DLP**
4. **Navrhněte a realizujte DLP systém v testovacím prostředí**
5. **Vyhodnoťte implementaci DLP a zvažte další možnosti vývoje**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Data loss prevention – Ernst&Young [online]. 10/2011 [cit. 24. listopad 2016]. Dostupný z: http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_F**
2. **Internet access by platform [online]. 10/2016 [cit. 24. listopad 2016]. Dostupný z: https://ourworldindata.org/internet/ případně http://gs.statcounter.com/#desktop+mobile+tablet-comparison-ww-monthly-200812-201610**
3. **Symantec Data Loss Prevention Solution [online]. 5/2015 [cit. 24. listopad 2016]. Dostupný z: https://www.symantec.com/products/information-protection/data-loss-prevention/resources**
4. **McAfee Total Protection for Data Loss Prevention [online]. [cit. 24. listopad 2016]. Dostupný z: http://www.mcafee.com/us/products/total-protection-for-data-loss-prevention.aspx**
5. **Safetica Data Loss Prevention [online]. [cit. 24. listopad 2016]. Dostupný z: https://www.safetica.cz/produkty/safetica-dlp**
6. **ISO/IEC 27001:2013 [online]. 2013 [cit. 24. listopad 2016]. Dostupný z: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534**
7. **ISO/IEC 27002:2013 [online]. 2013 [cit. 24. listopad 2016]. Dostupný z: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533**
8. **Demingův cyklus PDCA [online]. 12/2011 [cit. 24. listopad 2016]. Dostupný z: https://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **16. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Diplomová práce řeší problematiku zabezpečení firemní infrastruktury proti úniku dat s využitím systému DLP (Data Leakage Prevention). Obsahuje seznámení se s řízením informační bezpečnosti, praktickými zkušenostmi s implementace a testování Proof of concept (PoC) systému DLP a jeho vyhodnocení. Poslouží i jako základní průvodce trhem v segmentu DLP. Dále je rozebrán princip, fungování a úskalí systémů DLP a integrace do firemní infrastruktury. V závěru jsou probrány budoucí možnosti vývoje systémů DLP.

Klíčová slova: DLP, systémy proti úniku dat, klasifikace dat, ISO27k, integrace systémů, informační bezpečnost, ISMS, bezpečnostní politiky a pravidla, GDPR

ABSTRACT

The thesis deals with securing corporate infrastructure against data leakage using DLP (Data Leakage Prevention) system. Text contains description of information security management, practical experience with implementation and testing of proof of DLP concept and its evaluation. It also can serve as a guide to DLP market. Functionality, main principles and restrictions of DLP system are described together with integration of DLP into company infrastructure. Finally, future possibilities of DLP development are discussed.

Keywords: DLP, data loss protection, data classification, ISO27k, systems integration, information security, ISMS, security policies and rules, GDPR

Děkuji panu Ing. Davidu Malaníkovi, Ph.D. za vstřícný přístup, ochotu, věnovaný čas, věcné připomínky a odborné vedení.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Dnes v době digitální revoluce, představují informace a data nejcennější aktivum, které firma vlastní. Nezáleží na tom, zda jde o data výrobního procesu, technických plánů, strategických dokumentů, databáze partnerů, seznamy kreditních karet či uživatelů a jejich osobních údajů. Většina aktiv je již zpracovávána, šířena i uložena pouze v elektronické podobě a představují existenční faktor firmy. Vzniká tak vysoká závislost na elektronických systémech a jejich zabezpečení.

Například v případě poškození dat hrozí firmě ochromení provozu s finančními dopady po dobu obnovy dat. Horší situace nastane při ztrátě či hůře úniku dat. Prakticky to může vést od naprosté paralýzy přes poškození dobrého jména a důvěryhodnosti, odliv klientů, právní dopady až po likvidaci firmy. Pokud bychom měli vyčíslit finanční ztráty, tak dle studie společnosti Ponemon Institute provedené v roce 2010 činila na americkém trhu průměrná ztráta za únik dat 7,2 milionu dolarů. To odpovídá ceně 214 dolarů za jeden uniklý záznam [1]. Dle zjištění až v osmdesáti procentech incidentů při úniku dat hrají podstatnou roli zaměstnanci. Hlavním podílníkem na těchto incidentech je lidský faktor. Dalším neméně důležitým faktorem je nové nařízení Evropské Unie ohledně ochrany osobních údajů General Data Protection Regulation (GDPR), kde výše pokuty za porušení je až 20 milionů EUR nebo 4 % z celosvětového ročního obratu [9]. Proto je dnes, více než kdy dříve, nutné věnovat zvýšené úsilí ochraně firemních dat, jakožto duševního vlastnictví firmy.

Práce na tato fakta reaguje a zabývá se problematikou zabezpečení firemní infrastruktury proti úniku dat s využitím systému DLP. Cílem bylo ověřit přínosy systému DLP společnosti v testovacím prostředí.

Práce je proto rozdělena do dvou hlavních částí, teoretické a praktické. V rámci teoretické části se lze seznámit s řízením informační bezpečnosti, fungováním DLP systémů a jejich úskalími. Dále zde lze nalézt přehled trhu s aktuálními lídry v segmentu systémů DLP.

Druhá část práce je věnována praktickému nasazení vybraného systému DLP v testovacím prostředí, kde jsou dle byznys požadavků a případu užití implementována konkrétní politiky a pravidla. Výstupem je zhodnocení PoC a posouzení případného nasazení DLP do firemního prostředí. Posledním bodem jsou budoucí možnosti vývoje DLP systémů.

I. TEORETICKÁ ČÁST

1 ZABEZPEČENÍ FIREMNÍ INFRASTRUKTURY PROTI ÚNIKU DAT

Tato kapitola osvětluje základní principy řízení informační bezpečnosti ve společnosti. Tyto principy jsou základním předpokladem pro úspěšné nasazení systému DLP a měli by být základním stavebním kamenem každé společnosti, která chce nebo musí brát ochranu citlivých dat vážně. Jsou zde popsány normy, standardy, legislativa a související prvky firemní ochrany. Navazuje na ni seznámení s fungováním DLP systémů a přehled trhu.

1.1 Systém řízení bezpečnosti informací

Jedná se o systém, který má za cíl chránit definovaná informační aktiva pomocí řízení rizik. A to postupem takovým, že se snaží minimalizovat ztráty a maximalizovat zisky. Tento systém se stal časem celosvětově uznávaným standardem ISO/IEC 27001 – Information Security Management Systems (dále jen ISMS). Tato norma poskytuje podporu v ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací. Principem celého ISMS je tzv. PDCA model (Demingův model). V tomto duchu je dobré postupovat i v rámci nasazení DLP systému.

1.1.1 Informační aktiva

Aktivem je v oblasti IT myšleno cokoliv, co je nutné chránit. Může jít o data klientů, obchodní tajemství, personální údaje, citlivé databáze informačních systémů a jejich servery, informace o infrastruktuře, zálohy apod.

Oporou nám může být aktuálně zákon č. 101/2000 Sb., o ochraně osobních údajů. V budoucnu tento zákon nahradí implementace nařízení o ochraně osobních údajů GDPR. Toto nařízení je platné od 25. května 2018 pro celou Evropskou Unii a významně ovlivní ochranu osobních údajů. Proto je nutné s tímto nařízením počítat již nyní. Více v kapitole legislativa.

Důležitým krokem je analýza těchto aktiv. Na základě výstupu se pak provádí řízení rizik. Pokud nějaké aktivum opomineme, může být problematické jej do procesu později doplnit a bude potenciálním rizikem, kde nám celý proces selže.

1.1.2 Klasifikace informací

Klasifikace patří k základním krokům při řízení informační bezpečnosti. Navazuje na proces analýzy aktiv. V této fázi je nutné stanovit kategorie klasifikací, do kterých následně budeme aktiva přiřazovat. Doporučení dle ISO 27002 [7] je kategorizovat aktiva, respektive dokumenty podle jejich hodnoty, právní citlivosti, citlivosti obsahu a kritičnosti. Pro jednotlivé kategorie by pak měla být sepsána pravidla, která říkají, kdo může s danými dokumenty disponovat a jakým způsobem s nimi může nakládat. Tato pravidla by měla být zanesena do vnitřního předpisu a schválena vedením společnosti. Pak jsou tato pravidla závazná pro každého zaměstnance, který je zodpovědný za správnou klasifikaci dokumentu.

V praxi se snaží firmy klasifikaci informací zjednodušit a volí základní model o třech stupních. Prvním stupněm jsou všeobecné, veřejné dokumenty, které nejsou žádným způsobem chráněny. Druhý stupeň říká, že se jedná o dokumenty určené pouze pro interní firemní prostředí. Ty se například nesmí objevit na nešifrovaném nefiremním zařízení. Posledním stupněm jsou pak nejcitlivější dokumenty, které jsou určeny pouze pro určitou vybranou skupinu lidí, například personální oddělení, management, VIP apod. Zde jsou pravidla nejpřísnější a vlastník má značnou odpovědnost.

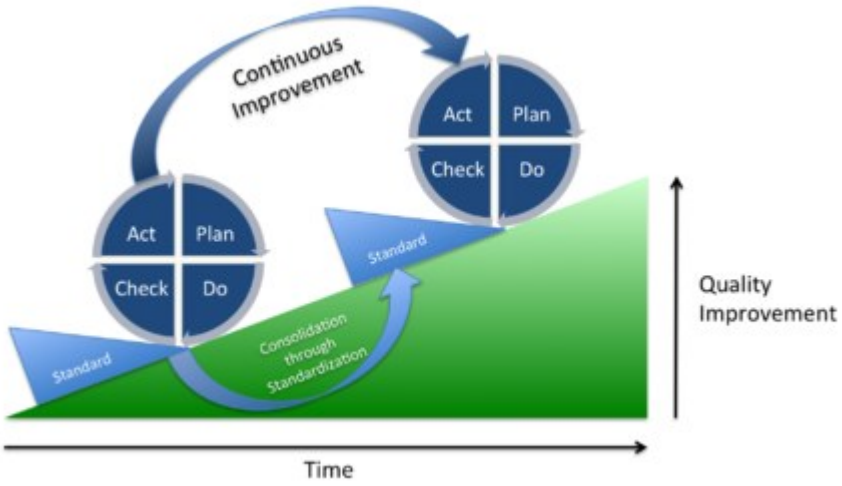
Tento krok není dobré přeskočit, ani pokud firma data neklasifikuje. Klasifikace nám v budoucnu velice ulehčí implementaci DLP, hlavně politik, pravidel a workflow. Klasifikovat dokumenty není u některých DLP systémů nutností, ale dojde ke snížení jejich schopnosti detekce, zvýší množství false positive a složitost pravidel.

Je běžné, že vedení i zaměstnanci mají na klasifikaci dokumentů negativní náhled. Hlavními argumenty jsou pracnost a odpovědnost. Dalšími důvody bývají například začlenění klasifikace do již existujícího informačního systému nebo systému pro řízení dokumentů. Tento fakt může hrát významnou roli při výběru DLP systému.

1.1.3 Demingův cyklus

Demingův cyklus je metoda postupného zlepšování služeb, procesů, aplikací či dat. Jejím autorem je William Edwards Deming, který tuto metodu prosazoval v Japonsku po druhé světové válce, a její myšlenky byly postupně nasazeny do japonského průmyslu. Díky tomuto přístupu došlo ke zlepšení kvality, snížení nákladů a zvýšení produktivity, což přineslo japonské společnosti úspěch na celosvětovém trhu, posun mezi špičku světového průmyslu a leadery ve světě technologií, kde se drží dodnes. Je součástí normy

ISO/IEC 20000-1 Informační technologie – Management služeb, konktrétně části jak využít metodologii PDCA, která je složena ze čtyř činností Plan - naplánuj, Do - proveď, Check - ověř, Act - jednej.



Obr. 1. Demingův cyklus a jeho postupné kroky [8]

Jak vyplývá z obrázku (obr. 1), jedná se o kontinuální nekončící iterační proces neustálého zlepšování systému, kde mimo jiné může cílem být certifikace ISMS, nebo nasazení systémů DLP, apod.

Plánování je prvním krokem cyklu. Na základě podmínek vstupů dojde ke stanovení cílů. Obsahuje popis stávajících nedostatků, úkolů a procesů k pokrytí řešení daného problému.

Druhým krokem je realizace plánu z prvního kroku dle vytvořeného plánu. Jsou implementovány jednotlivé procesy. Dochází i ke sběru podkladových dat pro zpracování v následujících krocích. Veškeré změny a zásahy by měly být pokryty dostatečnou dokumentací.

Následujícím krokem je ověření a kontrola dat a podkladů z předchozí fáze cyklu. Provede se analýza a porovnání mezi reálnými a očekávánými výsledky. Hledají se rozdíly v implementaci zadání a realizaci. Výstupem je pak zhodnocení vhodnosti a úplnosti požadovaného zlepšení systému včetně trendů a přehledných podkladů pro vyhodnocení v posledním kroku.

Cyklus uzavírá krok „jednej“. Ten je proveden, pokud z předchozího kroku vyplývají jednoznačně pozitivní výsledky a požadované zlepšení. V opačném případě se dané změny

do praxe nezavedou a vše zůstává při starém. Výsledkem může být také nové zjištění, které povede k přehodnocení celé změny, pak se celý proces s těmito daty vrací do první fáze.

1.2 Legislativa

Z legislativního hlediska je v souvislosti s DLP systémy zajímavý zákon o ochraně osobních údajů a nařízení GDPR. Obě normy mohou sloužit jak pro definici aktiv, tak i pro správné zpracování informací.

1.2.1 Zákon o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů stanoví a vymezuje, co jsou osobní údaje, kdo a jakým způsobem s nimi muže zacházet. Tento zákon platí pro státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby [10].

Osobním údajem je myšlena jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, tedy uživatele a dat, pomocí kterých lze daného uživatele identifikovat a to jak přímo tak i nepřímo. Takovým identifikátorem je číslo, kód jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou nebo sociální identitu.

Citlivý osobní údaj je pak informace vypovídající o národnostním, rasovém či etnickém původu, politických postojích, členství v odborových organizacích, náboženství, filozofické přesvědčení, odsouzení za trestný čin, zdravotní stav a sexuální život. Dále lze považovat za citlivé údaje genetické a biometrické, které umožňují přímou identifikaci nebo autentizaci uživatele.

Z pohledu soukromého sektoru, lze tedy považovat za osobní údaje personální data zaměstnanců, data o klientech, smlouvy či telemetrická data. Konktrétně jde o jméno, příjmení, adresu, datum narození a rodné číslo. Zákon se vztahuje na veškeré zpracování osobních údajů a nezáleží na tom, zda je automatizované nebo provedené jiným způsobem. Zákon myslí i na anonymní data, což je údaj, který v původním tvaru či po zpracování nelze vztáhnout k žádnému určenému nebo určitelnému subjektu.

K získání a uchovávání dat je vždy nutný souhlas subjektu, uživatele. Firma, jakožto správce a zpracovatel, má povinnost uchovávat a nakládat s takovými daty jen pouze po nezbytně nutnou dobu dle stanoveného účelu. Po té je povinné provést likvidaci osobních údajů. Dále je nutné zajistit, že v rámci firmy či organizace bude mít k osobním údajům přístup pouze pověřená osoba. Je nutné mít stanovena taková opatření, která zabrá-

ní neoprávněnému nebo nahodilému přístupu k osobním údajům. Poslední z nejdůležitějších bodů je oznamovací povinnost. Správce osobních údajů, jakožto zpracovatel, je povinen písemně oznámit záměr Úřadu pro ochranu osobních údajů (UOOU) ještě před zpracováváním osobních údajů. Ten může při nedodržení tohoto zákona udělit pokutu za přestupek až do výše pěti miliónů korun a v případě deliktu až deset miliónů korun.

Zákon obsahuje více detailů. Výše uvedené body jsou ty nejdůležitější, které hrají do karet DLP systémům. Firma, která zpracovává velké množství osobních dat, má míru rizika úniku dat vyšší. Například jde o finanční domy, banky, pojišťovny, telefonní operátory či internetové obchody. Případná pokuta za únik osobních dat by tak mohla překonat náklady na pořízení DLP systému.

1.2.2 GDPR

General Data Protection Regulation je obecné nařízením EU 2016/679 o ochraně osobních údajů, které vstoupí v platnost 25. května 2018 [9]. Klade si za cíl chránit a sjednotit digitální práva občanů EU. Vznikl z důvodu rychlého technologického vývoje dnešní doby, kdy jsou nyní platné předpisy zastaralé a nedostatečné. Do budoucna proto nahradí i český zákon č. 101/2000 Sb., o ochraně osobních údajů. Nařízení bude platné a jednotné pro celou Evropskou Unii jakožto oblast jednotného digitálního trhu. Dopad bude mít na každého, kdo shromažďuje nebo zpracovává osobní údaje a to včetně firem mimo území EU, které na evropském trhu působí.

Pro subjekt, občana, jsou změny formálního rázu. V platnosti zůstává souhlas uživatele, definice osobního údaje rozšířeného o IP adresu a fotografický záznam. V oblasti citlivých osobních údajů došlo k rozšíření o kategorie genetických, biometrických údajů, osobní údaje dětí, které lze již dnes považovat za citlivý osobní údaj. Přibylo právo na výmaz (právo být zapomenut), právo na přenos údajů, právo na omezení zpracování, právo vznést námitku a právo na přístup. Právě právo na přístup by občanům mělo dát větší možnosti kontroly. V rámci kontroly lze zjistit, za jakým účelem se osobní údaje zpracovávají, po jakou dobu budou údaje uchovávány, kdo je příjemcem osobních údajů a jakým způsobem probíhá automatizované zpracování (například profilováním).

