Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Implementace DLP (Data Loss Prevention) řešení ve firmě

Veronika Jiráčková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Veronika Jiráčková, DiS.

Informatika

Název práce

Implementace DLP (Data Loss Prevention) řešení ve firmě

Název anglicky

DLP (Data Loss Prevention) implementation in the company

Cíle práce

Cílem této bakalářské práce je zhodnotit dopad implementace bezpečnostního systému DLP (Data Loss Prevention) ve vybraném podniku, s důrazem na funkční i ekonomické důsledky, zjištěné nevýhody a slabá místa DLP řešení. Na základě analýzy dat získaných z informačních systémů podniku a dat poskytnutých zainteresovanými osobami bude zhotoveno srovnání očekávaných a skutečných důsledků.

Metodika

Bakalářská práce bude založena na kombinovaném výzkumu, tj. kvalitativních i kvantitativních metodách. Data budou získávána a) skrze polostrukturované interview s klíčovými osobami, obzvlášť informace o očekávaném přínosu v době implementace a osobních zkušenostech s prací s DLP řešením, b) z informačních systémů vybraného podniku. Dále se s informacemi bude pracovat pomocí statistické metody výzkumu, především deskriptivní a klasifikační.

Doporučený rozsah práce

35-45s.

Klíčová slova

DLP, Data Loss Prevention, ochrana dat, únik dat, data leakage, informační bezpečnost, klasifikace dat, prevence úniku dat, osobní data, GDPR

Doporučené zdroje informací

Arbel, L. (2015). Data loss prevention: the business case. Computer Fraud & Security, 2015(5), 13–16. https://doi.org/10.1016/s1361-3723(15)30037-3

Blokdyk, G. (2020). Data Loss Prevention a Complete Guide – 2020 Edition.

Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market Price Effects of Data Security Breaches. Information Security Journal: A Global Perspective, 20(6), 263–273. https://doi.org/10.1080/19393555.2011.611860

Romansky, Radi. (2022). Digital Age and Personal Data Protection.

Securosis, L.L.C. (2017). Understanding and Selecting a Data Loss Prevention Solution. Dostupné z https://securosis.com/

Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016(6), 5–8. https://doi.org/10.1016/s1353-4858(16)30056-3

Vacca, J. (Ed.). (2017). Computer and Information Security Handbook. Morgan Kaufmann.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 9. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 28. 01. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Implementace DLP (Data Loss Prevention) řešení ve firmě" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 14. 3. 2024 _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Martinu Havránkovi, Ph.D., za odborný dohled a vedení mé bakalářské práce. Zároveň bych také chtěla poděkovat zkoumanému podniku a jeho zaměstnancům za pomoc a ochotu při sběru dat.

Implementace DLP (Data Loss Prevention) řešení ve firmě

Abstrakt

Bakalářská práce se zabývá problematikou ochrany podnikových aktiv pomocí DLP (Data Loss Prevention) systému. Hlavním cílem je zhodnocení dopadu již proběhlé implementace bezpečnostního systému DLP ve vybraném podniku a posouzení, zda systém naplňuje očekávání.

Teoretická část vychází z literární rešerše aktuálně dostupných odborných zdrojů. Věnuje se základním informacím o technologii DLP systémů a doporučeným postupům při implementaci řešení. Zároveň jsou popsány i zdroje rizik v oblasti ochrany citlivých údajů, jaké mohou být následky úniku těchto dat a jak jsou DLP systémy spojené s ochranou soukromí.

V hlavní části práce je představen zkoumaný podnik a následně je provedena analýza dat získaných z a) polostrukturovaných interview se zainteresovanými osobami, které se podíleli na implementaci a správě DLP systému, b) statistik záchytů DLP systémem. Otázky v interview jsou zařazeny do okruhů spojených s jednotlivými fázemi projektu.

Analýzou bylo zjištěno, že z technologického hlediska systém naplňuje očekávání, ale aby mohl efektivně chránit data, je potřeba mít kvalitně postavené bezpečnostní politiky. Výsledkem práce jsou také hodnocené klíčové aspekty DLP systému vybrané na základě poznatků od respondentů.

Klíčová slova: DLP, Data Loss Prevention, ochrana dat, únik dat, data leakage, informační bezpečnost, klasifikace dat, prevence úniku dat, osobní údaje, GDPR

DLP (Data Loss Prevention) implementation in the company

Abstract

The bachelor thesis deals with the issue of corporate assets protection using DLP (Data Loss Prevention) system. The main objective is to evaluate the impact of the previously implemented DLP security system in the selected company and to determine whether the system meets expectations.

The theoretical part is based on literary research of currently available academic sources. It focuses on basic information about the technology of DLP systems and recommended practices for DLP solutions implementation. It also describes the sources of risks in the area of sensitive data protection, what the consequences of data leakage can be and how are DLP systems connected to privacy protection.

In the main part of the thesis, the researched company is introduced followed by an analysis of data obtained from a) semi-structured interviews with people involved in the implementation and management of the DLP system, b) statistics of interceptions by the DLP system. The interview questions are placed into categories associated with the different phases of the project.

Based on the analysis, it was found that from a technological point of view the system meets the company's expectations, but in order to protect data effectively, it is necessary to have well-constructed security policies. The results of the work also include the evaluated key aspects of the DLP system based on the findings from the respondents.

Keywords: DLP, Data Loss Prevention, data protection, data leakage, information security, data classification, data leakage prevention, personal data, GDPR

Obsah

1 Úvod

Informační a komunikační technologie hrají klíčovou roli v moderním světě, kde se obrovské množství citlivých a důvěrných dat pohybuje skrze sítě a připojená digitální zařízení. S tím souvisí vzrůstající obavy o bezpečnost dat a nutnost prevence úniku informací. Systémy určené k prevenci úniku dat se nazývají Data Loss Prevention, případně Data Leak Prevention, a v dnešní době jsou nezbytným nástrojem pro organizace, které si uvědomují hodnotu svých informačních aktiv.

DLP systémy monitorují, kontrolují a řídí tok dat v podniku a identifikují potenciálně rizikové aktivity. Tato technologie minimalizuje riziko úniku citlivých informací a zároveň také napomáhá organizacím zůstat v souladu s regulačními požadavky a standardy týkající se ochrany dat.

V DLP systémech se využívá široká škála metod k zajištění bezpečnosti dat, včetně sledování pohybu dat v síti i na koncových stanicích, detekce škodlivého softwaru, šifrování dat a správy přístupů. V kontextu stále se zvyšujících kybernetických hrozeb a obav o bezpečnost informací se DLP systémy stávají nedílnou součástí strategie informační bezpečnosti pro podniky v různých odvětvích.

Implementace DLP řešení je pro podniky obvykle náročným úkolem. Součástí IT infrastruktury jsou různorodá zařízení od mobilních telefonů až po serverová úložiště a je potřeba zajistit, aby byl DLP systém schopný efektivně pracovat s různými platformami a formáty dat. Tato práce se zabývá zpětným zhodnocením proběhlé implementace v konkrétním podniku a pokouší se poskytnout praktický pohled na skutečné využití DLP technologie při ochraně podnikových dat.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je zhodnocení dopadu implementace bezpečnostního systému DLP (Data Loss Prevention) ve vybraném podniku a posouzení, zda systém naplňuje očekávání. Dílčími cíli je zmapování procesu již dokončené implementace, identifikace nevýhod a slabých stránek DLP řešení a určení klíčových aspektů DLP na základě poznatků od odborníků z praxe.

2.2 Metodika

V první části práce bude provedena literární rešerše odborné literatury týkající se technologie DLP a ochrany podnikových dat. Součástí bude základní terminologie a rozdělení DLP systémů a doporučené postupy při integraci DLP řešení do existující infrastruktury podniku. Zároveň se teoretická část práce zaměří na klasifikaci rizik v oblasti ochrany citlivých dat, následky úniku těchto dat a problematiku DLP systémů v kontextu ochrany soukromí a osobních údajů.

Na základě poznatků z literární rešerše bude pro praktickou část práce sestaven seznam otázek, který bude složit jako podklad k polostrukturovanému interview. Respondenti, kteří se budou interview účastnit, budou vybráni ze zaměstnanců zkoumaného podniku na základě jejich znalostí a praktických zkušeností s implementací a správou DLP systému.

Data získaná od respondentů budou zpracována pomocí kvalitativní obsahové analýzy se zaměřením na hledání klíčových aspektů a souvislostí napříč tématy. Kvalitativní data budou doplněna údaji ze statistik záchytů poskytnutých podnikem.

V závěrečné části práce budou shrnuty klíčové aspekty daného DLP systému ohodnocené respondenty z hlediska plnění očekávání a bude zhodnocena efektivita systému.

3 Teoretická východiska

3.1 Technologie DLP

Systémy navržené k identifikaci citlivých dat a jejich ochraně před únikem zevnitř firemního systému se poprvé objevily v roce 2006. (Ghorbanian et al. 2015). Obvykle se objevují pod názvy Data Loss Prevention (Ochrana před ztrátou dat) nebo Data Leak Prevention (Ochrana před únikem dat). Jejich hlavním účelem je detekovat a zabránit neoprávněnému nakládání s citlivými údaji v síti, koncových zařízeních a uložištích. Nejčastěji se využívají v korporátním prostředí, kde je kriticky důležité zajistit bezpečnost a integritu dat. Na základě poznatků získaných ze zachycených incidentů může organizace zavést preventivní opatření skrze upřesnění bezpečnostních politik DLP, tak aby se předešlo budoucímu výskytu podobných incidentů. (Faiz et al. 2020)

3.1.1 Typy DLP podle koncepčního přístupu

- **Network DLP** – Monitoruje datové toky a komunikaci ve firemní síti. Na základě definovaných bezpečnostních politik analyzuje data v síťové infrastruktuře a umožňuje blokovat nebo šifrovat citlivé informace na úrovni transportní vrstvy. Aplikovaný je například na e-mailovou komunikaci, webovou komunikaci a proxy servery. Pro zajištění komplexní ochrany síťového prostředí je často integrován společně s dalšími bezpečnostními nástroji jako je firewall a systémy pro detekci a prevenci průniku (IDS/IPS).

- **Endpoint DLP –** Monitoruje data, která jsou uložena nebo přenášena na firemních koncových zařízení, tj. počítačích, mobilních telefonech, serverech apod. Sleduje aktivity uživatelů na koncových zařízeních, přesněji jejich interakci s citlivými daty, a asistuje při klasifikaci důvěrných informací. Ve firemním prostředí je často integrován se SIEM nástroji, které umožňují centralizované sledování a analýzu bezpečnostních událostí na koncových zařízeních pro detekci neobvyklých nebo podezřelých aktivit. (Vanderburg 2023)

- **Storage DLP / Cloud DLP** – Storage DLP se zaměřuje na monitorování a ochranu citlivých dat uložených v různých formách úložišť, včetně souborových systémů, databází, datových centrech a dalších lokálních úložišť v organizaci. Cloud DLP systém může být integrován s cloudovými úložišti, jako jsou Google Drive, Dropbox nebo Microsoft OneDrive, aby poskytoval ochranu důvěrných informací i v prostředí cloudu. Data jsou před uložením do cloudu oskenována a automaticky se detekují a šifrují citlivé údaje. Tím se vytváří komplexní přehled o všech datech v cloudu. (CrowdStrike 2023)

3.1.2 Typy DLP podle způsobu implementace

- **Agent-based systém** – DLP systémy na bázi agentů využívají speciální software (agenty), který je nainstalován na koncových zařízeních, jako jsou počítače, notebooky nebo mobilní telefony. DLP software pak komunikuje s DLP serverem, který spravuje bezpečnostní politiky.

- **Agentless systém –** Agentless DLP systémy fungují na úrovni sítě nebo úložiště dat a nevyžadují instalaci speciálního softwaru na koncových zařízeních. Každý koncový bod vede svůj síťový provoz skrze jeden nebo více DLP serverů, které ho monitorují a analyzují.

- **Hybridní systém** – Systém je kombinací předchozích dvou typů. Obsahuje agenta v každém koncovém zařízení a zároveň jeden nebo více monitorovacích serverů. (Ghorbanian et al. 2015)

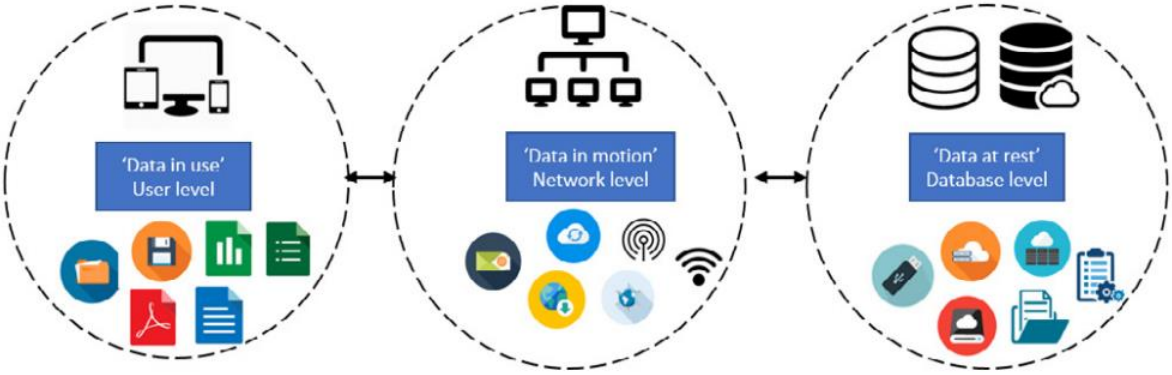
3.1.3 Rozsah ochrany podle typu dat

V kontextu bezpečnosti dat a DLP systémů se často objevují pojmy *data in use, data in motion* a *data at rest,* které popisují různé fáze, v nichž mohou data existovat a cirkulovat v informačním systému. (Stolfo et al. 2008)

- **Data in use –** Jedná se o data právě využívaná uživatelem skrze koncové zařízení ve formě textu, dokumentů a aplikací. Mezi činnosti monitorované DLP systémem může patřit komunikace dovnitř a ven, operace kopírování a přenosu dat, tisk nebo snímání obrazovky.

- **Data in motion** – Tranzitní data se pohybují v počítačové síti mezi jednotlivými uzly. Podstatným faktorem je, zda se jedná o přenos dat ve veřejné síti, privátní síti nebo v místním zařízení (Local device).