Pro firmy, jakožto správce, je situace poněkud komplikovanější. Hlavní myšlenkou nařízení je princip tzv. „privacy by design“. Volně by se tento princip dal přeložit jako: „soukromí základem návrhu“. Nařízení cílí na všechny správce, zpracovatele osobních údajů, bez ohledu na jejich velikost nebo počet zaměstnanců. Došlo ke zrušení ohlašovací povin-

nosti dozorovým úřadům, protože se ukázala jako neefektivní pro zlepšení ochrany osobních údajů. Místo toho zavádí povinnost správci provést analýzu dopadů zpracování, kterou je povinen probrat s dohledovými orgány. Přibyla povinnost oznamovat bezpečnostní incidenty do 72 hodin. Nově vznikne role pověřence pro ochranu osobních údajů DPO (Data Protection Officer). Pro správce, zpracovatele, bude nařízení znamenat nemalé časové a finanční investice a to hlavně v oblastech: implementace technických opatření, procesní změny: analýza dopadů, DPO, pseudonymizace osobních údajů a konzultace s dozorovým orgánem ještě před samotným zpracováním. Podstatnou změnou je výše pokut. Ta je za porušení ochrany osobních údajů až 20 miliónů EUR nebo 4% z celosvětového ročního obratu s tím, že se vždy bere ta vyšší hranice.

DLP systémy mohou výrazně snížit riziko úniku dat, proto investice do systému DLP nabývají nemalého významu.

1.3 Systémy DLP

Z předchozí kapitoly je patrná důležitost ochrany firemních dat. Odpovědí na tento komplexní problém jsou DLP systémy. Jejich hlavním úkolem a cílem je ochránit citlivá data a to proti úniku, ztrátě či zneužití.

Každý výrobce DLP systému se snaží dodat na trh své unikátní řešení, které se snaží poskytnout určité výhody před ostatními. V tomto kontextu lze najít i různé definice výkladu zkratky DLP. V různých materiálech se lze setkat se slovním spojením Data Loss Prevention, Data Leakage Prevention, Data Loss Protection a Data Leakage Protection. V doslovném překladu znamená Loss ztráta a Leakage únik dat. V prvním případě ztráta znamená preventivní ochrana proti neúmyslnému vynesení dat ze společnosti. Kdežto únik dat lze chápat jako úmyslné vynesení dat, kdy například zaměstnanec cíleně změní klasifikaci dokumentu tak, aby byl považován za nedůležitý. Podobný významový rozdíl lze pozorovat i u slov Prevention a Protection. Prevence významově odpovídá statické ochraně dat. U protekce (ochrany) se systém snaží hrozby nejen detekovat, ale i předvídat možný únik dat.

1.3.1 Princip DLP

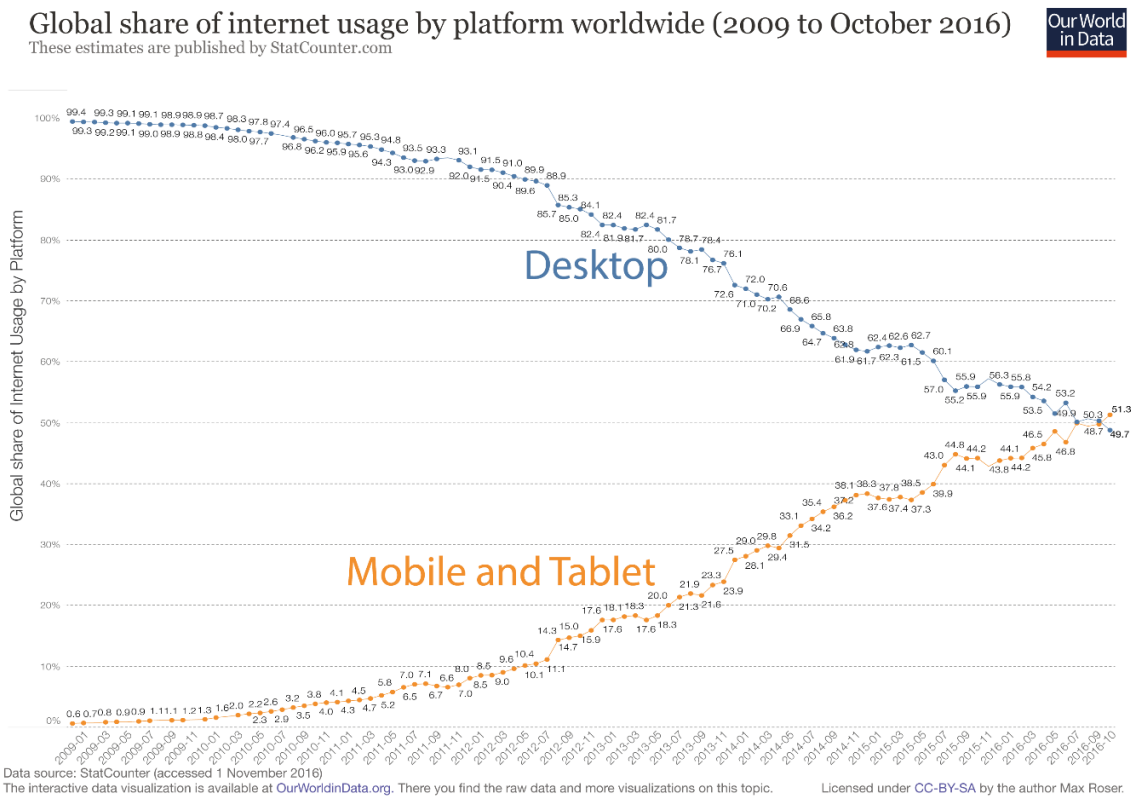
Systém řeší problematiku úniku dat z důvodu selhání lidského faktoru. Zajišťuje, že oprávnění uživatelé, kteří nakládají s citlivými informacemi a daty, budou s těmito svěřenými daty nakládat požadovaným a firmě prospěšným způsobem. Umožňuje monitorování, detekci a aktivní zásah proti úniku citlivých dat. Tyto kroky mohou být s či bez vědomí uživatele včetně jeho interakce. Vše se řídí definicí politik a pravidel. Ty jsou základem každého DLP a mohou provádět například hloubkovou inspekci obsahu, kontextovou bezpečnostní analýzu či analýzy na základě strojového učení [3]. Každé pravidlo může vyvolat incident různé vážnosti a dopadu. Incidenty pak spadají pod klasické workflow, kdy je nutné ručně zpracovat všechny incidenty a identifikovat false positive. U každého incidentu existuje vždy auditní stopa s přesnými informacemi o důvodu vzniku, uživateli, datu, čase, důkaze a případně podniknuté kroky. Důležitým faktorem pro co nejmenší počet false positive incidentů jsou vyladěné politiky, pravidla a také integrace s ostatními firemními systémy.

1.3.2 Dělení DLP

DLP se dají rozdělit do dvou druhů. Host-based DLP je zaměřené na koncové body (Endpoint). Druhé je network DLP. Obě tato řešení mají své výhody a nevýhody, proto většina komerčních DLP systémů obsahuje oba dva druhy, které se takto optimálně doplňují. Aktuální vývojový trend velí hluboké integraci s dalšími produkty např. proxy serverem, které jsou nezbytné pro pokrytí co nejširšího záběru.

1.3.2.1 Host-based DLP

Za koncový bod je primárně považována pracovní stanice, nicméně bylo by chybou opomenout například mobilní telefony či tablety. V nejbližším výhledu bude firemní vývoj používání mobilní platformy sledovat zákaznický trend, na kterém je patrné, že mobilní telefony využíváme stále více a to i ke složitějším úkonům [2], viz obrázek (obr. 2).



Obr. 2. Vývoj přístupu k internetu (desktop a mobilní platforma) [2]

1.3.2.2 Network DLP

Síťové DLP poskytuje ochranu na úrovni vnější komunikace. Chrání tak data, která firmu opouští. Je realizováno buď jako hardwarová appliance nebo v podobě virtuálního serveru. Síťové DLP je vždy umístěno v perimetru odchozích síťových prvků. Analýza síťového provozu je provedena pomocí SPAN portu. Pro analýzu mailové komunikace se využívá vestavěný SMTP modul. Dále je možné kontrolovat i instant messaging, webové stránky či cloudové služby. Prakticky jakýkoliv síťový provoz.

Jediným zádrhelem zůstává šifrovaná komunikace, která do jisté míry v poslední době zažívá boom. Z povahy věci nelze do této komunikace vstoupit, aniž bychom ji nerozbili a neovlivnili její funkčnost. Proto je potřeba počítat spolu s DLP i s nákupem proxy serveru, který umí na slušné úrovni man-in-the-middle a je integrovatelný s DLP (ICAP - Internet Content Adaptation Protocol). Též je nutné mít vlastní certifikační autoritu v rámci domény, která nám umožní podepsat náš podvržený certifikát z proxy tak, aby bylo vše transparentní. Pak už zbývá pouze distribuce na koncové stanice či do konkrétní aplikace (pokud má své úložiště důvěryhodných certifikátů např. Firefox).

Velkou výhodou síťových DLP je jejich rozložení zátěže na instance DLP (servery). Ve většině řešení není pouze jeden síťový DLP server, ale je možné clusterové řešení. Není problém výkon dostatečně naddimenzovat a vyvážit. Vhodnou strategií je proto přenést co největší zátěž z pracovních stanic na síťové DLP. Toho se dá dosáhnout pomocí vhodně napsaných politik a pravidel.

Celé DLP řešení se dá postavit prakticky na míru každé firmě přesně podle jejích potřeb. Z toho plyne i jedna nevýhoda a to ta, že každá implementace je jedinečná a s tím spojené finanční nároky.

1.3.3 Obsah a kontext

Většina systémů je založena na analýze obsahu dokumentu, kdy dojde na základě definovaných politik a pravidel k záchytu dat při jejich úniku z perimetru a vzniku incidentu. Obsah lze hodnotit například na základě klíčových slov, hlavičky dokumentu, metadat, vlastníka, naučených citlivých dat či klasifikace dokumentu a podobně. V případě shody lze dokument zablokovat na hranicích perimetru, a tím zabránit úniku dat.

Tento přístup není problém aplikovat u souborů, které jsou výstupem například z aplikací Word či Excel, kde je jasně definovatelný obsah. Horší situace nastává u jiných druhů souborů, u nichž není možné jasně definovat obsah, například technická dokumentace, výkresy, zvukové soubory, zdrojové kódy a podobně. Lze postupovat blokací na základě přípon souborů, nebo zablokovat odesílání šifrovaných souborů, kde není možné obsah přečíst. Tento přístup ovšem není vždy vhodný.

Druhým přístupem je pak hodnocení na základě kontextu, ve kterém s daty uživatelé pracují a kde se nachází. Pokud uživatel zpracovává kupříkladu strategický dokument mimo firmu, je pak uživatel omezen tak, aby nemohlo dojít k úniku dat z daného perimetru. Možnou ochranou je pak zablokování jakýkoliv komunikačních portů PC (USB, Bluetooth, sériového portu), omezení kopírování dat do schránky a podobně. Veškeré s tím spojené akce se pak provádí na koncové stanici (End-point).

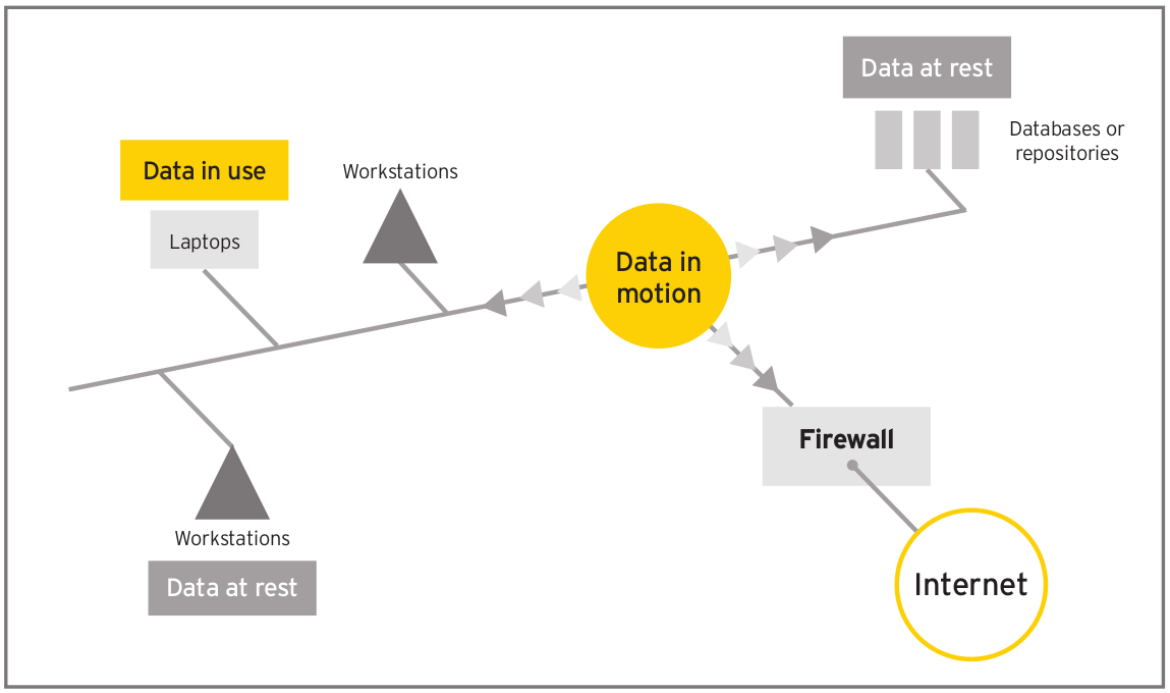
Oba přístupy se navzájem doplňují, proto se výrobci DLP systémů snaží kombinovat oba dva přístupy, byť vycházeli převážně z obsahového přístupu. Podrobné porovnání principů, vektorů pokrytí a přístupu k analýze obsahu je uvedeno v tabulce níže (Tab. 1).

Tab. 1. Přehled systémů DLP a jejich vlastností

DLP	Princip DLP		Vektory pokrytí			Přístup	
	Host-based	Network	Data in use	Data in motion	Data at rest	Obsahový	Kontextový
Symantec	✓	✓	✓	✓	✓	✓	✓
McAfee	✓	✓	✓	✓	✓	✓	✓
Safetica	✓	✗	✓	✗	✗	✗	✓

1.3.4 Vektory pokrytí dat

DLP systémy mají tři základní vektory pokrytí dat, viz obrázek níže (Obr. 3). Prvním je **in use** probíhající na Endpointu. Druhým je **in motion** na úrovni síťového provozu. Posledním je vektor **at rest**, který pokrývá síťová úložiště, zálohy.



Obr. 3. Vektory pokrytí dat [1]

1.3.4.1 Data in use

Jde o vektor koncových stanic či mobilních zařízení, kde probíhá ochrana dat při jejich používání. Jedná se o host-based typ DLP. Typicky jde o otevírání, kopírování a editaci dat, ale také jejich tisk, distribuci mailem či cloudem. Pokročilé DLP umožňují i detekci firemní, či jiné sítě, a na základě toho omezit možnou práci s citlivými daty.

1.3.4.2 Data in motion

K ochraně dochází na síťové úrovni, kdy jsou data distribuována klientovi za pomocí počítačové sítě. Využívá se síťového DLP. Analyzují se veškeré komunikační kanály, jako jsou e-maily či cloudové služby.

1.3.4.3 Data at rest

Stará se o data, která jsou uložena na pevném disku, síťovém úložišti, souborovém serveru. Data mohou být archivována či v zálohách (na páskách nebo v záložním úložišti). Zde je vhodné využít funkcionality řízení přístupu a šifrování dat. Jde o situaci, kdy jsou data někde uložena, ale nikdo s nimi aktivně nepracuje a přesto je nutná jejich ochrana. Po čase nastává nepříjemná situace, kdy už nikdo konkrétně neví, ve které záloze data jsou zálohována, a jak moc jsou citlivá. Pak takové DVD může být omylem vyhozeno do odpadu a podobně.

1.4 Přehled trhu s DLP systémy

Přehled je vypracován na základě reportů a analýz společnosti Gartner z roku 2016. Tato společnost působí celosvětově v oblasti výzkumu a poradenství IS/ICT technologií od roku 1979 a je považována za jeden z nejspolehlivějších zdrojů.

Obr. 4. Přehled trhu - DLP systémy za rok 2016 [11]

Z obrázku níže (obr. 4) je možné vyčíst postavení DLP systémů v rámci čtyř kvadrantů. Z pohledu schopností a komplexnosti produktu je nejzajímavější kvadrant lídrů. Ostatní kvadranty slouží pro přehled, který je zajímavé sledovat s vývojem času a prosazování produktu. Absolutním lídrem je DLP od společnosti Symantec, následované Forcepointem a Digital Guardian. Posledním hráčem je Intel Security, který je dnes znám opět pod značkou McAfee. Společnost Digital Guardian nemá oficiální zastoupení v České republice, proto není dále uváděna. DLP od společnosti Forcepoint má nevhodnou cenovou politiku pro středně velké podniky kolem 700 zaměstnanců, její řešení je výrazně dražší, proto také i toto řešení není uvažováno. Zbývající dvě společnosti Symantec a McAfee mají v ČR zastoupení a jsou si blízké cenovou politikou.

Pokud bychom brali v potaz segment Endpoint řešení i tam, dle obrázku níže (obr. 5), je patrné, že společnosti Symentec a McAfee (Intel Security) patří mezi lídry. Pokud by nás zajímalo DLP pouze na principu **Host-based** jsou na trhu i další významní hráči, jako Kaspersky Lab a Trend Micro.

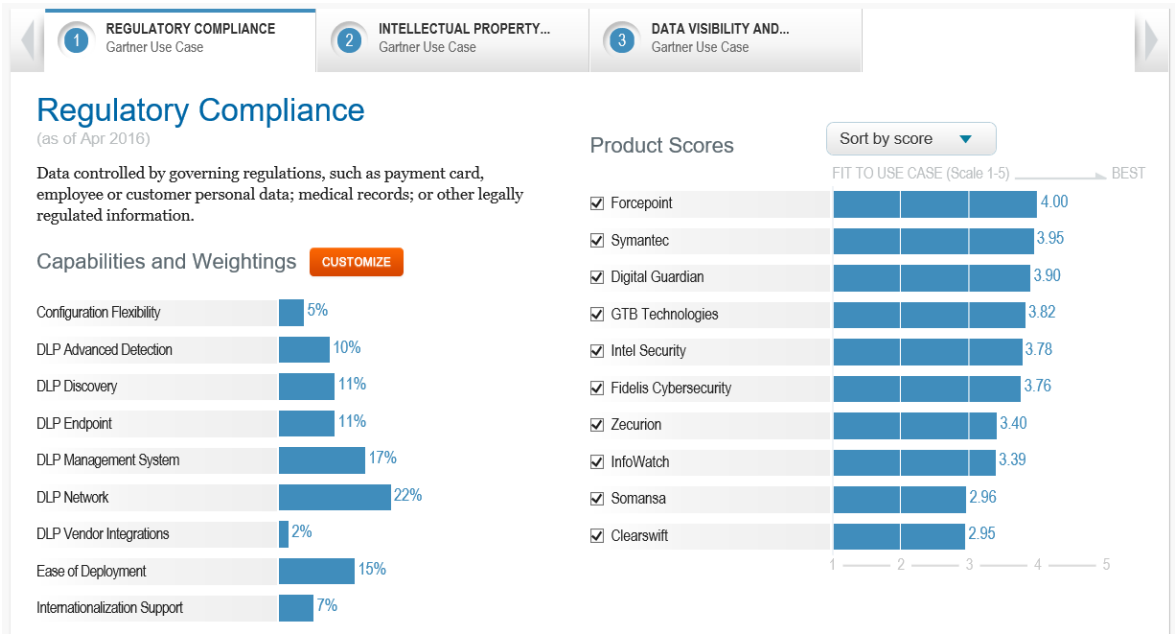
Obr. 5. Přehled trhu - Endpoint platformy za rok 2016 [12]

Začátkem roku 2017 společnost Symantec koupila společnost BlueCoat, a získala tak výhradní postavení na trhu, viz obrázek (obr. 6). McAfee (Intel Security) je pro rok 2016 v kvadrantu vyzyvatelů, a bude do budoucna přímým konkurentem. Byť webové brány nejsou nutnou součástí systémů DLP a lze využít i jiné produkty z řad systémů proxy či firewallů nové generace, tak v rámci ceny a funkčnosti mají důležitou roli.

Obr. 6. Přehled trhu - Web Gateway za rok 2016 [13]

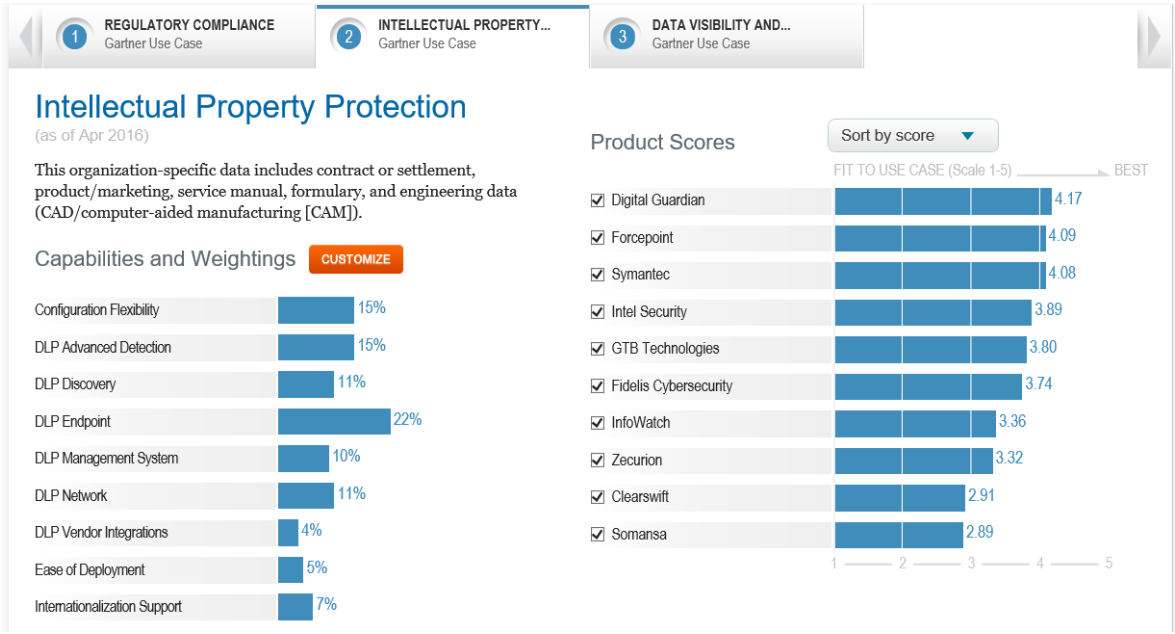
Vhodnost vybraných DLP lze posoudit i v rámci scénářů (viz obrázky 7,8,9). Je patrné, že se mezi prvními vždy umístila společnost Symantec se svým DLP, proto byl tento produkt vybrán pro PoC.

Na obrázku (Obr. 7) je vidět, že na vahách toho scénáře má priority síťová část, management systému a jednoduchost nasazení.



Obr. 7. Porovnání DLP z pohledu dodržování předpisů [11]

V následujícím scénáři na obrázku výše (Obr. 8) je patrné výrazné upřednostnění řešení pro koncové body.



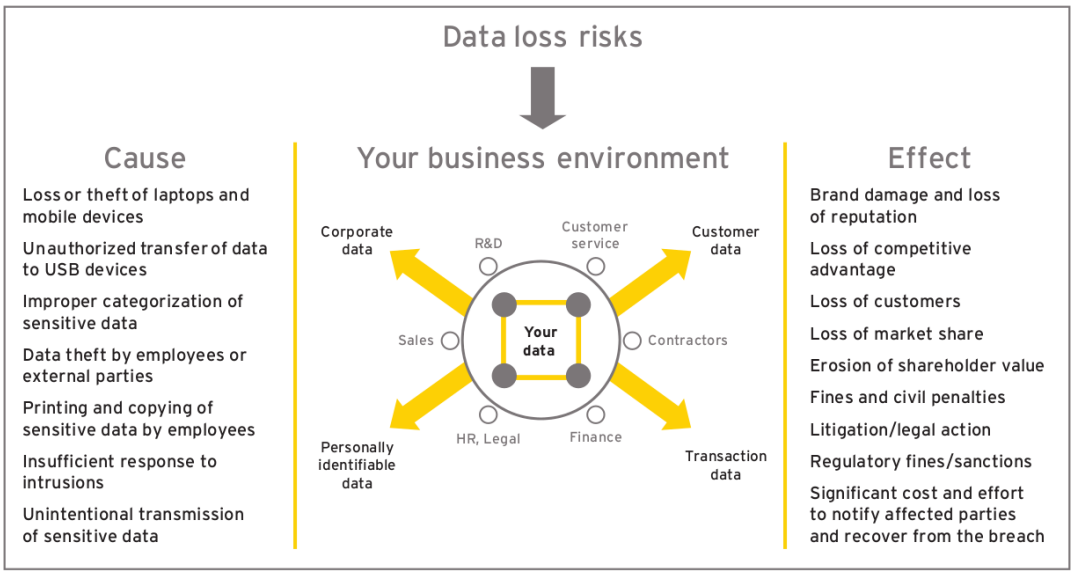
Obr. 8. Porovnání DLP z pohledu ochrany intelektuálního vlastnictví [11]

Poslední scénář na obrázku níže (Obr. 9) představuje vyvážený přístup, který poslouží jako obecný model pro většinu společností.

Obr. 9. Porovnání DLP z pohledu monitoringu a přehledu dat [11]

2 VYUŽITÍ SYSTÉMŮ DLP VE FRIEMNÍ INFRASTRUKTUŘE

Hlavním cílem systémů DLP je minimalizace rizik a finančních ztrát spojenými s únikem firemních dat, viz obrázek (Obr. 10). Používají se jako nástavba stávajících standardních bezpečnostních opatření technického i formálního rázu. Mezi standardní technická opatření lze považovat například firewally, systémy detekce průniku (IDS/IPS), mailové brány, proxy, segmentace sítě, doménové politiky, patch management, antiviry, fyzickou bezpečnost, VPN, šifrování stanic, systémy správy dokumentů (DMS) ale i systémy pro řízení a správu identit (IDM) či dohledové systémy SIEM. Do formálních lze zařadit bezpečnostní směrnice, správně nastavené byznys procesy a řízení rizik, workflow procesy, například dohled čtyř očí či service desk, licencování nebo proškolené zaměstnance v IT bezpečnosti. DLP se do jisté míry dotýká a rozšiřuje každého výše uvedeného zabezpečení.



Obr. 10. Možná rizika ztráty dat [1]

Z obrázku výše (Obr. 10) jsou patrná hlavní oddělení, která pracují s určitými typy dat, jako jsou zákaznická, personální, firemní či transakční data. Jejich ztráta představuje únik dat. Důvodem takového úniku může být například krádež notebooku, neoprávněné stažení dat na USB zařízení, vytištění citlivých dat nebo ukradení dat zaměstnancem. Dopadovým efektem je poškození dobrého jména firmy a její reputace, ztráta zákazníků a podílu trhu, finanční ztráty nebo právní důsledky.

Použití

Všechna uvedená opatření mají společného jmenovatele, a tím je uživatel. Ten hraje při úniku dat podstatnou roli. DLP systémy jsou zaměřeny právě na ochranu dat před pochybením lidského faktoru ať chtěného či nechtěného. Používají se pro sledování a automatické vyhodnocování činnosti a chování uživatele. DLP pokrývá všechny jeho činnosti, jako je klasifikace a práce s firemními dokumenty, informačními systémy a jejich výstupy, maily, tiskem, kopírování dat například na sdílené disky, USB disky či cloudové služby. V případě potřeby má možnost DLP systém zareagovat a uživateli znemožnit citlivý dokument otevřít, uložit, či poslat tak, aby nedošlo k úniku dat.

Primárně DLP systémy chrání proti úniku mimo společnost, ale lze je využít i pro dohled uvnitř společnosti, aby se citlivá data nedostala do nepovolaných rukou a volně „nepovalovala“ na síťových discích, úložištích nebo v zálohách. Systém DLP může procházet i logové soubory serverů, kontrolovat skripty a servisní automatizované maily, jestli náhodou neobsahují citlivá data nebo například hesla v prostém textu, doménová jména administrátorů apod.

DLP se drží i aktuálního trendu mobility, a snaží se pokrýt i využívání mobilních telefonů nebo tabletů. U nich je situace složitější, protože z pohledu firemního nasazení nejsou chytré telefony uzpůsobeny například na správu bezpečnostních politik apod. Nicméně uživatelé chtějí mít firemní data i tam, aby případně mohli pracovat s dokumenty, prohlížet si intranet, mít přístup do informačních systémů, to vše odkudkoliv a kdykoliv. Proto DLP systémy dnes v sobě integrují i mobile device management systémy (MDM).

Z výše uvedeného textu je patrné, že scénářů pro využití DLP systémů je celá řada. DLP systémy jsou modulární. Lze použít základní funkcionality a vynechat například MDM část.

2.1 Nasazení

Celé DLP lze nasadit jen s minimálními výpadky infrastruktury a služeb pro uživatele. Postupuje se od základních částí hlavního managementu až po kritické, například detekční, servery. Vše až na síťovou sondu/monitor může běžet na virtiualizační platformě, což je i doporučované řešení. Síťová sonda je závislá na fyzickém serveru a nelze ji virtualizovat. Hlavním důvodem je využití SPAN portu, na který je přesměrovaná veškerá síťová komunikace určená ke sledování. V poslední fázi je nutné nasadit agenty na koncové body

pomocí softwaru třetích stran. Například v rámci Microsoft ekosystému lze využít funkcionalit produktu System Center.

Doba nasazení je závislá na architektuře řešení a složitosti politik a pravidel. Nasazení infrastruktury pro DLP se základní konfigurací je možné zvládnout během měsíce. Výrazně delší doba je potřeba k odladění první verze politik a pravidel. Tento proces je pak kontinuální a slouží k odstranění false positive incidentů, je vhodné postupovat pomocí PDCA. Odhadovaná doba pro odladění politik a pravidel je až jeden rok.

2.2 Výstupy

Výstupem DLP systémů jsou incidenty, které je nutno vyhodnotit. Každý incident obsahuje auditní záznam s informacemi, kde se stal, uživatel, který incident vyvolal, jaký důvod je pro vznik incidentu, jaká politika/pravidlo bylo porušeno, krátká ukázka porušující pravidlo a případně může obsahovat i kompletní soubor jako důkaz. Incident může obsahovat i další informace, které DLP samo doplní z integrovaných systémů například z Active Directory doplní konkrétní údaje o uživateli, jako odbor, oddělení, telefon, apod. Takové údaje pak značně ulehčují práci se systémem při řešení incidentu. Přínosnou informací u incidentu jsou také korelace s ostatními incidenty nebo trendy. V souvislosti s incidenty je důležitý pojem archivace, který říká, jak dlouho budou data dostupná v systému DLP. Standardní doba se volí od třech měsíců po rok, dle vnitřních předpisů firmy.

Jedním z dalších možných výstupů jsou dashboardy, které slouží především pro rychlý přehled. Obsahují většinou manažerský přehled s grafy a tabulkami. Dají se organizovat například na základě politik, pravidel nebo organizační struktury organizace a podobně.

Systém umí pracovat i s reporty a třeba je zasílat automatizovaně na e-mail. Reporty většinou obsahují kombinaci dashboardů a trendů. Do jisté míry jsou modifikovatelné a mohou obsahovat i detailnější informace. DLP může reportovat i svůj stav, využívání kapacit, velké množství incidentů, tedy i provozní informace.

2.3 Oblasti pokrytí a integrace

Na koncových stanicích je nasazený Endpoint agent, který se stará o data **at rest** i data **in use**. Agent řídí využití fyzických rozhraní, jako jsou USB, sériové, LAN porty, bluetooth, Wi-Fi nebo šifrování celého zařízení. Lze také omezit fungování standardních funkcí operačního systému jako je copy&paste či snímky obrazovky. Je nutné zajistit, že agenti

z koncových stanic budou mít viditelnost na detekční server pro sběr informací z Endpointů.

Pro data **at rest** na síťových úložištích, SharePointu, SQL databázích, které umí většina DLP procházet, je vhodné, aby ležela na stejném síťovém segmentu. Zjednodušuje to ladění implementace DLP.

Detekční server síťové sondy je vhodné umístit poblíž centrálního switche, který umožňuje odesílat kompletní síťový provoz na SPAN port serveru. Pokud je architektura dané sítě složitější a firma má i záložní centrum, je pravděpodobné, že bude nutné umístit další server i tam. Jinak by v době výpadku nemohla být sledovaná komunikace.

Poslední částí je detekční server webové brány. Na ten musí mít přístup uživatelské stanice, a zároveň přes něj proudí veškerá data do Internetu. Všechny detekční servery musí mít dostupný centrální management.

Integrace je důležitým bodem. Je vhodné zvážit stávající systémy a jejich napojení na DLP. Prvním bodem, který je doslova nezbytný, je integrace s Active Directory (nebo podobnou službou) a to nejen pro autentizaci. Důležité jsou údaje o uživatelích, které se doplňují k incidentům. Integrace s proxy nebo web gateway patří na druhé místo. Kompatibilitu by měl zaručit protokol ICAP. Integrace je díky tomu možná i s produkty jiných výrobců. Integrace i s dalšími nejvíce používanými systémy, jako je Sharepoint či MSSQL server, SIEM, AD RMS, je již připravena.

2.4 Hardwarové nároky

Množství serverů záleží na zvolené architektuře a použitém scénáři. Specifikace HW jsou převzaty od společnosti Symantec [3]. Z tabulek (Tab. 2,3,4) je patrné, že stačí čtyř jádrové CPU o frekvenci 3 GHz s 8 až 16 GB RAM a 140 až 500 GB úložištěm. HW požadavky nejsou překvapivé nebo výjimečné. Požadavky pro koncové klienty jsou uvedeny v tabulce (tab. 5), zde jsou uvedeny minimální požadavky.

Tab. 2. HW nároky - hlavní management server

Komponenta	Parametr	Provedení
CPU	4 CPU (vCPU) 3 GHz	virtuální
RAM	16 GB	
Použitelný diskový prostor	500 GB+ (dle požadavků na skladování incidentů)	
Operační systém	Windows Server 2008 R2 a vyšší	

Z výše uvedené tabulky (Tab. 2) je patrné, že management server klade hlavní nároky na paměť RAM a volné místo na disku z důvodu požadavku na skladování incidentů.