- **Data at rest** – Myšleny jsou data trvale umístěné v uložištích jako jsou pevné disky, databáze, souborové servery apod. Tento stav je považován za bezpečnější než ostatní, jelikož data obvykle neopouštějí kontrolované prostředí a DLP systémy je mohou proaktivně monitorovat. (Faiz et al. 2020)



Obrázek 1 - Různé oblasti působnosti systémů DLP
Zdroj: (Faiz et al. 2020)

3.1.4 **Metody detekce**

DLP systémy obvykle používají více typů detekčních metod, aby byla pokryta co největší oblast rizik. Kontextová metoda detekce je založená na analýze kontextuálních informací jako je velikost, zdroj, cíl, odesílatel nebo příjemce monitorovaných dat. Oproti tomu se obsahová metoda detekce soustředí na vlastní obsah dat. K tomu se využívá řada specializovaných technik, příkladem může být komparace řetězců a vzorců, vyhledávání regulárních výrazů a textová analýza. Základem pro detekční metody je také tagování (značkování) obsahu, které přiřazuje specifické značky citlivým datům. (Costante et al. 2016)

3.1.5 **Klasifikace dat**

Kvalitně zpracovaná data jsou důležitým předpokladem pro úspěšnou práci s DLP systémem. V podniku se data klasifikují do kategorií podle jejich vlastností a především jejich hodnoty. Podle přidělené klasifikace se pak u aktiv ve formě dat stanovuje priorita jejich ochrany, tj. jak moc zdrojů je potřeba přidělit na jejich ochranu. (Poyilan 2023) Základními principy klasifikace obvykle jsou:

1) **Identifikace kategorií dat** – Data je potřeba nejprve roztřídit do smysluplných kategorií. Může se jednat o data zákaznická, finanční, projektová data apod.

2) **Přiřazení klasifikačních značek** – Klasifikační značky se kategoriím přidělují podle jejich citlivosti. Mezi nejčastěji používané značky patří „Veřejné“ „Interní“ a „Důvěrné“ nebo „Chráněné“.

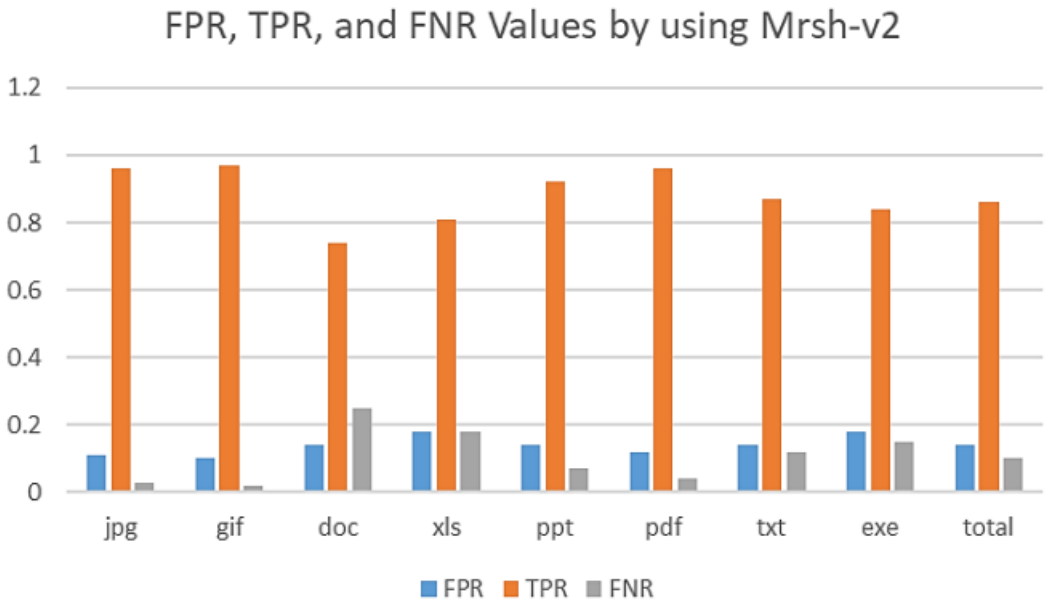
3) **Implementace kontroly přístupů** – K určitým datům by měly mít přístup jen oprávněné osoby. Aby nedocházelo ke zneužívání citlivých dat, je potřeba mít nastavený kontrolní proces pro všechny evidované přístupy.

4) **Pravidelné kontroly a aktualizace klasifikace** – Kontroly klasifikací by neměly probíhat, jen když se objeví nový typ dat nebo přístupů. Aby data byla trvale chráněná, musí se klasifikace pravidelně kontrolovat a aktualizovat.

3.1.6 False positive záchyty

V kontextu DLP systémů je pojmem false positive myšlena taková detekce, která se v systému zachytila jako zakázaná aktivita, přestože se jedná o povolenou činnost. Protože jsou DLP řešení závislá na parametrech z bezpečnostních politik, často se potýkají s velkým množstvím false positive záchytů. (Faiz et al. 2020) Každý incident má ale jiné charakteristiky, které je potřeba rozklíčovat expertem za danou oblast. To poté omezuje kapacitu na šetření skutečných upozornění na potencionální únik dat a vystavuje společnost zbytečnému riziku.

Minimalizaci počtu false positive záchytů se věnuje mnoho studií, které se experimentací s novými metodami detekce snaží zlepšit detekční schopnosti DLP systémů. Mezi testovanými metodami lze nalézt koncept metaskóre, který využívá agregovaný výstup z DLP systémů k detekování a označení chování, které by mohlo indikovat únik dat. (Kongsgård et al. 2017) Další možností je nová metoda strojového učení k posílení funkcí detekce ztráty dat v systému DLP a zvýšení efektivity predikce ztráty dat. (Faiz et al. 2020). Jinou metodou je i specifický typ aproximační shody Mrsh-v2, kde výzkum prokázal, že generuje velký počet true positive záchytů, a naopak malý počet false negative a false positive záchytů. (Ali et al. 2020)



Graf 1 - Výsledky měření záchytů v DLP metodou Mrsh-v2 u různých typů souborů. Vysvětlivky: False Positive Rate (FPR), True Positive Rate (TPR), False Negative Rate (FNR)

Zdroj: (Ali et al. 2020)

3.2 Implementace DLP systémů

Na základě posouzení expertů v kyberbezpečnosti bylo identifikováno sedm problematických oblastí při implementaci DLP systémů. Aby mohlo DLP řešení efektivně plnit svůj účel, je vhodné tyto faktory zvážit. (Waziri et al. 2016)

A. **Únikové kanály** – Pro výměnu informací mezi uživatelem a médii existuje stále větší množství zprostředkujících kanálů. S jejich neustálým vývojem je obtížné zajistit jejich zabezpečení a je potřeba kombinovat vícero technologií pro kompletní ochranu. Implementovaný DLP systém by měl být schopen filtrovat provoz na těchto kanálech, aniž by narušoval jejich komunikaci.

B. **Lidský faktor** – Nejvíce nepředvídatelným aspektem výměny informací je obvykle člověk**.** Jeho chování je založeno na mnoha psychologických a sociologických faktorech a nelze vždy stoprocentně odhadnout, jak se zachová v různých situacích. DLP systém dokáže zamezit některým lidským chybám nebo úmyslným útokům, ale je nutné počítat s tím, že se vždy najde někdo, kdo bude schopný překonat všechna bezpečnostní opatření.

C. **Přístupová práva** – Rozdělování rolí, a k nim příslušných přístupových oprávnění, je klíčovým aspektem většiny systémů, včetně DLP řešeních. Důležité je ale také udržovat tato oprávnění aktuální, protože zastaralé přístupové právo může být zdrojem rizika pro celý systém.

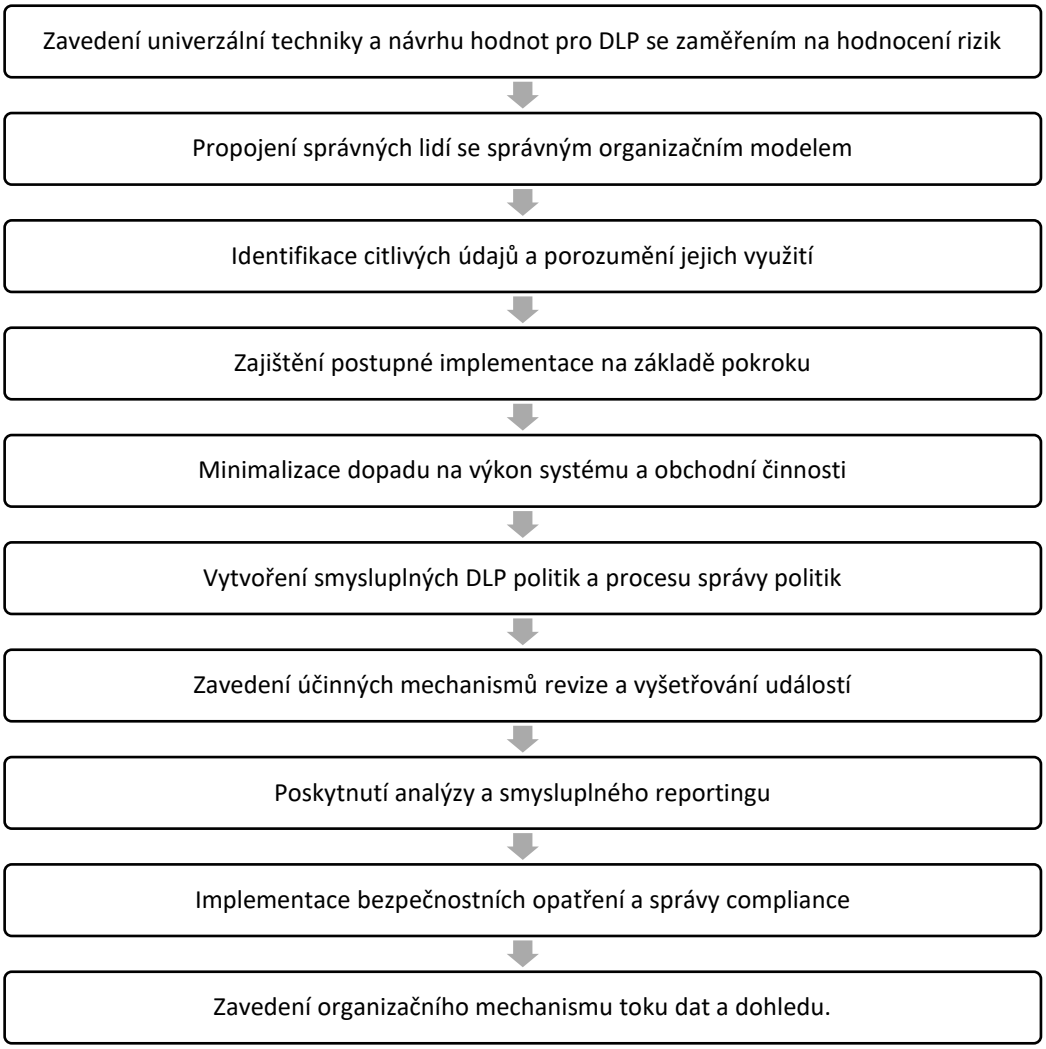
D. **Šifrování a steganografie** – Pro některé DLP systémy může být problémem šifrování chráněných dat. Obsahově zaměřené DLP řešení nahlíží do datového obsahu a analyzuje ho na základě nastavených bezpečnostních politik. Pokud je ale obsah zašifrován takovým způsobem, který znemožňuje DLP systému ho analyzovat, vzniká riziko úniku dat. Podobným případem je i steganografie, kdy uživatel může chráněná data ukrýt v jiných médiích, která nedokáže DLP analyzovat. (Zou a Chen 2023)

E. **Modifikace dat** – Některé DLP systémy využívají metody komparace původních dat s kontrolovanými daty. Tímto způsobem se hledají datové stopy a vzory, které má DLP detekovat. Data ale mohou být modifikovaná prostředky dostupnými v koncovém zařízení a na internetu, a tím vzniká šance, že DLP nebude schopné data zachytit.

F. **Škálování a integrace** – Před implementací DLP je nutné brát v potaz jeho aspekty jako výpočetní schopnosti a techniky analýzy. Množství dat, které se navíc obvykle s časem stále zvětšuje, může mít vliv na výkon systému a způsobovat opožděnou odpověď. Stejně tak je nutné myslet na to, že DLP je integrováno společně s jinými bezpečnostními mechanismy, a některé funkce proto mohou být redundantní.

G. **Klasifikace důvěrnosti dat** – Klasifikace důvěrnosti dat znamená dělení dat do několika úrovní a hlavním účelem je stanovení základní úrovně bezpečnostních kontrol, které mají být použity pro ochranu těchto dat. Problémem je, že tato klasifikace je často v rukách osob, které nemají dostatek znalostí na správné určení stupně důvěrnosti. To výrazně snižuje efektivitu DLP systémů.

Ve studii *Data Loss Prevention and Challenges Faced in their Deployments* je doporučen následující postup při implementaci DLP systému.



Obrázek 2 - Postup implementace DLP systému
Zdroj: Vlastní zpracování dle (Waziri et al. 2016)

3.3 Zdroje rizik

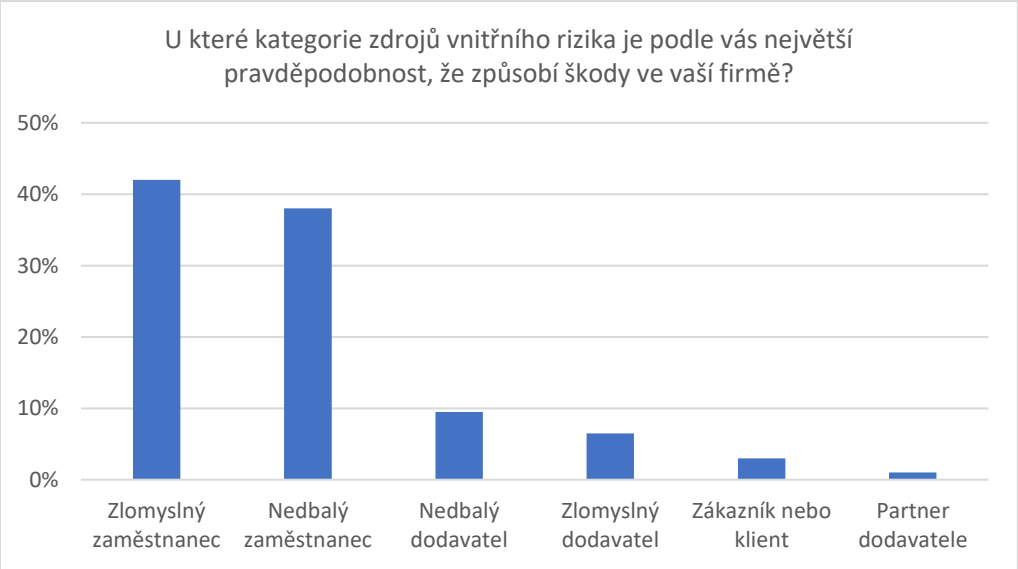
Při zabezpečení citlivých dat ve firmách je často kladen důraz na externí zdroje rizik – hackery, ransomware, sociální inženýrství i fyzické hrozby (krádeže koncových zařízení a poškození infrastruktury). Firmy využívají široké spektrum prostředků k ochraně svých

aktiv před útočníky z vnějšku, podle výzkumu SANS institutu z roku 2017 jsou ale největším zdrojem škod ve společnostech vnitřní hrozby. (Cole 2017)

Hrozba zevnitř může být definována jako kombinace technických, behaviorálních a organizačních problémů. Vnitřní hrozby, které jsou založené na lidském jednání, bývají zesílené psychologickým rozpoložením pověřených osob, a je proto nutné činnost lidí uvnitř podniku monitorovat, aby nedošlo k úniku dat. (De Sousa a Shahzad 2021) K tomu jsou navrženy právě DLP systémy, jejichž hlavním účelem je detekce, monitorování a řízení toku dat v rámci informačních systémů organizací.