Tab. 3. HW nároky - síťová sonda/monitor

Komponenta	Parametr	Provedení
CPU	4 CPU (vCPU) 3 GHz	fyzický server
RAM	8 GB	
Použitelný diskový prostor	140 GB	
Operační systém	Red Hat Enterprise Linux /Windows Server 2008 R2 a vyšší	

Síťová sonda (monitor) nemá výrazné hardwarové požadavky, viz tabulka (Tab. 3), jediným požadavkem je využití fyzického serveru z důvodu fyzické síťové karty, její datové propustnosti a její přímé napojení na páteřní switch.

Tab. 4. HW nároky - ostatní detekční servery

Komponenta	Parametr	Provedení
CPU	4 CPU (vCPU) 3 GHz	virtuální
RAM	8 GB	
Použitelný diskový prostor	140 GB	
Operační systém	Red Hat Enterprise Linux /Windows Server 2008 R2 a vyšší	

V tabulce níže (Tab. 5) je uvedena minimální konfigurace pro stanici, kde má být nasazen Endpoint Client. Z praktického hlediska dnešní doby a náročnosti dnešních operačních systémů je dobré volit 4GB RAM a procesor výkonnostně na úrovni řad Intel i5u (mobilní verze).

Tab. 5. HW nároky - Endpoint Client

Komponenta	Parametr	Provedení
CPU	Intel Core 2 Duo	Virtuální/fyzický
RAM	1 GB	
Použitelný diskový prostor	850 GB	
Operační systém	MAC OS 10 a vyšší /Windows 7 a vyšší	

II. PRAKTICKÁ ČÁST

3 SLABÁ MÍSTA SYSTÉMŮ DLP

Jako neexistuje dokonalý člověk, neexistuje ani dokonalý svět. Je nutné se slabými místy DLP systémů počítat, a tím minimalizovat možná rizika a dopady. Je nutné předem říci, že DLP nemůže zabránit nejjednodušším typům úniku dat v podobě vyfotografování, opsáním citlivých dat a také nezabrání úniku dat pomocí nějaké sofistikované metody, například pomocí obfuskace dat.

3.1 Politiky, pravidla a false positive

Základním kamenem funkčnosti DLP systémů jsou pravidla, politiky a false positive. Každý výrobce má pojetí politik trochu jiný přístup, nicméně se shodují v základních vlastnostech. Každá politika lze poskládat z jednotlivých pravidel. Ty lze kombinovat pomocí logických spojek Booleovské logiky (např. OR, AND). Stejným způsobem lze vytvářet i výjimky například na doménové skupiny, IP rozsahy, uživatele či odesílatele mailové pošty. Takto sestavené politiky by měly odpovídat předem definovaným bezpečnostním politikám firmy a mít oporu ve vnitřních normách.

DLP společnosti Symantec [3] nabízí vzorová pravidla například pro detekci čísel kreditních karet, SWIFT kódů, rodných čísel, důvěrných dokumentů či zaměstnaneckých dat. Tato vzorová pravidla lze využít a modifikovat pro vlastní potřeby.

3.1.1 Typy pravidel

Prvním typem jsou pravidla na základě obsahu, například za použití regulárních výrazů, klíčových slov, strojového učení (hlavičky dokumentů, klientská data, vzory smluv, otisku dokumentu). Druhým typem jsou pravidla na základě vlastnosti dokumentů a posledním typem na základě použitého protokolu. Každý typ má vždy svou působnost, některá pravidla budou platná například pouze na pracovní stanici a jiná na webové bráně či při procházení obsahu na síťových discích.

3.1.2 Ladění politik, pravidel a false positive

Kombinací předdefinovaných a vlastních pravidel lze dosáhnout rozsáhlé komplexity. Problém nastává při ladění dané politiky. Vzniknout může hned několik problematických situací. První a méně závažná situace je v případě vzniku velkého počtu false positiv incidentů bez citlivých dat. Zde je možné pomocí výjimek a zpřesněním daných pravidel politiky snížit počet false positiv incidentů. V tomto problému můžou pomoci pokročilé tech-

niky Vector Machine Learningu (VML) [3]. VML provádí statistickou analýzu na nestrukturovaných datech (zdrojové kódy, finanční ztráty, těžce popsatelná data) a porovnává je s již vyhodnocenými daty. V průběhu času, jak jsou DLP false positiv incidenty obsluhou vyhodnocovány, pak dokáže zpřesnit výstup, a tím snížit množství false positive incidentů.

Druhou problémovou situací je zachycení citlivých dat v rámci testování politiky. Systém DLP má přístup ke všem datům skrz všechny integrované systémy, například sdílené disky, maily a podobně. Tím vzniká samo o sobě bezpečnostní riziko, kdy administrátor DLP systémů zanese ať úmyslně nebo neúmyslně chybu do pravidel. Vytvoří si například pravidlo: „Vrať mi všechny e-maily, které obsahují slovo ‚Výplatní páska' a obsahují přílohu *.pdf". Takové pravidlo zachytí po dobu platnosti všechny výplatní pásky zaslané všem zaměstnancům do mailu. Proto je důležitý dohled čtyř oči v každé fázi nasazení DLP systémů a sběr logů napojením na SIEM server. Proti nechtěnému zachycení citlivých dat pak pomůže testovat pravidla na dedikovaném zařízení, které lze specifikovat jako hlavní pravidlo. Po té, co je otestována správná funkčnost politiky dojde k odstranění pravidla na dedikované zařízení a politika je v tu chvíli platná pro vydefinované oblasti.

Výše uvedené problémy poukazují na fakt, že je nutné mít správně nastaveny všechny workflow procesy týkající se DLP systémů.

3.2 Rizika úniku

I přes dokonale napsané politiky je možný únik dat. Prvním příkladem, který k tomu může vést, je oprávnění lokálního administrátora. Pokud má uživatel tato oprávnění, je schopen prakticky DLP obejít, včetně jiných firemních zabezpečení. Proto i z důvodu bezpečnosti samotné by lokální práva administrátora mělo mít v rámci organizace minimum uživatelů. Dalším rizikem jsou mobilní firemní zařízení (notebooky), které si zaměstnanci berou domů, na cesty nebo jednání. První nedostatkem je fyzický přístup k disku, kde se bez spolehlivého šifrování dat, nejlépe celého disku, DLP neobejde. Druhým nedostatkem je možnost se připojit k jakékoliv jiné než firemní síti ať už přes Wi-Fi (WLAN), LAN, Bluetooth a další rozhraní. Zde je nejrozumnější využití vynucené VPN do firemní sítě. Posledním úskalím jsou porty a to hlavně USB. DLP umožňuje šifrování dat a kontrolu zápisu na USB zařízení, nicméně je to běžná ochrana, která proti sofistikovanějším metodám útoku neobstojí. Proto zákaz USB a veškerých portů je nejrozumnější. I z pohledu DLP

je dobré uživatele naučit pro výměnu dat používat sdílené disky jakožto perimetr data **at rest** místo USB klíčenek.

Slabé vnitřní předpisy mohou také představovat riziko úniku. Pokud nebude přesná a správná specifikace v rámci interních předpisů, tak následná implementace v DLP nebude dostatečně účinná. Například, v případě odchozí e-mailové pošty je důležité specifikovat přesně jaké typy příloh a v jaké podobě je možné posílat. V opačném případě může skrz DLP mailovou bránu odejít e-mail se šifrovanou přílohou a celé úsilí s DLP vyjde vniveč. Proto je nutné zároveň v rámci nasazení DLP i nastavit vnitřní procesy a upravit firemní politiky.

3.3 Šifrovaná spojení

Posledním místem, na které by samotné DLP bylo krátké, je šifrované webové spojení. Ano, je možné využít Endpoint agenta, nicméně na úkor výkonu na pracovní stanici či notebooku a s omezenými politikami. Dodavatelé DLP systémů si jsou tohoto nedostatku vědomi, a každý z nich již nyní (za příplatek) nabízí vlastní webovou bránu či proxy server (dále jen proxy). Například společnost Symantec koupila v roce 2016 proxy společnosti Bluecoat. Druhým neméně významným důvodem koupě je stávající trend šifrování webového spojení a obsahu. Aby proxy byla schopná analyzovat daný obsah, musí dané spojení transparentně rozbít a opět složit. Zjednodušeně se dá říci, že dělá autorizovaný realtime útok typu „man in the middle“. Má to zjednodušené díky firemní důvěryhodné certifikační autoritě. Je zde ale důležité zmínit, že i přes to neumí všechny proxy či web gateway provést rozklad transparentně a internetový prohlížeč na příslušné stránce zahlásí chybu zabezpečení. Zmatení uživatele je vždy nežádoucí. DLP Symantec využívá pro plnou integraci s proxy serverem pomocí ICAPu. Přes tento protokol proxy dostává zprávu i zpět, zda dané spojení má či nemá povolit. Proto je vhodné spolupráci proxy, ať už vlastní nebo nabízené, v rámci PoC DLP otestovat. Je dobré se zaměřit i na transparentnost celého procesu, například u Google Drive či jiných cloudových služeb, které jsou největším rizikem úniku dat s ohledem na zvyklosti v rámci organizace.

3.4 Koncové stanice a DLP agent

Instalace DLP agenta na koncové stanice je poměrně jednoduchou záležitostí. Agent se nakonfiguruje, zabalí do instalačního balíčku a je distribuován pomocí softwaru třetích stran. Po nasazení se automaticky objeví v administraci DLP systému a je plně sledován

jeho stav. Pokud by se neautorizovaná osoba pokusila odstranit, vypnou či provést jiný zásah do DLP agenta (například vypnout proces či službu) dojde automaticky ke vzniku incidentu s nejvyšší prioritou. V administraci probíhá veškerá správa koncových stanic včetně aktualizace agentů a není již potřeba znovu používat distribuce pomocí instalačních balíčků.

Za slabé místo lze považovat zátěž, kterou klade agent na koncové stanice. Zátěž je závislá na množství, složitosti politik a jejich pravidel. Proto je vhodné brát v potaz výkonost všech koncových stanic, kde bude agent nasazen. Politiky a pravidla pro tento perimetr pak vytvářet podle nejslabšího článku. Pokud bude pravidlo velmi obecné, tak například při ukládání dokumentu bude neúměrně zatěžovat danou stanici a navíc zpomalí práci s dokumenty. Což vyvolá nežádoucí efekt a dopady na IT oddělení v podobě zvýšené kontroly stanic z důvodu zpomalení až po stížnosti určené vedení. S tímto faktem je proto dobré počítat už při návrhu architektury DLP tak, aby bylo možné oddělit politiky na koncové stanice a zbytku DLP. Výhodné je díky modularitě DLP systémů přenést co největší množství zatížení z koncových stanic na ostatní části DLP. Například, e-maily neskenovat na úrovni Endpointu, ale zátěž přenést na webovou bránu DLP systému.

3.5 Časová složitost a lidské zdroje

Z výše uvedených slabých míst je patrné, že proces odladění politik a celé infrastruktury DLP není elementární problém a má výraznou časovou náročnost. Je náročný i na lidské zdroje, protože vyžaduje spolupráci nejen experta na DLP z oddělení IT bezpečnosti, ale i IT oddělení, odboru interního auditu, ale i vedení. Podpora vedení je pro projekt DLP klíčová. Zvyšuje důvěryhodnost mezi IT a zaměstnanci. Čím více části společnosti je nutné do projektu DLP zapojit, tím více vzrůstá časová náročnost. Úspěšné nasazení a implementace všech požadovaných politik se může protáhnout i na rok. Proto je vhodné daný přínos společnosti a problematiku DLP vyzkoušet v rámci PoC.

Dodavatele DLP také reagují na trendy dnešní doby a nabízí různé části DLP systému pro cloudová řešení. V tuto chvíli je lepší v případě citlivých firemních dat a outsorcingu či SaaS DLP prosazovat zdrženlivost až do doby, kdy tato řešení budou prověřena. V oblasti IT bezpečnosti je konzervativní, střídmý přístup z dlouhodobého hlediska přínosem a představuje malé riziko. Proto je jako nejvhodnější řešení volena **on premise** varianta.

3.6 Právní pohled na DLP

Z pohledu zákoníku práce § 316 k tomu, aby zaměstnavatel mohl kontrolovat elektronickou poštu zaměstnance, musí nejen vymezit závažný důvod, který ho k tomu opravňuje, ale je rovněž povinen informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění. Existují ale i další zákony, které tento upřesňují, ale jejich výklad se liší dle institucí.

3.6.1 Sporný výklad zákona č. 101/2000 Sb., o ochraně osobních údajů

Pokud bychom se měli držet striktního výkladu (ÚOOÚ - Úřad pro ochranu osobních údajů) nelze obsah e-mailové komunikace zaměstnance kontrolovat téměř nikdy (resp. nikdy systematicky), jelikož převáží právo zaměstnance na soukromí/listovní tajemství. Právní rizika s tím spojená jsou pokuta až do výše 10 miliónů korun (reálně stovky tisíc), náhrada nemajetkové újmy (ochrana osobnosti) a trestněprávní odpovědnost.

Dle WP29 nezávislého poradního orgánu komise EU lze obsah e-mailové komunikace monitorovat prostřednictvím automatizovaných systémů, jsou-li dodrženy následující zásady. První zásadou je nutnost, kdy opatření musí být nezbytné k dosažení daného účelu (prevence úniku citlivých údajů), pro který se zřizuje a současně neexistuje jiný způsob (méně invazivní do soukromí zaměstnanců). Údaje jsou uchovávány po nezbytně nutnou dobu. Druhou zásadou je transparentnost. Tou je myšlena povinnost informovat zaměstnance, notifikovat ÚOOÚ a umožnit zaměstnancům přístup k údajům. Další zásadou je proporcionalita, tedy nutnost, vhodnost a přiměřenost opatření. Posledním opatřením je bezpečnost, tedy technická a organizační opatření pro zajištění bezpečnosti uchovávaných údajů.

3.6.2 Správný režim DLP dle výkladu

Z výše uvedeného vyplývá, že nasazení sytému DLP ve firemní infrastruktuře za účelem ochrany duševního vlastnictví firmy je možné. Jedinou podmínkou je nasazení v souladu s následujícími zásadami. Účelem je prevence úniku citlivých údajů. V rámci proporcionality by e-mail neměl z firmy odejít (resp. zůstat uchováván). Nejvhodnější je varování uživatele vyskakovacím oknem nebo vrácením e-mailu jako nedoručitelným s případným odůvodněním nedoručení. Doba uchovávání e-mailu je pouze po nezbytně dlouhou dobu pro zjištění úniku, maximálně v řádu jednotek dnů. Monitoring soukromých webmailů je právně rizikový, protože zaměstnavatel nemá k poskytovateli webmailu žádný právní

vztah. Reakce DLP systému je přípustná v podobně varovného vyskakovacího okna. Důležitou zásadou je správná informovanost zaměstnanců. Ta spočívá ve správně napsané vnitřní směrnici, kde je striktně zakázané používání e-mailu pro soukromé účely, respektive i pracovní stanice či notebook.

Tento bod je kontrolován, připomínán a školen. Směrnice musí obsahovat: jaké údaje budou kontrolovány a shromažďovány, kde a po jakou dobu budou uchovány, kdo k nim má přístup, kdo bude provádět kontrolu, jaká jsou bezpečnostní opatření k neoprávněným zásahům apod. Poslední zásadou je notifikovat úřad o zpracovávání osobních údajů například pomocí online registrace. V případě vyskakovacího okna s varováním není nutné notifikovat. Pro upřesnění, není nutné notifikovat tam, kde neprobíhá další zpracování a uchovávání. Pokud v rámci varování ve vyskakovacím okně vznikne incident, který obsahuje přesnou auditní stopu i se záznamem proč, se již jedná o zpracování, a tedy podléhá notifikaci.

3.7 Podpora, aktualizace, servis

Většina DLP systémů pochází od výrobců ze severní Ameriky a v České Republice mají pouze zastoupení skrz jiné společnosti. S tímto faktem je spojena i podpora a servis. Většina dodavatelů nabízí podporu úrovně L1, tedy základní podporu. Pokročilejší podporu druhého stupně nabízejí v rámci České a Slovenské republiky pouze jednotky dodavatelů. Takový dodavatel má experty na daný DLP systém, kteří jsou s větší částí problémů schopni pomoci. Většinou je nabízena podpůrná služba, která vám v rámci vaší smlouvy zajistí podporu přímo u dodavatele. Průběh pak reálně vypadá tak, že technik dodavatele zadá váš požadavek do Service Desku výrobce, a podle úrovně jejich vlastní smlouvy mu výrobce odpoví. Reakce nebývají nejrychlejší, proto je vhodnější zvolit dodavatele, který je schopen reakční doby smluvně garantovat, má kladné reference a již několik úspěšně provedených implementací.

Většina výrobců nabízí v rámci licencí aktualizace v rámci hlavní verze. Je možné dané aktualizace provádět vlastními silami. Existuje tu však možnost, že se něco pokazí a dodavatel například bude mít dle smlouvy dva dny reakční doby. V tu chvíli může dojít i k ochromení společnosti, proto je vhodné aktualizace systému DLP provádět ručně ve spolupráci s dodavatelem.

4 NÁVRH A REALIZACE DLP SYSTÉMU V TESTOVACÍM PROSTŘEDÍ POC

Kapitola je zaměřena na vlastní návrh a realizaci PoC DLP. První část kapitoly je věnována vektorům pokrytí pro navržená aktiva, způsobu výběru DLP dle funkcionality a očekávanému přínosu PoC. Další část obsahuje popis navržené architektury, implementace a potřebné procesy. Závěr kapitoly je věnován testovacímu scénáři a navazujícím politikám a pravidlům.

4.1 Aktiva a vektory pokrytí

Prvním a nejdůležitějším krokem PDCA je činnost plánování, do této fáze spadá i definice aktiv, díky které je pak možné určit vektory pokrytí. Definice aktiv slouží také jako podklad pro návrh testovacího scénáře a politik. Vektory pak poslouží pro správný výběr DLP systému.

4.1.1 Aktiva

Pro příklad uvažujme o nasazení z pohledu bankovního sektoru. Zde lze definovat běžná informační aktiva. V první řadě jde o aktiva, která jsou dána regulátorem na ochranu citlivých dat, jako jsou klientská či zaměstnanecká data a všechny dokumenty, které tato data obsahují. Příkladem takových dat může být smlouva či životopis. Mezi firemní citlivá data lze zařadit strategické dokumenty, smluvní či technickou dokumentaci. Dále je nutné považovat z pohledu bezpečnosti za aktiva i logovací soubory, šifrované soubory a certifikáty. Dalším rizikem jsou konfigurační soubory, které mohou obsahovat jméno a heslo v prostém textu.

Tab. 6. Přehled informačních aktiv PoC DLP

Aktiva	Legislativní	Firemní	Technická
	klientská data zaměstnanecká data	strategické dokumenty smluvní dokumentace	technická dokumentace provozní dokumentace
Příklad	smlouva	smlouva	log soubor
	životopis	report analýza prezentace	šifrovaný soubor certifikát konfigurační soubor
Typ	obsah	obsah	obsah + kontext

S výše uvedenými aktivy (Tab. 6) může zaměstnanec libovolně disponovat, například zaslat elektronickou poštou, uložit na USB disk nebo vytisknout. Tedy je vynést mimo organizaci, a tím způsobit nemalé finanční ztráty. Únik dat může být chtěný například od zaměstnance, který dostal výpověď. Druhou možností je nechtěný náhodný únik dat, například ztrátou USB klíčenky nebo přeposlání e-mailu. Cílem PoC je pak otestovat funkčnost DLP systému v podobných případech, a tím potvrdit jeho pozitivní dopady na prevenci úniku dat.

4.1.2 Vektory pokrytí

Mezi základní místa, kde je potřeba provádět DLP kontrolu, patří výše uvedená aktiva, která mohou představovat riziko úniku. Jde především o sdílené disky, webový provoz, e-mailové komunikace, firemní zařízení a síťový tisk. Pokud firma disponuje dalšími místy, jako je kupříkladu centrální místo pro spolupráci (SharePoint), dokumentové úložiště či veřejné složky na e-mailovém serveru, je vhodné, aby vybrané DLP taková místa pokrývalo a umožňovalo jejich integraci. Cílem PoC není provádět test všech integračních vazeb, proto jsou zahrnuta pouze základní místa.

Tab. 7. Tabulka pokrytí PoC DLP

Vektory pokrytí		
Data in use	**Data in motion**	**Data at rest**
firemní zařízení (notebook, PC)	e-mailová komunikace	sdílené disky
	webový provoz síťový tisk	firemní zařízení (notebook, PC)

Z výše uvedeného pak plynou vektory pokrytí (Tab. 7). Sdílené disky představují data **at rest**, e-mailová komunikace, webový provoz a síťový tisk představují data **in motion** a firemní zařízení (notebook, PC) a práce s dokumenty spadá pod data **in use**.

4.2 Výběr systému DLP pro PoC

V prvním kroku je nutné zjistit, který princip DLP je vyžadován. Z definovaných aktiv lze vidět, že kontrola bude nutná na koncovém zařízení a jde o princip Host-based a také, že nám primárně jde o kontrolu obsahu. Z vektoru pokrytí pak plyne, že kontrola bude nutná i na síťových prvcích, proto požadovaný systém musí obsahovat i funkcionalitu network

DLP. Je patrné, že požadované DLP musí obsahovat oba principy k DLP, všechny vektory pokrytí a přístup k analýze souborů musí být primárně obsahový a částečně kontextový.

Druhým krokem je pak výběr DLP dle požadavků z nabídky trhu. K tomu nám poslouží přehled trhu na základě výsledků z analýz společnosti Gartner. Mezi lídry jak na poli DLP, Endpoint řešení, ale i Web Gateway jsou společnosti McAfee a Symantec, které splňují dle tabulky (Tab. 1) zmíněné požadavky. Obě tato řešení mají zastoupení produktu v ČR u několika firem.

4.2.1 Porovnání funkcionalit DLP pro PoC

Následujícím krokem je rozhodnutí, které DLP řešení pro PoC vybrat. Výběr je vhodné provést porovnáním požadavků na funkcionalitu, viz podkapitoly níže. Sloupec „podporováno“ za jednotlivá řešení vyplnili dodavatelé, kteří nabízí DLP řešení v ČR. Jména dodavatelů nejsou v práci zveřejněna záměrně, protože autor diplomové práce má podepsanou dohodu o mlčenlivost (NDA - Non-disclosure agreement).

4.2.1.1 Data Discovery

Z tabulky níže (Tab. 8) vychází hůře řešení společnosti McAfee a z důvodu absence integrace s cloudovými službami.

Tab. 8. Přehled porovnání funkcionality Data Discovery

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
Data Discovery		
a) Data Discovery modul je součástí DLP nástroje	Ano	Ano
b) Data Discovery je prodáván jako samostatný produkt	Ano	Ano
c) Tento produkt discovery modul neobsahuje, ale DLP umožňuje spolupráci s produktem třetí strany	Ano	Částečně
Úrovně Data Discovery		
a) Možnost skenovat a zjišťovat citlivé dokumenty v rámci síťových úložišť na základě nastavených politik	Ano	Ano
b) Možnost klasifikovat citlivé dokumenty na síťových discích	Ano	Ano

c) Možnost Data Discovery v rámci cloudových služeb (Dropbox, Google Drive, SkyDrive apod.)	Ano	Ne
d) Možnost konfigurace zatížení vnitřní sítě/ IT infrastruktury při spuštěném skenu	Ano	Ano

4.2.1.2 Kontrola obsahu

Chybějící podpora využití technologie fingerprintu a chybějící podpora Machine learningu řadí McAfee opět na druhé místo, viz tabulka (Tab. 9). Za velký nedostatek je považována chybějící podpora OCR u obou řešení. OCR by našlo uplatnění v několika scénářích proti úniku dat.

Tab. 9. Přehled porovnání funkcionalit kontrol obsahu

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
1. Kontrola obsahu		
1.1. Metody kontroly		
a) Klíčová slova	Ano	Ano
b) Regulární výrazy	Ano	Ano
c) Částečná shoda dokumentu (hlavička smlouvy, podpis smlouvy apod.)	Ano	Ano
d) Přesná shoda dokumentu	Ano	Ano
e) OCR	Ne	Ne
f) Dictionary analysis	Ano	Ano
g) Informace o uživateli (možnost specifikovat politiku na základě statusu uživatele např. VIP)	Ano	Ano
h) Informace o USB (šifrované/nešifrované)	Částečně	Ano
i) Informace o stavu systému (patch level, local LAN-connected)	Částečně	Ano
j) Object tagging	Ano	Ano
k) Structured data fingerprinting	Ano	Ne
l) Character analysis	Ano	Ano
1.2. Metody minimalizace false positives		
a) Statistická analýza	Ano	Ano
b) Threshold analysis	Ano	Ano
c) Whitelisting	Ano	Ano
d) Checksum matching	Ne	Ne
e) Machine learning	Ano	Ne

4.2.1.3 Konfigurace politik

Dle tabulky (Tab. 10) jsou si v otázce konfigurace politik rovnocenné.

Tab. 10. Přehled porovnání možností politik

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
2. Konfigurace výchozí politiky		
a) Regulace bankovního sektoru (PCI DSS)	Ano	Ano
b) Předdefinovaná best practise pravidla z oblastí finance a bankovnictví	Ano	Ano
c) Předdefinované šablony lokalizované pro ČR a SR (rodná čísla, čísla občanských/řidičských průkazů a kreditních karet, IČ atd.)	Ano	Ano
3. Možnosti definice politik		
a) Možnost reportovat souhrn nastavených politik (např. z důvodu auditu)	Ano	Ano
b) Možnost kombinovat nastavená pravidla pro odladění false positives	Ano	Ano
c) Efektivní aplikace nastavené politiky bez nutnosti restartů	Ano	Ano
d) Organizace DLP politik do stromové struktury	Ano	Ano

4.2.1.4 Endpoint a jeho možnosti

V případě možností Endpoint DLP je situace opět vyrovnaná, viz tabulka níže (Tab. 11).

Tab. 11. Přehled porovnání funkcionality Endpoint DLP

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
4. Endpoint DLP - Podporovaný OS		
a) Microsoft Windows	Ano	Ano
b) Mac OS	Ano	Ano
5. Monitoring funkcí		
a) copy/paste	Ano	Ano
b) operace se soubory (kopírovat, ukládat a otevírat)	Ano	Ano
c) CD/DVD	Ano	Ano
d) kontrola USB zařízení	Ano	Ano
e) WiFi	Ano	Ano

4.2.1.5 Network DLP a podpora protokolů a aplikací

V rámci Network DLP obě řešení patří mezi špičku, proto i zde nejsou patrné žádné rozdíly, viz tabulka (Tab. 12).

Tab. 12. Přehled porovnání funkcionalit Network DLP

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
6. Network DLP		
a) E-mail	Ano	Ano
b) Web traffic	Ano	Ano
c) Instant messenger	Ano	Ano
d) Přenos souborů	Ano	Ano
7. Podpora protokolů a aplikací		
a) TCP (TFTP, FTP, sFTP, FTPS)	Ano	Ano
b) HTTP/HTTPS (Web sites, Web mail apod.)	Ano	Ano
c) P2P (BitTorrent, DC++)	Ano	Ano
d) Instant messenger (Skype for business, ICQ, Pidgin)	Ano	Ano
e) Sociální média (Facebook, Twitter, Instagram, Linke-dln apod.)	Ano	Ano
f) Cloudová úložiště (DropBox, Box, Google drive, apod.)	Ano	Ano
g) Web mail (Gmail, Seznam, Yahoo mail, apod.)	Ano	Ano

4.2.1.6 Management

Řešení společnosti Symantec dle tabulky (Tab. 13) v oblasti managementu ztrácí ve dvou bodech.

Tab. 13. Přehled porovnání funkcionalit managementu

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
8. Management		
a) Centralizované konzole umožňující správu celého pro-středí napříč instancemi DLP (Endpoint, Discovery a Network)	Ano	Ano
b) Centralizované konzole umožňující náhled na eventy a reporty napříč instance DLP (Endpoint, Discovery a Network)	Ano	Ano
c) Snadná instalace, která nabízí optimální nastavení v závislosti na velikosti prostředí	Ano	Ano

d) Case management součástí centrálního managementu	Ano	Ano
e) Možnost definovat přístupová oprávnění do centrální administrační konzole na základě rolí	Ano	Ano
f) Možnost vytvořit různé náhledy v managementu GUI podle rolí typu admin, helpdesk atd.	Ano	Ano
g) Možnost aktualizace DLP agentů na koncová zařízení přímo z centrální administrační konzole	Ano	Ano
h) Zálohování konfigurace před upgradem	Ne	Ano
i) Jednoduchý způsob aplikování updatů včetně možnosti rollback	Ne	Ano

4.2.1.7 Reporting

V oblasti reportingu je situace opět téměř vyvážená, viz tabulka níže (Tab. 14).

Tab. 14. Přehled porovnání funkcionality pro reporting

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
9. Reporting		
a) Dashboard pro vyhodnocování incidentů	Ano	Ano
b) Z dashboardu je možnost prokliku na podobné události k označenému incidentu	Ano	Ano
c) Dashboard umožňuje korelaci incidentů vztahujících se k danému uživateli/objektu	Ano	Ano
d) Možnost vytvoření custom reportů (XML, HTML, PDF)	Částečně	Ano
e) Možnost nastavit příjemce reportu (emailem) na základě údajů v AD (nadřízený zaměstnance)	Ano	Ano
f) Možnost reportování o stavu čerpaných licencí	Ano	Ano
g) Možnost reportování o využití politik na jednotlivých částech DLP (agenti na konc. zařízeních, discovery sondy, proxy servery, apod.)	Ano	Ano
h) Možnosti reportování o zatížení koncových stanic	Ne	Ne
i) Možnost auditního logování všech přístupů, akcí a změn konfigurace konsole	Ano	Ano
j) Databáze umožňující rychlé reportování dat a schopnost data ukládat na dlouhou dobu	Ano	Ano

4.2.1.8 Podpora

Z tabulky níže (Tab. 15) vyplývá, že zákazník buď získá podporu v češtině a obětuje přímý kontakt na L2, nebo bude bez češtiny, ale s podporou L2.

Tab. 15. Přehled porovnání možností podpory

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
10. Podpora		
a) Dedikované podpůrné prostředky a přímý kontakt na L2 podporu	Ne	Ano
b) Podpůrný materiál včetně "best practices"	Ano	Ano
c) Asistence při instalaci a zaškolení	Ano	Ano
d) Dostupnost podpory při nasazení	Ano	Ano
e) Komunikace s L1 podporou v češtině	Ano	Ne

4.2.1.9 Napojení na vlastní infrastrukturu

Pokud je ve firmě využito Microsoft Exchange, tak řešení McAfee má podstatnou nevýhodu v podobě absence podpory integrace, viz tabulka (Tab. 16).

Tab. 16. Přehled porovnání možností napojení na vlastní infrastrukturu

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
11. Možnosti napojení na vlastní infrastrukturu		
a) Microsoft Active Directory	Ano	Ano
b) Microsoft Exchange	Ano	Ne
c) SIEM	Ano	Ano
d) Proxy server (SQUID)	Ano	Ano
e) IDM nástroje	Ano	Ano

4.2.1.10 Možnosti implementace

Možnosti implementace dle tabulky níže (Tab. 17) mají obě řešení totožné.

Tab. 17. Přehled porovnání možností implementace

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
12. Možnosti implementace/deploymentu		
a) Serverové komponenty DLP řešení mohou být nasazeny ve virtuálním prostředí	Ano	Ano
b) Jaký je doporučený sizing pro deployment ve virtuálním prostředí	Nevyplněno	Nevyplněno
c) Serverové komponenty DLP řešení jsou dostupné pouze jako HW appliance	Ne	Ne
d) Řešení podporuje deployment serverových komponent DLP řešení ve více geograficky oddělených DC	Ano	Ano
e) Pro případ výpadku je podporován active-passive mód centrálních serverových prvků	Ano	Ano

4.2.1.11 Licencování

Dle tabulky (Tab. 18) má řešení Symantec výrazně vyšší variability v licencování.

Tab. 18. Přehled porovnání licencování

DLP řešení	**Symantec**	**McAfee**
Požadavky na funkcionalitu	**Podporováno**	**Podporováno**
13. Licencování		
13.1. Síťové komponenty (proxy, email, apod.)		
a) Centrální síťové komponenty jsou licencovány nezávisle na DLP	Ano	Ne
b) Centrální síťové komponenty podporují subscription licence model	Ano	Ne
c) Centrální síťové komponenty podporují perpetual licence model	Ano	Ano

13.2. Licence DLP nástroj		
a) Centrální DLP server je licencován samostatně	Ano	Ne
a.1) Centrální DLP server podporuje subscription licence model	Ano	Ne
a.2) Centrální DLP server podporuje perpetual licence model	Ano	Ne

4.2.2 Vyhodnocení funkcionalit DLP

Finální rozhodnutí výběru je pak jednoduchým krokem. Nejjednodušším modelem vyhodnocení je provést sečtení všech „Ano“, „Ne“ a podobně. Váhový model nemá smysl provádět v rámci PoC, protože se požadavky na funkcionalitu mohou v průběhu PoC měnit. Model vah je pak dobré použít pro výběr DLP systému do ostrého provozu, kde nám výsledky a zkušenosti z PoC pomohou váhový model stanovit. Přehledné srovnání výsledků je v tabulce (Tab. 19). Je patrné, že v podporovaných požadavcích na funkcionalitu vede DLP Symantec a to i včetně započítání částečné podpory. Preferovaným řešením pro PoC je Symantec DLP.

Tab. 19. Přehled vyhodnocení DLP

DLP řešení	Ano	Částečně	Ne	Nevyplněno	Celkem	Ano a částečně
Symantec	78	3	7	1	89	81
McAfee	73	1	14	1	89	74

4.2.3 Předpokládané přínosy a cíle PoC

Cílem Proof of Concept DLP je ověření přínosů v podobě prevence úniku dat a tím zvýšení bezpečnosti společnosti. Sekundárním cílem je ověření náročnosti implementace a vnitřních procesů, nároků na lidské zdroje, shody vnitřních předpisů, zvýšení znalostí a problematiky v oblasti DLP a jejich uplatnění v praxi. Významným přínosem je načerpání zkušeností pro budoucí implementaci GDPR. DLP představuje jediné řešení pro skutečné naplnění požadavků GDPR.