Vnitřní hrozby lze rozdělit následujícím způsobem:

- Neúmyslný únik dat
- Záměrné vynesení dat



Graf 2 - Potencionální zdroje škod ve firmě podle názorů dotázaných zaměstnanců
Zdroj: Vlastní zpracování dle (Cole 2017)

3.3.1 Neúmyslný únik dat

Neúmyslnou ztrátou dat způsobenou zevnitř se myslí únik na základě lidské chyby bez úmyslu způsobit škody. Taková chyba může vzniknout neopatrností, nešikovností, ignorováním bezpečnostních opatření ale i nedostatečným proškolením zaměstnance.

I když většina zaměstnanců společnosti obvykle rozumí důležitosti základních bezpečnostních opatření, mohou mít problém s pochopením jejich dílčích částí. Některé bezpečnostní mechanismy mohou být chápány jako nedostatek důvěry ze strany zaměstnavatele. Kvůli nedostatečným technickým a případně i právním znalostem zaměstnanců se některá pravidla také mohou zdát přehnaná nebo přímo zbytečná.

V jiných případech používané bezpečnostní mechanismy mohou nějakým způsobem omezovat pracovní činnost zaměstnanců a zvyšovat časovou náročnost úkolů. To vede k frustraci a některé zaměstnance to může vést až k pokusům bezpečností opatření obcházet. (Bertrand et al. 2020)

Typickým příkladem neúmyslného úniku dat je odeslání e-mailu s citlivými daty nesprávnému příjemci. (Faiz et al. 2020) Pokud se jednalo o další interní osobu v rámci korporátní sítě, existuje ještě možnost data zachránit, ale data odeslaná mimo šifrované prostředí společnosti jsou považovaná za ztracená.

3.3.2 **Záměrné vynesení dat**

Záměrné vynesení dat se děje s plným vědomím koncového uživatele. Zaměstnanec si je vědom, že s údaji nenakládá v souladu s interními předpisy, případně i porušuje zákon. Důvodem může být snaha obohatit se prodáním vynesených dat nebo přímo způsobit újmu firmě. (Bertrand et al. 2020)

V knize *Insider attack and cybersecurity* byl vznesen zajímavý dotaz, a to: Pokud interní osoby vědí, že je jejich činnost monitorována, je více pravděpodobné, že se nebudou pokoušet o neoprávněné aktivity? (Stolfo et al. 2008, str. 13) V oblasti kyberbezpečnosti k tomu momentálně neexistují odborná data, ale autoři knihy se odkazují na způsoby monitoringu v maloobchodech, které mají bránit krádežím zboží zaměstnanci.

V případech úmyslného vynesení dat se také často hovoří o fenoménu „malicious insider“, tedy zlomyslného insidera. V roce 2021 byla provedena studie zahrnující 79 poskytovatelů cloudových služeb sídlících v Austrálii a Novém Zélandu, jejíž cílem bylo zjistit, do jaké míry jsou společnosti připraveny na záměrnou snahu vypustit nebo ukrást data osobou zevnitř firmy. (De Sousa a Shahzad 2021) V této studii je „malicious insider“ popsán jako současný nebo bývalý zaměstnanec, obchodní partner, dodavatel nebo dokonce zákazník.

U otázky bezpečnosti cloudových prostředí hraje roli i fakt, že odpovědnost za ochranu dat je rozdělena mezi poskytovatele služby a firmu, jež služby využívá. Poskytovatel zaručuje dostatečně silné zabezpečení infrastruktury cloudu, zatímco vlastník dat nastavuje přístupová práva a další interní bezpečnostní procedury. Tímto způsobem však firma ztrácí částečně kontrolu nad tím, kdo má k jejím datům přístup. Třetí osoby, jako například IT zaměstnanci poskytovatele, jsou z podstaty své práce schopni k cizím datům přistupovat.

Studie společnosti IBM poukázala na skutečnost, že ke konci roku 2020 bylo více než 20 miliard zařízení IoT (Internet of Things) připojeno k nějakému cloudovému systému. Zároveň bylo ale také zjištěno, že hlavním rizikem jsou právě vnitřní hrozby, které jsou zodpovědné za 60 % všech dosavadních útoků na zařízení IoT. (Khan et al. 2020)

3.4 **Následky úniku dat**

Podnikové informační a komunikační systémy jsou čím dál tím více závislé na digitálních technologiích a datech v nich zpracovávaných. Proto je na prvním místě ve sféře kyberbezpečnosti zachování dostupnosti, důvěrnosti a integrity těchto dat. (Kuipers a Schonheit 2021)

Úniky dat mohou mít dopad na soukromé osoby a podniky, kterým hrozí finanční újma a újma na pověsti v důsledku ztráty dat. Ve většině případů společnost odpovědná za ztrátu

utrpí značnou finanční škodu. (Markos et al. 2023) Kromě ekonomických dopadů mohou vést úniky dat také k:

- poškození goodwill společnosti,
- poškození reputace a dobrých obchodních vztahů,
- vyzrazení obchodního tajemství a
- ztrátě duševního vlastnictví.

3.4.1 Ekonomické následky

Vyčíslení finančních ztrát následkem úniku dat není jednoduchou záležitostí, protože ztráty zpravidla nejsou viditelné ihned po incidentu. Počítat je třeba s přímými a odhadovanými právními náklady, dopady na budoucí zisky a náklady na zákaznickou podporu, pokud se uniklá data týkala zákazníků firmy. Komparativní studie *Data Breaches and Efective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises* dělí náklady spojené s únikem dat na přímé a nepřímé. Mezi přímé patří především: přerušení a obnova provozu, soudní řízení a regulační poplatky, forenzní vyšetřování a monitorování bankovních údajů zákazníků. V nepřímých lze nalézt: škodu na pověsti firmy a ztrátu důvěry spotřebitelů, která z dlouhodobého pohledu změní jednorázový kybernetický incident na podnikovou reputační krizi. (Kuipers a Schonheit 2021) V tabulce 1 níže jsou uvedeny společnosti, u kterých došlo k úniku dat, a náklady spojené s řešením incidentu.

	Společnost	***Rok***	***Dotčení uživatelé***	***Odhadované náklady***
1.	Epsilon	2011	250 milionů	~ 90,2 miliard CZK
2.	Equifax	2019	147 milionů	~ 31,5 miliard CZK
3.	Veteran’s Affairs	2006	26,5 milionů	~ 11,2 miliard CZK
4.	Yahoo	2016	500 milionů	~ 10,6 miliard CZK
5.	Target	2013	70 milionů	~ 6,7 miliard CZK
6.	TJX	2007	45,7 milionů	~ 5,7 miliard CZK
7.	Hannaford Bros	2007	4,2 milionů	~ 5,6 miliard CZK
8.	Sony	2011	77 milionů	~ 3,8 miliard CZK
9.	Uber	2016	57 milionů	~ 3,1 miliard CZK

Tabulka 1 - Úniky dat s nejvyššími odhadovanými náklady k roku 2023
Zdroj: Vlastní zpracování dle (Stewart 2023)

Průměrná konečná cena nákladů se, alespoň podle nedávných výzkumů, může pohybovat mezi $18,120 až $35,730 u úniku malého rozsahu dat a mezi $5 miliony až $15,6 miliony u úniku s velkým rozsahem. (Rock a Rock 2024) Důležité je ale pamatovat na

mnoho faktorů, které mohou ovlivnit výši této částky. Závisí na velikosti podniku, v jaké oblasti podniká a o jaký typ uniklých údajů se jednalo.

Nejrozšířenější metoda měření ekonomických důsledků nežádoucích incidentů je analýza vycházející z fluktuace tržní hodnoty akcií dané společnosti ve vztahu k celkovému vývoji trhu. V časových bodech před a po incidentu se sledují hodnoty akcií a celkových příjmů a pozoruje se trend kolísání jejich hodnot. (Kuipers a Schonheit 2021)

V roce 2020 proběhla studie *Financial Loss due to a Data Privacy Breach: An Empirical Analysis*, v rámci které se analyzovaly informace ze 131 případů narušení ochrany osobních údajů v podnicích mezi lety 2012 až 2014. Ve výzkumu byl zdůrazňován rozdíl mezi narušením v oblasti kybernetické bezpečnosti a v oblasti ochrany osobních údajů, dvě instance, které jsou často považované za totožnou záležitost. Zajímavým poznatkem studie bylo, že tržní hodnota menších firem je narušením ochrany obvykle ovlivněna více než tržní hodnota velkých podniků. (Tripathi a Mukhopadhyay 2020)

Otázkou reakce akciového trhu na kybernetické útoky se zabývala studie *Time-varying effects of cyberattacks on firm value*. Výsledkem bylo zjištění, že na okamžité ztráty z přerušení provozu businessu následkem kybernetického útoku reagují investoři více negativně než na jiné, ne tolik přímé ztráty. Důležitým zjištěním ale bylo i to, že negativní reakce je také silnější, pokud ke ztrátě dat došlo skrze zaměstnance společnosti. (McShane a Nguyen 2020)

3.4.2 **Obchodní tajemství**

Obchodní tajemství podle ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, „*tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení.“* Obchodní tajemství je nehmotnou movitou věcí ve vlastnictví společnosti a status obchodního tajemství ji přiděluje přímo sám podnik.

- **Konkurenčně významné –** Informace musí jejich vlastníkovi poskytovat konkurenční výhody vůči ostatním podnikatelům v daných obchodních kruzích.

- **Určitelné** – Obchodní tajemství jsou údaje v téměř jakékoliv formě, například výrobní postupy, smlouvy nebo její části, marketingové analýzy, podnikové strategie, počítačový software nebo i databáze. Důležité je, že tyto informace lze objektivně definovat a nejsou jen obecným pojmem.

- **Ocenitelné –** Informace musí být možné ohodnotit finanční částkou a jejich ztráta by měla mít dopad na hospodářský výsledek podniku.

- **Běžně nedostupné v příslušných obchodních kruzích –** K informaci má přístup pouze omezený a přesně definovaný okruh subjektů. Zpravidla to bývá

podnik, který informaci vlastní, ale může jít i o sdílenou informacemi mezi podnikem a jejím dodavatelem.

- **Související se závodem –** Informace se může týkat jakéhokoliv firemního procesu, platí pouze, že musí souviset s obchodním závodem, který informaci vlastní.

- **Adekvátně chráněné –** V občanském zákoníku nejsou uvedena konkrétní pravidla ochrany obchodního tajemství, záleží vždy na daném podniku, jakým způsobem nastaví bezpečnostní pravidla pro ochranu obchodního tajemství. Nicméně, pravidla musí odpovídat skutečnosti, že se jedná o hodnotné informace.

Aby informace mohla nabýt statusu obchodního tajemství, musí plnit všechny výše popsané znaky. Pokud některý ze znaků přestane být platným, zaniká i status obchodního tajemství.

The US Chamber of Commerce uvádí, že obchodní tajemství může tvořit až 80 % hodnoty informačního portfolia společnosti. (Bradley et al. 2023) Vzhledem k tomu, že obchodní tajemství ze své podstaty staví podnik na výhodnější pozici, než je jeho konkurence, je vystaveno neustále hrozbě vyzrazení. Když pomineme možné pokusy konkurence o špionáž a krádež obchodního tajemství, je druhou největší hrozbou právě již popsaný „insider“, tedy zaměstnanec nebo dodavatel, který má k datům oprávněný přístup. (De Sousa a Shahzad 2021) Motivací k odcizení dat v tomto typu situace může touha zaměstnance pomstít se podniku jako odplata za nějakou křivdu, kterou vůči firmě pociťuje. Obchodní tajemství je obzvlášť ohrožené zneužitím, a je proto v nejlepším zájmu podniku ho patřičně ochránit před hrozbami externími i interními.

3.4.3 Škody na reputaci podniku

Goodwill podniku je celková pozitivní pověst a vnímání společnosti ze strany zákazníků, obchodních partnerů a veřejnosti. Když se citlivá data, obzvlášť ty týkající se zákazníků, dostanou do neoprávněných rukou, může to vyvolat obavy o ochranu soukromí, bezpečnost a důvěryhodnost podniku. Ztráta důvěry zákazníků pak může vést k zhoršení obchodních vztahů, ztrátě klientů a tím i snížení příjmu. Podnik také obvykle čelí právním a regulačním důsledkům, což může dále zhoršit jeho pověst.

Velkou roli hraje také způsob, jak společnost na únik dat reaguje. Obecně platí, že na transparentní a komunikativní přístup při řešení následných škod bude veřejnost reagovat pozitivněji než na pokusy o vyhýbání se zodpovědnosti.

Krizová reakce by měla začínat „základní odezvou“, tedy instrukčními a korekčními informacemi. (Kuipers a Schonheit 2021) Instrukční informace slouží k ochraně zúčastněných stran před hmotným poškozením a dalšími škodami vyvolanými krizí. Korekční informace poukazují na to, co podnik dělá, aby zabránil opakování incidentu. Zároveň poskytují veřejnosti informace o nápravných opatřeních a předávají zprávy o zájmu

podniku o postihnuté strany. Jak korekční, tak instrukční informací signalizují, že společnost dává bezpečnost veřejnosti na první místo a nejsou jí lhostejné oběti krize. (Park 2017)

Porušení ochrany osobních údajů představuje porušení společenské smlouvy; jakmile je smlouva porušena, musí se spotřebitelé rozhodnout, zda podniknou kroky k nápravě porušení ochrany osobních údajů či nikoli, a poté se rozhodnout, zda budou nadále obchodovat (tj. nakupovat nebo využívat služby) se společností, která porušila společenskou smlouvu. (Markos et al. 2023)

K posouzení, jak silně byla poškozena pověst společnosti, lze použít metodu, která se používá k obecnému výzkumu reputace firmy. (Kuipers a Schonheit 2021) Hlavní složkou je sledování mediálního pokrytí, tj. mediálních zpráv o zkoumané společnosti, a přiřazování indexu reputace. Zprávy jsou kódovány na základě kvantifikace a analýzy výroků, které buď zvyšují nebo snižují úroveň připisované odpovědnosti, závažnosti incidentu a dosavadního hospodářského výkonu firmy. Index reputace pak přiřazuje firmě skóre mezi -100 až 100, kdy první hodnota značí pouze negativní zprávy v médiích a druhá hodnota pouze pozitivní. K výpočtu se použije následující rovnice:

$$\frac{Pozitivní\ média - negativní\ média}{Všechna\ média} \times 100$$

3.5 **GDPR**

S narušením ochrany osobních údajů ale souvisí i následné sankce udělené na základě legislativních nařízení v dané zemi. V roce 2018 v zemích Evropské unie nabylo účinnosti Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů, známé také jako Obecné nařízení o ochraně údajů (GDPR). Do českého právního řádu bylo adaptováno zákonem č. 110/2019 Sb., o zpracování osobních údajů (ZZOÚ). (ÚOOÚ 2024)

Nařízení nahradilo doposud platnou Směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Přestože byl na této směrnici postaven právní základ pro ochranu osobních údajů v EU, její vymáhání a právní úpravy napříč jednotlivými členskými státy bylo velmi nejednotné a nedostávalo se mu takové vážnosti, jako mělo. Jukka Ruohonen ji v práci *The GDPR enforcement fines at glance* dokonce nazvala „papírovým tygrem“, tedy něčím, co se snaží vypadat mocně a hrozivě, ale ve skutečnosti je neschopné a neúčinné. (Ruohonen a Hjerppe 2022)

GDPR bylo odpovědí jak na nejednotnost v ochraně osobních údajů, tak i na neustále vzrůstající využívání nových technologií, jako jsou cloudové služby a čipové karty. (Mike 2022) Tyto technologie zpracovávají stále větší množství osobních údajů, které se v dnešní době staly žádanou komoditou.