4.3 Architektura řešení

Následná realizace je navržena dle doporučení Symantec DLP a vůči jiným DLP řešením se může v určitých oblastech lišit. Pro PoC je použit produkt Symantec Data Loss Prevention Suite ve verzi 14.5. V řešení DLP bude využito virtualizační platformy VMware vSphere. Na prvním serveru bude probíhat administrace celého řešení. Základním stavebním kamenem je jeden Enforce server, který zajistí jednotný management pro EndPoint, síťové komponenty DLP, management pro řízení politik a vyhodnocování incidentů. Na tento server budou nainstalovány i všechny ostatní detekční servery včetně centrální konzoly Enforce Platform.

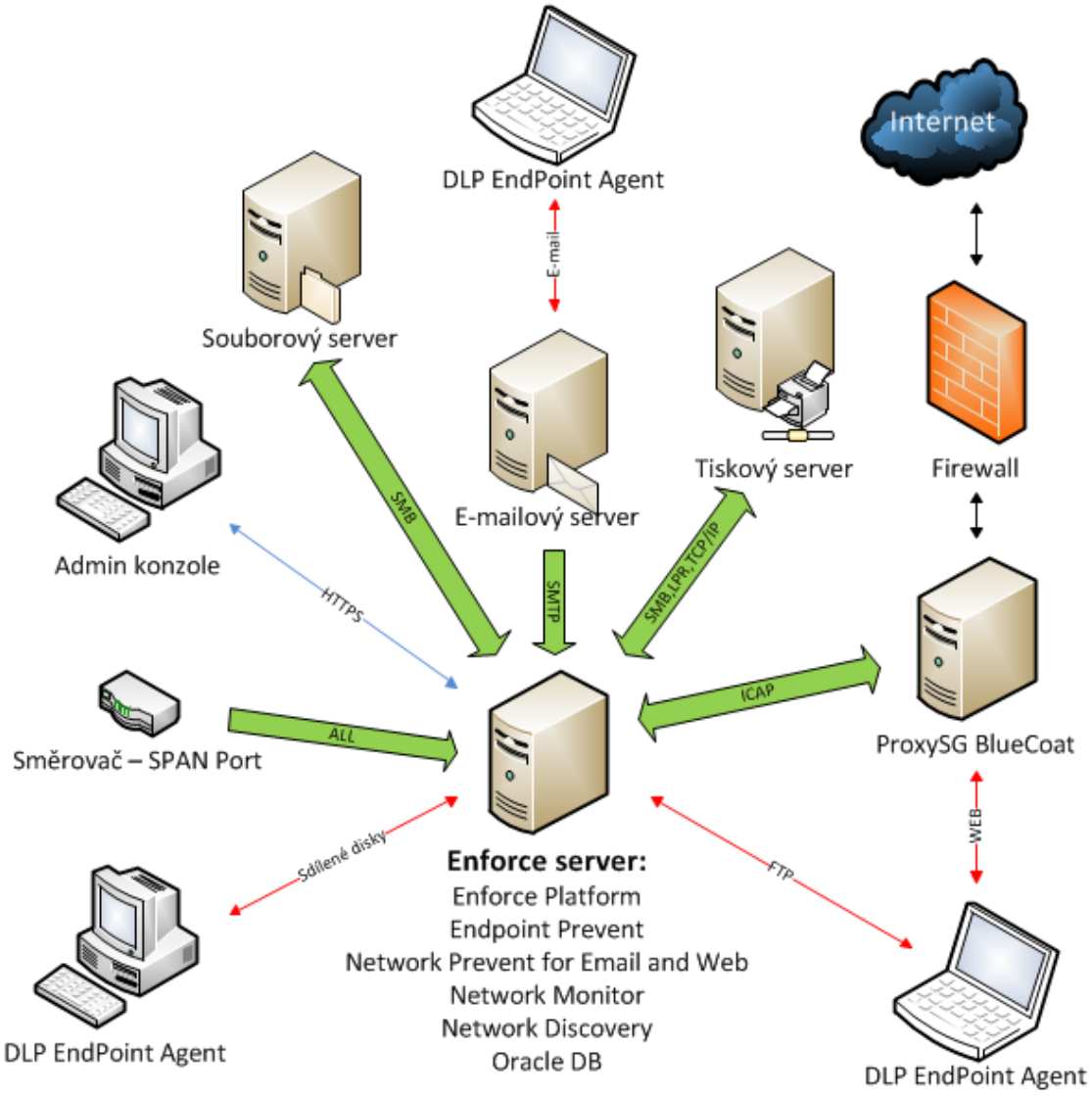
Detekční servery jsou:

- Endpoint Prevent – zajišťuje komunikaci a sběr dat z koncových stanic
- Network Monitor – slouží k analýze veškerého síťového provozu, přes SPAN port
- Network Prevent for Email and Web – stará se o kontrolu mailového provozu a také o komunikaci s proxy serverm, přes který probíhá webový provoz
- Network Discovery – je zodpovědný za procházení datových úložišť

Dalším serverem bude ProxySG BlueCoat, který se bude starat o analýzu webového provozu a rozklad zabezpečeného spojení (SSL/TLS). Jedná se o hardwarovou applianci zapůjčenou od dodavatele po dobu trvání PoC. Tento server bude sloužit ke komunikaci s detekčním serverem Network Prevent for Email and Web, Internetem a testovacím PC. Bude mu vystaven certifikát od vnitřní doménové důvěryhodné autority, který mu dovolí podepisovat vlastní vygenerované certifikáty. Dá se říci, že tím se stane proxy server subautoritou, a tak bude zajištěna důvěryhodnost takto připravených certifikátů na doménovém testovacím PC. Tímto způsobem bude pro uživatele zajištěn dostatečný komfort, protože spojení bude stále šifrované, i když firemním certifikátem.

Celý návrh je znázorněn na obrázku (Obr. 11). Červeně jsou znázorněny obousměrné komunikační cesty z testovacích PC či notebooků. Tučné zelené šipky vyjadřují komunikaci pro vnitřní potřeby DLP. Černé šipky značí obyčejnou komunikaci. Modrá šipka znázorňuje přístup k administraci DLP. Souborový server bude obsahovat testovací data pro detekci a dočasný odkládací prostor pro firemní data. E-mailový server pouze přeposílá e-mailovou komunikaci na Enforce Server, který ji zpracuje a zahazuje. V ostré implementaci by pak Enforce server e-mailovou komunikaci posílal dále na odchozí mailovou bránu. V rámci PoC by takové chování bylo nežádoucí. Tiskový server dokumenty pouze sbírá

do fronty. Směrovač má nakonfigurováno přeposílání veškerého síťového provozu z firemní testovací VLANy na SPAN port Enforce Serveru. ProxySG BlueCoat sleduje veškerou webovou aktivitu přes ni proudící, rozebírá šifrovaná spojení a zároveň komunikuje ICAPem s Enforce serverem a zjišťuje, zda komunikaci propustit či nikoliv.



Obr. 11. Architektura řešení PoC DLP

Pro lepší představu, který detekční server pokrývá jaký vektor pokrytí je níže uvedena tabulka (Tab. 20). Navržená architektura řešení PoC pokrývá všechny požadované vektory pokrytí.

Tab. 20. Detekční servery a vektory pokrytí

Vektory pokrytí		
Data in use	**Data in motion**	**Data at rest**
Endpoint Prevent	Network Prevent for Email and Web	Network Discovery
DLP Endpoint Agent	Netowork Monitor	
	ProxySG BlueCoat	

4.4 Plán nasazení PoC

Nasazení DLP byť jako PoC není jednoduchý proces, proto je potřeba mít připravený plán s postupnými kroky implementace.

Plán implementace obsahuje tyto kroky:

- Instalace Enforce serveru a ProxySG BlueCoat
- Zprovoznění administrace Enforce Platform
- Instalace detekčních serverů Enforce Prevent, Monitor, Discovery, …
- Konfigurace Enforce serveru i jeho komponent a Proxy SG BlueCoat
- Vystavení potřebných certifikátů a jejich nasazení
- Instalace Endpoint Agentů a jejich napojení na DLP
- Napojení Enforce serveru (jeho detekčních serverů) na e-mailový, souborový a proxy server
- Konfigurace switche a SPAN portu
- Kontrola všech nastavení zainteresovaných serverů a stanic
- Příprava základního setu politik
- Nasazení politik
- Kontrola funkčnosti politik a správného generování incidentů
- Vyhodnocení politik, v případné změny se poustupuje dle cyklu PCDA
- Testovaní administrace, managementu DLP a integrace s navázanými systémy
- Vyhodnocení PoC DLP

Před posledním krokem vyhodnocení PoC DLP je nutné úspěšně splnit všechny předcházející. Jinak by nedošlo k transparentnímu hodnocení a výsledek by mohl být zkreslený.

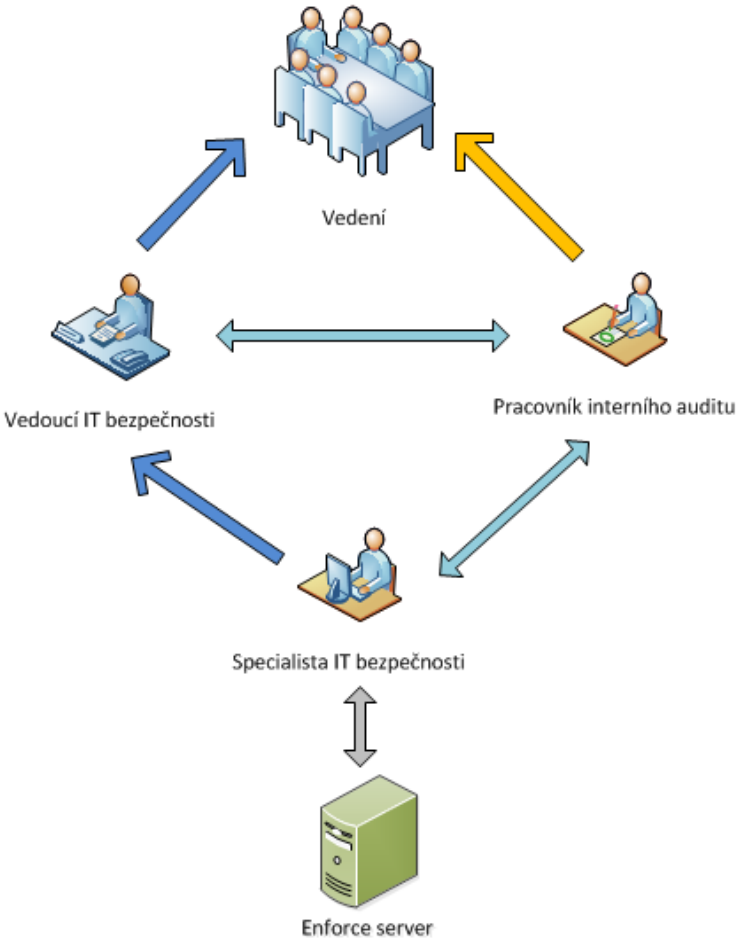
4.5 Návrh podpůrných procesů

Pro zajištění transparentnosti průběhu PoC, je nutné definovat podpůrné procesy. Byť je prostředí PoC izolováno od většiny produkční části infrastruktury společnosti, i přesto se neobejde bez podpůrných systémů, které není možno do PoC duplikovat a zajistit tak plnou izolaci. Zahrnutí podpůrných systémů do PoC je nutné z důvodů otestování integračních vazeb. Mezi podpůrné systémy lze zařadit například doménový řadič, souborový a e-mailový server nebo switch (pro SPAN port). Z důvodu NDA pro práce neobsahuje konkrétní názvy a verze podpůrných systémů.

V rámci navržených procesů je otestována komunikace a časové možnosti zainteresovaných stran. Případné zkušenosti pak poslouží i jako základ pro budoucí nasazení DLP systému do firmy, což urychlí fáze ostré implementace.

4.5.1 Proces bezpečnostního dohledu a kontroly využívání DLP

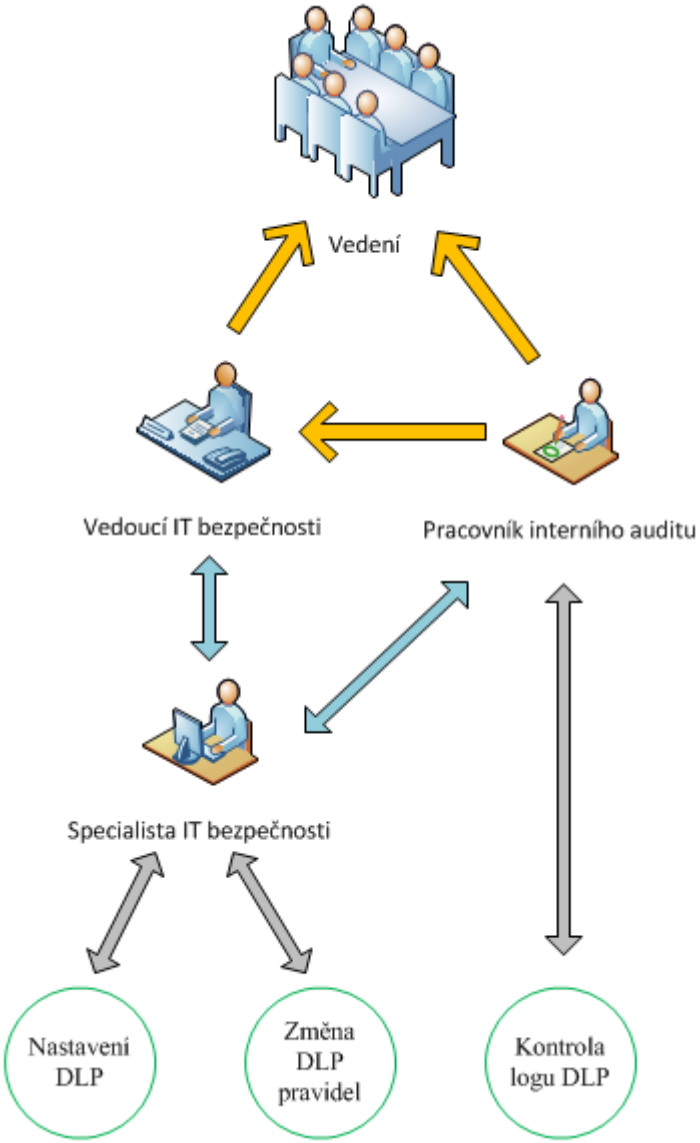
Prvním, a nejdůležitějším procesem, je samotný dohled na PoC a jeho využívání. Byť by měl být využíván pouze nad testovacími daty, může se stát, že se do procesu dostanou i citlivá data. Pak by samotné PoC představovalo jistou míru rizika úniku. Proto je na celé PoC aplikován princip čtyř očí, viz obrázek (Obr. 12). Kontrolorem je v procesu zaměstnanec z jiného nezávislého odboru interního auditu. Dohledovým orgánem je pak vedení společnosti, kterému jsou vedoucím IT bezpečnosti pravidelně poskytovány reporty o porušení pravidel a závažné incidenty. Do PoC je dobré zahrnout i dohledový orgán a seznámit ho s reporty a detaily incidentů, tak aby byl jasný přínos v prevenci úniku dat.



Obr. 12. Proces dohledu a kontroly využívání DLP

4.5.2 Proces dohledu nad administrací DLP

DLP systém, jak už bylo zmíněno, by mohl představovat sám o sobě bezpečnostní riziko úniku a to především zneužitím od specialisty IT bezpečnosti. Proto je dohled nad administrací dalším důležitým procesem. Specialista IT bezpečnosti má dohled ze dvou stran, od svého přímého nadřízeného a od nezávislého odboru interního auditu. Pracovník interního auditu má pak dohled nad implementací politik, také nad logy samotného DLP. V záznamech je pak patrná auditní stopa provedených změn. Veškeré provedené změny musí být schváleny dohledem a tím je zajištěn správný postup, viz obrázek níže (Obr. 13). Jakékoliv nekorektní nastavení je reportováno vedení společnosti. Proces obsahuje tři hlavní kroky: nastavení DLP, změna politik a kontrola logů.



Obr. 13. Proces dohledu nad administrací DLP

4.6 Návrh testovacího scénáře

Cílem testů je ověřit funkčnost, a tím přínos DLP organizaci. Testovány byly především možnosti, vlastnosti, funkcionalita DLP, integrační vazby s podpůrnými systémy, práce s administrací DLP. V druhé korku následovala práce s politikami, pravidly a jejich funkčnost, management incidentů, správné nastavení kontrolních procesů.

Ověření požadavků na DLP probíhalo pomocí administrace DLP, kde byla daná funkcionalita nalezena a případně otestována. Pokud daná funkcionalita nebyla nalezena nebo ji nebylo možno otestovat, bylo využito podpory dodavatele pro doplnění informací. Pokud

v rámci testu byla nalezena zajímavá funkcionalita, která nebyla v původním přehledu požadavků na funkcionalitu, tak byla doplněna.

Testy požadavků na DLP obsahovaly:

- Data Discovery
- Kontrola obsahu
- Konfigurace politik
- Endpoint a jeho možnosti
- Network DLP, podpora protokolů a aplikací
- Management
- Reporting
- Podpora
- Napojení na vlastní infrastrukturu
- Možnosti implementace

Testy na funkcionalitu politik byly prováděny z testovací stanice s nainstalovaným DLP agentem. Stanice byla napojena na testovací mailový server, tiskový a souborový server. Pro komunikaci do internetu byla napojena na proxy server. Test probíhal záměrným pokusem o porušení politiky. Pokud vznikl incident odpovídající politiky s požadovaným detailem, pak byl test úspěšný. V rámci testu politik byla také otestována správná funkcionalita rozbíjení šifrovaného spojení proxy serveru, kdy například u testu úniku klientských dat byl soubor nahrán na webmail. Testy politik představují možné úniky aktiv.

Testy funkcionalit politik obsahovaly:

- Test úniku klientských dat
- Test úniku zaměstnaneckých dat
- Test úniku strategických dokumentů
- Test úniku smluvní dokumentace
- Test úniku dat na soukromé e-maily
- Test úniku skrze paměťová zařízení
- Test úniku ostatních citlivých dat (logovací a šifrované soubory, certifikáty, přihlašovací údaje)

4.7 Návrh politik, pravidel

Návrh je proveden na základě aktiv. Každé významné aktivum má svou politiku z důvodu přehlednosti, ale také z důvodu tvorby incidentu a jejich reportování. Každá politika představuje jeden možný vektor úniku. Rozdělení do více politik pak umožňuje různé možnosti hodnocení a eskalace incidentů. Další výhodou je využití specifických pravidel pro každou politiku, a tím zvýšení přesnosti detekce a minimalizace false postive incidentů. Politiky obsahují možnosti výjimek a jsou do nich zahrnuty. S výjimkami se pracuje stejným způsobem jako s pravidly a obsahuji podobné možnosti. Do výjimek je zařazeno jediné pravidlo a to seznam VIP osob, na které se nemají za žádných okolností politiky aplikovat. Tato výjimka je zde z důvodu požadavku vedení společnosti.

Politiky jsou navrženy s primárním cílem zabránit úniku dat mimo společnost, proto některá pravidla nejsou aplikována na vektoru koncových stanic (Endpoint). V rámci PoC bude jakýkoliv pokus o únik dat pouze logován, nikoliv blokován, a bude zaznamenán v podobě incidentu. Ke každému incidentu jsou pak data, která kolidovala s politikami, uložena po dobu jednoho měsíce.

4.7.1 Politika prevence úniku klientských dat

Politika cílí na data o klientech, která jsou pro bankovní sektor nejdůležitějším aktivem. Citlivá data se mohou vyskytovat v dokumentech, e-mailech, prezentacích, reportech a podobně. Politika je aplikována na všech vektorech pokrytí až na vektor koncových stanic. Systém DLP získal data o klientech z informačního systému pro správu klientů, v případě PoC šlo tabulkový soubor nahraný na server DLP. DLP Symantec tato data načte pomocí technologie Exact Data Matching (EDM) pouze jednou. V rámci administrace DLP je pak již není možné přečíst, protože DLP je má uloženy v podobě hashe. Specialista IT bezpečnosti by neměl mít přístup ke všem informacím, se kterými DLP pracuje.

Za citlivé informace o klientech je považováno:

- Jméno a příjmení
- Rodné číslo
- Číslo obřanského průkazu (OP) nebo pasu
- Číslo účtu nebo smlouvy
- Číslo karty
- E-mail nebo telefon

Pravidla jsou koncipována jako kombinace jednotlivých citlivých informací a výskytu jejich četnosti, viz tabulka níže (Tab. 21). Z tabulky je patrné, že pro všechny případy je minimální výskyt dvakrát z důvodu minimalizace incidentů. Jedinou výjimkou je číslo kreditní karty, které by nemělo firmu opustit v žádné podobě. Ampersand „&“ představuje logický operátor AND.

Tab. 21. Politika pro klientská data - kombinace pravidel a výskytů

Data klientů	výskytů v 1 dokumentu
Jméno, příjmení & rodné číslo	> 2
Jméno, příjmení & číslo OP nebo pasu	> 2
Jméno, příjmení & číslo účtu	> 2
Jméno, příjmení & číslo smlouvy	> 2
Jméno, příjmení & telefon	> 2
Jméno, příjmení & e-mail	> 2
Číslo kreditní karty	> 0

4.7.2 Politika prevence úniku dat o zaměstnancích

Data o zaměstnáních představují pro jakoukoliv společnost citlivé informace, proto je nutné tato data chránit. Politika je sestavena obdobným způsobem jako předchozí a je platná pro všechny vektory pokrytí mimo koncové stanice. Data o zaměstnancích získá DLP stejným způsobem jako u předchozí politiky s tím rozdílem, že jsou data načtena s personálního systému, též simulovaného tabulkovým souborem.

Za citlivé informace o zaměstnancích je považováno:

- Jméno a příjmení
- Rodné číslo
- Číslo OP nebo pasu
- Číslo účtu
- Soukromý email
- Soukromý telefon

Kombinace jednotlivých pravidel je uvedena v tabulce níže (Tab. 22). Výskyt citlivých informací v jednom dokumentu je stanoven na dva záznamy.

Tab. 22. Politika pro zaměstnanecká data - kombinace pravidel a výskytů

Data zaměstnanců	výskytů v 1 dokumentu
Jméno, příjmení & rodné číslo	> 2
Jméno, příjmení & číslo účtu	> 2
Jméno, příjmení & telefon	> 2
Jméno, příjmení & e-mail	> 2
Jméno, příjmení & telefon	> 2

4.7.3 Politika prevence úniku strategických dokumentů

Politika má za cíl odchytit jakýkoliv únik strategického dokumentu. Za takový dokument je považován jakýkoliv dokument (textový, tabulkový, prezentace, report), kde jeho autorem je člen VIP skupiny (vedení) anebo pokud provedl poslední úpravy dokumentu. Toto pravidlo nahrazuje do jisté míry chybějící klasifikaci dokumentů, která není pro vedení přínosem. Proto klasifikace dokumentů a spolupráce s DLP není testována.

Incident vznikne vždy, pokud takto vyhodnocený strategický dokument opustí perimetr společnosti. Tato politika není nasazena na vektoru koncových bodů.

4.7.4 Politika prevence úniku smluvní dokumentace

Politika je postavena na indexaci smluv, které systém DLP nalezne na vyhrazeném úložišti dat pomocí detekčního serveru Enforce Discovery. Každý dokument či smlouva, která se nachází v tomto úložišti, je považována za citlivá data. Pravidlo říká, že jakýkoliv dokument, jehož míra podobnosti je vyšší než 80 % s indexovanou skupinou smluv vede ke vzniku incidentu.

Druhé pravidlo v rámci této politiky označí jakýkoliv dokument za smluvní dokumentaci, pokud obsahuje standardní hlavičku smluv společnosti. V obou případech stačí jediný výskyt ke vzniku incidentu.

4.7.5 Politika odesílání dat na soukromé e-maily

Závažným prohřeškem je považováno využívání soukromých e-mailů k firemním účelům. Běžná praxe je pak přeposílání rozdělané práce do soukromých e-mailových schránek s tím, že se jedná o „práci na doma“. Politika pak takové chování postihuje. Pravidlo vyvo-

lá incident pro jakýkoliv odchozí e-mail z firemní schránky, který je adresován na soukromý e-mail zaměstnance. Pravidlo je aplikované pouze na detekčním serveru pro mailovou komunikaci.

4.7.6 Politika prevence úniku dat skrze paměťová zařízení

Pravidlo v této politice je zjednodušené z důvodu snížení zatížení koncové stanice a je platné pouze na tomto vektoru. Pravidlo nezaloží incident v klasickém slova smyslu, ale pouze informační záznam. Ten je vytvořen v případě, že jsou dokumenty kopírovány na USB zařízení. Do záznamu je pak uložen název kopírovaného souboru a jeho metadata. Samotný soubor se k záznamu nepřikládá.

4.7.7 Politika prevence úniku ostatních typů citlivých dat

Poslední politika obsahuje více drobných pravidel a je platná pouze pro e-mailovou komunikaci jdoucí mimo firemní perimetr. Politika je aplikovaná pouze na detekčním serveru pro mailovou komunikaci. Pro vznik incidentu stačí jeden výskyt porušení pravidla. První pravidlo kontroluje logovací soubory a zachycuje každý dokument, který v názvu či příponě obsahuje slovo „log“. Druhé pravidlo postihuje odesílání souborů s certifikáty, tedy každý soubor s příponami „pfx, cer, p7b“. Další pravidlo založí incident vždy, když narazí na šifrovaný soubor. Poslední pravidlo řeší únik přihlašovacích údajů na základě obsahu. Incident vznikne, pokud dokument nebo e-mail obsahuje kombinaci slov „jméno, heslo“ či „username, password“ v libovolném pořadí. Jedná se o jednoduché pravidlo, ale účinné například proti programátorské chybě, kdy v logovém souboru lze takové kombinace nalézt.

5 VYHODNOCENÍ IMPLEMENTACE DLP

Posledním krokem dle plánu implementace je vyhodnocení PoC DLP. Důležitým předcházejícím krokem bylo zprovoznění PoC a jeho integrace s podpůrnými systémy dle architektury řešení, viz obrázek v kapitole „Architektura řešení“ (Obr. 11). Bez toho kroku by nebylo možné provést objektivní hodnocení. Vyhodnocení proběhlo na základě testovacího scénáře v časovém období jednoho měsíce.

5.1 Vyhodnocení

Vyhodnocení proběhlo v hlavních dvou oblastech. První oblastí bylo ověření očekávaných požadavků, podle kterých byl proveden výběr řešení DLP od společnosti Symantec. Druhou oblastí bylo ověření ochrany definovaných aktiv pomocí nastavených politik a ověření funkčnosti na jednotlivých vektorech pokrytí.

5.1.1 Vyhodnocení požadavků na DLP

Vyhodnocení bylo rozděleno do několika oblastí dle testovacího scénáře. Každý vyhodnocený požadavek může nabývat šesti hodnocení, viz tabulka níže (Tab. 23).

Tab. 23. Vyhodnocení požadavku

Hodnocení	Popis
Zcela splňuje požadavky	Všechny testy či ověření proběhly v pořádku
Částečně splňuje požadavky	Hodnocení nebylo na 100%, chybí méně podstatné části, hodnocení s výhradami
Nesplňuje požadavky	Závažné nedostatky
Ano dle dodavatele	Doplněno dodavatelem, nebylo možné ověřit, předpokládaný výsledek OK.
Částečně dle dodavatele	Doplněno dodavatelem, nebylo možné ověřit, předpokládaný výsledek je s výhradami
Ne dle dodavatele	Doplněno dodavatelem, nebylo možné ověřit, předpokládaný výsledek je nedostatečný

Oblasti vyhodnocení požadavků na DLP jsou:

- Data Discovery
- Kontrola obsahu
- Konfigurace politik
- Endpoint a jeho možnosti

- Network DLP a podpora protokolů a aplikací
- Management
- Reporting
- Podpora
- Napojení na vlastní infrastrukturu
- Možnosti implementace

V celkovém hodnocení lze konstatovat, viz tabulka níže (Tab. 24), že požadavky na funkcionalitu byly potvrzeny byť s drobnými výhradami, které jsou popsané v následujících podkapitolách. Během testování byly nalezeny nové zajímavé funkce, které nebyly v původních požadavcích, a proto byly přidány do testovacího scénáře.

Tab. 24. Celkový přehled vyhodnocení požadavků DLP

Vyhodnocené	**Výsledky**
Zcela splňuje požadavky	46
Částečně splňuje požadavky	19
Nesplňuje požadavky	14
Celkem	79
Zcela a částečně	65
Doplněné dodavatelem	**Výsledky**
Ano dle dodavatele	11
Částečně dle dodavatele	2
Ne dle dodavatele	2
Celkem	15
Ano a částečně	13
Dohromady	**Výsledky**
Zcela splňuje požadavky	57
Částečně splňuje požadavky	21
Nesplňuje požadavky	16
Celkem	94
Ano a částečně	78

5.1.1.1 Data Discovery

Z tabulky vyhodnocení (Tab. 25) je patrné, že splňuje téměř všechny požadavky. Jediným nesplněným bodem v části úrovně Data Discovery bod b), protože detekční server Data Discovery nedokáže automatizovaně klasifikovat dokumenty na sdílených discích. Následující bod c) splňuje požadavky pouze částečně, protože tato funkcionalita není v základním balíku a podléhá vlastnímu licencování.

Tab. 25. Přehled vyhodnocení požadavku na funkcionalitu Data Discovery

Požadavky na funkcionalitu	Výsledek testu
Data Discovery	
a) Data Discovery modul je součástí DLP nástroje	Zcela splňuje požadavky
b) Data Discovery je prodáván jako samostatný produkt	Zcela splňuje požadavky
c) Tento produkt discovery modul neobsahuje, ale DLP umožňuje spolupráci s produktem třetí strany	Zcela splňuje požadavky
Úrovně Data Discovery	
a) Možnost skenovat a zjišťovat citlivé dokumenty v rámci síťových úložišť na základě nastavených politik	Zcela splňuje požadavky
b) Možnost klasifikovat citlivé dokumenty na síťových discích	Nesplňuje požadavky
c) Možnost Data Discovery v rámci cloudových služeb (Dropbox, Google Drive, SkyDrive apod.)	Částečně splňuje požadavky
d) Možnost konfigurace zatížení vnitřní sítě/ IT infrastruktury při spuštěném skenu	Částečně splňuje požadavky
e) Možnost procházení Exchange veřejných složek/ mailboxů	Ano dle dodavatele
f) Možnost procházení Sharepoint	Ano dle dodavatele
g) Možnost procházení SQL Database	Ano dle dodavatele

5.1.1.2 Kontrola obsahu

V kontrole obsahu dle tabulky (Tab. 26) jsou splněny všechny podstatné metody a kontroly. Jediné dva body, které lze považovat za nevýhodu jsou kontroly obsahu OCR a Exact data z SQL. OCR je z pohledu praktičnosti vhodné pro únik naskenovaných dat. Exact data z SQL je naopak vhodné pro zjednodušený import dat například z personálního systému, kde pak není nutné dělat hlubší integraci.

Tab. 26. Přehled vyhodnocení požadavku na funkcionalitu kontroly obsahu

Požadavky na funkcionalitu	Výsledek testu
1. Kontrola obsahu	
1.1. Metody kontroly	
a) Klíčová slova	Zcela splňuje požadavky
b) Regulární výrazy	Zcela splňuje požadavky
c) Částečná shoda dokumentu (hlavička smlouvy, podpis smlouvy apod.)	Zcela splňuje požadavky
d) Přesná shoda dokumentu	Zcela splňuje požadavky
e) OCR	Nesplňuje požadavky
f) Dictionary analysis	Zcela splňuje požadavky
g) Informace o uživateli (možnost specifikovat politiku na základě statusu uživatele např. VIP)	Zcela splňuje požadavky
h) Informace o USB (šifrované/nešifrované)	Nesplňuje požadavky
i) Informace o stavu systému (patch level, local LAN-connected)	Částečně dle dodavatele
j) Object tagging	Nesplňuje požadavky
k) Structured data fingerprinting	Zcela splňuje požadavky
l) Character analysis	Částečně dle dodavatele
m) Identifikace na základě typu, velikosti, názvu, metadat souboru	Částečně splňuje požadavky
n) Identifikace na základě typu protokolu	Zcela splňuje požadavky
o) Exact data z SQL	Nesplňuje požadavky
1.2. Metody minimalizace false positives	
a) Statistická analýza	Zcela splňuje požadavky
b) Threshold analysis	Zcela splňuje požadavky
c) Whitelisting	Zcela splňuje požadavky
d) Checksum matching	Zcela splňuje požadavky
e) Machine learning	Zcela splňuje požadavky

Důležitými metodami, které DLP od Symantecu zcela splňuje, jsou metody pro minimalizaci false positive. Ty jsou nedocenitelným pomocníkem při dalším rozvoji DLP systému.

5.1.1.3 Konfigurace politik

Úskalím každého produktu je přizpůsobení dané zemi a jejích zvyklostem. Většina šablon pro využití v ČR je prací zastoupení firmy, nikoliv samotného Symantecu. Lokalizovaných šablon je řádově méně než pro americký trh. Za větší nedostatek lze považovat nepřehlednost nastavených politik a jejich pravidel, nelze je například organizovat do stromové struktury, více v tabulce níže (Tab. 27).

Tab. 27. Přehled vyhodnocení požadavku na funkcionalitu konfigurace politik

Požadavky na funkcionalitu	Výsledek testu
2. Konfigurace výchozí politiky	
a) Regulace bankovního sektoru (PCI DSS)	Zcela splňuje požadavky
b) Předdefinovaná best-practise pravidla z oblastí finance a bankovnictví	Zcela splňuje požadavky
c) Předdefinované šablony lokalizované pro ČR a SR (rodná čísla, čísla občanských/řidičských průkazů a kreditních karet, IČ atd.)	Částečně splňuje požadavky
d) Oddělení politik Endpoint a NetMon	Ano dle dodavatele
3. Možnosti definice politik	
a) Možnost reportovat souhrn nastavených politik (např. z důvodu auditu)	Částečně splňuje požadavky
b) Možnost kombinovat nastavená pravidla pro odladění false positives	Zcela splňuje požadavky
c) Efektivní aplikace nastavené politiky bez nutnosti re-startů	Zcela splňuje požadavky
d) Organizace DLP politik do stromové struktury	Nesplňuje požadavky

5.1.1.4 Endpoint a jeho možnosti

Endpoint řešení podporují většinu operačních systémů na trhu. Jejich omezení spočívá například u Windows v pomalém přizpůsobení rychlosti vydávání nových verzí. Větším omezením je například nemožnost využití detailních informací o Wi-Fi připojení, viz tabulka (Tab. 28).