3.5.1 **Osobní údaje**

Podle čl. 4 odst. 1 obecného nařízení jsou osobními údaji veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby. Osobu lze identifikovat přímým či nepřímým způsobem, buď na základě jednoznačného identifikátoru jako je například rodné číslo nebo i možnou kombinací osobních údajů (jméno a příjmení + datum narození + místo narození). GDPR definuje i zvláštní kategorii osobních údajů (Článek 9), kam patří velmi citlivé informace, jako jsou údaje o rasovém a etnickém původu, politické nebo odborové příslušnosti, náboženském vyznání, sexuální orientaci a zdravotním stavu.

3.5.2 **Sankce**

	Společnost	***Rok***	***Stát***	***Udělená pokuta***
1.	Meta	2023	EU	~ 29 bilionů CZK
2.	Amazon	2021	Lucembursko	~ 17, 6 miliard CZK
3.	Meta Platforms Limited (Instagram)	2022	Irsko	~ 9,9 miliard CZK
4.	Meta Platforms Ireland Limited (Facebook & Instagram)	2023	Irsko	~ 9,5 miliard CZK
5.	TikTok Limited	2023	Irsko	~ 8,5 miliard CZK
6.	Meta Platforms Ireland Limited (Facebook)	2022	Irsko	~ 6,5 miliard CZK
7.	WhatsApp	2021	Irsko	~ 5,5 miliard CZK
8.	Google LLC	2021	Francie	~ 2,2 miliard CZK
9.	Google Ireland Ltd.	2021	Irsko	~ 1,4 miliardy CZK
10.	Facebook Ireland Ltd.	2021	Irsko	~ 1,4 miliardy CZK

Tabulka 2 - Nejvyšší GDPR pokuty k roku 2023
Zdroj: Vlastní zpracování dle (Komnenic 2023)

Každý, jakkoliv velký podnik, disponuje množstvím osobních údajů svých zaměstnanců, zaměstnanců dodavatelů nebo klientů či zákazníků. Aby se zabránilo zneužívání těchto dat, mohou určené správní úřady (Úřad pro ochranu osobních údajů v ČR) ukládat sankce za nesplňování podmínek pro ochranu osobních údajů. Pokud dojde k zneužití údajů následkem úniku dat ze společnosti, může být sankciován právě podnik, kterému je zákonem uloženo data v jeho vlastnictví chránit. V některých případech je i samotné uniknutí považováno za nedostatečné dodržování zákonných povinností.

K srpnu 2023 bylo uděleno 1801 pokut ve výši až 1 200 000 000 eur. V České republice se nejvyšší pokuty pohybuji v jednotkách milionů Kč. (ÚOOÚ 2024) Výše pokut se stanovuje na základě mnoha faktorů, které se liší stát od státu, ale obecně mezi ně patří:

- Povaha, závažnost a doba trvání incidentu,
- kategorie osobních údajů, kterých se incident dotkl,
- akce přijaté k nápravě,
- spolupráce s úřadem a
- předchozí porušení ochrany osobních údajů. (Mike 2022)

Vzhledem k tomu, že narůstá nejen počet pokut, ale i jejich výše, zajištění ochrany dat, a tím i osobních údajů, před jejich únikem se stává nezbytnou záležitostí všech firem. Podle článku *Our New Normal Of Remote Work Makes Data Loss Prevention Crucial For GDPR Compliance* je prevence ztráty dat pomocí DLP systémů klíčem k úspěšnému plnění GDPR podmínek.

3.6 DLP systém a ochrana soukromí

Právo na soukromí v České republice zaručuje Listina základních práv a svobod, která je součástí ústavního pořádku ČR. V čl. 10 odst. 3 je uvedeno: „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“

DLP systémy monitorují data patřící společnosti v koncových zařízení uživatelů ve všech fázích jejich existence (data in use, data in motion, data at rest). Protože se ale na zařízeních mohou nacházet i data soukromá, vyvstává otázka, do jaké míry je monitoring dat oprávněný a do jaké míry DLP řešení zasahují do soukromí zaměstnanců. Cílem systémů DLP sice není zaměstnance sledovat, ale bezpečnostní politiky, metody detekce a neustálý dohled DLP systému mohou ovlivňovat pracovní činnost i soukromí uživatelů.

Tímto tématem se zabývala i studie *What Do You Think About Your Company's Leaks? A Survey on End-Users Perception Toward Data Leakage Mechanisms* (2020). Studie přišla s myšlenkou, že příliš komplikované bezpečnostní systémy mohou kompletně odradit běžné zaměstnance (tj. bez specializovaných znalostí systému) od jejich využívání, a zpravidla tedy i dodržování interních předpisů. Řešením by byl takový ochranný systém, který by byl intuitivní, nerušivý a uživatelsky přívětivý. Přínosnými zjištěními studie, které se zúčastnilo 150 osob z různých oblastí a různých podniků, bylo následující:

- Téměř čtvrtina (23,8 %) zúčastněních měla povědomí o existenci bezpečnostních opatřeních v jejich zaměstnání, ale přesto si nebyli jisti, co je a není při práci s citlivými daty povoleno.
- 43,7 % zúčastněných někdy v minulosti omylem porušilo nastavené bezpečnostní opatření.
- 21,2 % zúčastněných porušilo nastavené bezpečnostní opatření úmyslně.
- Při hodnocení rušivosti systémů ochrany před únikem dat 45,3 % zúčastněných (v Tabulce 3 sečtený level 4 a 5) vnímalo systém jako silně narušující jejich práci.

- Pokud by si zúčastnění měli vybrat mezi „větší svobodou, ale menší bezpečnostní“ a „větší bezpečnostní, ale menší svobodou“, 55 % zúčastněných volilo bezpečnost před svobodou.

TABLE 9 | Perceived level of intrusiveness on a scale from 1 to 5 (5 is very intrusive).

Level of intrusiveness	Numbers of participants
1	20/150 (13.3%)
2	25/150 (16.6%)
3	37/150 (24.6%)
4	53/150 (35.3%)
5	15/150 (10%)

Tabulka 3 - Vnímání rušivosti systému ochrany před únikem dat
Zdroj: (Bertrand et al. 2020)

Kritizovaným aspektem DLP řešení je, že osoby s přístupem do systému mají možnost nahlížet na soukromé konverzace zaměstnanců. Zde se na druhou stranu staví argument, že v interních předpisech společnosti bývá zpravidla vymezeno povolené užívání svěřených koncových zařízení a využívání k soukromým činnostem je zakázáno. (Mityushin 2021)

3.6.1 Soukromé údaje zachycené DLP systémem

Není také výjimkou, že se při detekování skrze DLP systémy vyskytnou v záchytech omylem označená soukromá data zaměstnanců, tedy false positive záchyty. Bezpečnostní politiky DLP je třeba aktualizovat tak, aby se takovýchto záchytů objevovalo co nejméně. (Kim et al. 2013)

Studie *Privacy Level Indicating Data Leakage Prevention Systém* (2013) navrhuje několik různých modelů, které mají pomoct s minimalizací výskytu soukromých údajů v záchytech DLP systémů:

- **Model měření úrovně zásahu do soukromí na základě hledání klíčových slov –** Model funguje na jednoduchém principu sčítání výskytů hledaných klíčových výrazů.
- **Statická úroveň zásahu do soukromí (SPVL) –** Model definuje dvě nová měřítka. Prvním je míra aktuálního narušení soukromí a druhým je postoj systému DLP k soukromým údajům.
- **Dynamická úroveň ochrany soukromí (DPVL**) – Přidává k předchozímu modelu další faktor: četnost výskytu soukromého klíčového slova v systému DLP.

4 Vlastní práce

Data použitá v praktické části této studie byla poskytnuta vybraným podnikem a jeho zaměstnanci se svolením manažerů ochrany společnosti. Protože se tato data týkají především bezpečnostních složek podniku, jsou některé informace, včetně jména firmy, jmen respondentů a některých dalších údajů, upraveny nebo zakryty. Úpravy dat nemají vliv na výsledky studie, pouze zaručují zachování bezpečnosti a integrity zkoumaného podniku.

4.1 Představení společnosti

Zkoumaný podnik je dle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), kapitálová akciová společnost podnikající v energetickém sektoru. Svými parametry se řadí mezi velké podniky a je nadnárodní korporací působící v ČR i dalších státech Evropy. Společnost disponuje několika tisíci zaměstnanci a v ČR působí již několik desítek let.

Společnost si je plně vědoma bezpečnostních rizik v oblasti informačních a komunikačních technologií (ICT) a investuje do efektivního systému řízení s cílem zajistit úroveň informační a kybernetické bezpečnosti (IKB) v souladu s platnou legislativou a mezinárodními standardy. Informační aktiva podniku jsou zabezpečena z hlediska jejich důvěrnosti, dostupnosti a integrity. Řízení IKB ve společnosti zahrnuje mimo jiné oblasti:

- Politiky bezpečnosti informací (Information security policies)
- Organizace bezpečnosti informací (Organization of information security)
- Řízení přístupu (Access control)
- Fyzická ochrana a bezpečnost prostředí (Physical and environmental security)
- Bezpečnost komunikací (Communications security)
- Akvizice, vývoj a údržba systémů (System acquisition, development and maintenance)
- Zvládání incidentů bezpečnosti informací (Information security incident management)
- Soulad s požadavky (Compliance)

Bezpečnostních cílů se dosahuje skrze organizační, technické, procesní a personální opatření, které jsou adekvátně zaváděny v souladu s relevantními standardy, normami a legislativními požadavky, mezi které patří například:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

4.2 Specifikace zavedeného DLP systému

Ve společnosti je využíváno DLP řešení od firmy Symantec, které používá dvouúrovňovou detekční architekturu k analýze aktivit na koncových bodech. U tohoto typu architektury je k detekci vyžadován přenos dat a komunikace mezi DLP agentem, tj. softwarem nainstalovaným na koncových zařízeních, a endpoint serverem. Bezpečnostní politiky vyžadující dvouúrovňovou detekci jsou odeslány na endpoint server ke zpracování bez předchozího vyhodnocení v koncovém bodě, kde došlo k záchytu. Tyto metody jsou uvedeny v tabulce níže.

Detekční Metoda	***Podmínka shody***	***Popis***
Exact Data Matching (EDM)	Obsah odpovídá přesným datům z profilu Exact Data Profile (EDP)	EDM dokáže vyhledat strukturované i nestrukturované záznamy, které jsou součástí indexovaného zdroje dat. Používá se k detekci z databází, tabulek, adresářů nebo CSV souborů.
Profiled Directory Group Matching (DGM)	Uživatel nebo příjemce dat je uveden v adresáři v profilu EDP	Pomocí EDM detekuje profilové DGM identity, které se nachází v profilu EDP. Slouží k analýze aktivity v síti nebo správě pohybu dat e-maily.
Synchronized Directory Group Matching (DGM)	Příjemce dat je uveden ve skupině v adresářovém serveru	Synchronizované DGM umožňuje napojení na adresářové servery firmy. Detekce pak probíhá na základě příslušnosti ke skupinám v daném adresáři.
Indexed Document Matching (IDM)	Obsah odpovídá signatuře dokumentu z indexovaného profilu dokumentů	Pracuje s informacemi v nestrukturovaných souborech. Skrze IDM lze monitorovat například textové soubory, PDF a obsah, který z nich byl kopírován.

Tabulka 4 - Dvouúrovňové detekční metody
Zdroj: Vlastní zpracování dle (Broadcom 2024)

4.3 Sběr dat metodou polostrukturovaného interview

V průběhu interview byly respondentům pokládány otázky ohledně implementace a správy DLP systému ve společnosti, kde jsou respondenti zaměstnaní. Předem připravené otázky byly rozdělené do čtyř chronologicky na sebe navazujících okruhů podle aktuálního stavu, kde se implementace nacházela. Citace z rozhovorů jsou uvedeny v uvozovkách a psány kurzívou.

Zkoumané okruhy a otázky probírané v rámci rozhovoru:

A. Podnět a příprava před implementací
- Odkud přišel podnět k zavedení systému?
- Jaký byl proces výběru konkrétního řešení?

B. Průběh implementace
- Jak probíhalo testování systému?
- Jaká byla nejtěžší výzva při integrování řešení do stávajícího prostředí?
- Nastaly nějaké závažné komplikace v průběhu integrace?

C. Výsledky a zhodnocení implementace
- Jak hodnotíte dosažené výsledky po implementaci systému?
- Jak byste popsal/a reakce uživatelů na nový systém?
- Existuje nějaký konkrétní případ, kdy systém efektivně předešel úniku citlivých dat?
- Jaké byly zjištěny nedostatky stávajícího systému?

D. Aktuální stav a budoucnost systému DLP
- Jakým způsobem měříte úspěch DLP implementace ve vašem podniku?
- Jaké nové výzvy nebo příležitosti očekáváte v oblasti datové bezpečnosti?

4.3.1 **Respondenti**

Respondent A	Specialista řízení kybernetické bezpečnosti	Respondent A se přímo účastnil projektu implementace DLP systému ve zkoumaném podniku z pozice člena kybernetické bezpečnosti.
Respondent B	Gestor politiky DLP	Respondent B se podílel na tvorbě bezpečnostní politiky ochrany osobních údajů a nyní je jejím gestorem.
Respondent C	Forenzní auditor DLP	Respondent C pracuje v bezpečnostním dohledu v týmu forenzních auditorů, kteří zpracovávají záchyty z bezpečnostních politik DLP systému.

Tabulka 5 - Detaily respondentů
Zdroj: Vlastní zpracování

4.4 Okruh A. Podnět a příprava před implementací

Rozhovory bylo zjištěno, že projekt implementace systému DLP probíhal v letech 2011 až 2012. Téma DLP se v té době objevovalo často na bezpečnostních konferencích a workshopech, kde poskytovatelé prezentovali svá DLP řešení. *„To, co nás primárně na těch prezentacích zajímalo, nebyl ani tak výrobce, jako spíš co to DLP samotné umí.“*

V podniku byly v tomto období již využívány produkty, například antivirová ochrana, od technologické společnosti Symantec, která byla tehdy dle názoru respondenta A lídrem

v oblasti Data Loss Prevention. *„Zástupce výrobce nám tady představil to řešení, takže víceméně v té době už se to řešení nebo výrobce nevybíralo, ale měli jsme nějakou jasnou představu o tom, co chceme.“*. Projekt implementace DLP řešení byl podnikem nazván Ochrana dat a dokumentů.

4.4.1 Chráněné kanály

Spíše než výběr poskytovatele, je dle respondentů podstatný způsob uchopení počátku projektu. *„Samozřejmě ta první otázka byla, které kanály bychom chtěli chránit. Ten kanál lze víceméně chápat jako nějaký soubor protokolů nebo komunikací, které jsou uvnitř té společnosti anebo jdou z té společnosti ven.“* Na první místo tehdy byla dána ochrana komunikace jdoucí směrem ven a zkoumaly se kanály, které v této souvislosti byly považovány za riziko. Respondent A zdůraznil tyto příklady:

- E-mailový provoz neboli SMTP komunikace
- Webový provoz, tedy HTTP/HTTPS
- Koncové stanice

Koncové stanice, mezi které v tomto případě patří zejména pracovní notebooky a služební telefony, jsou dle respondentů samostatnou kapitolou, jelikož je zde více zpracovávaných protokolů a více analyzovaných informací.

Z hlediska infrastruktury bylo vybráno hybridní řešení, tedy kombinace detekčních serverů ve firemní síti a DLP agentů nainstalovaných na koncových zařízeních zaměstnanců. O správu DLP agentů se pak stará Endpoint Detection Server.

4.4.2 Tvorba bezpečnostních politik

Na jedné straně byla budována infrastruktura systému a na druhé probíhaly přípravy bezpečnostních politik. Projektovému týmu byla poskytnuta pomoc od poradenské firmy, jelikož před samotnou integrací DLP systému bylo třeba nejprve identifikovat a klasifikovat citlivá data. To je obecně doporučovaným postupem i dle výzkumů popsaných v teoretické části této práce (Waziri et al. 2016). *„Ten začátek byl hodně o procesech, o nějakých popisech a tabulkách. Všechny politiky, které jsme tvořili, byly nejprve zpracovány v excelových tabulkách se strukturou.“* Příprava politik na základě informací získaných z rozhovorů probíhala ve třech fázích.

1. Ve spolupráci s vlastníky procesů byly identifikovány kritické činnosti. K těm byly uvedeny bližší údaje jako stupeň kritičnosti, typy dokumentů spouštěných v daném procesu a aplikace, které procesy zpracovávají.

2. V další fázi se získaná data dále analyzovala a začaly se na jejich základě stavět bezpečnostní politiky. Gestoři vytvářených politik byli vybíráni na základě predeterminovaných odpovědných osob. *„Historicky se tady totiž používal ještě termín KDI, což tuším, že byla kategorizována datová informace.*

Existoval k tomu nějaký číselník, kde každá kategorizována datová informace měla svého garanta.“ Gestoři pak dále poskytovali vzorové dokumenty, podle kterých byly vybírány detekční metody.

3. V poslední fázi byly k politikám doplněny další detaily získané z tzv. interview s vlastníky (gestory) politik a řešilo se už, jak konkrétně budou politiky fungovat. V interview byly opět podrobně popsané procesy, v jakých formátech se data zpracovávají, jestli jsou například v nějakých databázových službách jako Sharepoint, Fileshare nebo ECM a zda existují jejich kopie na koncových zařízeních.

Na obrázcích 2-4 jsou ukázky poskytnutých tabulkových podkladů pro tvorbu prvních bezpečnostních politik. Citlivá data byla v tabulkách zakryta.

Tabulka č. 1 Rizikové procesy a činnosti

Proces ID	Proces	Kritické činnosti	KBO	Aplikace	Kritičnost ve vztahu ke ztrátě dat
P1	[redacted]	[redacted]	[redacted]	Share na file systému (AD)	Nízká
		[redacted]	[redacted]	MS SCOM, MS Outlook	Vysoká
P2	[redacted]	[redacted]	[redacted]	MS Outlook	Střední

Obrázek 3 - Počáteční fáze přípravy bezpečnostních politik
Zdroj: Poskytnuto zkoumaným podnikem

Tento postup tvorby politik se ve zjednodušené formě přenesl i do současnosti. *„Víceméně dneska tyto úrovně už nepoužíváme, ale ten mechanismus pořád ano. To znamená, potřebujeme od uživatele nějaké vstupy a opíráme se de facto o ty interview.“*

Příkladem je bezpečnostní politika na ochranu osobních údajů, která byla implementována v letech 2016 až 2018 v souvislosti s nabytím účinnosti obecného nařízení o ochraně osobních údajů (GDPR). *„…a pak jsme rozjeli ten program, kde jsme dávali dohromady mapování zpracování. Řekli jsme, že uděláme opatření na takové věci, které se dají chytit. To znamená, jestli dokážeme najít telefonní číslo, jestli dokážeme najít rodné číslo, jestli dokážeme najít bankovní karty.“*

Skupina politik - Policy Group	Skupina politik - Policy Group	nasazení politiky vyhodnocení incidentů	Politika ID	Garant dat	Pokrytí KDI (KDI ID)	Metoda	Klíčová slova, regulérní výraz, vzorový dokument, typ dokumentu	Klíčová slova, regulérní výraz, vzorový dokument, typ dokumentu - Použité při vytváření testovací politiky	Limity nastavení závažnosti
		3	P06	[redacted]	Dokumenty DDP	DCM	[redacted]	[redacted]	Při shodě dokumentu nastav severity=Medium
		3	P16		[redacted]	DCM			Při shodě dokumentu nastav severity=Medium
		3	P17		[redacted]	DCM			Při shodě dokumentu nastav severity=Medium Při shodě dokumentu nastav severity=Medium Při shodě dokumentu nastav severity=Medium
		3	P18		Dokumenty technického hodnocení	DCM			Při shodě dokumentu nastav severity=Medium
		2	P20		Dokumenty zápisů, podkladů a prezentací	DCM DCM			Při shodě dokumentu nastav severity=Medium

Obrázek 4 - Detailnější zpracování prvních bezpečnostních politik
Zdroj: Poskytnuto zkoumaným podnikem

Jméno vedoucího interview	[redacted]
Oblast dat	
KDI	
Jméno vlastníka KDI	
Datum	
Interview #	

Skupina otázek	Otázka #	Otázka	Očekávaná forma odpovědi	Odpovědi vlastníků dat	Poznámky vedoucího interview
Obecné	1	Pokuste se specifikovat, zda-li existují pro citlivá data skupiny KDI společné parametry pro jejich seskupení do podskupin. Pokud ano, jaké podskupiny by to byly? *Tato segmentace pomůže pro rozdělení citlivých dat v rámci politik.*	• Účetní uzávěrky • IT - plán sítě • Smlouvy • Data dodavatelů	[redacted]	
	2	Jaký objem citlivých dat představuje daná skupina KDI (v Gb/Mb)?	• 100 Mb • 20 Gb	20GB	
	3	Kdo by měl být notifikován při incidentech v rámci této dané KDI.	• Manager • Vlastník (vlastníci dat) • Help Desk apod.	[redacted]	
Kritické procesy a činnosti	4	Definujte kritické procesy, kterými prochází citlivá data během jejich životního cyklu? Uveďte činnosti daného procesu.	• **P1 - Administrativní řízení** **Činnosti** - příprava dat - komunikace v rámci přípravy dat	[redacted]	
	5	Klasifikujte identifikované procesy a činnosti dle jejich kritičnosti ve vztahu k možné ztrátě citlivých dat.	• **Vysoká kritičnost** – existuje vysoké riziko úniku dat z důvodu velkého počtu osob, které v rámci dané činnosti k datům mají umožněn přístup, nebo velké množiny dat, která jsou v rámci procesu zpracována. • **Střední kritičnost** – existuje střední riziko úniku dat. • **Nízká kritičnost** – existuje pouze nízké riziko úniku dat, protože má v rámci činnosti k datům přístup omezený okruh osob, nebo mají osoby přístup pouze k omezené množině dat. ***P1 - Administrativní řízení = Vysoká kritičnost***	Vysoká kritičnost	

Obrázek 5 - Interview s garanty procesů, které slouží jako podklad pro tvorbu bezpečnostní politiky
Zdroj: Poskytnuto zkoumaným podnikem

4.5 Okruh B. Průběh implementace

Ve fázi testování DLP systému byla stanovena rozsáhlá sada akceptačních kritérií. *„Na konci projektu jsme si na testovacích scénářích zkoušeli jednotlivé metody, kde jsme požádali členy týmu projektu, aby nám pomohli DLP otestovat, ať už to byly ty síťové sondy nebo DLP agent.“*

Ukázkovým scénářem mohlo být například zkopírování dokumentu z místa A do místa B, následný monitoring chování DLP agenta a analýza výsledků testu v DLP konzoli, zda došlo k zablokování či ne.

Co se týče integrace DLP s existující infrastrukturou podniku, respondent A ji hodnotí jako v podstatě bezproblémovou. Výhodou je, že řešení není třeba integrovat s informačními systémy typu SAP, ale je vázané pouze na uložiště a například na adresářový servis Active Directory (AD). Později ještě proběhla integrace klasifikačních systémů, detaily k tomuto jsou uvedeny v kapitole 4.5.2 Testování bezpečnostních politik.

V reakci na nově vznikající bezpečnostní týmy v České republice i ve světě a na rozvíjející se hrozby v kybernetické sféře bylo podnikem v následujících letech vytvořeno bezpečnostní dohledové centrum, na které se postupně integrovaly všechny politiky.

V bezpečnostním dohledu zaměstnanci v roli forenzních auditorů zpracovávají záchyty ze všech aktivních politik DLP a následně je přidělují příslušným respondentům k vyřešení. Tímto způsobem je urychlena reakce na bezpečnostní události, které by mohly vést k úniku dat, a zároveň jsou eliminovány některé false positiv záchyty.

4.5.1 Výběr režimů DLP systému

Během testování se také rozhodovalo, jakým způsobem bude systém reagovat na různé typy záchytů. DLP řešení podniku umožňuje vybrat ze tří režimů reakce:

1. Notifikace
2. Notifikace a alertování
3. Notifikace, alertování a blokace

Notifikace byla, a v současnosti i stále je, výchozím stavem nastavení DLP systému. Jedná se o pouhý monitoring a logování záchytů do evidence, s kterou pak dále může pracovat gestor.

V druhém stupni už docházelo kromě notifikace i k **alertování,** buď přímo dotčených zaměstnanců nebo jejich nadřízených, o tom, že se chystají provést nepovolenou manipulaci s daty. Tento mechanismus reakce se eventuálně přestal využívat. *„Pak se ukázalo, že oni se samozřejmě ptali, co to znamená, proč a tak dál. Takže potom, myslím, že se od toho odstoupilo a nechalo se, že se informovali jenom ti gestoři.“*

V posledním stupni už šlo přímo o **blokaci** komunikace, resp. o notifikaci, alertování a zablokování komunikačního kanálu. Tento způsob se dle zjištěných poznatků používá pouze u malého množství politik, jelikož je velmi obtížné ho nasadit. Nutností je umět s naprostou jistotou rozlišit mezi oprávněným a neoprávněným nakládáním s daty, což není vždy možné. *„…sám ten respondent – jakoby ti znalci těch procesů, není třeba schopný ani*

říct, co je dobře a co špatně, protože ten uživatel třeba pro komunikaci používá víc nějakých kanálů nebo víc různých metod.“

4.5.2 **Testování bezpečnostních politik**

Protože testování funkčnosti systému DLP je zároveň i testováním bezpečnostních politik, využívají se obdobné scénáře i dnes. Zásadní změnou oproti testům v minulosti je, že dnes podnik integruje s DLP řešením nástroje na klasifikaci a šifrování dat jako jsou Azure Information Protection (AIP) a Microsoft Information Protection (MIP). Tímto přístupem lze usnadnit monitoring dokumentů pomocí jasně dané struktury klasifikačních značek. *„Testování probíhá tím stylem, že se v podstatě berou nějaké dokumenty, které se označí jenom značkou jako důvěrné nebo nějakým způsobem chráněné, a zkouší se posílat ven na nějaký námi určený e-mail.“* Testují se i reakce systému na změny šifrování, změny v metadatech dokumentu, způsoby odeslání apod.

Dle informací od respondentů se testuje i přímo v produkčním prostředí, jelikož není jiný způsob, jak otestovat efektivitu bezpečnostních politik. Obecně ze všech interview vyplynulo, že nejkomplikovanější částí DLP řešení je správné nastavení politik:

- Respondent A: *„Záleží hodně na tom, jak kvalitně máte ty politiky postavené a co vám všechno sledují… to je jakoby podstatné. Takže z mého pohledu není až tak to množství důležité jako spíš kvalita.“*
- Respondent B: *„…ve finále to bylo tím, že jsme měli ten filtr nastavený moc najemno. To znamená, když řeknu, že tam bude nulová tolerance, tak mně tam spadne úplně všechno, tak jsem musel najít ten rozsah údajů, který jsme ještě schopni tolerovat...“*
- Respondent C: *„Nejsložitější je odladit, jak moc utáhnout ta pravidla. Tak, aby to ukazovalo, když ty informace někdo vynáší, ale zároveň, aby nás to nespamovalo při každém souboru přeneseném ven.“*

Před spuštěním politik v průběhu implementace bylo potřeba nejprve získat souhlas gestorů. To se v některých případech ukázalo jako problém, jelikož i přesto, že s gestory proběhly všechny přípravné kroky včetně interview, někteří se spuštěním i tak nesouhlasili. *„Na začátku panovaly poměrně velké obavy z toho, že to bude generovat nějakou pracnost pro ty gestory, což se samozřejmě ukázalo jako pravdivé.“*

Nedůvěra byla i na straně managementu. Primárně šlo o strach, že bude v rámci DLP docházet ke sledování veškeré komunikace, a proto se už i v implementační fázi připravovaly prezentace pro management, kde bylo ve zjednodušené formě představeno fungování DLP systému.

Na otázku, co bylo největší výzvou při implementaci DLP systému, respondent A uvedl právě prvotní zpracování bezpečnostních politik. *„Jednoznačně to byla tvorba politik. Identifikace procesů, identifikace kritických činností, příprava interview s gestory a samotné politiky. To bych řekl, že bylo nejtěžší na té implementaci.“*

4.6 Okruh C. Výsledky a zhodnocení implementace

DLP systém zkoumaného podniku vstoupil do ostrého provozu v roce 2012, ale některé oblasti implementační práce svým způsobem nikdy neskončily. Každoročně jsou zaváděny nové politiky a do systému se průběžně integrují nové moduly nebo uložiště.

Zpětný pohled respondentů na průběh implementace systému DLP i jednotlivých politik byl převážně pozitivní. *„Myslím si, že ten postup byl správný. Identifikovat procesy, kritické činnosti a pak postupovat dál. Zatím jsem se nesetkal s ničím lepším, že by to někdo dělal jiným způsobem, protože to je přesně to, o čem DLP je.“* Jedinou výtkou, kterou uvedl respondent A, bylo množství politik, které se hned ze začátku nasazovalo. I přes snahu co nejvíce zúžit rozsah procesů, které měly být systémem chráněny, bylo v první vlně implementováno 44 politik. Podle respondenta A by bylo vhodnější nasazovat politiky ve více etapách podle kritičnosti, od více kritických činností až po ty méně kritické.

4.6.1 Reakce uživatelů

Zaměstnanci podniku byly o zavedení DLP systému informováni oficiálními komunikačními kanály podniku, primárně skrze intranetovou síť a interní dokumentaci. *„Došlo tam k tomu, že nám vlastně v rámci toho procesu seznamování s dokumenty i ti uživatelé odsouhlasili, že se s tou problematikou DLP seznámili.“* Na přípravě vnitřních dokumentů spolupracovali kromě metodiků DLP i firemní právníci, kteří zajišťovali, aby se k zaměstnancům dostaly všechny důležité informace o zpracování a monitoringu informací skrze DLP řešení.

Jak byly, a do jisté míry i stále jsou, úspěšné pokusy seznámit běžné uživatele s monitorovacími technikami, je otázkou, u které se respondenti částečně rozcházejí v názorech. Podle respondenta B většina zaměstnanců ani nezaregistrovala, že došlo ke změnám ve sledování aktiv podniku.

Otázka ochrany soukromí se dostala více do popředí s nabytím účinnosti obecného nařízení GDPR v roce 2018. Kromě zavedení nové bezpečnostní politiky k ochraně osobních údajů to znamenalo pro zaměstnance i určité změny v povolených způsobech využívání komunikačních kanálů. *„Nejvíc problémové je to, že u nás jsou ti lidé zvyklí v korporátu všechno posílat všem.“* Hromadné přeposílání e-mailů, u kterých se v těle zprávy kumulují e-mailové adresy původních adresátů, je zmiňováno jako jedna z nejčastějších příčin vzniku false positiv záchytů u souvisejících politik.

Zároveň se více lidí začalo zabývat tím, jak je nakládáno s jejich osobními údaji, a proč podnik sleduje jejich aktivity na koncových zařízeních. *„Tam je jenom ten problém, že většinou se ozve ten, kdo něco provedl. Dostane sadu otázek, na kterou má odpovědět – co to bylo, proč to bylo, kam to bylo, eventuelně to smažte… ale naprostá většina těch událostí je o tom, že si posílají svoje soukromá data a porušují něco úplně jiného.“* Využívání zapůjčených koncových zařízení k soukromým činnostem je ve firmám zpravidla zakázáno, a tak je tomu i ve zkoumaném podniku. *„Ale kdo z nás nepoužil počítač pro soukromé účely? To je věc, které nezabráníte.“* Stížností na narušení soukromí se ale neobjevilo za dobu fungování systému mnoho, podle respondenta B ne více než 10.

4.6.2 **Ochrana soukromí**

DLP řešení umožňuje vidět nejen hlavičku a metadata zachyceného souboru, ale i jeho obsah. Tato vlastnost ale byla považována za kontroverzní už od začátku využívání DLP systému v podniku. Vzhledem k tomu, že velká část záchytů v DLP se týká e-mailové komunikace, neoprávněným otvíráním a čtením cizích zpráv by docházelo k porušování listovního tajemství. To se podle článku 13 Listiny základních práv a svobod vztahuje nejen na písemnosti, ale i na zprávy podávané telefonem, telegrafem nebo jiným podobným zařízením, tedy i na elektronickou poštu.

Přestože tedy DLP v běžném režimu umožňuje nahlížet do příloh záchytu, podnik toto nastavení na radu firemních právníků už od počátku omezil. *„…do těch dokumentů nebo do toho extraktu z bezpečnostního incidentu je možné nahlédnout, ale za nějakých jasně stanovených pravidel. Ve výchozím nastavení tady u nás ta role, která může nahlížet na extrakt, není.“*

4.6.3 **Zkušenosti s false positiv záchyty**

Nejčastěji zmiňovaným problémem, s kterým se respondenti v oblasti DLP setkali, byly frekventované záchyty false positive případů. *„Zachytávají se hlavně, řekl bych až z 95 %, ty false positive, a tak v 5 % je to potvrzené jako únik informací nebo nějaký pokus o přenesení informací.“*

Podle zkušeností respondentů lze do určité míry false positive záchyty eliminovat skrze kvalitně nastavená pravidla bezpečnostních politik, případně udělování bezpečnostních výjimek tam, kde se skutečně jedná o oprávněnou pracovní činnost. Dobrou praxí při úpravě politik je spolupráce mezi útvary, které se danou oblastí zabývají z různých pohledů, např. metodiky DLP a forenzními auditory.

Špatně nastavené politiky, které generují někdy i stovky false positive záchytů měsíčně, zatěžují jak gestory, tak auditory, a zároveň zvyšují šanci, že bude přehlédnut skutečný bezpečnostní incident. *„Máme tam 300 záchytů za sebou a neděláme nic jiného, než jenom prověřujeme jeden dokument, co byl přeposlaný čtyřicetkrát, a v podstatě o nic nešlo.“*

Ale ani u dobře nastavených politik není stoprocentní záruka, že se nebudou false positiv záchyty objevovat. V předchozí kapitole 4.6.1 bylo zmíněno využívání pracovních koncových stanic k soukromým účelům, což obvykle znamená, že se v zařízeních vyskytují soukromé osobní údaje uživatelů. Detekční metody DLP systémů, které se zaměřují na hledání klíčových slov jako jsou třeba rodná čísla, nejsou schopny rozeznat, zda se jedná o aktiva společnosti nebo ne, a v záchytech se pak často objevují i data uživatelů.

Podle respondentů je tedy při třídění záchytů důležitý i vstup lidí, například forenzních auditorů, kteří už podle určitých scénářů dokážou zařadit záchyty do správných kategorií. *„Ta politika je ve své podstatě tupá, dokud se do toho nepodívá člověk… protože to, co dělá ten počítač, nikdy není stoprocentní. A obzvlášť u tady těch věcí, které se odvíjí vlastně od čísel.“*

4.6.4 **Řešené případy z praxe**

Respondenti uvedli několik příkladů, kdy se systému DLP podařilo zachytit podezřelou aktivitu a zabránit úniku dat. Některé detaily byly z popisu vypuštěny, aby nebyla narušena bezpečnost podniku. Příklady jsou označeny podle toho, zda šlo o **neúmyslný únik** dat (NÚ), pokus o **záměrné vynesení** dat (ZV) nebo o případ s prvky z **obou variant** (OV).

1.	NÚ	V hromadně rozeslaném e-mailu byl nedopatřením seznam adresátů uveden v otevřené kopii, místo kopie skryté, která se zpravidla v těchto případech využívá. Adresáty bylo proto možné propojit s citlivým obsahem zprávy. Ihned po zachycení došlo ke stáhnutí e-mailu, byl informován ÚOOÚ a dotčeným adresátům bylo podáno vysvětlení s omluvou. Dále neeskalováno.
2.	ZV	Zaměstnanec, s kterým byl ukončován pracovní poměr, se před svým odchodem pokusil stáhnout a vynést velké množství chráněných dat pomocí USB flash disku. Pokus o stažení byl přerušen, obsah USB disku se zašifroval a záchyt byl dál předán k řešení manažeru ochrany a nadřízenému dotčeného zaměstnance.
3.	OV	Byl zachycen pokus o neoprávněné vynesení dokumentu se strukturovanými chráněnými daty, který byl pro podnik vypracován na zakázku. Dotčený zaměstnanec, který dříve s daty pracoval, ukončil pracovní poměr a chtěl si dokument uchovat jako ukázku své předchozí praxe pro příštího zaměstnavatele. Řešeno interně s nadřízeným.

Tabulka 6 - Příklady řešených případů úniku dat ve zkoumaném podniku
Zdroj: Vlastní zpracování

4.7 Okruh D. Aktuální stav a budoucnost systému DLP

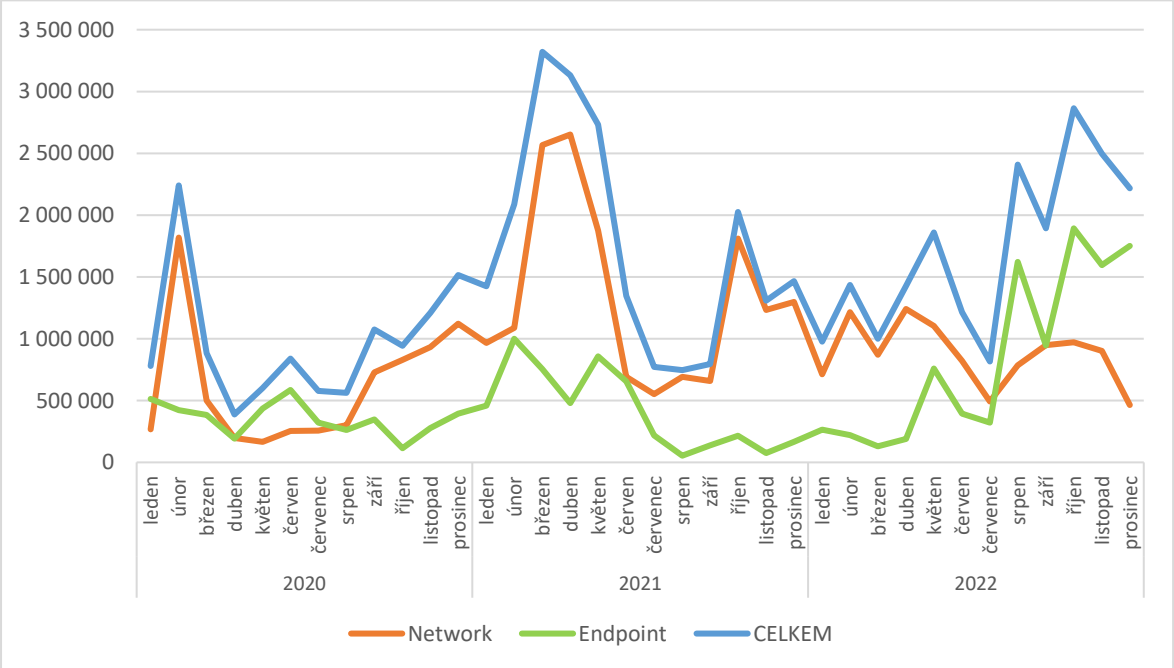
V DLP systému podniku je k roku 2024 evidováno 92 politik, z toho 32 je neaktivních. Primárně je systém využíván na kontrolu informací odcházejících ven mimo perimetr firmy, ale u některých typů dokumentace, jako jsou například veřejné zakázky, se používá i ke kontrolám pohybu dat uvnitř firemní sítě.

Nárůst počtu politik a změny v parametrech detekce způsobují výkyvy v množství zachycených případů v DLP řešení, takže nelze s jistotou určit nakolik se dnešní počty záchytů liší od těch v minulosti. V datech uvedených ve statistikách záchytů podniku je ale možné sledovat jiné faktory, které mají vliv na to, jak jsou využívány (nebo zneužívány) firemní komunikační kanály.

V grafu 3 je zobrazena křivka počtu záchytů v letech 2020 až 2022. Skutečné hodnoty získané ze statistik byly s ohledem na jejich citlivý charakter upraveny podle rovnice níže, kde k je skrytá konstanta. Kolísání dat zobrazené na křivce není změnou ovlivněno.

$$Původní\ hodnota \times k = nová\ hodnota$$

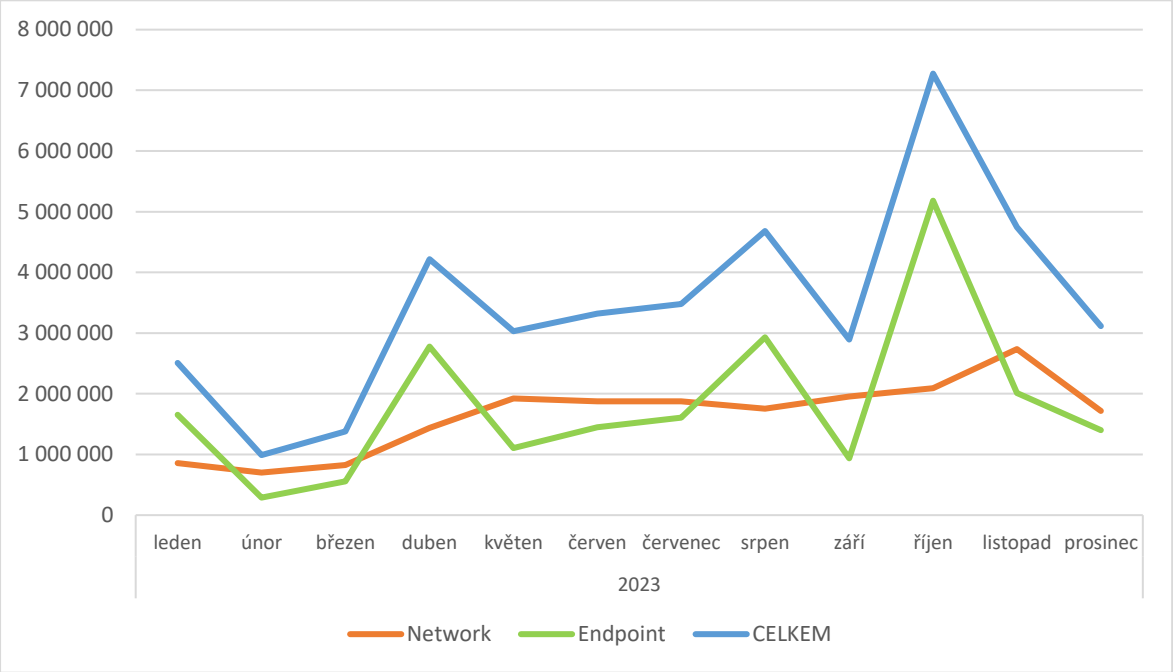
Na křivce grafu je vidět, že v období mezi prosincem 2020 a červencem 2021 došlo k velkému nárůstu počtu záchytů, který byl způsoben nařízenou prací z domova v důsledku pandemie covid-19. Změna pracovních podmínek vedla ke snížené pozornosti a častějšímu nedodržování interních předpisů, což se promítlo i do výsledků práce systému DLP. Nárůst je zřetelný obzvlášť u síťového (network) DLP díky výrazně většímu počtu zaměstnanců připojených do interní sítě.



Graf 3 - Statistika záchytů DLP systému podniku v letech 2020 až 2022

Zdroj: Vlastní zpracování

Jak počet záchytů kolísá v průběhu jednoho roku je vidět v grafu 4 s údaji z roku 2023. Zde jsou zajímavé obzvlášť výkyvy u endpoint DLP v měsících dubnu, srpnu a říjnu, které jsou spojeny s konci účetních kvartálu. V těchto obdobích se vypracovávají reporty a výkazy, což zvyšuje jak síťový provoz (data in motion), tak i množství dat zpracovávaných v koncových zařízeních (data in use), což se opět promítá do počtu záchytů v DLP systému.



Graf 4 - Statistika záchytů DLP systému podniku v roce 2023
Zdroj: Vlastní zpracování

V tabulce 7 je uvedeno procentuální složení záchytů v systému DLP u jedné z bezpečnostních politik za rok 2023. Pro potřeby této práce byly záchyty rozděleny do čtyř kategorií:

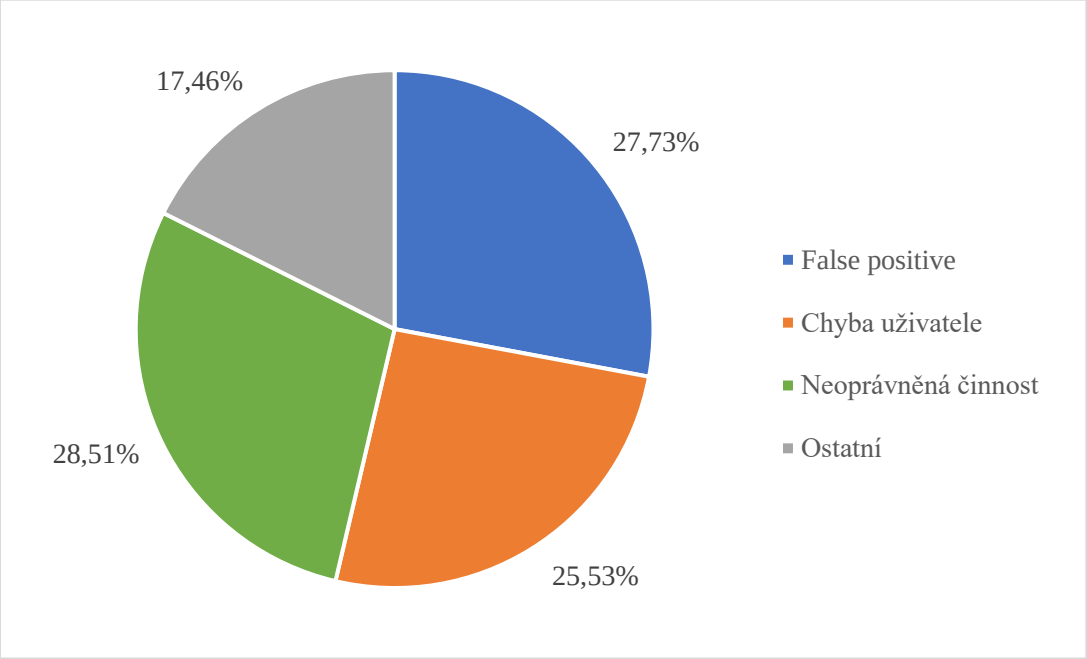
- **Neoprávněná činnost**: Záchyt na základě nepovoleného zacházení s pracovními daty, například stažení nebo odeslání do soukromého zařízení.
- **Chyba uživatele**: Záchyt způsoben neúmyslně koncovým uživatelem, například nasdílení dokumentů špatnému příjemci.
- **False positive**: Záchyt se netýká pracovních dat nebo se jedná o legitimní pracovní činnost na základě udělené výjimky.
- **Ostatní**: Do této kategorie patří například technické závady, oznámení o ztrátě nebo odcizení koncového zařízení apod.

Při porovnání složení záchytů v DLP v jednotlivých měsících je možné sledovat velké výkyvy. Například v lednu 2023 tvořila neoprávněná činnost 53,49 % všech záchytů, ale v dubnu 2023 to bylo pouze 5,88 %. Z dostupných informacích nelze stoprocentně určit jasnou příčinu těchto výkyvů, ale podle zkušeností pracovníků v této oblasti se jedná o kombinaci více vnějších a vnitřních faktorů.

Graf 4 zobrazuje aritmetický průměr složení záchytů v DLP za celý rok 2023 podle výše zvolených kategoriích, vypočítaný z dat v tabulce 7. I přes opakovanou optimalizaci sledované bezpečnostní politiky tvoří false positive případy průměrně 27,73 % všech záchytů.

	False positive (%)	Chyba uživatele (%)	Neoprávněná činnost (%)	Ostatní (%)
Leden 2023	25,58	27,91	53,49	9,30
Únor 2023	41,67	22,92	27,08	10,42
Březen 2023	33,33	21,43	23,81	16,67
Duben 2023	29,41	35,29	5,88	17,65
Květen 2023	25,45	18,18	38,18	16,36
Červen 2023	21,62	27,03	27,03	18,92
Červenec 2023	39,13	17,39	8,70	30,43
Srpen 2023	14,71	35,29	29,41	20,59
Září 2023	23,08	20,51	38,46	15,38
Říjen 2023	18,18	27,27	32,73	21,82
Listopad 2023	34,09	29,55	25	11,36
Prosinec 2023	26,47	23,53	32,35	20,59
Průměr	27,73	25,53	28,51	17,46

Tabulka 7 - Procentuální složení záchytů v DLP ve vybrané politice za rok 2023
Zdroj: Vlastní zpracování



Graf 5 - Průměrné složení záchytů v DLP ve vybrané politice za rok 2023
Zdroj: Vlastní zpracování

Jako většina technologií se DLP systémy rychle vyvíjí, aby udržely krok s narůstajícími riziky v kyberprostoru. Jednou oblastí je stále populárnější využívání cloudových uložišť. *„To, že se nám ta infrastruktura taky trošičku posouvá směrem k hybridním scénářům, třeba i do cloudu, samozřejmě v dnešní době hraje roli i ve společnostech, které používají DLP.“*

Cloudové DLP jsou relativně novým typem produktu na ochranu před únikem dat, ale jsou již nabízené mnoha dodavateli včetně Symantecu. Podle názoru respondenta A je ochrana cloudových uložišť využívaných ve zkoumaném podniku (např. O365) oblastí, kam se lze dále posunout v rámci zajišťování kybernetické bezpečnosti.

Do budoucna je prostor na zlepšení dle respondenta C i v možnostech nastavení pravidel bezpečnostních politik *„V tuhle chvíli je to takové ne úplně optimální, co se týče pravidel, protože se nedají aplikovat úplně na všechno. A pořád jsou tam nějaké skulinky, kterými se dá protáhnout.“* Zde by se mohla nacházet možnost využít jednoduché AI ke zpracování opakujících se podnětů, to je ale nyní spíše vnímáno jako velké budoucí riziko. *„Pokud se AI naučí určité kroky, tak to zvládne vyhledávat velmi rychle a efektivně chyby, které se potom dají rychle zneužít.“*

Podle respondenta B ale nadále budou největším rizikem lidé, a to ať z pohledu neúmyslných úniků dat, tak i záměrného vynesení informací. Jakkoliv je DLP řešení efektivní, žádný systém není stoprocentní, a problémem v této oblasti je, že na případnou mezeru v ochraně se zpravidla přijde, až když dojde k bezpečnostnímu incidentu. *„Samozřejmě dřív nebo později se někdo pokusí ta data dostat nějakým způsobem ven. Jde o to, jak vytečou, protože jsme, jako strategický podnik, ve středu zájmu z hlediska konkurenčního boje.“*

5 Výsledky a diskuse

5.1 Hodnocení DLP systému respondenty

Podnik zvolil hybridní řešení kombinující síťové DLP monitorující firemní síť a endpoint DLP fungující skrze DLP agenty nainstalované v koncových zařízeních, které komunikují s endpoint serverem, jak bylo popsáno v kapitole 4.2. Respondenti se při hodnocení úspěšnosti projektu a efektivity systému zaměřovali na dílčí části DLP řešení.

Shrnutí hodnocených prvků podle toho, zda splnily očekávání jednotlivých respondentů, je uvedeno v Tabulce 8. Konkrétní poznatky a výtky ke korespondujícím aspektům jsou rozvedeny v kapitolách 5.1.1 až 5.1.3.

5.1.1 Hodnocení podle koncepčního přístupu

Endpoint DLP

Komunikace na koncových zařízeních, kterou lze monitorovat, je podle názoru respondentů mnohem více granulární než u síťových serverů. Používá se zde více protokolů a pracuje s více informacemi. Sledovat se dá kopírování dat do uložišť a na USB flash disky, vypalování dat na CD / DVD apod.

Zásadním problémem zmíněným respondenty B a C bylo zpoždění endpoint DLP při nahlašování podezřelé aktivity. Agent DLP nainstalovaný na koncovém zařízení detekované incidenty zasílá na endpoint server až ve chvíli, kdy se uživatel připojí do interní sítě. Tím vzniká časová prodleva mezi vznikem záchytu a jeho posouzením a zpracováním v bezpečnostním dohledu. *„Záleží na tom, kdy se uživatel synchronizuje do sítě. Jakmile se synchronizuje, tak se odešlou veškerá data nebo veškeré eventy, co byly v DLP.“*

Naopak výhodou endpoint DLP je podle respondenta C to, že se v systému zachytí i přeposílaný soubor, který může být důležitý při vyhodnocování legitimity záchytu.

Síťové DLP

Síťové DLP je podle názoru respondentů v některých ohledech spolehlivější, ale také má omezenější využití než endpoint DLP. Opakovaným technologickým problém, o kterém hovořil respondent A, je navazování šifrované komunikace mezi klientem a serverem pomocí SSL pinning. *„Veškerá komunikace, která je na síťové úrovni kontrolovaná, musí být zároveň terminovaná na proxy. To znamená, proxy musí terminovat spojení, pošle DLP dotaz na kontrolu, DLP to zkontroluje a vrátí se to zase zpátky.“* V některých případech při navazování komunikace do SSL pinning ale nelze komunikaci terminovat a nemůže tak dojít ani k její kontrole.

Z pohledu zpětné kontroly záchytů je také síťové DLP více limitované. Podle respondenta C poskytuje síťové DLP jen velmi omezené informace o přenášených souborech, což často komplikuje šetření možného úniku dat.

5.1.2 Hodnocení podle metody detekce

Klíčová slova, fingerprinting

Detekce skrze klíčová slova a fingerprinting (otisky dokumentů porovnávané na základě podobnosti) respondent A z technologického hlediska hodnotí jako 100 % úspěšné, pokud je správně nastavená bezpečnostní politika. Respondent C považuje tyto metody za velmi efektivní, problémem je pouze to, že DLP systém nedokáže v některých případech vyfiltrovat legitimní komunikaci, je tedy potřeba vybalancovat obsahovou i kontextovou detekci. Respondent B nemá k těmto detekčním metodám žádné výtky.

Podporované formáty souborů

Využívaný DLP systém podporuje velké množství formátů se strukturovanými i nestrukturovanými daty. Podle respondenta A ale chybí podpora OCR (Optical Character Recognition), která umožňuje rozpoznat text i z grafických formátů a například PDF souborů, a také podpora některých specializovaných aplikací, které jsou firmou využívány. Respondenti B a C také zdůrazňují problémy s PDF soubory a respondent C jako problém vnímá i limitované schopnosti DLP systému nahlížet do zašifrovaných (zazipovaných) dat s heslem.

Integrace s klasifikačními systémy

Respondent A možnost využití integrace s klasifikačními nástroji hodnotí kladně. Podle respondentů B a C je propojení klasifikačních nástrojů s DLP systémem funkční, ale velmi závislé na tom, zda uživatelé dokumenty správně klasifikují. *„Tam kde jsou zprávy, kde jsou kontroly, kde jsou nějaké souhrny… tam by to mělo být vždy chráněno. A kde jsou osobní údaje, tak je to vždy chráněný dokument.“*

5.1.3 Ostatní hodnocení

Reportování

Podle respondenta A je v rámci možností nabídka customizace reportů z DLP systému dostačující, ale někteří zaměstnanci, kteří tyto funkce využívají, mají příliš vysoké nároky. *„Samozřejmě, že jsou tady respondenti, kteří by to rádi celé ohnuli a zlomili, ale to prostě nejde v žádném softwaru…“*. Respondenti B a C možnosti reportingu moc často nepoužívají a nedokážou je tudíž posoudit.

Logování

K logování dochází skrze bezpečnostní dohled a v evidenci se záchyty udržují po dobu maximálně 90 dnů, aby nedošlo k přetečení databáze. Z pohledu respondenta A je logování v systému DLP spolehlivé a není si vědom žádných specifických problémů. Respondent B jako gestor politiky považuje logování za dostačující, v případě jiných politik je dobrá i možnost alertovat nebo blokovat komunikaci. Respondent C vnímá logování jako velmi účinné, jen zdůrazňuje potřebu správně nastavit rozsah pravidel politik.

Zabezpečení systému

Protože DLP systém sám zpracovává velké množství dat, může být také považován za riziko. Základním způsobem ochrany dat je nastavení omezených přístupů a rolí, které umožňují zaměstnancům zpracovávat pouze pro ně relevantní informace. V systému DLP funguje standardní systém autentizace a autorizace. Gestorům jsou přidělované role s nadefinovanými response pravidly, kam má daný gestor v konzoli DLP přístup.

Podle respondenta A je systém z pohledu bezpečnosti ošetřen dobře a efektivní je i granularita přístupů, kdy je možné mít přiděleno vícero menších dílčích rolí a přepínat mezi nimi. Systém také loguje veškerou aktivitu forenzních auditorů, gestorů politik a manažerů ochrany, kteří do konzole přistupují, což zdůrazňují respondenti B a C s tím, že pro zajištění komplexní ochrany musí někdo hlídat i „strážce". *„V tuhle chvíli je to dostatečné pro zpětnou investigaci, kdyby tam někdo provedl něco, co by neměl."*

Aktualizace systému

Aktualizace systému DLP může být iniciována z různých směrů, jelikož se o systém stará v různých rolích více útvarů. Dle respondenta A může být důvodem například potřeba rozšířit funkcionalitu DLP řešení, ale někdy je aktualizace spojená s upgradem jiné části infrastruktury, jako je operační systém nebo databáze.

V případě rozšíření funkcionalit může při aktualizaci dojít k zanesení chyby do systému, a proto je potřeba mít všechny aktualizace předem naplánované, aby byl dostatek času k otestování systému a potencionálně k opravě. „*Není to jako aktualizovat si koncovou stanici. Všechny tyhle věci se musejí naplánovat, jsou tam odstávky těch systémů nebo i v infrastruktuře."* Výjimkou jsou podle respondenta A upgrady s cílem odstranit nějakou technickou zranitelnost, které se řeší prioritně. Respondent B zaznamenává aktualizace pouze z pohledu občasného uživatele konzole.

Ze zkušenosti respondenta C se aktualizace na straně poskytovatele obvykle dělají v nočních hodinách, takže nedochází zpravidla k žádným nečekaným výpadkům. Problémem dle něj ale mohou někdy být upgrady systému, jejichž součástí jsou drobné úpravy ve fungování atributů v konzoli DLP, které se ale nepromítnou do lokálního nastavení a je potřeba je upravit manuálně.

Podpora poskytovatele

Podnik s poskytovatelem spolupracoval již před zavedením systému DLP, takže byl nějakým předpokladem dobrý obchodní vztah. Respondent A to potvrzuje s tím, že ke spolupráci během implementace nemá žádné výtky. V současnosti se podnik může obrátit na zástupce dodavatele s dotazy k nastavení systému i s řešením případných problémů. Dle respondenta C poskytovatel reaguje přiměřeně rychle v závislosti na řešeném problému a v případě urgence má poskytovatel i pohotovostní režim. Respondent B nemá s komunikací s dodavatel zkušenosti.

Hodnocené kritérium		Respondent A				Respondent B				Respondent C			
		Splňuje	Splňuje s výtkami	Nesplňuje	Nelze posoudit	Splňuje	Splňuje s výtkami	Nesplňuje	Nelze posoudit	Splňuje	Splňuje s výtkami	Nesplňuje	Nelze posoudit
Metody detekce	Klíčová slova, fingerprinting	■				■				■			
	Klasifikace dat	■				■				■			
	Podpora formátů souborů		■				■			■			
Koncepční přístup	Endpoint DLP		■				■				■		
	Síťové DLP		■			■					■		
Práce s konzolí	Možnosti reportování	■							■				■
	Možnosti logování	■				■				■			
	Nastavení politik	■				■					■		
	Zabezpečení dat	■				■					■		
	Aktualizace systému	■							■		■		
Poskytovatel	Podpora při implementaci	■							■				■
	Konzultace a troubleshooting	■							■	■			

Tabulka 8 - Shrnutí hodnocení implementovaného DLP systému a jeho prvků jednotlivými respondenty
Zdroj: Vlastní zpracování

5.2 Silné a slabé stránky DLP řešení

Na základě poznatků získaných od respondentů byly identifikovány silné a slabé stránky současného DLP řešení v podniku, které mohou sloužit jako podklad pro volby strategií budoucího vývoje bezpečnostního systému.

Silné stránky	*Slabé stránky*
• Spolehlivé obsahové i kontextové detekční metody • Variace režimů reakce DLP systému • Integrace klasifikačních nástrojů • Efektivní logování • Granulace přístupů do DLP • Komunikace s poskytovatelem • Specializovaný útvar v pohotovostním režimu • Spolupráce s odborníky s praktickými zkušenostmi • Preventivní účinek systému • Možnost zpětné investigace • Možnost implementace nových modulů	• Častý výskyt false positive záchytů • Chybějící pokrytí cloudových uložišť • Chybějící podpora OCR • Chybějící podpora specializovaných aplikací • Limitace monitorování zašifrovaných souborů s heslem • Náročnost aktualizací systému • Problém se SSL pinning • Zpoždění u detekcí v endpoint DLP • Omezené logy u síťového DLP • Možnost narušení ochrany osobních údajů • Nedostatek součinnosti gestorů politik

Tabulka 9 - Přehled silných a slabých stránek DLP systému
Zdroj: Vlastní zpracování

5.3 Efektivita DLP systému

Z technického pohledu splňuje DLP systém podle respondentů až na některé výjimky popsané v kapitole 5.1 všechna očekávání. Velký důraz byl ale kladen na fakt, že DLP je jen nástrojem, který musí být správně využíván, aby efektivně vykonával svou činnost. Nejčastěji se v rozhovorech opakovalo téma důsledné přípravy a nastavení bezpečnostních politik, které se také musí průběžně přizpůsobovat měnícím se podmínkám ve firmě.

Možným způsobem určení efektivity bezpečnostních politik je sledování počtu záchytů, který by se měl pohybovat uvnitř nějakého očekávaného intervalu. *„Ideální je, aby vám to zachytávalo jenom ty bezpečnostní události, u kterých to očekáváte. Neměli byste tam mít velké množství false positive… pokud se tam ale nic nechytá, tak je to zase podezřelé. Že to prostě nefunguje.“*

Pokud bychom se řídili tímto pravidlem, je tedy počet záchytů značící dobře nastavenou bezpečnostní politiku (n) v intervalu mezi n_{min}, které musí být větší než 0, a n_{max}, které označuje maximální očekávané (povolené) množství záchytů pro danou politiku očištěné o false positive záchyty. Cokoliv nad tímto intervalem značí buď příliš široce nastavená pravidla politiky nebo neočekávaný nárůst nelegitimních aktivit v této oblasti.

$$n_{max} - false\ positive > n_{min} > 0$$

Protože je systém DLP nástroj prevence, který negeneruje žádné zisky, je obtížné za použitých metod přímo určit dlouhodobé finanční dopady na podnik. Je ale možné pro srovnání využít data získaná průzkumem odborné literatury, která se zaměřují na reálné incidenty úniku dat u jiných společností. V některých případech jsou finanční ztráty dotčených firem až v biliónech korun, viz tabulky 1 a 2. Vzhledem k velikosti zkoumaného podniku a existujících regulačních norem v ČR by jen náklady ve formě pokut mohly dosáhnout miliónů, potencionálně i miliard korun. Do toho nejsou započítány náklady související se ztrátou goodwill společnosti a postavení na trhu. Z ekonomického hlediska tedy systém DLP není ziskový, ale náklady spojené s následky úniku dat by mnohonásobně převyšovaly investici do bezpečnostního systému.

6 Závěr

Při průzkumu odborné literatury k vybranému tématu byly zmapovány možné následky úniku citlivých dat, které mohou výrazně poškodit podnik jak po stránce finanční, tak i z pohledu reputace. Zároveň bylo zjištěno, že zdrojem rizik při ochraně podnikových aktiv jsou velmi často vnitřní hrozby v podobě zaměstnanců, obchodních partnerů a dalších interních subjektů. Tyto poznatky sloužily jako základ k vypracování vlastní části bakalářské práce

Cílem práce bylo zhodnotit dopad implementace bezpečnostního systému DLP u vybraného podniku na základě dat získaných z polostrukturovaných interview se zainteresovanými osobami a poskytnutých dat z podnikových statistik.

Pro tento účel byli vybráni respondenti z řad zaměstnanců podniku, kteří měli praktické zkušenosti s implementací a správou zkoumaného DLP řešení. Respondentům byly pokládány otázky ohledně příprav na implementaci, jejího průběhu a následného zpětného zhodnocení. Respondenti také ohodnotili podle svých odborných znalostí vybrané klíčové aspekty DLP systému. Jako podpůrná data byly použity podnikem poskytnuté údaje ze statistik záchytů v DLP řešení za poslední 4 roky.

Ve výsledku byla respondenty implementace systému DLP a souvisejících bezpečnostních politik hodnocena pozitivně. Z technologického pohledu systém splňuje očekávání, důraz byl ale kladen na kvalitně zpracované politiky, které jsou klíčové pro efektivní fungování DLP řešení. Údaje ze statistik záchytů a úspěšné detekce, které zabránily potencionálnímu úniku podnikových dat, svědčí o účinnosti zavedeného systému.

7 Seznam použitých zdrojů

ALI, Basheer Husham, Ahmed Adeeb JALAL a Wasseem N. Ibrahem AL-OBAYDY, 2020. Data loss prevention (DLP) by using MRSH-v2 algorithm. *International Journal of Power Electronics and Drive Systems* [online]. **10**(4), 3615. Dostupné z: doi:10.11591/ijece.v10i4.pp3615-3622

BERTRAND, Yoann, Karima BOUDAOUD a Michel RIVEILL, 2020. What do you think about your company's leaks? A survey on End-Users Perception toward data leakage Mechanisms. *Frontiers in Big Data* [online]. **8**. Dostupné z: doi:10.3389/fdata.2020.568257

BISHOP, Edward, 2020. Our new normal of remote work makes data loss prevention crucial for GDPR compliance. *Forbes* [online]. Dostupné z: https://www.forbes.com/sites/forbestechcouncil/2020/06/15/our-new-normal-of-remote-work-makes-data-loss-prevention-crucial-for-gdpr-compliance/

BRADLEY, Daniel, Dan HU, Xiaojing YUAN a Chi ZHANG, 2023. Trade secret protection and product market dynamics. *Journal of Corporate Finance* [online]. **83**, 102470. Dostupné z: doi:10.1016/j.jcorpfin.2023.102470

COLE, Eric, 2017. Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey. *Cyber Security Training | SANS Courses, Certifications & Research* [online]. Dostupné z: https://www.infopoint-security.de/media/defending-wrong-enemy-2017-insider-threat-survey-37890.pdf

COSTANTE, Elisa, Davide FAURI, Sandro ETALLE, Jerry Den HARTOG a Nicola ZANNONE, 2016. A Hybrid Framework for Data Loss Prevention and Detection. *2016 IEEE Security and Privacy Workshops* [online]. Dostupné z: doi:10.1109/spw.2016.24

CROWDSTRIKE, 2023. What is Data Loss Prevention (DLP)? [Guide] - CrowdStrike. *crowdstrike.com* [online]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/

DE SOUSA, Edson Machado a Abid SHAHZAD, 2021. Data Loss Prevention from a Malicious Insider. *Journal of Computer Information Systems* [online]. **62**(6), 1101–1111. Dostupné z: doi:10.1080/08874417.2021.1980748

FAIZ, Mohamed Falah, Junaid ARSHAD, Mamoun ALAZAB a Andrii SHALAGINOV, 2020. Predicting likelihood of legitimate data loss in email DLP. *Future Generation Computer Systems* [online]. **110**, 744–757. Dostupné z: doi:10.1016/j.future.2019.11.004

GHORBANIAN, Sara, Glenn FRYKLUND a Stefán AXELSSON, 2015. DO DATA LOSS PREVENTION SYSTEMS REALLY WORK? V: *IFIP advances in information and communication technology* [online]. p. 341–357. Dostupné z: doi:10.1007/978-3-319-24123-4_20

KHAN, Ahmed Yar, Rabia LATIF, Seemab LATIF, Shahzaib TAHIR, Gohar BATOOL a Tanzila SABA, 2020. Malicious insider attack detection in IoTs using data analytics. *IEEE Access* [online]. **8**, 11743–11753. Dostupné z: doi:10.1109/access.2019.2959047

KIM, Jinhyung, Choonsik PARK, Jun HWANG a Hyung-Jong KIM, 2013. Privacy level indicating data Leakage Prevention system. *Ksii Transactions on Internet and Information Systems* [online]. **7**(3), 558–575. Dostupné z: doi:10.3837/tiis.2013.03.009

KOMNENIC, Masha, 2023. Biggest GDPR Fines & Penalties So Far [2024 update]. *Termly* [online] [accessed. 2024-01-14]. Dostupné z: https://termly.io/resources/articles/biggest-gdpr-fines/

KONGSGÅRD, Kyrre Wahl, Nils Agne NORDBOTTEN, Federico MANCINI a Paal ENGELSTAD, 2017. An Internal/Insider Threat Score for Data Loss Prevention and Detection. *ACM* [online]. Dostupné z: doi:10.1145/3041008.3041011

KUIPERS, Sanneke a Michael SCHONHEIT, 2021. Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. *Corporate Reputation Review* [online]. **25**(3), 176–197. Dostupné z: doi:10.1057/s41299-021-00121-9

MARKOS, Ereni, Priscilla PEÑA, Lauren I. LABRECQUE a Kunal SWANI, 2023. Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *Journal of Consumer Affairs* [online]. **57**(3), 1089–1119. Dostupné z: doi:10.1111/joca.12554

MCSHANE, Michael K. a Trung NGUYEN, 2020. Time-varying effects of cyberattacks on firm value. *The Geneva Papers on Risk and Insurance - Issues and Practice* [online]. **45**(4), 580–615. Dostupné z: doi:10.1057/s41288-020-00170-x

MIKE, Nimród, 2022. Data Protection has Entered the Chat: Analysis of GDPR Fines. *Masaryk University Journal of Law and Technology* [online]. **16**(2), 163–213. Dostupné z: doi:10.5817/mujlt2022-2-3

MITYUSHIN, Dmitry A., 2021. On DLP systems at objects of informatization and employees rights. V: *Lecture notes in networks and systems* [online]. p. 264–271. Dostupné z: doi:10.1007/978-3-030-77448-6_25

PARK, Hanna, 2017. Exploring effective crisis response strategies. *Public Relations Review* [online]. **43**(1), 190–192. Dostupné z: doi:10.1016/j.pubrev.2016.12.001

POYILAN, Niyaz, 2023. Declutter Your security: How Data Classification Aids Loss Prevention | QRTD Information Technology. *QRTD Information Technology* [online]. Dostupné z: https://www.qrtd.qa/declutter-your-security-how-data-classification-aids-loss-prevention/

ROCK, Tracy, 2024. What is the Cost of Data Loss in 2024? *Invenio IT* [online]. Dostupné z: https://invenioit.com/continuity/cost-of-data-loss/

RUOHONEN, Jukka a Kalle HJERPPE, 2022. The GDPR enforcement fines at glance. *Information Systems* [online]. **106**, 101876. Dostupné z: doi:10.1016/j.is.2021.101876
STEWART, 2023. *Top 10 most expensive cyber attacks in history | EM360* [online]. Dostupné z: https://em360tech.com/top-10/expensive-cyber-attacks

STOLFO, Salvatore J., Steven M. BELLOVIN, Angelos D. KEROMYTIS, Shlomo HERSHKOP, Sean W. SMITH a Sara SINCLAIR, 2008. *Insider attack and cyber security* [online]. Dostupné z: doi:10.1007/978-0-387-77322-3

TRIPATHI, Manas a Arunabha MUKHOPADHYAY, 2020. Financial Loss due to a Data Privacy Breach: An Empirical Analysis. *Journal of Organizational Computing and Electronic Commerce* [online]. **30**(4), 381–400. Dostupné z: doi:10.1080/10919392.2020.1818521

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ, 2024. *ÚOOÚ* [online]. Dostupné z: https://uoou.gov.cz/

VANDERBURG, Eric, 2023. Security and Compliance Synergies with DLP and SIEM. *TCDI* [online]. Dostupné z: https://www.tcdi.com/security-compliance-synergies-dlp-siem/

WAZIRI, Victor O., Ismaila IDRIS, John K. ALHASSAN a Bolaji O. ADEDAYO, 2016. Data Loss Prevention and Challenges Faced in their Deployments. *International Conference on Information and Communication Technology and Its Applications (ICTA 2016)* [online]. Dostupné z: https://ceur-ws.org/Vol-1830/Paper17.pdf

ZOU, Han a Guohua CHEN, 2023. Reversible data hiding in encrypted image with local-correlation-based classification and adaptive encoding strategy. *Signal Processing* [online]. **205**, 108847. Dostupné z: doi:10.1016/j.sigpro.2022.108847

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů

8.4 Seznam použitých zkratek

DLP = Data Loss Prevention / Data Leak Prevention
GDPR = General Data Protection Regulation
ZZOÚ = Zákon o ochraně osobních údajů
ÚOOÚ = Úřad pro ochranu osobních údajů
IKB = Informační a kybernetická bezpečnost
ICT = Information and Communication Technologies