Tab. 28. Přehled vyhodnocení požadavku na funkcionalitu Endpoint DLP

Požadavky na funkcionalitu	Výsledek testu
4. Endpoint DLP - Podporovaný OS	
a) Microsoft Windows	Částečně splňuje požadavky
b) Mac OS	Ano dle dodavatele
5. Monitoring funkcí	
a) copy/paste	Zcela splňuje požadavky
b) operace se soubory (kopírovat, ukládat a otevírat)	Zcela splňuje požadavky
c) CD/DVD	Zcela splňuje požadavky
d) kontrola USB zařízení	Částečně splňuje požadavky
e) WiFi	Nesplňuje požadavky
f) Detekce protokolů	Zcela splňuje požadavky
g) Uvnitř/vně firemní sítě	Zcela splňuje požadavky
h) Síťový tisk Endpoint	Částečně splňuje požadavky

5.1.1.5 Network DLP a podpora protokolů a aplikací

Co se ukázalo jako nedostatečné řešení od výrobce, je monitoring síťového tisku, viz tabulka (Tab. 29). Kontrolu tisku bylo možné pouze na Endpointu.

Tab. 29. Přehled vyhodnocení požadavku na funkcionalitu Network DLP

Požadavky na funkcionalitu	Výsledek testu
6. Network DLP	
a) E-mail	Zcela splňuje požadavky
b) Web traffic	Zcela splňuje požadavky
c) Instant messenger	Částečně splňuje požadavky
d) Přenos souborů	Zcela splňuje požadavky
e) Síťový tisk	Nesplňuje požadavky
7. Podpora protokolů a aplikací	
a) TCP (TFTP, FTP, sFTP, FTPS)	Zcela splňuje požadavky
b) HTTP/HTTPS (Web sites, Web mail apod.)	Zcela splňuje požadavky
c) P2P (BitTorrent, DC++)	Nesplňuje požadavky
d) Instant messenger (Skype for business, ICQ, Pidgin)	Nesplňuje požadavky
e) Sociální média (Facebook, Twitter, Instagram, Linke-dln apod.)	Zcela splňuje požadavky
f) Cloudová úložiště (DropBox, Box, Google drive, apod.)	Zcela splňuje požadavky
g) Web mail (Gmail, Seznam, Yahoo mail, apod.)	Zcela splňuje požadavky

5.1.1.6 Management

Byť proxy Bluecoat byla koupena společností Symantec už více než před rokem, stále vyžaduje samostatnou administraci a nedošlo k její plné integraci s DLP. V tabulce (Tab. 30) je vidět, že řešení od společnosti Symantec v oblasti GUI ztrácí.

Tab. 30. Přehled vyhodnocení požadavku na funkcionalitu managementu

Požadavky na funkcionalitu	Výsledek testu
8. Management	
a) Centralizované konzole umožňující správu celého pro-středí napříč instancemi DLP (Endpoint, Discovery a Network)	Částečně splňuje požadavky
b) Centralizované konzole umožňující náhled na eventy a reporty napříč instance DLP (Endpoint, Discovery a Network)	Částečně splňuje požadavky
c) Snadná instalace, která nabízí optimální nastavení v závislosti na velikosti prostředí	Zcela splňuje požadavky
d) Case management součástí centrálního managementu	Částečně splňuje požadavky

e) Možnost definovat přístupová oprávnění do centrální administrační konzole na základě rolí	Částečně splňuje požadavky
f) Možnost vytvořit různé náhledy v managementu GUI podle rolí typu admin, helpdesk atd.	Částečně splňuje požadavky
g) Možnost aktualizace DLP agentů na koncových zařízeních přímo z centrální administrační konzole	Částečně splňuje požadavky
h) Zálohování konfigurace před upgradem	Ne dle dodavatele
i) Jednoduchý způsob aplikování updatů včetně možnosti rollback	Ne dle dodavatele

5.1.1.7 Reporting

V tabulce níže (Tab. 31), je patrné, že v oblasti reportingu také ztrácí. Reporty sice existují, ale jejich přizpůsobení či tvorba vlastních reportů je velice obtížná. Míra detailu logování různých akcí administrace je také nízká, například pro audit až nedostatečná, neobsahuje totiž bližší detail.

Tab. 31. Přehled vyhodnocení požadavku na funkcionalitu reportingu

Požadavky na funkcionalitu	Výsledek testu
9. Reporting	
a) Dashboard pro vyhodnocování incidentů	Zcela splňuje požadavky
b) Z dashboardu je možnost prokliku na podobné události k označenému incidentu	Částečně splňuje požadavky
c) Dashboard umožňuje korelaci incidentů vztahujících se k danému uživateli/objektu	Částečně splňuje požadavky
d) Možnost vytvoření custom reportů (XML, HTML, PDF)	Částečně splňuje požadavky
e) Možnost nastavit příjemce reportu (emailem) na základě údajů v AD (nadřízený zaměstnance)	Nesplňuje požadavky
f) Možnost reportování o stavu čerpaných licencí	Ano dle dodavatele
g) Možnost reportování o využití politik na jednotlivých částech DLP (agenti na konc. zařízeních, discovery sondy, proxy servery, apod.)	Nesplňuje požadavky
h) Možnosti reportování o zatížení koncových stanic	Nesplňuje požadavky
i) Možnost auditního logování všech přístupů, akcí a změn konfigurace konsole	Částečně splňuje požadavky
j) Databáze umožňující rychlé reportování dat a schopnost data ukládat na dlouhou dobu	Ano dle dodavatele

5.1.1.8 Podpora

Podpůrné materiály jsou v anglickém jazyce, což není překážkou. Ve fázi PoC je horší se k materiálům dostat, je nutné oslovit zastoupení v ČR, aby materiály dodala ona, viz tabulka (Tab. 32).

Tab. 32. Přehled vyhodnocení požadavku na funkcionalitu podpory

Požadavky na funkcionalitu	Výsledek testu
10. Podpora	
a) Dedikované podpůrné prostředky a přímý kontakt na L2 podporu	Zcela splňuje požadavky
b) Podpůrný materiál včetně "best practices"	Ano dle dodavatele
c) Asistence při instalaci a zaškolení	Zcela splňuje požadavky
d) Dostupnost podpory při nasazení	Zcela splňuje požadavky
e) Komunikace s L1 podporou v češtině	Zcela splňuje požadavky

5.1.1.9 Napojení na vlastní infrastrukturu

V tabulce (Tab. 33) je možné si všimnout, že kompatibilita s jinými proxy servery není vždy zaručena.

Tab. 33. Přehled vyhodnocení požadavku na funkcionalitu napojení

Požadavky na funkcionalitu	Výsledek testu
11. Možnosti napojení na vlastní infrastrukturu	
a) Microsoft Active Directory	Zcela splňuje požadavky
b) Microsoft Exchange	Zcela splňuje požadavky
c) SIEM	Ano dle dodavatele
d) Proxy server (SQUID)	Nesplňuje požadavky
e) IDM nástroje	Ano dle dodavatele

5.1.1.10 Možnosti implementace

V tabulce (Tab. 34) je potvrzena vysoká škálovatelnost implementace. Všechny uvedené body DLP zcela splňuje.

Tab. 34. Přehled vyhodnocení požadavku na funkcionalitu možnosti implementace

Požadavky na funkcionalitu	Výsledek testu
12. Možnosti implementace/deploymentu	
a) Serverové komponenty DLP řešení mohou být nasazeny ve virtuálním prostředí	Zcela splňuje požadavky
c) Serverové komponenty DLP řešení jsou dostupné pouze jako HW appliance	Zcela splňuje požadavky
d) Řešení podporuje deployment serverových komponent DLP řešení ve více geograficky oddělených DC	Zcela splňuje požadavky
e) Pro případ výpadku je podporován active-passive mód centrálních serverových prvků	Ano dle dodavatele
e) Škálovatelnost řešení, rozložení zátěže …	Zcela splňuje požadavky

5.1.2 Vyhodnocení funkcionality politik

Politiky fungovaly ve většině případů správně, viz tabulka (Tab. 36). U méně přesně specifikovaných politik docházelo ke zvýšenému počtu false positive incidentů. Druhým důvodem pouze částečného hodnocení, dle tabulky níže (Tab. 35), bylo nezachycení všech testovacích případů a malá míra detailu v incidentu. Tento fakt se týká především testu úniku skrze paměťová zařízení.

Tab. 35. Vyhodnocení politiky

Hodnocení	Popis
V pořádku	Politika zachytila všechny testovací případy
Částečné	Politika nezachytila část testovacích případů, zvýšený počet false positive
Nedostatečné	Politika nefungovala korektně, velké množství false positive
Vyřazeno	Politika na tomto vektoru nebyla nasazena

Lze konstatovat, že metody pro snížení počtu false positiv, jsou u DLP Symantec účinné a to především a automatizovaných metod strojového učení. To je potvrzeno prvními čtyřmi testy úniku. Kde počet false positive byl v jednotkách a přesně dle daných pravidel. Všechny politiky se chovaly přesně dle jejich definovaných pravidel a nedošlo k žádnému nečekanému selhání.

Tab. 36. Přehled vyhodnocení funkcionality politik

Test úniku	Vektory pokrytí		
	Data in use	**Data in motion**	**Data at rest**
klientských dat	Vyřazeno	V pořádku	V pořádku
zaměstnaneckých dat	Vyřazeno	V pořádku	V pořádku
strategických dokumentů	Vyřazeno	V pořádku	V pořádku
smluvní dokumentace	Vyřazeno	V pořádku	V pořádku
dat na soukromé e-maily	Vyřazeno	Částečné	Vyřazeno
skrze paměťová zařízení	Částečné	Vyřazeno	Vyřazeno
ostatních citlivých dat	Vyřazeno	Částečné	Vyřazeno

Práce s managementem politik a tvorbou pravidel je přívětivá a schválené změny se projeví téměř okamžitě. Takže i ladění politik je pak příjemnější a schůdnější. V rámci testu politik proběhl zároveň test odposlechu šifrovaného spojení. Proxy BlueCoat je schopna ve většině případu správně spojení rozebrat a složit bez dopadu na uživatele. V některých případech nedošlo k zachycení a vzniku incidentu. Při simulaci problému byl proveden odposlech paketů, který ukázal, že proxy nedoručí informaci o incidentu do DLP. Toto je přisuzováno problému proxy, které je samo o sobě velice komplexní nástroj a vyžadovalo by samostatné PoC. Práce se samotnými incidenty z pohledu vyšetřování incidentu byla dobrá a s dostatečnou mírou detailu. V ostrém provozu by bylo zajímavé vidět fungování schopností korelace dat a trendů.

5.2 Další možnosti vývoje

V rámci dalšího vývoje PoC by bylo vhodné provést vylepšení a rozšíření politik o další možné scénáře úniku dat a zároveň zvýšit míru přesnosti detekce. PoC by tak sloužilo jako testovací prostředí pro ostrou implementaci, kde relativně v bezpečném prostředí s nízkou mírou rizika lze pravidla odladit. Celý proces ostré implementace by pak byl urychlen. Dalším krokem, který by urychlil ostrou implementaci, je změna modelu priorit incidentu, a tím odstupňování závažnosti.

Možným scénářem by pak mohlo být rozšíření o pravidla, která by na rozdíl od stávajících nebyla orientovaná na únik dat z firmy ven, ale o pohyb dat uvnitř. Taková pravidla pak poslouží pro detekci neautorizovaného přístupu, a tím i minimalizace rizika úniku dat.

Vhodným vývojem by pak byl i test integrace s dalšími produkty v rámci firmy. Například, napojení na dohledový SIEM server a integrace s IDM, SharePoint a Exchange serverem či otestování napojení na SQL databázový server.

Do dalšího stádia vývoje mohou postoupit reporty pro vedení, kde je dobré zjistit, jaké další informace požadují na základě stávajících reportů. Poslední možností vývoje standardizace navržených procesů, které je nutno zahrnout do vnitřních norem.

ZÁVĚR

Cílem diplomové práce bylo ověřit přínos DLP systému jakožto prvku pro zvýšení zabezpečení firemní infrastruktury proti úniku dat, který by vedl k nežádoucím dopadům v podobě finančních ztrát či ohrožení dobrého jména společnosti. Tyto dopady jsou nemalou motivací pro firmy, které otázku ochrany dat doposud podceňovaly. Tvrzení lze podpořit i aktuálně vzrůstajícím trendem a tlakem na ochranu dat. Lze tak soudit nejen z úniků dat velkých společností v posledním roce, ale i z pohledu Evropské Unie v podobě nařízení GDPR. Nařízení klade ochranu osobních a citlivých informací na první místo a razantně zvedá požadavky na jejich zpracovatele. Nové výrazně vyšší finanční postihy plynoucí z porušení nařízení jsou dalším důvodem k implementaci toho systému. Nařízení nabývá platnosti v květnu roku 2018, i proto je ochrana dat aktuálním a ožehavým tématem.

Teoretická část byla koncipována tak, aby bylo jasné, k čemu DLP slouží, jakým způsobem funguje, jaké má využití ve firemní infrastruktuře a jak si takové řešení vybrat dle trhu s DLP. Byly zde rozebrány podpůrné standardy, informační aktiva, klasifikace informací a legislativa. Zmíněné položky tvoří základ ISMS v každé společnosti coby základní stavební kámen řízení IT. Dále práce seznamuje čtenáře se systémy DLP a jejich principy, typy, vlastnostmi a aktuálním přehledem na trhu. Poslední část byla věnována využití systému DLP ve firemní infrastruktuře. Konktrétně se zabývá použitím, nasazením, výstupy, integrací a hardwarovými nároky vybraného DLP.

Praktická část odhaluje slabá místa a úskalí systému DLP, a to jak z provozního pohledu, tak i z pohledu legislativního, kde je například možné se nevhodným pojetím DLP systému ve firmě dostat až na hranici se stávajícím zákonem na ochranu osobních údajů. Aby bylo možné reálně zhodnotit praktické přínosy systému DLP, je nutné jej otestovat. Této problematice se věnuje kapitola s návrhem a realizací PoC následovaná jeho vyhodnocením. Návrh PoC byl uzpůsoben tak, aby maximální měrou pokryl možná definovaná aktiva, vektory pokrytí a flexibilnost politik a pravidel.

Z výše uvedeného vyplývá, že problematika DLP přesahuje samotný systém, který klade zvýšené nároky na vedení společnosti, zaměstnance, specialisty IT bezpečnosti, ale i samotné firemní procesy a vnitřní normy. Přes všechny komplikace lze považovat systém DLP za přínos v ochraně proti úniku dat a duševnímu vlastnictví firmy. Vyhodnocení PoC dokazuje funkčnost řešení a jeho schopnost minimalizovat rizika spojená s únikem dat, a to především z dlouhodobého hlediska.

SEZNAM POUŽITÉ LITERATURY

[1] Data loss prevention - Ernst&Young [online]. 10/2011 [cit. 2017-05-12]. Dostupný z: http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf

[2] *Internet access by platform* [online]. 10/2016 [cit. 2017-05-12]. Dostupný z: https://ourworldindata.org/internet/ případně a také z: http://gs.statcounter.com/#desktop+mobile+tablet-comparison-ww-monthly-200812-201610

[3] *Symantec Data Loss Prevention Solution* [online]. 5/2015 [cit. 2017-05-12]. Dostupný z: https://www.symantec.com/products/information-protection/data-loss-prevention/resources

[4] McAfee Total Protection for Data Loss Prevention [online]. [cit. 2017-05-12]. Dostupný z: http://www.mcafee.com/us/products/total-protection-for-data-loss-prevention.aspx

[5] *Safetica Data Loss Prevention* [online]. [cit. 2017-05-12]. Dostupný z: https://www.safetica.cz/produkty/safetica-dlp

[6] *ISO/IEC 27001:2013* [online]. 2013 [cit. 2017-05-12]. Dostupný z: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[7] ISO/IEC 27002:2013 [online]. 2013 [cit. 2017-05-12]. Dostupný z: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

[8] Demingův cyklus PDCA [online]. 12/2011 [cit. 2017-05-12]. Dostupný z: https://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm

[9] GDPR aneb (R)evoluce v ochraně osobních údajů? [online]. 7-8/2016 [cit. 2017-05-12]. Dostupný z: https://www.systemonline.cz/it-pravo/gdpr-aneb-r-evoluce-v-ochrane-osobnich-udaju.htm

[10] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016 [online]. 10/2016 [cit. 2017-05-12]. Dostupný z: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-6-rijna-2016/ds-3109/

[11] 2016 Magic Quadrant for Enterprise Data Loss Prevention [online]. 1/2016 [cit. 2017-05-12]. Dostupný z: http://www.gartner.com

[12] 2016 Magic Quadrant for Endpoint Protection Platforms [online]. 2/2016 [cit. 2017-05-12]. Dostupný z: http://www.gartner.com

[13] 2016 Magic Quadrant for Secure Web Gateways [online]. 6/2016 [cit. 2017-05-12]. Dostupný z: http://www.gartner.com

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
DC	Domain Controler
DLP	Data Loss Prevention
DPO	Data Protection Officer
EDM	Exact Data Matching
ICAP	Internet Content Adaptation Protocol
ICT	Information and Communication Technologies
IDM	Identity Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
LAN	Local Area Network
MDM	Mobile device management
NDA	Non-disclosure agreement
OCR	Optical Character Recognition
PCDA	Plan-Do-Check-Act
PoC	Proof of Concept
RMS	Rights Management Services
SaaS	Software as a Service
SIEM	Security Information and Event Management
SPAN	Switched Port Analyzer
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TLS	Transport Layer Security
VML	Vector Machine Learning
WLAN	Wireless Local Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK