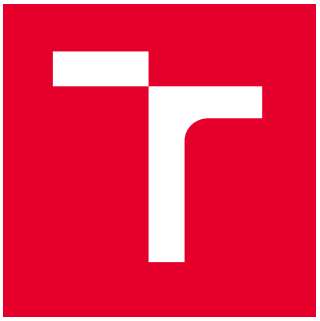


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NASAZENÍ DLP ŘEŠENÍ V ENERGETICKÉ SPOLEČNOSTI

DEPLOYMENT OF A DLP SOLUTION IN AN ENERGY COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Adam Přikryl**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Adam Přikryl**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2023/24
Studijní program:	Informační management

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

Nasazení DLP řešení v energetické společnosti

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Cílem práce je posouzení nasazení DLP řešení ve společnosti.

Základní literární prameny:

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN isbn978-80-88260-39-4.

SEDLÁK, Petr a KONEČNÝ, Martin, 2023. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2023/24

V Brně dne 4.2.2024

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práce se zabývá posouzením nasazení DLP řešení v energetické společnosti se zvážením přechodu na jiného dodavatele. První část shrnuje teoretická východiska potřebná pro pochopení problematiky ochrany dat a DLP systémů. V druhé části je provedena analýza současného stavu společnosti s analýzou vybraných částí. Třetí část představuje návrh řešení, ten se opírá o teoretická východiska a analýzu současného stavu, zahrnuje popis systémů, návrh přechodu na jiného dodavatele a ekonomické zhodnocení.

Klíčová slova

DLP, Data Loss Prevention, ochrana dat, bezpečnost dat, únik dat, bezpečnost informací, ISMS, kybernetická bezpečnost

Abstract

The diploma thesis deals with the assessment of the deployment of DLP solutions in an energy company with the consideration of transition to another supplier. The first part summarizes the theoretical background needed to understand the issues of data protection and DLP systems. The second part provides an analysis of the current state of the company. The third part presents a proposed solution, which is based on the theoretical background and analysis of the current state, includes a description of the systems, a proposal for switching to another supplier and an economic evaluation.

Key words

DLP, Data Loss Prevention, data protection, data security, data leak, information security, ISMS, cyber security

Bibliografická citace

PŘIKRYL, Adam. *Nasazení DLP řešení v energetické společnosti*. Brno, 2024. Dostupné také z: https://www.vut.cz/studenti/zav-prace/detail/158750. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. 97 s, Vedoucí práce Petr Sedlák.

Čestné prohlášení

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

V Brně dne 13. 5. 2024

Bc. Adam Přikryl

autor

Poděkování

Tímto bych velmi rád poděkoval vedoucímu práce Ing. Petru Sedlákovi za připomínky a čas věnovaný mé práci. Dále bych rád poděkoval Ing. Jindřichovi Veselému, MBA. a ostatním zaměstnancům oddělení ochrany dat a informační bezpečnosti za předané zkušenosti a ochotu.

OBSAH

ÚVOD

V současném světě informačních technologií, digitální transformace a rostoucí kybernetické kriminality je ochrana citlivých dat zcela zásadní výzvou pro každou organizaci. Data představují jedno z nejcennějších aktiv organizací. Společnosti vytvářejí, zpracovávají, shromažďují a uchovávají stále větší a větší množství dat. Jejich únik může mít řadu dopadů, jako právní postihy, finanční ztráty či ztrátu obchodního tajemství. Prevence úniku důvěrných informací proto představuje kritický bezpečnostní požadavek, a to zejména pro firmy ze strategických odvětví jako je energetika.

Příčinami úniku dat bývají krádeže, ale i interní faktory, a to hlavně nepozornost zaměstnanců. Tyto úniky lze nejen detekovat, ale také je zastavit. K tomu může přispět zasazení technologie DLP (Data Loss Prevention) k ostatním opatřením chránící data. DLP systémy představují komplexní opatření pro monitorování, detekci a prevenci úniků citlivých dat z organizace. Jelikož se jedná o komplexní systémy, je třeba aby byly pro správné a efektivní využití řádně spravovány, integrovány do stávajících systémů v organizaci a měly vhodně nastaveny politiky.

Tato práce se zabývá posouzením nasazení systému prevence úniku dat (DLP) se zvážením přechodu na jiného dodavatele v nadnárodní energetické společnosti. Společnost využívá DLP řešení od dodavatele Trellix. S rozvojem informačních technologií, rostoucími požadavky na efektivitu a snižováním provozních nákladů se oddělení informační bezpečnosti společnosti rozhodlo zvážit přechod na DLP řešení od společnosti Microsoft, které má nižší náklady na vlastnictví a umožní centralizaci správy bezpečnostních nástrojů.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem diplomové práce je posouzení nasazení DLP řešení ve společnosti se zvážením přechodu na jiného dodavatele. Posouzení se týká nadnárodní energetické společnosti. Společnost má již nasazené DLP řešení, ale zvažuje přechod k jinému dodavateli z důvodů usnadnění správy, úspory nákladů a lepší integraci s ostatními nástroji. Práce je rozdělena na tři hlavní části.

První část shrnuje teoretická východiska nutná pro pochopení řešené problematiky a ze kterých vychází návrh řešení. V druhé části je provedena analýza současného stavu, je zde představena společnost, její činnost, struktura a klíčové části.

Ve třetí části je obsažen návrh vlastního řešení. Je popsán současný nástroj a jeho nasazení, které je následováno popisem zvažovaného nástroje. V druhé polovině návrhové části je popsána problematika přechodu a jsou uvedeny důvody pro přechod s požadavky na DLP řešení. Následně jsou identifikovány intervenční oblasti, do kterých by změna mohla zasáhnout a klíčové role pro úspěšnou realizaci změny. Následně jsou navrženy činnosti migrace a rizika, včetně jejich opatření, která by migraci mohla ohrozit. Ke konci návrhu řešení je provedeno zhodnocení DLP systémů a možné migrace. Na závěr jsou ekonomicky zhodnoceny náklady na projekt migrace.

1 TEORETICKÁ VÝCHODISKA

Tato část práce zpracovává teoretická východiska, která je dobrá znát k porozumění zbytku řešené problematiky, ze kterých vychází návrhová část práce.

1.1 Základní pojmy

Data

Data lze definovat jako základ, ze kterého vychází informace a tím i znalosti, jsou tedy plněním informace, kterou tvoří. Sama o sobě nemusí nést žádný význam. Jedná se o surové, nezpracované posloupnosti znaků, nebo i fakta a čísla, například jména a čísla v tabulkách. V informatice lze obrátit logiku a data definovat informací, data tedy lze chápat jako opakovaně interpretovatelnou a formalizovanou podobu informace vhodnou pro komunikaci, vyhodnocování a zpracování (nejčastěji za použití ICT techniky). [1; 2]

Informace

Jsou to organizovaná a kontextualizovaná data, která dávají konkrétní význam. Jsou často uložená v dokumentech a jiných souborech. Lze ji také definovat jako pojem popisující formou údajů reálné prostředí a procesy, které v něm probíhají. V informatice je tvořena kódovanými daty (fyzikálně interpretovaná na úložném zařízení). [1; 2]

Informační systém

Systém vzájemně propojených procesů a informací se kterými pracují. Systém jako funkční celek zabezpečuje shromažďování, zpracování, uchovávání a zpřístupňování informací a dat. Zahrnuje zdroje dat i informací, nosiče, programové a pracovní prostředky , postupy, technologie i pracovníky. [1; 3]

Síťová infrastruktura

Jedná se množinu síťových prvků a technických zařízení zajišťujících možnost komunikace v ICT prostředí. Fyzicky se jedná o kabelážní systémy a aktivní prvky sítě. Může se také označovat aktiva v oblasti ICT pro podporu a tvorbu informačních systémů. [1]

Kritická infrastruktura

KI je prvek nebo systém prvků (stavby, zařízení, prostředky a veřejná infrastruktura), jejichž narušení by mělo závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu, zdraví osob a zabezpečení základních životních potřeb obyvatelstva. Kritická informační infrastruktura (KII) je prvek KI v odvětví komunikačních a informačních systémů, jestliže je tento IS, služba nebo ICT pro provoz daného prvku KI nenahraditelný (jedná se o takové o informační a komunikační systémy a technologie, které naplní kritéria pro určení prvků KI, např. dohledové systémy SCADA). [1]

1.1.1 Kybernetická a informační bezpečnost

Bezpečnost informací

Bezpečnost informací (nebo také informační bezpečnost) se zabývá ochranou a dostupností informací. Cílem je zajistit, aby informace byly přístupné oprávněným subjektům, byly chráněné před neoprávněným přístupem a nebyly poškozeny nebo zneužity. Spolu se zajištěním bezpečnosti IS/ICT ji lze zahrnout do bezpečnosti organizace, která má za úkol zajištění objektů a majetku organizace. Kromě bezpečnosti IS/ICT na průniku s kybernetickou bezpečnosti (bezpečnost IS/ICT chránící aktiva, která jsou součástí IS a podporovaná ICT) zahrnuje také bezpečnost informací v nedigitální podobě. [1; 3]

CIA

Vztahuje se k bezpečnosti informací, jejíž úlohou je zachování této triády. Skládá se ze tří částí:

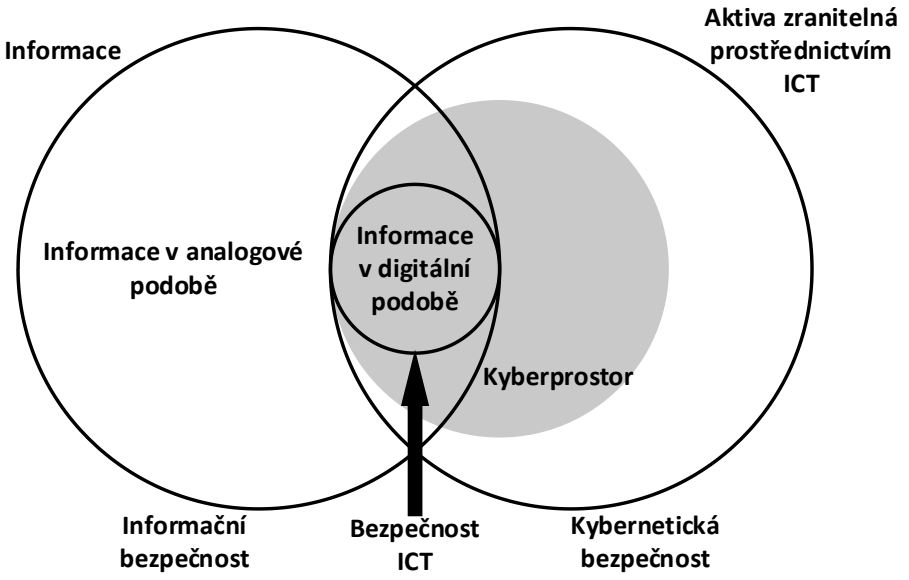
- Důvěrnost (Confidentiality) – k informaci mají přístup pouze oprávněné osoby;
- Dostupnost (Availability) – informace je přístupná oprávněnému uživateli v požadovaný okamžik;
- Integrita (Integrity) – informace je správná a úplná. [1; 4]

Kybernetická bezpečnost

Podobně jako bezpečnost informací je to souhrn technických, organizačních a vzdělávacích prostředků s cílem zajištění ochrany aktiv v kybernetickém prostoru.

Kybernetický prostor (Cyberspace) je globální digitální prostředí, které se skládá z internetu a dalších počítačových sítí, informačních systému, služeb a procesů na nich. Tím zajišťuje infrastrukturu pro vznik, zpracování a výměnu informací, které umožňují osobní, podnikatelské a správní aktivity a jejich propojení. Kybernetická bezpečnost tak chrání osoby, organizace a národy před digitálními hrozbami. [2; 3]

Rozdílem mezi informační a kybernetickou bezpečností je, že cílem informační bezpečnosti je zejména chránit důvěrnost, dostupnost a integritu informací, zatím co kybernetická bezpečnost má za cíl řešení kybernetických incidentů a ochranu jiných aktiv než jen informací. [3]



Obrázek č. 1: Vztah informační a kybernetické bezpečnosti
(Zdroj: 3)

1.1.2 ISMS

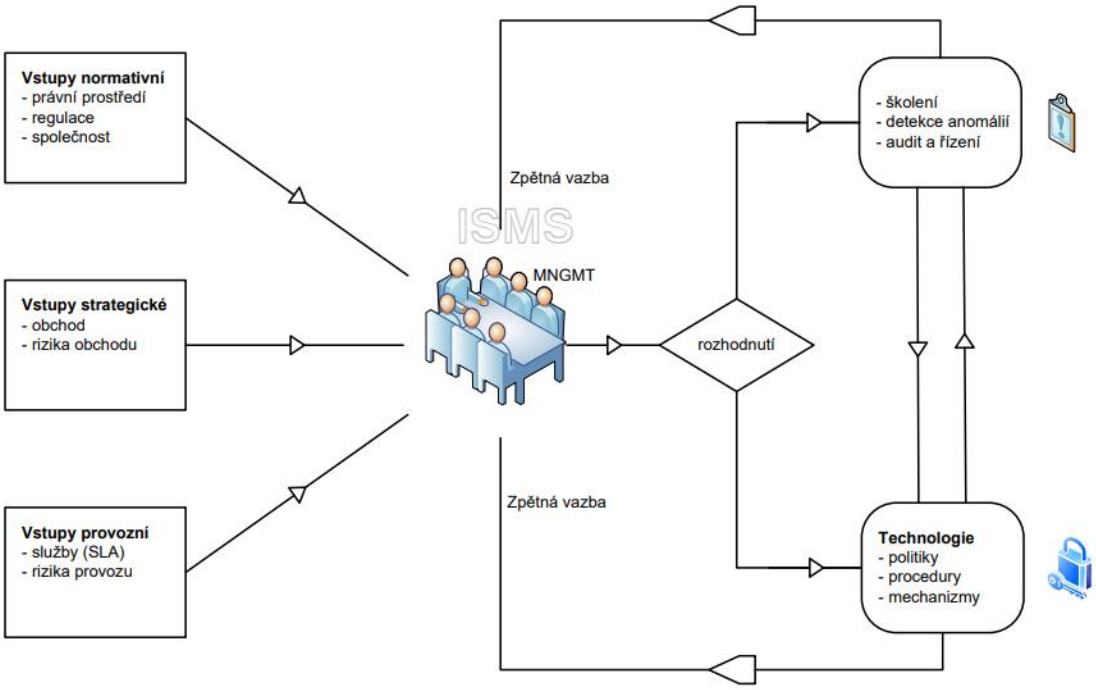
Systém řízení informační bezpečnosti (Information Security Management System) se skládá ze zásad a činností, které organizace kolektivně řídí za účelem ochrany svých informačních aktiv. Jedná se tedy o zavádění, řízení, udržování a zlepšování informační bezpečnosti organizace, jako takový musí být součástí celkového systému řízení organizace. Jako spousta jiných aspektů informační a kybernetické bezpečnosti se řídí PDCA (Demingovým) modelem. [1; 4]

- **Plan** – určení rozsahu a odpovědností (ustanovení ISMS);
- **Do** – výběr a zavedení bezpečnostních opatření (zavedení ISMS);

- **Check** – zajištění zpětné vazby (monitorování a přezkoumávání ISMS);
- **Act** – odstraňování slabin a průběžné zlepšování (údržba a zlepšování ISMS). [1]

K úspěšné realizaci systému také přispívá zavedení následujících principů:

- povědomí o potřebě bezpečnosti informací
- přidělení odpovědnosti za bezpečnost informací
- začlenění závazku vedení a zájmů zainteresovaných stran
- posouzení rizik a určení vhodných opatření k dosažení přijatelné úrovně rizika
- začlenění bezpečnosti jako základního prvku informačních sítí a systémů
- aktivní prevence a odhalování incidentů
- zajištění komplexního přístupu k řízení bezpečnosti informací
- průběžné přehodnocování a provádění případných úprav [4]



Obrázek č. 2: Struktura ISMS
(Zdroj: 1)

Aktivum

Aktivum (Asset) v oblasti IT představuje cokoliv, co má pro organizaci nějakou hodnotu, tedy veškerý hmotný a nehmotný majetek organizace, který má smysl chránit. [1]

- Hmotná aktiva – převážně technické prostředky výpočetní techniky (počítače, tiskárny, aktivní a pasivní prvky síťové infrastruktury a ostatní zařízení)
- Nehmotná aktiva
    - Data – vytvořená činností organizace anebo převzatá z vnějšího prostředí, která jsou důležitá pro její provoz;
    - Pracovní postupy – postupy využívané v organizaci v oblasti IS/ICT;
    - Programové vybavení – základní programové vybavení (OS, SW potřebný pro provoz počítačových sítí, kryptografické systémy atd.) a aplikační programové vybavení (textové editory, tabulkové kalkulátory, ERB, BI aplikace atd.);
    - Služby – komunikační a počítačové služby a základní služby (zajištění provozu, např. světlo, vytápění apod.). [2; 3]

Událost

Událost, která může způsobit stav systému, služby nebo sítě, ve kterém je možnost porušení bezpečnosti informací, předpisů, nebo selhání kontrolních mechanismů, nebo dříve neznámá situace, která může být bezpečnostně relevantní. [4]

Incident

Jednotlivá nebo řada nechtěných nebo neočekávaných událostí v oblasti bezpečnosti informací, které mají významnou pravděpodobnost ohrožení obchodních operací a narušení bezpečnosti informací. [4]

Hrozba

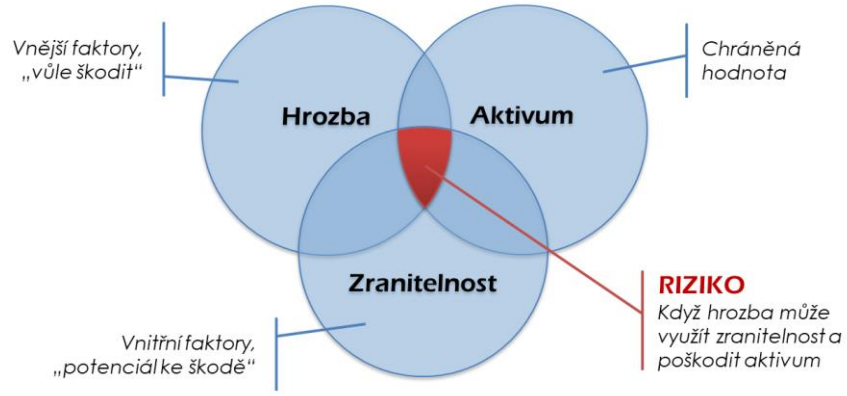
Potenciální příčina nechtěné události nebo incidentu, jejichž výsledkem může být poškození organizace nebo jejich systémů. [3]

Zranitelnost

Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami. Je to vnitřní vlastnost aktiva, která může negativně působit na aktivum. [1]

Riziko

Pravděpodobnost, že hrozba využije zranitelnosti aktiva nebo jejich skupiny a tím způsobí bezpečností událost a škodu organizaci. [2]



Obrázek č. 3: Aktivum, hrozba, zranitelnost a riziko
(Zdroj: 1)

PDCA

Také Demingův cyklus. Jedná se o metodu schématického znázornění životního cyklu systému řízení a postupného zlepšování formou opakovaného provádění čtyř činností. [1; 3]

- Plan (plánuj) – naplánování zamýšleného zlepšení.
- Do (dělej) – realizace plánu.
- Check (kontroluj) – ověření výsledků realizace a průběžné monitorování.
- Act (jednej/zlepšuj) – úpravy cíle a provedení na základě kontroly a zavedení zlepšení do praxe. [1]

Koncept zavedl W. E. Deming a formuloval pomocí něj zásady na vymezení systému řízení, jeho realizaci a neustále zlepšování. Využíván je v mnoha oblastech pro zdokonalování procesů, výrobků služeb, aplikací, systémů řízení a v rámci standardů v oblasti ISM (Information Security Management). [3]

1.2 Data v prostředí organizace

Tempo růstu množství dat celosvětově zrychluje, mezi roky 2013 a 2020 se množství vygenerovaných dat minimálně zdesetinásobilo (za rok 2020 to bylo 45 ZB). Pro podniky platí to samé: neustále generují větší a větší množství dat, z toho roste pro podniky potřeba jejich data efektivně spravovat a chránit. [1]

1.2.1 Typy dat

Data lze v podniku rozdělit mnoha způsoby, například podle toho, čeho se týkají (osobní data, data o trzích, výrobcích atd.) nebo také jejich důvěrnosti a struktury, pro problematiku této práce je podstatná právě důvěrnost a struktura dat.

Data a informace, které tvoří se řadí mezi informační aktiva, v rámci ISMS je tedy třeba provést jejich klasifikaci, ta se provádí podle klasifikačního schématu. Nejčastěji se pro důvěrnost v komerční sféře používají čtyři stupně. [1]

- Veřejné – veřejně známé informace;
- Interní – informace vytvořené zaměstnanci ;
- Důvěrné/citlivé – s negativním dopadem na organizaci;
- Přísně důvěrné/velmi citlivé – se zničujícím dopadem na organizaci. [1]

Uváděn je i stupeň soukromé, který lze zařadit do klasifikace důvěrné/citlivé, obsahují osobní údaje o zaměstnancích a zákaznících.

Z hlediska ukládání a organizace dat a práci s nimi lze rozlišovat na strukturovaná a nestrukturovaní data.

Strukturovaná

Data například uložená v tabulkách a relačních (SQL) databázích. Jsou tedy organizována předem definovaným způsobem a mezi jednotlivými daty (data point) a datovými struktury jsou modelem jasně definované vazby. Mohou být generovány automaticky senzory, weblogy, síťovými zařízeními., ale také lidmi vyplňováním tabulek apod. Nejčastěji se jedná o textová data, ale mohou to být i obrázky, zvuky a videa. [5]

Nestrukturovaná

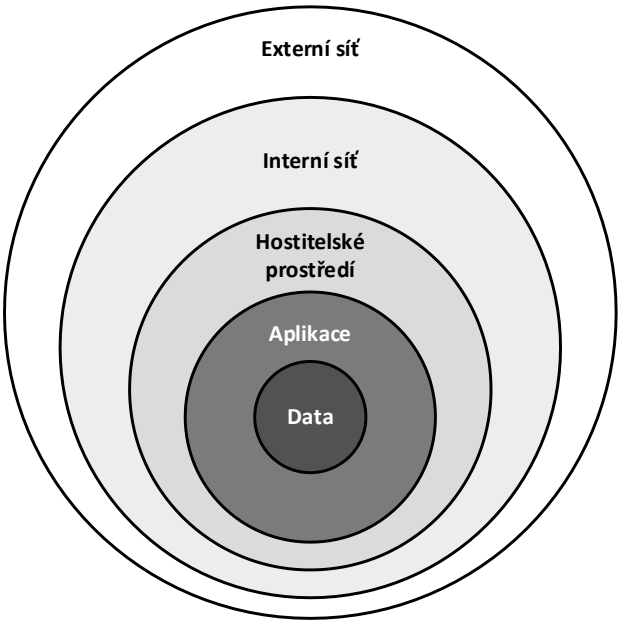
Neorganizovaná data, která nemají definovány vztahy mezi jednotlivými daty (data point). Jedná se o prostý text (tok bytů). Ukládány jsou v nerelačních databázích. Hůře se na nich provádí analýza, protože je třeba zkoumat po jednotlivých částech. Většina dat je v nestrukturovaných formátech (odhaduje se kolem 80 %). [5]

1.2.2 Ochrana a zabezpečení dat

Problematiku lze rozdělit do více oblastí.

- Ochrana dat (Data Protection) – ochrana dat a informací před ztrátou například pomocí zálohování.
- Zabezpečení dat (Data Security) – ochrana integrity dat pomocí opatření proti manipulaci a malwaru, týká se vnitřcích i vnějších hrozeb.
- Ochrana osobních údajů (Data Privacy) – ochrana a kontrola přístupu k osobním údajům, týká se nařízení GDPR. [1]

Jako základní opatření zajišťující ochranu a zabezpečení dat lze uvést kryptologii, IDS (Intrusion Detection System) a IPS (Intrusion Prevention System) a DLP systémy. Na zabezpečení a ochranu dat je možné nahlížet skrz vrstvové modely, jeden z nich byl z části představen v podkapitole 1.1.1, kde nejvyšší úrovní je bezpečnost organizace (zajištění majetku organizace, například kontrolou přístupů, strážní službou apod.), pod ni spadá bezpečnost informací, ve které nejužší část představuje bezpečnost IS/ICT. Dalším možným pohledem je také model vrstev kybernetické bezpečnosti s vertikálními vrstvami. Vrstvy kybernetické bezpečnosti odpovídají opatřením a implementaci technologií kybernetické bezpečnosti v jednotlivých vrstvách, tento model se také nazývá hloubková ochrana. [1; 3]



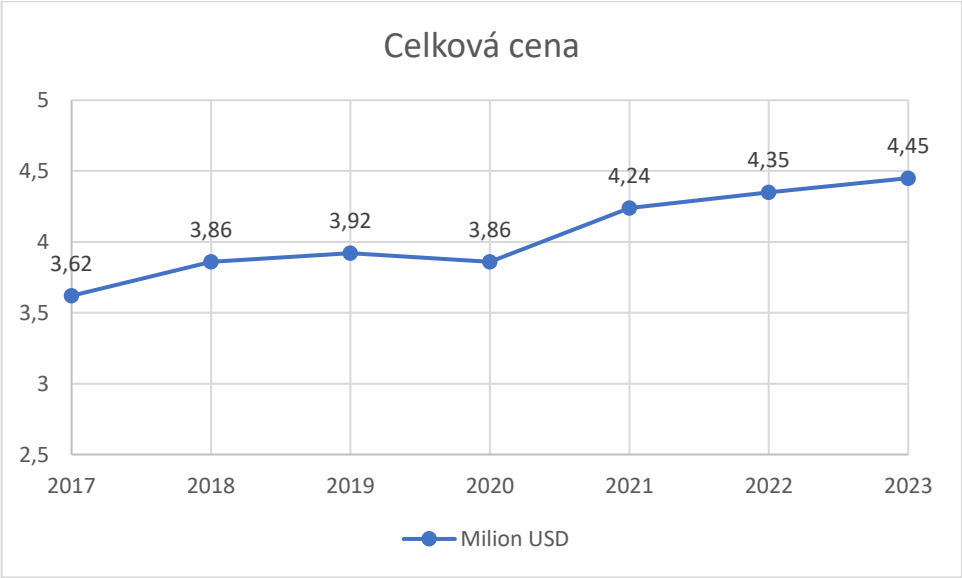
Obrázek č. 4: Vrstvy kybernetické bezpečnosti
(Zdroj: Vlastní zpracování dle [2])

1.2.3 Úniky dat

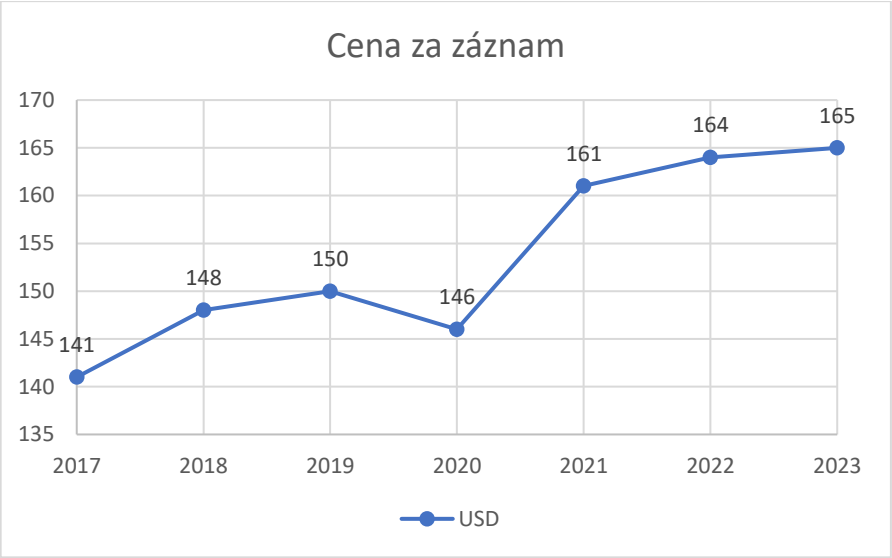
Krádeže a úniky dat se v současně stávají nejčastějším dopadem na organizace. Podle reportu IBM *X-Force Threat Intelligence Index* představovaly úniky a krádeže dat v roce 2023 s nejčastější dopad útoku na organizaci a to ve 32 % procentech případů, oproti 19 % v roce 2020. Tato část vychází ze dvou reportů (zpráv) společnosti IBM, a to *Threat Intelligence Index* a *Cost of Data Breach*. První vychází z činnosti týmu X-Force zaměřujícího se na monitorování kybernetických hrozeb, který sleduje více než 150 miliard bezpečnostních událostí denně ve více než 130 zemích. Druhý je vytvořen ve spolupráci s Ponemon Institute a vychází ze zkoumání více než 550 organizací, které byly postiženy únikem dat. [6; 7]

Vývoj ceny

Celkové náklady na narušení bezpečnosti dat i cena za záznam má v posledních letech téměř neustálý rostoucí trend. V roce 2023 byla průměrná celková škoda 4,45 milionů USD a cena za záznam 165 USD. Vývoj ceny je zachycen na následujících dvou obrázcích. [7]



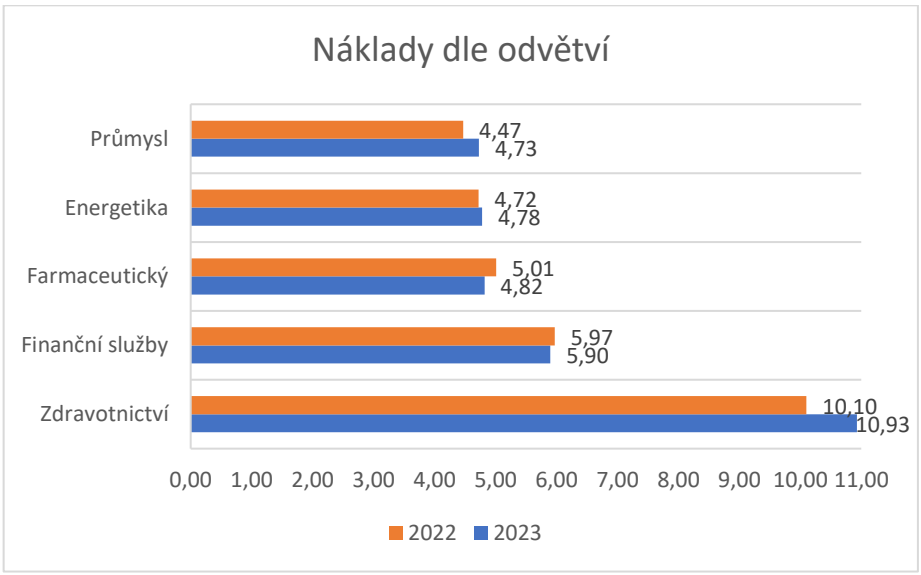
Obrázek č. 5: Celkové náklady narušení dat
(Zdroj: Vlastní zpracování dle [7])



Obrázek č. 6: Cena za záznam
(Zdroj: Vlastní zpracování dle [7])

Energetika

Energetický průmysl představoval čtvrtou nejčastěji obecně napadanou oblast, reprezentující 11,1 % útoků, nejvíce jich proběhlo na území Evropy. Nejčastější metodou útoku byl malware a nejčastějším dopadem byla krádež a únik dat, a to ve 33 % sledovaných případů. V případě narušení dat jsou pro energetický průmysl čtvrté nejvyšší náklady a to 4,78 mil. USD, celkově energetika zastupovala 5. nejčastější obor ze zkoumaných společností (8 %). [7]

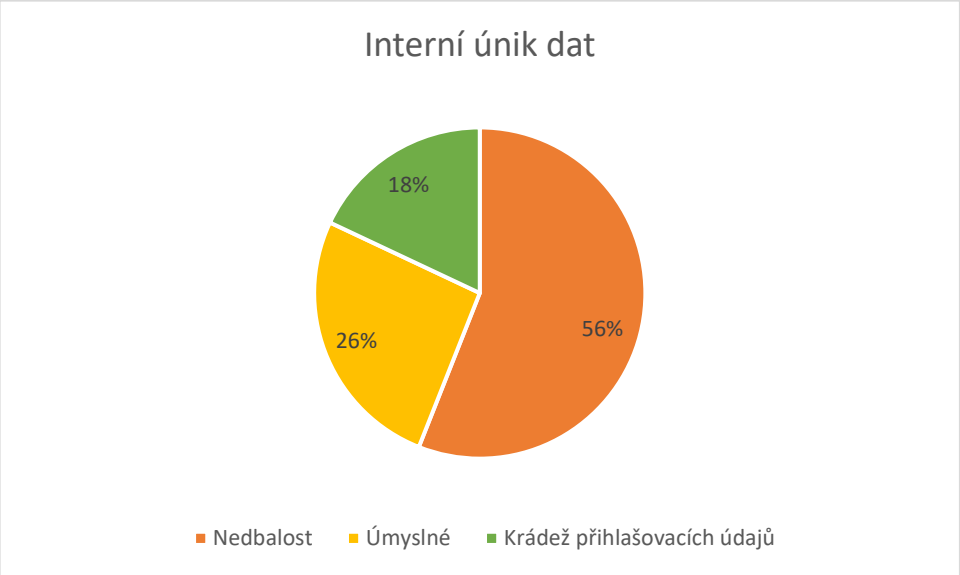


Obrázek č. 7: Náklady dle odvětví v milionech USD
(Zdroj: Vlastní zpracování dle [7])

Vektory úniku

Interní úmyslné a neúmyslné úniky tvořily za rok 2023 dohromady celkem 12 % (úniky způsobené úmyslně i omylem tvořily každý 6 %) z celkových úniků dat. Útoky iniciované interními útočníky (insidery) byly navzdory relativní vzácnosti nejnákladnější, s náklady 4,9 mil. USD, což je o 9,6 % vyšší hodnota než světový průměr. [7]

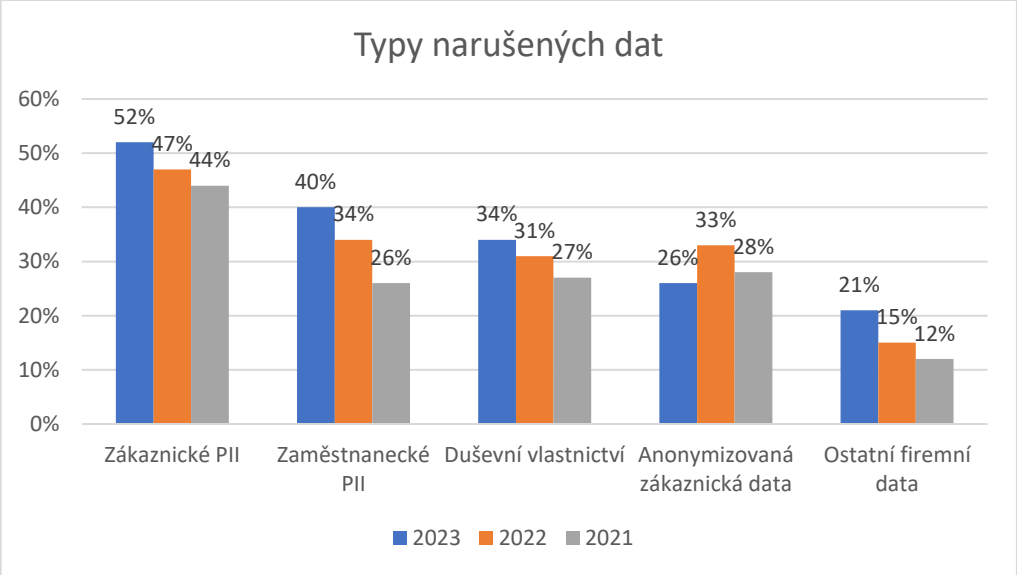
Tyto čísla se ale týkají pouze úniky dat vyšetřovanými v rámci zprávy IBM *Cost of Data Breach Report*. Celkově jsou insideři bráni jsou hlavní příčina úniků dat, často neúmyslně. V důsledku digitální transformace a také pandemie a následný přesun na práci z domova se jimi způsobený počet úniků zvyšuje. Podle zpráv *2021 Data Exposure Report* od Code42 a *2022 Cost of Insider Threats Global Report* od Ponemon Instute je 56 % interních úniků dat způsobeno nedbalostí zaměstnanců (nedodržení pravidel o nakládání s citlivými daty, ztráty anebo nezajištění bezpečnosti jejich zařízení), pravděpodobnost úniku kvůli insiderům je o 85 % vyšší, než byla v době před pandemií. Podle další zprávy, *Insider Data Breach Survey 2021* od Egress, v roce 2020 94 % organizací zažilo únik dat způsobený zaměstnancem. [8; 9; 10]



Obrázek č. 8: Interní úniky dat
(Zdroj: Vlastní zpracování dle [9])

Nejčastější předměty úniku dat

Nejčastějším předmětem narušení dat byla zákaznická data, která měla také nejvyšší cenu za záznam 183 USD, druhé byla data o zaměstnancích s druhou nevyšší cenou 181 USD. Nejméně ohrožená byla obecná interní data. [7]



Obrázek č. 9: Úniky dat dle typu
(Zdroj: Vlastní zpracování dle [7])

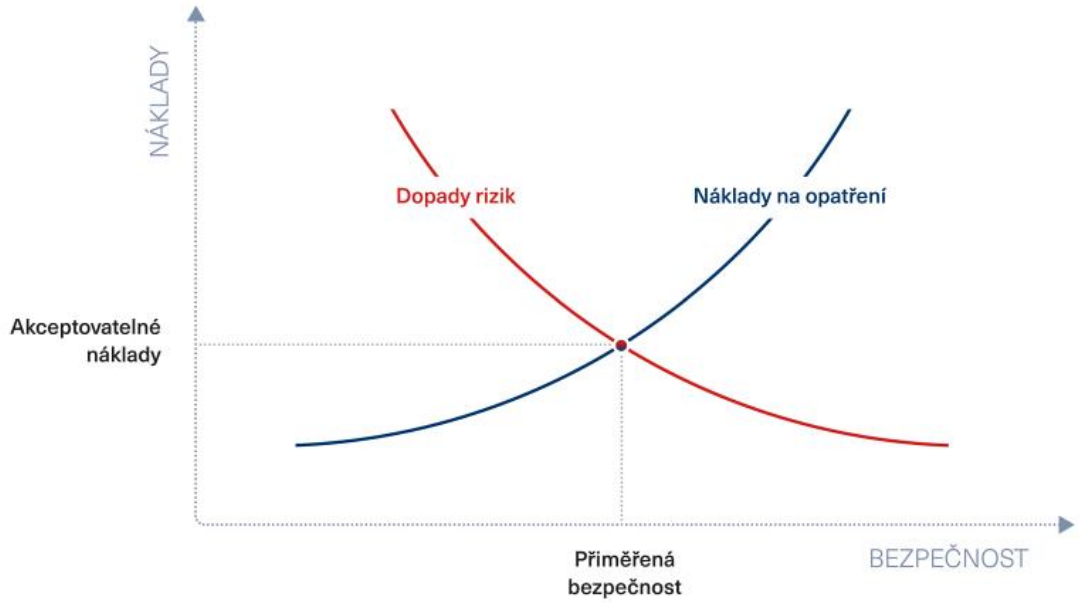
1.3 Bezpečnostní opatření

Opatření je faktor řídící a upravující riziko (snížení pravděpodobnosti nebo dopadu). Může se jednat o politiky, procesy, organizační struktury, postupy, zařízení nebo jiné prvky a/nebo akce řídící nebo upravující riziko. Dle směrnice ISO/EIC 27002 lze opatření rozdělit na organizační, personální, fyzická a technická. [1; 11]

- **Organizační a personální opatření** – lze tako nazvat jako administrativní opatření. Zahrnují například směrnice pro práci s IS/ICT a definování procesů, může se jednat o specifikaci klasifikace informací a pravidel nakládání s nimi, nebo pravidla pro práci na dálku a zavedení dohody o mlčenlivosti (NDA) pro zaměstnance apod. [3; 11]
- **Fyzická opatření** – Patří mezi ně stanovení fyzických bezpečnostních perimetrů, kontrola vstupů, používání zámků, používání čipových karet při vstupu do hlídaných prostorů atd. [3; 11]

- **Technická a technologická opatření –** např. autentizace a autorizace, oddělení přístupových práv, zaznamenávání logů a také prevence úniku dat. [1; 11]

Velikost investice do bezpečnosti musí odpovídat hodnotě ohrožených aktiv a mírám možných rizik stanovenými bezpečností politikou organizace. Náklady na opatření by neměly být vyšší než náklady na podstoupení rizika. Tuto problematiku znázorňuje graf na obrázku č.10. [1]



Obrázek č. 10: Přiměřená bezpečnost
(Zdroj: 1)

1.4 DLP systémy

Zkratka DLP nemá jednoznačný význam, nejčastěji se můžeme setkat s Data Loss Prevention, tedy ochranou (prevencí) před ztrátou dat, ale můžeme také narazit na Data Loss Protection, Data Leak Prevention či Data Leak Protection. V tomto případě nastává mírná změna významu, protože Leak lze přeložit jako únik, tedy ochrana (prevence) před únikem dat. Únik i ztráta dat mohou být úmyslnou či neúmyslnou hroznou, únik lze chápat jako převážně narušení důvěrnosti dat a jejich přenos do prostředí mimo organizaci, kdežto ztrátu dat jako interní či externí narušení dostupnosti nebo integrity dat, tedy jejich ztrátu či poškození. Nicméně, DLP systémy mají nezávisle na významu zkratky danou funkci – identifikovat, monitorovat a chránit data organizace. Nejčastěji se

specializují na ochranu před úmyslnými a neúmyslnými interními hrozbami týkající se úniku dat. [1; 12]

Data chrání skenováním dat, identifikováním a monitorováním citlivých dat a aplikováním příslušné politiky (zablokování, upozornění, žádost o odůvodnění apod.).

DLP opatření jsou popsaná normou ISO/EIC 27002 jako Data leakage prevention (prevence úniku dat) v části technických opatření. Měly by být nasazeny na systémy, sítě a jakákoliv zařízení, která zpracovávají, ukládají nebo přenáší citlivé informace za účelem detekce a prevence neoprávněného získání a vyzrazení informací jednotlivci nebo systémy. [11]

Tabulka č. 1: Taxonomie DLP dle ISO/EIC 27002:2022

Typ opatření	Vlastnosti bezpečnosti informací	Koncepty kybernetické bezpečnosti	Provozní schopnosti	Domény bezpečnosti
# Preventivní # Detekční	# Důvěrnost	# Ochrana # Detekce	# Ochrana informací	# Ochrana # Obrana

(Zdroj: 1; 11)

1.4.1 Analýza dat DLP

Aby mohly DLP systémy monitorovat a chránit citlivá data, musí být schopné citlivá data identifikovat. Pro identifikaci provádí analýzu dat, dle které je možno provést klasifikaci. K identifikaci dat se přistupuje dvěma způsoby: na základě kontextu a na základě obsahu. [14]

Na základě kontextu

Kontextová analýza zahrnuje prostředí obsahu a jeho použití. V nejjednodušší formě se jedná o skenování hlaviček e-mailů a metadat souborů. Analýzou transakcí v kontextu jsou zahrnovány atributy jako místo kde data vznikla a kde se nacházejí, odesílatel, datový objekt, médium, čas, příjemce atd. Vyhodnocována je i řada dalších faktorů, jako: [13; 14]

- Vlastnictví a oprávnění k souborům;

- Využití šifrovaných formátů nebo síťových protokolů;
- Role uživatele a obchodní jednotka (v případě integrace adresáře, např. AD);
- Konkrétní webové služby;
- Webové adresy;
- Používané aplikace (např. rozpoznání, že něco bylo zkopírováno z dokumentu Office a vloženo do jiného);
- Informace o zařízení. [14]

Kontextová analýza poskytuje oporu pro analýzu obsahu, na data není nahlíženo ve vakuu, ale v kontextu jejich použití v organizaci a zohlednění různých aspektů od role autora souboru až po používané aplikace. [14]

Na základě obsahu

DLP systémy k této analýze využívají tzv. file cracking (prolamování souborů). File cracking je technologie, která umožňuje analyzovat obsah souboru, i když je jeho obsah uložen ve více vrstvách. Například je možné číst obsah buňky v Excelové tabulce souboru, která je vložena do souboru MS Word a ten je následně zazipovaný. Systémy jsou schopny rozbalit zip soubor, přečíst zanalyzovat Word dokument, najít Excelová data a ta také přečíst a analyzovat. Dalším příkladem je PDF vložené do CAD souboru. Některé nástroje mohou analyzovat i zašifrovaná data za použití podnikových obnovovacích šifrovacích klíčů. Většina dokáže identifikovat standardní šifrování a použít ho jako vodítko k blokování nebo karanténě obsahu. Celkově nástroje podporují mnoho typů souborů a jazyků (včetně asijských) a extrahování prostého textu z neidentifikovatelných typů souborů. [14]

Po zpřístupnění obsahu pomocí file crackingu se pro analýzu na základě obsahu využívá řada technik:

- **Založené na pravidlech a obecných výrazech** (RegEx): Porovnává obsah pomocí specifických pravidel a RegEx pro detekci strukturovaných dat jako jsou čísla kreditních karet, rodná čísla a čísla smluv. Nejlépe se hodí jako prvotní filtr snadno identifikovatelných dat.
    - Výhody: Snadno srozumitelná a použitelná technika, při které jsou pravidla zpracovávána rychle.

    - Nevýhody: Náchylnost k vyšší míře false positive výsledků a malá ochrana pro nestrukturovaný obsah. [14]
- **Database fingerprinting/Exact Data Matching:** Využívá připojení k databázi na hledání přesných shod nebo kombinace informací (např. jméno + příjmení + rodné číslo) Nejlépe se hodí pro strukturovaná data.
    - Výhody: Málo false positive výsledků a chránění skutečně citlivých údajů za ignorování běžně používaných podobných údajů.
    - Nevýhody: Při použití zálohy databáze nejsou zahrnuty nová data a při živém připojení může ovlivňovat výkon. [14]
- **Přesná shoda souborů** (Exact File Matching): Vytváří hashe (otisk souboru ve formě jedinečné sestavy znaků) důležitých souborů a monitoruje shody s těmito otisky. Nejlépe se hodí pro multimediální soubory a další binární soubory, kde není možná textová analýza.
    - Výhody: Funkčnost na všech typech souborů, nízký počet false positives.
    - Nevýhody: Vysoký počet false negatives, protože je snadné ji obejít upravením dat a tím změnou hashe, což činí tuto techniku nepoužitelnou pro upravený obsah. [14]
- **Částečná shoda dokumentů:** Tato technika hledá úplné nebo částečné shody s chráněným obsahem, DLP řešení hledá kompletní text nebo úryvky podle vytvořených zásad ochrany citlivého dokumentu. Je účinná při ochraně nestrukturovaných dat.
    - Výhody: Nízký počet false positives, oproti přesné shodě může najít porušení zásad i pro část textu.
    - Nevýhody: Omezení objemu chráněných dat, velký počet frází nebo obecná slovní spojení mohou vyvolat false positives – je třeba rozhodnout, které dokumenty je třeba chránit. [14]
- **Statistická analýza:** Využívá strojové učení, Bayesovskou analýzu a další statistické techniky k analýze vzorů obsahu a nalezení porušení politik u obsahu podobného chráněnému obsahu. Nejlépe se hodí pro nestrukturovaný obsah, kde by deterministické techniky jako hledání shody dokumentů nebyly účinné, jako například databáze, která je objemná a často se mění.

    - Výhody: Funguje u obsahu, u kterého není možné snadno izolovat přesné dokumenty nebo části pro porovnání. Politiky typu: Zablokovat vše odchozí, co se podobá dokumentům v určitém adresáři.
    - Nevýhody: Náchylná na false positives i negatives a vyžaduje velký objem zdrojového obsahu pro trénování. [14]
- **Konceptuální/lexikální:** Tato technika používá kombinaci slovníků, pravidel a dalších analýz k ochraně nejasného obsahu, který připomíná "myšlenku". Například upozornění na komunikaci, která se podobá insider tradingu (obchodování na základě neveřejných informací), provozování soukromého podnikání z pracovního zařízení atd. Vzory vyhledává pomocí klíčových frází, počtu slov a pozic. Nejlépe se hodí pro zcela nestrukturované myšlenky, které nelze kategorizovat, ale jsou podobné jiným známým zdrojům.
    - Výhody: Dokáže najít volně definovaná porušení zásad, která nejsou popsatelné pomocí konkrétních příkladů .
    - Nevýhody: Díky volným definicím náchylná k false positives i negatives a ve většině případků musí být pravidla se značným úsilím vytvořena dodavatelem DLP, zvyšujícím náklady. [14]
- **Kategorie:** Jsou to předem připravené kategorie s pravidly a slovníky pro běžné typy citlivých dat, jako čísla kreditních karet a PII. Nevjhodnější jsou pro cokoliv přesně zapadající do poskytnutých kategorií.
    - Výhody: Velmi jednoduché na konfiguraci. Politiky na základě kategorie mohou být použity jako základ pro vytvoření pokročilejších politik.
    - Nevýhody: Kvůli univerzálnosti nemusí vyhovovat specifickým potřebám organizace. Vhodné pouze pro snadno kategorizovaná pravidla a obsah. [14]

Ne všechna řešení na trhu nabízí všechny tyto techniky, ale často podporují komplexní techniky řetězení – komplexní politiky založené na kombinaci analýz na základě kontextu i obsahu. [14]

1.4.2 Data chráněná DLP systémy

Celkově lze data chráněná DLP systémy rozdělit na tři části podle stavu dat a jejich životního cyklu: v úložištích, v síti a na koncových bodech. Dělení dat je podle této logiky následující: [1; 14]

- **Data in Use** (používaná data) **–** Jejich ochrana realizována pomocí endpoint řešení, ta monitorují data na koncových stanicích při každodenní interakci se zaměstnanci. Dohlíží, jak je s daty nakládáno (kam se kopírují, jejich úpravy a kdo je používá). [1; 14]
- **Data in Motion** (data v pohybu) **–** Zabezpečení ochrany dat a datového toku spočívá v monitorování (a případném filtrování) provozu v síti s cílem identifikovat obsah odesílaný přes konkrétní komunikační kanály. Ochrana je zaměřena proti náhodným nálezcům i zlodějům, případně proti šíření dat po síti. [1; 14]
- **Data at Rest** (data v klidu) – Ochrana dat v síti, která nejsou aktivní, je realizována úložišť obsahu s cílem zjistit, kde se citlivý obsah nachází, tento proces bývá nazýván Discovery. Při nalezení citlivého obsahu na nepovoleném místě lze obsah zašifrovat nebo odstranit, případně odeslat upozornění vlastníkovi souboru. [1; 14]

1.4.3 Síťová DLP

Také Network DLP, někdy označována jako DLP bez agenta nebo bránové systémy (gateway based), poskytují kontrolu provozu, který prochází sítí. Obvykle se jedná o síťové zařízení instalované na perimetru sítě, která provádějí analýzu komunikace a vyhledávají citlivé informace v pohybu (typicky sledovanou komunikací je e-mail, FTP a HTTP(S). Oproti DLP koncových bodů jsou jednodušší na instalaci a mají nižší náklady na vlastnictví (TCO). Nevýhodou je složitější integrace a nutnost kombinace s proxy systémy pro blokování komunikace. Mohou být také ve formě softwarového modulu integrovány do firewallů na perimetru sítě. Do této části lze zařadit i další typy DLP. [1; 14; 15]

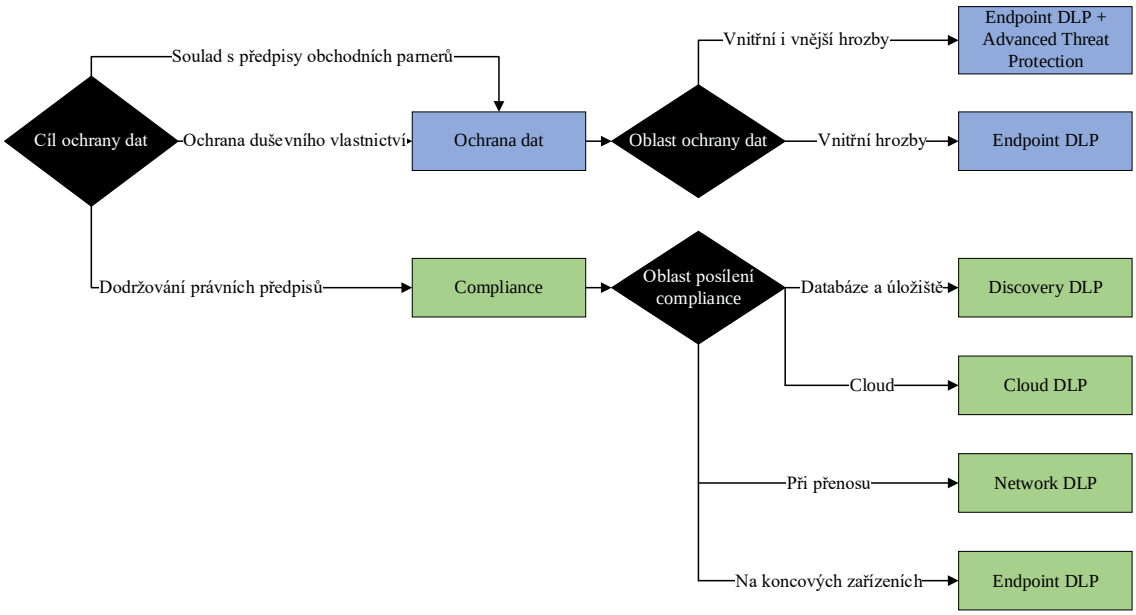
- **Discovery DLP** – Skenuje síť a uložiště v ní (pracovní stanice, servery a databáze), hledají data at rest a analyzují, kde se nachází citlivé informace. Pro

úplnost fungování je třeba, aby byl na některých zařízeních nainstalovaný agent, spadají tedy částečně i do DLP koncových bodů. [14, 15]

- **Cloud DLP** – Funguje podobně jako discovery DLP, skenuje úložiště a hledá citlivá data, ale zaměřuje se na data v cloudu. Cloud DLP se spoléhá na API (Application Program Interface) rozhraní k připojení se ke službě cloudového úložiště a následně skenuje obsah. [14; 15]

1.4.4 DLP koncových bodů

Také Endpoint DLP, představují softwarové agenty instalované na koncových stanicích, stejně jako síťová DLP kontrolují interní a externí komunikaci (e-mail a další protokoly). Kromě síťové komunikace mohou chránit i fyzicky připojená zařízení (například připojená přes USB porty, CD/DVD mechaniky apod.) anebo také bluetooth či kontrolovat akce prováděné na koncovém zařízení (zkopírování či screenshot citlivých informací). Oproti síťovým DLP musí správci spravovat řádově víc zařízení, z toho důvodu je nutná efektivní centralizovaná správa. [1; 14; 15]



Obrázek č. 11: Diagram pro výběr DLP řešení
(Zdroj: Vlastní zpracování dle [15])

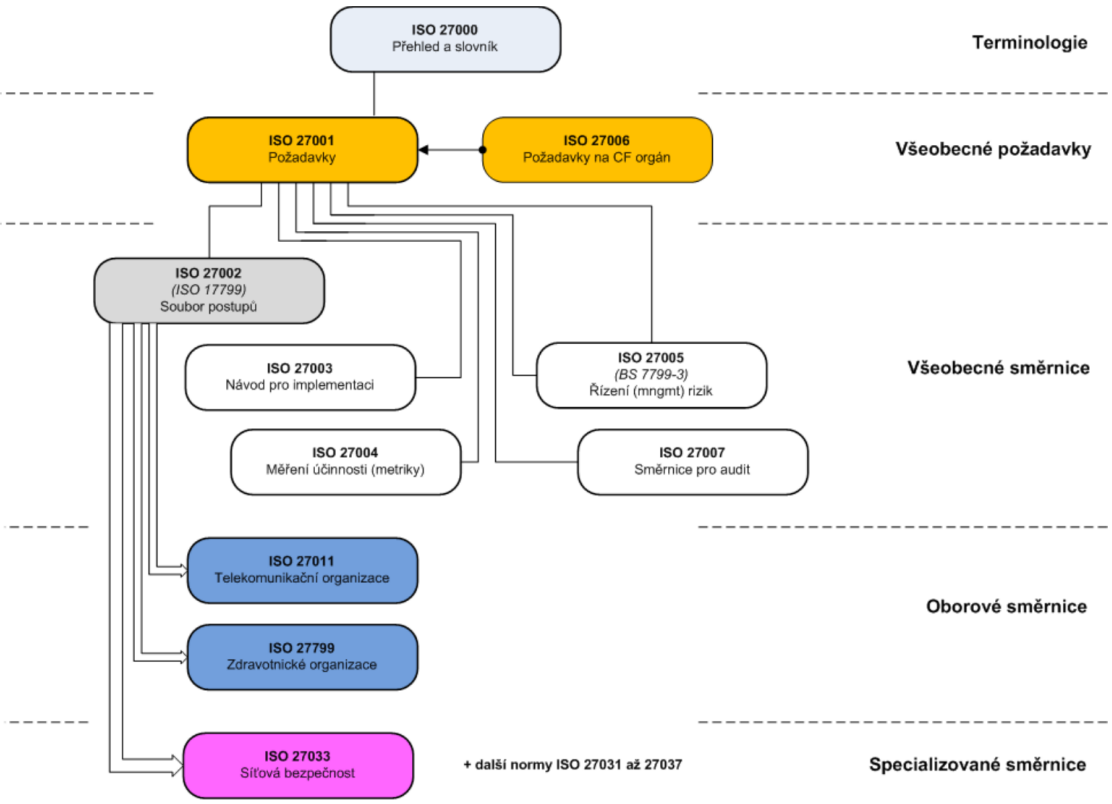
1.5 Normy

V rámci problematiky informační a kybernetické bezpečnosti existuje řada norem, nabízejících podporu organizacím pro zavádění a certifikaci ISMS. Normy jsou obecně platné, specifické pro daný obor činností organizace či podpůrné. Pro oblast bezpečnosti informací je rezervována řada ISO 27000. [1]

- **ČSN ISO/EIC 27000** – Přehled systému řízení bezpečnosti informací a slovník termínů užívaných v řadě norem 27k. [4]
- **ČSN ISO/EIC 27001** – Specifikace požadavků na ustanovení, řízení a zlepšování ISMS v organizaci dle PDCA cyklu. [16]
- **ČSN ISO/EIC 27002** – Definuje obecná bezpečnostní opatření včetně pokynů k jejich zavedení na základě ISO/EIC 27001. Opatření jsou rozdělena na organizační, personální, fyzická a technická. [11]
- **ČSN ISO/EIC 27003** – Norma poskytuje pokyny k požadavkům na systém řízení bezpečnosti informací definovaných v normě 27001. Obsahuje tedy obecný návod na implementaci ISMS, přičemž není důležité, o jakou organizaci se jedná. [1]
- **ČSN ISO/EIC 27004** – Poskytuje směrnice a metriky pro měření efektivity, monitorování, analyzování a hodnocení ISMS. [1]
- **ČSN ISO/EIC 27005** – Doporučení pro řízení rizik bezpečnosti informací. Podporuje koncepty ze směrnic ISO/EIC 27001 a 27002, jejichž znalost je nutná pro úplné pochopení konceptu této normy. [1]
- **ČSN ISO/EIC 27006** – Požadavky na orgány provádějící audit a certifikaci systému řízení bezpečnosti informací. Doplňuje normu ISO/EIC 17021-1, která nastavuje kritéria pro organizace zabývající se auditem a certifikací systémů řízení o dodatečné požadavky a doporučení týkající se certifikace ISMS v souladu s ISO/EIC 27001. [1]
- **ČSN ISO/EIC 27007** – Směrnice pro audit ISMS. Poskytuje všeobecné pokyny pro všechny druhy organizací a auditů ISMS. Norma by měla být použita ve spojení s normou ISO/EIC 19011. Pokyny by měly přizpůsobeny podle rozsahu a složitosti prováděného auditu. [1]

- **ČSN ISO/EIC 27010** – Doporučení pro řízení bezpečnosti informací při externí a interní komunikaci v organizaci. Zejména se může vztahovat na sdílení informací souvisejících s poskytováním, údržbou a ochranou kritické infrastruktury organizace nebo státu. [1]
- **ČSN ISO/EIC 27019** – Opatření pro energetický průmysl. Poskytuje směrnice pro energetické řídící systémy. Je postavena na bázi normy ISO/EIC 27002 a dává návod aplikovatelný na systémy řízení procesů používaných v energetice, jako například monitorování a řízení výroby, skladování a distribuce energetické energie a dalších podpůrných procesů. [1]

Problematiku řešenou jednotlivými normami a jejich návaznost zachycuje následující obrázek.



Obrázek č. 12: Řada norem ISO/EIC 27000 a jejich vazby
(Zdroj: 17)

2 ANALÝZA SOUČASNÉHO STAVU

2.1 Představení společnosti

V této části je stručně představena společnost, pro kterou je zpracováváno posouzení nasazení DLP systému. Společnost je vzhledem k tématu práce anonymizovaná, dále je na část, pro kterou je zpracováváno posouzení, odkazováno jako „společnost“ či „organizace“ a na celý nadnárodní celek, do kterého společnost patří odkazuje „skupina“ nebo „koncern“.

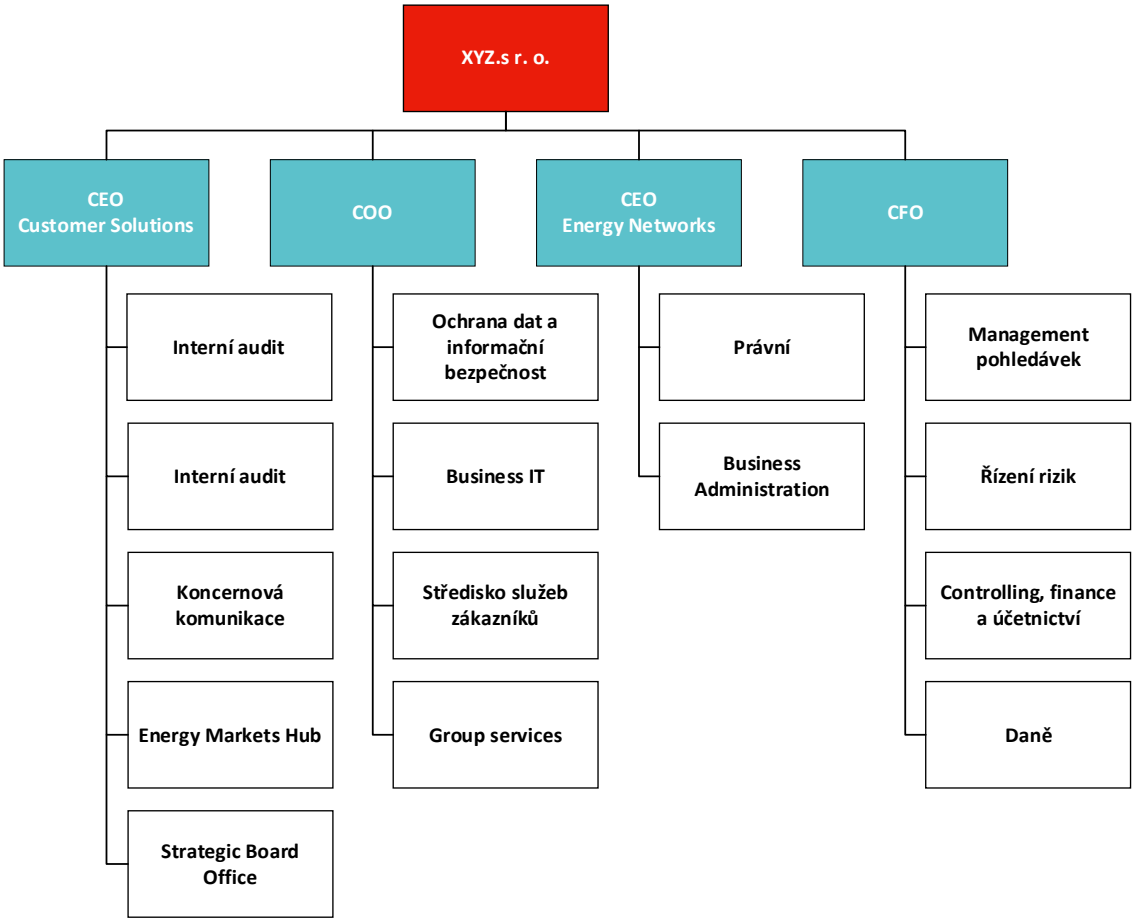
XYZ je nadnárodní energetická společnost provozující vlastní distribuční síť plynu a elektřiny v České republice. Tyto sítě buduje, spravuje a rozvíjí a je zodpovědná za provoz. Zajišťuje připojení odběrných míst pro zákazníky včetně nových zdrojů, montuje elektroměry i plynoměry a zajišťuje jejich odečty. Zaměřuje se také na budování inteligentních sítí neboli Smart Grids. Ty lépe řídí toky elektřiny v reálném čase a zvyšují efektivitu celého systému.

Společnost spolupracuje nejen se zákazníky, výrobci a obchodníky, ale také s jinými provozovateli distribučních soustav. V poslední době se snaží zákazníkům vyjít vstříc v mnoha ohledech, například prostřednictvím mobilní aplikace informující o plánovaných odstávkách dodávaných energií či jim pomáhá s instalací fotovoltaických elektráren, tepelných čerpadel, domácích dobíjecích stanic a podobně. Cílí na posilování dlouhodobých vztahů se zákazníky, zlepšování zákaznické zkušenosti a proaktivní přístup. Za účelem toho provádí rozvoj digitálních kanálů a moderních zákaznických center. Stejně jako ostatní distributoři energií v České republice podléhá společnost regulaci Energetického regulačního úřadu podle energetického zákona.

Jedná se tedy o provozovatele základních služeb a obstarává kritickou a kritickou komunikační infrastrukturu (KI a KII). Dle nového zákona o kybernetické bezpečnosti podle směrnice NIS2 bude spadat do režimu vyšších povinností. V rámci řešené problematiky je pro ni také důležité dodržování obecného nařízení o ochraně osobních údajů (GDPR). Informační a kybernetická bezpečnost je pro ni tedy zásadně důležitá jak pro zajištění bezpečného a spolehlivého provozu energetických sítí, tak pro splnění legislativních podmínek.

2.1.1 Organizační struktura

Jak bylo zmíněno, společnost je součástí nadnárodní skupiny. Regionální jednotka v České republice je dále rozdělena na čtyři další společnosti, které se soustředí na různé oblasti podnikání: distribuční sítě, administrativní a servisní podpora pro ostatní společnosti a trhy B2B a B2C. Práce se zaměřuje převážně na druhou zmiňovanou společnost, jejíž činnost zahrnuje realizaci strategických rozhodnutí a administrativní a servisní činnosti pro ostatní společnosti v rámci ČR a je tak nejúžeji navázána na celou nadnárodní skupinu. Organizační diagram zmiňované společnosti je vyobrazen na následujícím obrázku.



Obrázek č. 13: Organizační struktura
(Zdroj: Vlastní zpracování dle interní dokumentace)

Pro analyzovanou problematiku je nejdůležitější oddělení Ochrana dat a informační bezpečnost. Útvar zastřešuje několik centrálně řízených funkcí Data Protection, Cyber security a Business resilience, definuje bezpečnostní požadavky ochrany informací a dat a kontroluje jejich dodržování, řeší incidenty informační bezpečnosti, navrhuje implementaci technických a organizačních opatření, provádí bezpečnostní školení a osvětu zaměstnanců, s ohledem na ochranu údajů poskytuje konzultace a podporuje zavádění nových IT nástrojů a produktů ve společnosti. V rámci regionální jednotky skupiny funguje v jiné společnosti ještě oddělení Bezpečnosti distribučních systémů, které se zaměřuje na bezpečnost a odolnost KII a KI, tedy na bezpečností monitoring a analýzy distribuční sítě. Oddělení ochrany dat a informační bezpečnosti není nadále členěno.

2.2 Analýza vybraných částí společnosti

2.2.1 ISMS a směrnice

Organizace implementovala systém řízení bezpečnosti informací ISMS dle řady směrnic ISO/EIC 27000 a dalších relevantních norem. Dle těchto směrnic jsou vytvořeny skupinové směrnice, které slouží jako základ pro zpracování interní řídící dokumentace včetně bezpečnostního manuálu pro uživatele ICT a lokálních regionálních směrnic. V rámci směrnic jsou popsány klíčové procesy a pravidla pro uživatele jako klasifikace dokumentů, pravidla pro zacházení s ICK technikou atd. Podstatné části této dokumentace jsou popsány v následujících částech. Dále se připravuje na novou novelu zákona o KB dle NIS2.

2.2.2 Používání ICT a systémy

Téměř všichni zaměstnanci ke své práci používají notebooky, s operačním systémem Windows. Aktuálně probíhá postupná migrace z Windows 10 na 11. Většina činností běžného uživatele je pokryta řešeními od firmy Microsoft jako OneDrive a SharePoint pro sdílení dokumentů. Zaměstnanci mají přístup k datům většinou pouze v rámci svého oddělení a nemají povolen přístup k datům jiných oddělení či společností. Hojně je také využíván ERP systém SAP. Implementována je také firemní platforma, ve které jsou se zaměstnanci komunikovány koncernové novinky a události a také se mohou

přidávat do komunit či sledovat stránky jednotlivých oddělení a být informováni o případných novinkách či školeních.

Dále mají zaměstnanci mobilní telefony, které jsou mimo jiné používané ke dvoufaktorovému ověřování pomocí aplikace PingID či Microsoft Authenticator. Občasně jsou používány tablety či jiná zařízení, převážně technickými pracovníky.

V prostorách kanceláří jsou dostupné síťové tiskárny. Dokumenty klasifikované jako Citlivé nebo Velmi citlivé mohou být kopírovány/tištěny pouze na zařízeních s autentizací nebo na zařízením umístěném v chráněném prostoru a ihned po vytištění odebrány.

Bezpečnostní směrnice udávají povinnost minimálně jednou za 14 připojit zařízení do vnitřní sítě podniku a provést řádné přihlášení na svůj účet. Podniková data mohou být zpracována pouze za použití řešení, jež byly schváleny odpovědnou IT organizací nebo managementem.

2.2.3 Uživatelé

Pro přístup k počítačům, IT službám a k aplikacím v organizaci je vyžadováno zadání individuálních uživatelských přihlašovacích údajů – ID (např. uživatelského jména a hesla, PINu k čipové kartě, uživatelského ID a tokenu apod.). Uživatel odpovídá za všechny úkony učiněné pod svým ID. Uživatelské ID je vygenerováno při nástupu zaměstnance do pracovního poměru. Déle je zavedena infrastruktura veřejných klíčů (PKI), která pomocí certifikátů umožňuje podepisovat, šifrovat a dešifrovat e-maily, dokumenty a ověřovat se na zabezpečených webech a aplikacích.

2.2.4 Elektronická pošta

Zaměstnanci mají pro pracovní účely zřízenou e-mailovou adresu ve tvaru *jmeno.prijmeni@organizace.cz*. Pro pracovní e-maily je zakázáno používat soukromé e-mailové schránky. Pro přístup do pracovní schránky je využívána aplikace Microsoft Outlook. E-maily (informace v e-mailech) klasifikované jako citlivé nebo velmi citlivé mohou být posílány pouze v šifrované podobě.

2.2.5 Internet

Dle bezpečnostních směrnic je zakázáno ukládat či sdílet informace na veřejná internetová uložiště (úložiště typu Google Docs, Ulozto, Dropbox apod.) Je povolené používání interně schválených uložišť. Pokud je nezbytně nutné použít pro výměnu dat veřejných služeb v internetu, je nutné schválení časově omezené výjimky, kterou uděluje Information Security Officer. Je povinností toho, kdo data uložil, je následně smazat. Citlivá data uložená na veřejných uložištích musí být zabezpečena šifrováním. Dále je zakázáno obcházet nastavení připojení do internetu pomocí externích proxy serverů nebo jiných prostředků (např. anonymizérů) a připojovat se tak do internetu jiným než standardním způsobem. Zaměstnanci nesmí zadávat do webových formulářů, aplikací či podobných internetových služeb interní, citlivé nebo velmi citlivé informace (např. překlady v automatizovaných překladačích). Z pracovního počítače se nesmí zakládat osobní účty u poskytovatelů internetových online služeb bez ohledu na to, o jakou službu jde. Používání veřejných sítí peer-to-peer pro sdílení souborů, jako např. BitTorrent nebo uTorrent, je zakázáno. Provoz internetu může být z bezpečnostních důvodů průběžně monitorován. Lze tedy v případě potřeby vyhledat důkazy o činnosti uživatelů až na úroveň lokálních počítačů, na kterém se tato činnost vykonávala.

2.2.6 Vzdálený přístup

Pro vzdálené připojení firemních počítačů do firemní sítě (VPN) je možné využít pouze aplikace schválené společností. Připojení je povoleno pouze přes důvěryhodné sítě (sítě mobilních operátorů nebo přímo přes systémy organizace). Vzdálené připojení je poskytováno na základě schválené žádosti.

2.2.7 Rozvoj bezpečnostního povědomí

Pro zajištění rozvoje bezpečnostního povědomí zaměstnanců a dodavatelů je vytvořena na základě konceptu SATE (Security Awareness Training and Education) politika rozvoje bezpečnostního povědomí, včetně plánu rozvoje, v kterém se vymezí potřebné vzdělávací aktivity. Zaměstnanci jsou pravidelně školeni v oblasti obecného bezpečnostního povědomí a v zásadách bezpečného chování. Firma používá nástroj na phishingové simulace. V rámci školení nových zaměstnanců probíhá i školení o kybernetické

a informační bezpečnosti. Periodicky probíhají i specializovaná školení zaměřená na konkrétní role.

V rámci migrace a implementace nového DLP systému by měly proběhnout konkrétní školení.

2.2.8 Vyměnitelná média a USB

Mezi přenosná paměťová média se řadí např. USB flash disky, externí pevné disky, CD, DVD, paměťové karty apod. Používání paměťových médií je kontrolováno a monitorováno. Informace klasifikované jako citlivé nebo velmi citlivé mohou být nahrány pouze na šifrovaná paměťová média a musí být označena popiskem. Je zakázáno používat a zapojovat do pracovních zařízení paměťová média z neznámých nebo nedůvěryhodných zdrojů (např. zapomenuté USB flash disky, neznámá CD/DVD, rozdávaná paměťová média).

2.3 Klasifikace aktiv

Ve skupině je zaveden systém klasifikace aktiv. Tento systém je popsán ve skupinových směrnicích a odtud přejat společností do interní řídící dokumentace. DLP chrání data, tedy pouze informační aktiva, ostatní typy aktiv nemá smysl řešit. Klasifikace informací je součástí klasifikace aktiv. Aktiva jsou hodnocena z pohledu atributu důvěrnosti, dostupnosti a integrity, z čehož má pro řešenou problematiku největší význam atribut důvěrnost. Klasifikaci popisuje a řídí regionální směrnice. Za klasifikaci je zodpovědný vlastník aktiva.

2.3.1 Obecné klasifikační schéma

Pro stanovení úrovně ochrany aktiv a určení vhodných bezpečnostních opatření se vychází z klasifikace daného aktiva. Při klasifikaci se posuzují tři bezpečnostní atributy (Důvěrnost, Integrita, Dostupnost), které spolu s následujícími hodnotícími kritérii (dopady) slouží pro stanovení klasifikačního stupně.

- Finanční ztráta – základní ukazatel, pokud není možné vyčíslit, je možné použít i jiné kritérium;

- Poškození dobrého jména;
- Narušení práv a předpisů;
- Narušení obchodních aktivit;
- Dopad na bezpečnost osob;
- Únik osobních dat; dopad na ochranu soukromí osob.

Podrobněji jsou tyto kritéria popsána v klasifikačním schéma hodnocení dopadu, viz. příloha P.1.

Klasifikaci aktiv v organizaci z hlediska důvěrnosti popisuje následující tabulka.

Tabulka č. 2: Klasifikace informací

Název	Popis	Klasifikační stupeň	Příklad
Veřejné Public	Informace, které jsou poskytovány široké veřejnosti.	Nízký	Informace z letáků, webových stránek, tisková prohlášení. atd.
Interní Internal	Informace vytvořené během běžné každodenní práce, které nespadají do níže uvedených úrovní.	Střední	Směrnice, organizační diagramy, kolektivní smlouvy atd.
Citlivé Confidental	Informace, jejichž únik, ztráta nebo neoprávněná změna by mohla poškodit zákazníky, zaměstnance nebo značku.	Vysoký	Zákaznická data, hesla, plány sítí atd.
Velmi citlivé Stritctly confidental	Informace, jejichž únik, ztráta nebo neoprávněná změna by mohla ohrozit existenci společnosti, nebo jejích dceřiných společností. O tom, kdo bude mít k informaci přístup rozhoduje vlastník informace.	Velmi vysoký	Strategická rozhodnutí managementu, informace o plánovaných fúzích atd.
Zákonem předepsaný stupeň utajení	Zákonem předepsaný stupeň utajení (např. Zákon č. 412/2005 Sb. o ochraně utajovaných informací).	Dle příslušného zákona	

(Zdroj: Vlastní zpracování dle interní dokumentace)

2.4 Pravidla pro práci s daty

Pravidla pro práci s daty podle požadavků na důvěrnost jsou popsány v regionální směrnici poskytující informace a pravidla, kterými se řídí klasifikace a nakládání s informačními aktivy.

Konkrétní pravidla jsou popsána v následujících tabulkách. Pravidla se dělí na dvě části: obecná pravidla týkající se práce s daty v prostředí firmy a pravidla pro práci s daty mimo organizaci.

K usnadnění práce s klasifikovanými aktivy a dodržení následujících pravidel je ve společnosti implementován nástroj MIP (Microsoft Information Protection). Jedná se o nástroj vynucující klasifikaci dat pomocí štítků, fungujících napříč aplikacemi, službami a zařízeními. Podle těchto štítků poté vynucuje určitá pravidla, jako například šifrování e-mailu, který byl označený jako citlivý. Pokud uživatelem nebyla vybrána klasifikace, MIP s automaticky přiřazuje klasifikaci „interní“.

2.4.1 Obecná pravidla

Následující tabulka popisuje obecná pravidla pro práci s daty. Týkají se především činností v organizaci. Podle různých činností a klasifikací jsou stanovena různá pravidla. Levý sloupec udává klasifikační stupeň, pravý přiřazuje jednotlivá pravidla k danému stupni.

Tabulka č. 3: Pravidla pro práci s aktivy uvnitř organizace

Obecné požadavky	
Označování	
Veřejné	Žádné požadavky
Interní	Pokud není uvedena klasifikace, je dokument považován za interní
Citlivé	Autorem označeny „CITLIVÉ“ • MS Office dokumenty – na každé stránce • E-maily – označení v předmětu e-mailu • Listinné dokumenty – na každé stránce dokumentu/složky
Velmi citlivé	Autorem označeny „VELMI CITLIVÉ“ • MS Office dokumenty – na každé stránce

	• E-maily – označení v předmětu e-mailu • Na přenosném médiu (CD, USB, ...) • Listinné dokumenty – na každé stránce dokumentu/složky
Opakovaná klasifikace	
Veřejné	Vlastník udržuje aktuální klasifikaci
Interní	Vlastník udržuje aktuální klasifikaci
Citlivé	V pravidelných intervalech nebo při změnách
Velmi citlivé	V pravidelných intervalech nebo při změnách
Šíření v rámci organizace	
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Pouze mezi zaměstnanci, kteří aktivum potřebují pro svoji práci.
Velmi citlivé	Distribuční seznam proškolených osob Schválení vlastníkem aktiva
Uložení fyzických dokumentů a přenosných médií (USB, CD, …)	
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Při opuštění místnosti uzamčené (stůl, skříňka, celá místnost, …), šifrování média
Velmi citlivé	Při opuštění místnosti uzamčené (stůl, skříňka, trezor, celá místnost, …), šifrování média
Uložení elektronických dokumentů	
Veřejné	Žádné požadavky
Interní	Pouze schválená úložiště
Citlivé	Pouze schválená uložiště Definovaný distribuční list
Velmi citlivé	Pouze schválená uložiště Šifrované Definovaný distribuční list
E-mail	

Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Šifrovaný
Velmi citlivé	Šifrovaný
Zálohování	
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Šifrovaně nebo omezený přístup k zálohám
Velmi citlivé	Šifrovaně nebo omezený přístup k zálohám
Likvidace	
Veřejné	Žádné požadavky
Interní	Žádné požadavky
Citlivé	Bezpečné smazání (např. vícenásobný přepis, Data shredder) Bezpečná skartace/zničení
Velmi citlivé	Bezpečné smazání (např. vícenásobný přepis, Data shredder) Bezpečná skartace/zničení Záznam o skartaci/zničení

(Zdroj: Vlastní zpracování dle interní dokumentace)

2.4.2 Pravidla pro práci s daty mimo organizaci

Následující tabulka obsahuje pravidla pro zacházení s daty mimo organizaci. Struktura je stejná jako u předchozí tabulky s výjimkou odstranění řádku s klasifikací „Veřejné“, protože u této klasifikace nejsou, vzhledem k definici této klasifikace, v ani jednom z uvedených případů žádné požadavky.

Tabulka č. 4: Pravidla pro práci s aktivy mimo organizaci

Mimo organizaci	
Šíření mimo organizaci	
Interní	Pouze k pracovním účelům
Citlivé	NDA (dohoda o mlčenlivosti) Distribuční seznam Schválení vedoucím zaměstnancem
Velmi citlivé	NDA (dohoda o mlčenlivosti) Distribuční seznam Schválení vedoucím zaměstnancem
Přenosová média	
Interní	Vlastník udržuje aktuální klasifikaci
Citlivé	V pravidelných intervalech nebo při změnách
Velmi citlivé	V pravidelných intervalech nebo při změnách
Předávání mimo organizaci	
Interní	Žádné požadavky
Citlivé	Bezpečný způsob (osobní předání, kurýr, zapečetěné, …)
Velmi citlivé	Bezpečný způsob (osobní předání, kurýr, zapečetěné, …)
E-mail	
Interní	Zákaz zasílání přes osobní (nefiremní) e-maily
Citlivé	Šifrovaný Zákaz zasílání přes osobní (nefiremní) e-maily
Velmi citlivé	Šifrovaný Zákaz zasílání přes osobní (nefiremní) e-maily
Sdílená úložiště	
Interní	OneDrive,SharePoint
Citlivé	OneDrive,SharePoint
Velmi citlivé	Pouze schválené služby, např. Brainloop
Uložení fyzických dokumentů a přenosných médií (USB, CD,…) mimo organizaci	

Interní	Pod osobním dohledem nebo uzamčené
Citlivé	Pod osobním dohledem nebo uzamčené a zašifrované
Velmi citlivé	Pod osobním dohledem nebo uzamčené a zašifrované

(Zdroj: Vlastní zpracování dle interní dokumentace)

2.5 Současná komunikační infrastruktura

Společnost, vzhledem k současným trendům, funguje z velká části v cloudovém prostředí. V cloudu je na virtuálních serverech většina důležitých služeb i data zaměstnanců, která jsou všechna synchronizována do prostředí OneDrive. Společnost na našem území funguje ve více objektech. Vzhledem k její velikosti a rozsahu jejích činností není nutné pro řešenou problematiku popisovat síťovou architekturu či počet koncových zařízení. V rámci řešené problematiky je podstatný celkový počet uživatelských stanic, ten v současnosti přesahuje 3 000. Tyto stanice představují notebooky s operačním systémem Windows.

2.6 Rizika

Vzhledem k digitální transformaci a technickému pokroku společnost čelí novým hrozbám spojených s nárustem „chytrých“ zařízení a celkovému množství používaných IT nástrojů. Tím roste útočná plocha pro útočníky, ale také možnost vzniku incidentů ovlivňující kybernetickou bezpečnost. DLP systém pokrývá interní hrozby v organizaci a chrání organizaci a její data na koncových zařízeních a v síti. Události a incidenty před kterými DLP chrání mohou být jak úmyslné, tak nechtěné (uživatelské chyby). Pokryté oblasti jsou převážně data a programy kopírované z a do firemního prostředí.

2.6.1 Potenciálně nechtěné programy

Pomocí DLP lze snížit riziko výskytu nechtěných programů (Potentionaly unwanted program: PUP) ve firemním prostředí. Nechtěné programy mohou být zaměstnanci nakopírovány úmyslně, ale i omylem. Tyto programy mohou být legislativně závadné

jako například programy na prolamování licencí či hesel, nebo také nechtěné z hlediska firmy a compliance, jako audiovizuální materiály či těžiče kryptoměn.

2.6.2 Únik dat

DLP je schopno pokrýt úniky dat mimo organizaci. K těmto únikům může dojít z nedbalosti, ale i úmyslně. Dle zprávy společností IMB a Ponemom Institute *Cost of Data Breach Report 2023,* postavené na datech z více než 500 úniků dat, byly celosvětově průměrné náklady způsobené únikem dat 4,45 milionu USD (103 130 000 Kč), což přestavuje nárust o 15 % za poslední 3 roky. Energetický sektor patří mezi nejvíce ohrožená odvětví a pohybuje se v tomto případě nad průměrem s hodnotou 4,78 milionů USD, ale Česká republika ve zprávě nevystupuje. [6; 18]

3 VLASTNÍ NÁVRH ŘEŠENÍ

V této části je představen současný DLP nástroj a posouzeno jeho nasazení. Dále je popsáno alternativní řešení a posouzení a návrhu způsobu přechodu na jiného dodavatele.

3.1 Popis současného nástroje

Původní implementovaný systém byl DLP nástroj od společnosti McAfee.

V roce 2021 proběhla akvizice společností McAfee Enterprise a FireEye skupinou Symphony Technology Group (STG). Následovala fúze a rozdělení těchto společností za účelem lepšího zaměření na trhy s řešeními rozšířené reakce a detekce (Extended Detection and Response (XDR)) a Security Service Edge (SSE). Výsledkem byl na počátku roku 2022 vznik společností Trellix, soustředící se na XDR, a Skyhigh Security, která se soustředí na cloudová řešení. Po tomto přešla analyzovaná společnost na systém Trellix Data Loss Prevention, který je velmi podobný a navazuje na systém McAfee. Trellix nabízí bezpečnostní řešení, zpravodajství o hrozbách a služby, které chrání podnikové koncové body, sítě, servery, cloud a další. [19; 20]

Obrázek č. 14: Logo Trellix
(Zdroj: 21)

Trellix DLP je sada komponent, které slouží k zjišťování, monitorování a přecházení ztrátám dat v rámci sítě a jejích koncových bodů. V síti fungují network moduly, které reprezentují DLP Discover, Prevent a Monitor, ty jsou instalovány formou appliance. V rámci koncových bodů se jedná o host moduly, které jsou instalovány ve formě agenta na koncová zařízení. Představují je produkty DLP Endpoint a Device Control. V rámci řešení nabízí více produktů na ochranu různých typů dat. [21]

3.1.1 DLP Endpoint

Funguje na koncových bodech sítě, na kterých je instalován jako plug-in. Jedná se o agenta, který monitoruje akce uživatelů a přenosy dat prostřednictvím aplikací, vyměnitelných úložných zařízení, webu, e-mailu, schránky, snímání obrazovky, sdílení v síti a cloudu. Prověřuje používaná data (data in use) na zařízeních a dané činnosti blokuje, upozorňuje, oznamuje, dává do karantény, šifruje nebo provádí další akce, pokud jsou prováděny s daty označenými jako citlivá nebo důvěrná. Chrání tak při činnostech jako přesun citlivých souborů na USB flash disk nebo poslání e-mailu s přílohou. [22; 23]

Funkce Endpoint Discovery skenuje soubory místního souborového systému a e-mailového úložiště a uplatňuje pravidla na ochranu citlivého obsahu. Dále podporuje webovou poštu pro prohlížeče Google Chrome. Řešení je dostupné pro operační systémy Windows i macOS ve formě dvou různých produktů. [22; 23]

3.1.2 Device Control

Řídí a kontroluje vyměnitelných médií v koncových bodech. Tedy hlavně kopírování dat na vyměnitelná média a úložná zařízení, jako jsou paměti USB, disky CD, DVD, zařízení připojená přes Bluetooth, zobrazovací zařízení a další. Zařízení a přenosy lze povolit, nastavit pouze pro čtení či blokovat na základě obsahu, kontextu nebo typu zařízení. [22; 23]

3.1.3 DLP Discover

Identifikuje a chrání data v klidovém stavu (data at rest) pro síťová, cloudová i koncová úložiště. Nástroj skenuje a označuje obsah v rámci sítě, včetně sdílených složek CIFS/NFS, databází, Microsoft SharePoint, Box a koncových zařízení. Z naskenovaných dat a metadat vytváří databázi tím umožňuje Discover správcům zjistit, jak jsou data používána, kdo je vlastní, kde jsou uložena a další informace. Registrační skenování získává z úložišť souborů informace o otiscích prstů pro klasifikaci souborů a ukládá podpisy do databáze registrovaných dokumentů. [22; 23]

DLP Discover nabízí detekci a označování nestrukturovaných dat na základě funkce optického rozpoznávání znaků (OCR), která rozpoznává a chrání text na naskenovaných

obrázcích a formulářích, a otisků prstů (fingerprinting) a strukturovaných dat na základě Exact Data Matching, například pro citlivá data uložená v excelovém listu v databázi. Trellix DLP Discover dokáže také přesouvat a aplikovat MIP (Microsoft Information Protection) štítek pro správu práv. [22; 23]

3.1.4 DLP Prevent

Funguje ve spolupráci s webovým proxy serverem nebo MTA serverem a chrání webový a e-mailový provoz. Umožňuje šifrování, blokování přesměrovávání nebo umisťování do karantény citlivých dat přenášených prostřednictvím e-mailu, HTTP/HTTPS, IM (instant messaging), FTP přenosů a dalších metod. Příchozí a odchozí síťový provoz skenuje na všech portech, ve více protokolech a u různých typů obsahu. Umožňuje kontrolu e-mailů odeslaných z přenosných zařízení, ty jsou automaticky kontrolovány na citlivý obsah, pokud jsou integrovány s poštovní bránou a kontrolou webového obsahu. V takovém případě musí být přenosná zařízení nastavena tak, aby byl jejich provoz směřován přes webový proxy server integrovaný se službou Network DLP Prevent. Stejně jako Discover nabízí Prevent také OCR a detekci na základě otisků prstů pro nestrukturovaná data a na základě obsahu pro strukturovaná data. [22; 23]

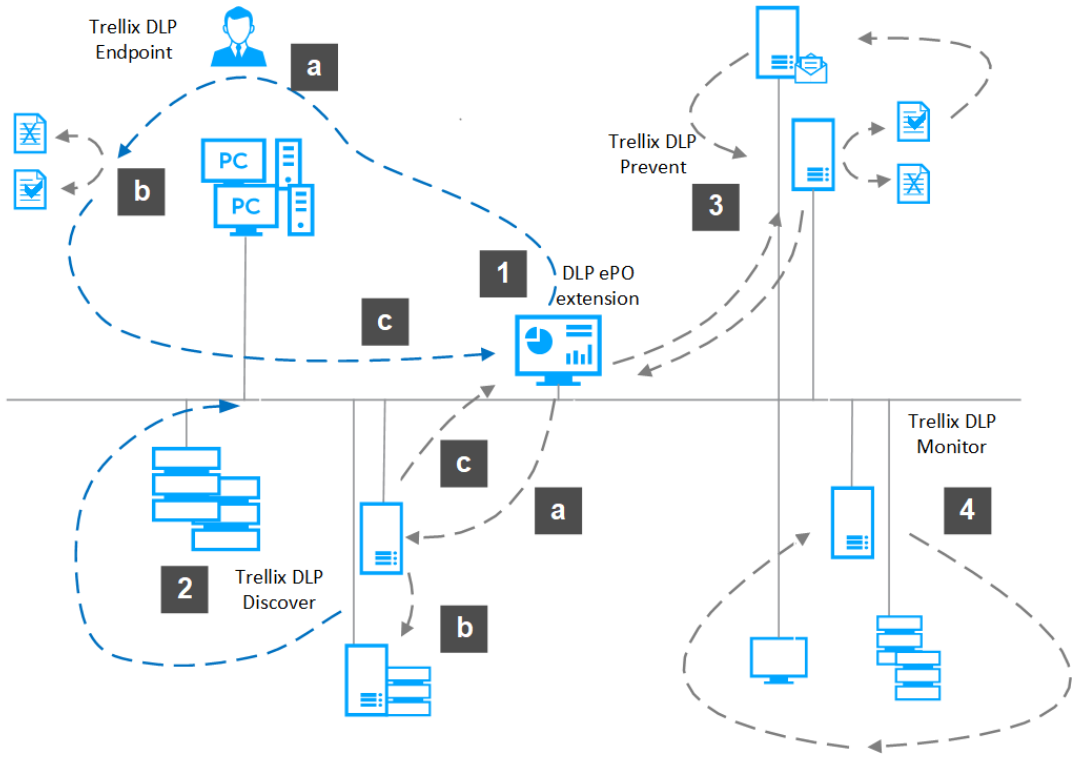
3.1.5 DLP Monitor

Pasivně skenuje síťový provoz (data v pohybu) v organizaci a odhaluje potenciální případy ztráty dat. Díky integraci s výstupními zařízeními přes SPAN/TAP dostává kopie paketů síťové komunikace a tím monitoruje veškerá odchozí data. Monitor je k dispozici jako fyzické nebo virtuální zařízení, které dokáže detekovat a spravovat více než 300 typů obsahu. [22; 23]

Tabulka č. 5: Produkty Trellix a vektory dat

Vektor dat	Popis	Produkty
Data in Use	Akce na koncových bodech, jako je kopírování dat a souborů na vyměnitelná média, tisk souborů na místní tiskárnu a pořizování snímků obrazovky.	Trellix DLP Endpoint Trellix Device Control
Data in Motion	Provoz v síti. Provoz je analyzován, kategorizován a ukládán do databáze Trellix ePO - On-prem.	Trellix DLP Prevent Trellix DLP Monitor
Data at Rest	Data uložená ve sdílených souborech, databázích a úložištích. Služba Trellix DLP dokáže skenovat, sledovat a provádět nápravná opatření u takových dat.	Trellix DLP Discover Trellix DLP Endpoint discovery

(Zdroj: Vlastní zpracování dle 22)



Obrázek č. 15: Produkty Trellix v síti
(Zdroj: 22)

3.1.6 Další nástroje Trellix

Tyto další produkty se neřadí do kategorie Trellix DLP produktů, ale lze je použít k jejich správě, či je s nimi integrovat.

Trellix ePolicy Orchestrator (ePO)

Trellix ePO je konzole, která umožňuje centralizovanou správu všech Trellix bezpečnostních produktů. Lze ji použít k nasazení, aktualizaci a odinstalaci produktů. Nastavení a vynucování zásad, správě incidentů a pracovních postupů, vytváření přehledů a zpráv pro všechny síťové a koncové komponenty. Trellix nabízí řešení on-premise nebo SaaS. [22; 23]

File and Removable Media Protection (FRP)

FRP slouží k automatickému šifrování souborů a složek uložených nebo sdílených v počítačích, cloudových úložištích, souborových serverech, e-mailech a na vyměnitelných médiích. Správa probíhá přes ePO konzoli. Zajišťuje, že konkrétní soubory a složky jsou vždy šifrovány bez ohledu na to, kde jsou data editována, kopírována nebo ukládána. Umožňuje například šifrování citlivých souborů, souborů synchronizovaných se službami cloudového úložiště a šifrování vyměnitelných médií nebo blokování kopírování nešifrovaných souborů na tyto média. [22]

Trellix FRP je možné integrovat s Trellix DLP Endpoint pro Windows a šifrovat tak citlivé soubory. [22]

Trellix Logon Collector (TLC)

TLC je monitoruje domény služby Active Directory a shromažďuje informace o přihlášení. Zjišťuje u řadičů domény AD události přihlášení uživatelů a odesílá tyto informace do bezpečnostních zařízení účelem korelace síťového provozu s chováním uživatelů. [22]

Lze jej integrovat s nástroji Trellix DLP Monitor a Trellix DLP Prevent pro informace o ověřování uživatelů.

3.1.7 Shrnutí a licence

Trellix nabízí komplexní řešení systému DLP nabízející ochranu dat napříč sítí, koncovými zařízeními i cloudem. Centrální konzole ePO umožnuje snadné nastavení pravidel a správu incidentů a porušení DLP zásad bez ohledu na to, zda porušení DLP pocházejí z podnikových zařízení nebo cloudových aplikací. [22; 23]

Výhodou tohoto řešení je jeho modularita, podnik tak může pokrýt pouze potřebné oblasti a tím si usnadňuje implementaci i snižuje pořizovací i celkové náklady. Další výhodu představuje integrace s jinými nástroji, a to jak bezpečnostními, tak těmi pro běžný provoz. To jsou například nástroje Microsoftu (které firma v široké míře používá), jako Outlook, MIP atd., a dále například integrace s Cloud DLP od výše zmíněné firmy Skyhigh Security. Logování dat v pohybu a incidentů do databáze usnadňuje analýzu toho, jak jsou data používána a přesouvána, což je užitečné i pro forenzní účely. [22; 23]

Slabými stránkami je chybějící OCR pro Endpoint. Trellix také neposkytuje podporu agenta pro Linux a podporu pro Microsoft Teams, obě tyto funkcionality má ale v plánu. Přestože produkt nabízí bohatou sadu funkcí, je pro správnou instalaci a údržbu řešení tak, aby byly plně využity jeho možnosti zapotřebí zkušený IT tým. [22; 23]

Licence

Trellix nabízí předplatné (subscription) a trvalé (perpetual) licence, ty se kombinují s obnovitelnými ročními smlouvami o podpoře. Jednotlivé produkty jsou rozděleny do různých sad dle jejich zaměření, ty jsou vyobrazeny níže v tabulce č. 6. [21]

Tabulka č. 6: Licenční balíčky Trellix

Sada --- Produkt	Data Security Endpoint Protection Suite	DLP Network Suite	DLP Suite	Data Security Suite
DLP Endpoint Complete (včetně Device Control)	✓		✓	✓
DLP Discover		✓	✓	✓
DLP Network Monitor		✓	✓	✓
DLP Network Prevent		✓	✓	✓

(Zdroj: Vlastní zpracování dle 21)

Data Security Suite a Data Security Endpoint Protection Suite nabízí kromě uvedených produktů ještě další produkty umožňující šifrování dat na discích či vyměnitelných

médiích (Drive a Native Drive Encryption a File & Removable Media Encryption) [21]

3.2 Posouzení nasazení současného řešení

V této části je popsáno současné nasazení nástroje Trellix DLP.

3.2.1 Přehled současného nasazení

Implementace současného systému byla zahájena v roce 2019 a plně dokončena byla v roce 2020. Společnost v současnosti disponuje licencí na 3 500 pracovních stanic. Byly implementovány produkty DLP Endpoint a File and Removable Media Protection (FRP). V té době se stále jednalo o McAfee produkty, protože společnost Trellix ještě neexistovala. Po odkoupení McAfee Enterprise, spojení s Fire Eye a následném vzniku společnosti Trellix přešla společnost na její řešení. Vzhledem k tomu, že Trellix v oblasti DLP nabízí prakticky stejné produkty jako McAfee, byly dopady této změny minimální, podobně jako by se jednalo o stejnou společnost, která prošla rebrandingem. Přechod byl prakticky automatický a obešel se bez potřeby úpravy procesů, politik či architektury. Za největší změnu lze považovat změnu podpory a pro běžné zaměstnance změnu jména a ikony na hlavním panelu.

Od původně implementovaného FRP bylo postupně upuštěno, protože jeho funkcionalita byla nahrazena BitLockerem od Microsoftu, který vynucuje šifrování připojovaných zařízení. V současnosti je tedy používán pouze Data Loss Prevention Endpoint for Windows.

DLP je v současnosti používáno pouze dvěma regionálními jednotkami společnosti, Českou republikou a Rumunskem. Každá jednotka využívá mírně jiné funkce a má nastaveny jiné politiky. Na našem území slouží převážně pro monitorování a kontrolu kopírovaných a uložených souborů na pracovní zařízení a tím omezení výskytu potenciálně nechtěných programů, a to převážně z USB zařízení.

Aktuálně je v případě vzniku události monitorováno:

- ID;
- Čas a datum vzniku události;
- Název počítače;
- IP adresa;
- ID uživatele;
- Název zařízení;
- GUID zařízení;
- Sériové číslo zařízení;
- Typ zařízení;
- Velikost zařízení;
- Název a velikost kopírovaného souboru .

Důvody implementace

V současnosti je implementace nutná pro splnění regionálních směrnic týkajících se ochrany dat a používání ICT techniky. Důvodem zavedení bylo, že ačkoliv má společnost nasazenou řadu technických opatření monitorující sdílení souborů, určité kanály zůstaly nehlídané (převážně USB zařízení). Tyto kanály představují rizika jako ztrátu dat, infikování PC malwarem a používání nepovolených programů.

Obecné zablokování USB portů ale nepředstavuje možné řešení, protože představují flexibilní řešení pro řadu činností, jako konektivitu (připojování externích zařízení jako klávesnice, myši atd.) přenosy dat (lokální zálohy, přenos informací třetím stranám) a technické operace (odečty a údržba zařízení v terénu). V místech se špatnou nebo žádnou konektivitou jsou tyto výhody ještě podstatnější. K doplnění již nasazených bezpečnostních opatření bylo tedy rozhodnuto o implementaci DLP k pokrytí nemonitorovaných komunikačních kanálů a tím snížení rizik spojených se ztrátou dat, či nedovoleným používáním ICT techniky.

Dalším využitím je lepší naplnění požadavků legislativy pro GDPR při práci s citlivými údaji či směrnice NIS2. Kromě technického zabezpečení nabízí DLP i zlepšení bezpečnostního povědomí mezi zaměstnanci, a to přímou komunikací při zjištění incidentu či vyskakovacími okny v reálném čase s upozorněními či tipy.

3.2.2 Role a zodpovědnosti

Pro úspěšné zavedení a provoz je třeba mít definovány a přiřazeny zodpovědnosti a role ve vztahu k produktu. Pomocí těch jsou jednotlivým zaměstnancům přiřazeny úkoly a činnosti odpovídající za správný provoz a rozvoj řešení.

Business role:

- **Business Owner** je vedoucí oddělení informační bezpečnosti a ochrany dat, který zastupuje také pozici DPO (Data Protection Officer – pověřenec pro ochranu osobních údajů);
- **Aplikační manažer** je Service Delivery Manager z oddělení IT Service Integration;
- **Klíčový uživatel** je zaměstnanec oddělení Informační bezpečnosti a ochrany dat.

Technické a procesní role:

Administrátor Aplikace ePO – externí integrátor (dále jen administrátor ePO)

- zodpovědnost za chod a správu aplikace ePO
- zodpovědnost za aktuální verze Trellix Produktů
- instalace a deinstalace produktů DLP na základě Tagů či pomocí podobných a jemu dostupných nástrojů
- řešení problémů s produkty DLP a FRP
- nastavení klientských a serverových tasků
- nastavení rolí

Operátor Produktů DLP ve společnosti – provoz IT

Operátor se pro potřeby dělí na:

- Administrátor DLP
    - modifikuje a tvoří politiky, klasifikace, Rule-sets, Definitions
    - reportuje v souvislosti s DLP incidenty a spolu s DPO rozhoduje, které incidenty se mohou vymazat
    - tvoří Queries

    - kopíruje exportované tabulky DLP incidentů na zálohované úložiště a vytváří manuální exporty DLP incidentů
    - dále má práva na všechny úkony rolí operátor DLP a reviewer DLP
- Operátor DLP
    - přesouvá systémy do požadovaných podskupin v System Tree
    - instaluje na koncové systémy pomocí instalačních Tagů
    - deinstaluje z koncových systémů pomocí deinstalačních Tagů
    - aplikuje politiky na koncové systémy
    - modifikuje a přiřazuje povolené/blokované zařízení do skupiny v DLP Definitions a aplikuje je v příslušných DLP politikách – proces Whitelistingu
    - spravuje a aktualizuje Seznam povolených zařízení, případně ostatní živé dokumenty
    - poskytuje uživatelský helpdesk servis -> Challenge/Response Code a DLP Endpoint Bypass
    - reportuje v souvislosti s počtem koncových systémů v jednotlivých podskupinách System Tree a stavu nainstalovaných produktů na koncových systémech (DLP a FRP)

Reviewer DLP Incidentů – DPO/Informační bezpečnost

- kontroluje a vyšetřuje DLP Incidenty s pomocí DLP Incident Manager, DLP Case Management a Queries & Reports
- dostává a kontroluje reporty o stavu a chodu řešení

Všechny úkony procesních rolí (administrátor, operátor a reviewer DLP), určených pro provoz, je schopna vykonávat jedna pověřená osoba v roli administrátora DLP. Kvůli potřebné zastupitelnosti a struktuře provozu se však předpokládá minimálně jedna osoba v roli administrátora DLP a jedna či více pověřených osob v roli operátora DLP.

Role jsou stanoveny podle zodpovědností za určité oblasti řešení. V případě značeného nárustu nároků na provoz systému, například vzrůstem počtu koncových uživatelů či systémů nebo zavedením dalších funkcionalit, by bylomožné rozdělit role i technicky podle zavedených produktů a funkcionalit. Tyto role by poté byly ve formě správce DLP,

správce DLP Device control, správce DLP incidentů, správci jednotlivých funkcí dle implementovaných produktů atd. Toto rozdělení není používáno, ale společnost by na něj zvážila přechod při výrazné změně DLP.

3.2.3 Architektura systému

Architektura řešení, z pohledu implementace produktů DLP musí zabezpečovat minimálně následující funkcionality:

- Instalace/upgrade/odstranění (odinstalace) DLP produktů na koncových stanicích spravovaných v ePO
- Správa chování DLP produktů, které jsou nasazeny v prostředí pomocí politik

Komponenty infrastruktury:

- **ePO Server**
  - Centralizovaný systém pro správu, instalaci, monitoring a prosazovaní bezpečnostních politik Trellix produktů
- **Agent Handler**
  - Snižuje pracovní zatížení serveru zpracováním událostí mimo načítání a povinnostmi připojení Agenta
- **ePO SQL Database**
  - Databáze uchovávající veškerá data s systémech spravovaných v síti, ePO serveru a agentech.

ePO Server se svojí infrastrukturou běží v cloudu mimo Českou republiku.

- **DLP řídící komponenty**
  - Nainstalovány v ePO jako extensions
- **DLP instalační balíčky**
  - Nainstalovány v ePO Master repository
- **Koncové systémy s MS Windows**
  - Mají nainstalovaného agenta a jsou řízeny z ePO
- **DLP Evidence Storage**
  - Úložiště pro ukládání důkazů (evidences)

3.2.4 Současné politiky

Jak bylo zmíněno, jsou využívány převážně politiky týkající se USB a vyměnitelných médií. Pro problematiku migrace a otestování dalšího systému by bylo vhodné zpracovat politiky do obecných pravidel, která by soužila jako opora pro otestování politik v novém systému. Následující tabulky a obrázky dávají příklad některých používaných politik v obecném formátu.

Tabulka č. 7: CZ pravidlo 1

Politika	**Monitorování – standardní DP politika**
Aktér	Kterýkoliv uživatel v CZ skupině
Akce	Veškerý přenos souborů (příchozí i odchozí) na vyměnitelná média a všechna připojená zařízení monitorována.
Reakce systému	Nahlásit DLP událost. Žádná interakce s uživatelem

(Zdroj: Vlastní zpracování dle interní dokumentace)

Tabulka č. 8: CZ pravidlo 2

Politika	**Blokování**
Aktér	Kterýkoliv uživatel v CZ skupině
Akce	Veškerý přenos souborů (příchozí i odchozí) na vyměnitelná média monitorován s klasifikační analýzou. Všechna připojená zařízení monitorována.
Reakce systému	Nahlásit DLP událost. Upozornění uživatele – vyskakovací okno s požadavkem na odůvodnění.

(Zdroj: Vlastní zpracování dle interní dokumentace)

Tento způsob zpracování je velmi obecný a při větším množství politik by mohl být značně nepřehledný, vhodnější by bylo zpracování ve formátu, který je uveden v tabulce č. 9., která obsahuje pravidla pro přenos na vyměnitelná média v případě klasifikace na základě analýzy obsahu označující překročení prahu citlivých údajů při přenosu. Stav klasifikace a překročení prahu citlivých dat by mohl být přidán do části Událost v tabulce jako další sloupec.

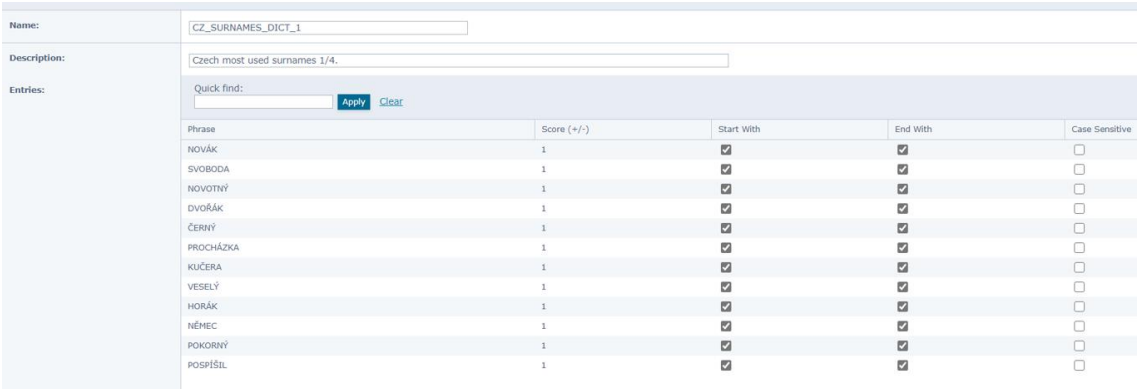
Tabulka č. 9: Pravidla pro přenos na vyměnitelná média

Událost				Zaznamenání akce	Upozornění uživatele	Blokování akce	Šifrování	Povolit výjimku od uživatele (na základě vyskakovacího okna s odůvodněním).	Vyžadovat výjimku od správce
Aktér	**Zařízení**	**Akce**	**Typ média**						
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun na	Externí USB úložiště	×	×			×	
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun z	Externí USB úložiště	×					
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun na	CD/DVD	×	×			×	
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun z	CD/DVD	×					
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun na	SD karta	×	×			×	
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun z	SD karta	×					
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun na	SIM karta/smartphone	×	×			×	
Kterýkoliv uživatel	Spravované klientské zařízení	Přesun z	SIM karta/smartphone	×					

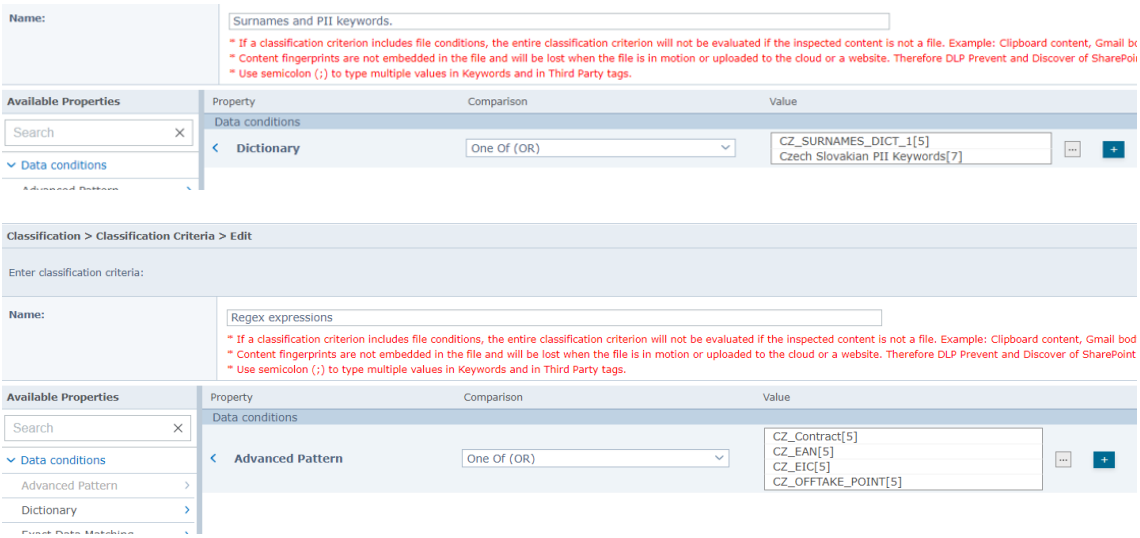
(Zdroj: Vlastní zpracování dle interní dokumentace)

Obrázky udávají příklad aplikace politiky od slovníku po konkrétní politiku v ePO prostředí. Obrázek č.x zachycuje slovník českých příjmení, ty jsou dalším obrázku použita pro spolu s dalšími slovníky pro vytvoření klasifikací na PII (Personally Identifiable Information) a RegEx (Regular Expresssion). Regulérní výrazy obsahují

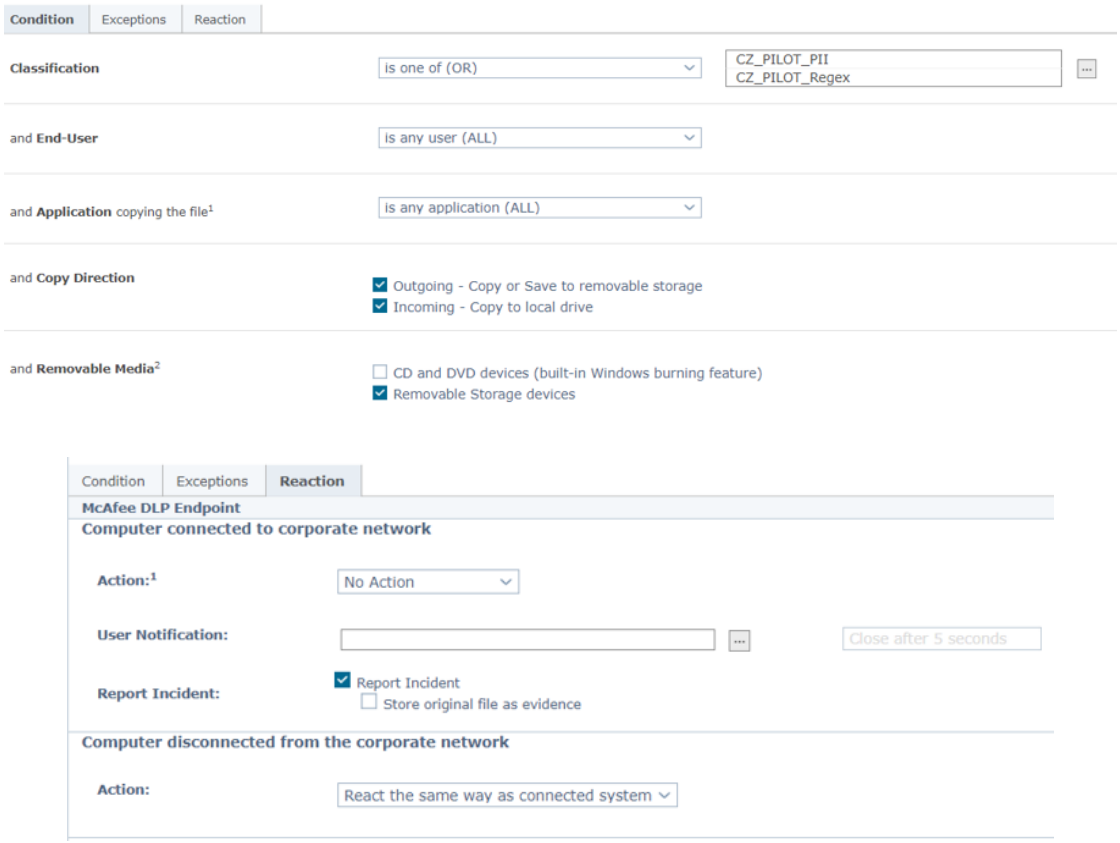
prvky jako čísla smluv, obchodních položek, energetické identifikační kódy a čísla odběrných míst.



Obrázek č. 16: Slovník
(Zdroj: interní dokumentace)



Obrázek č. 17: Využití slovníku pro klasifikace
(Zdroj: interní dokumentace)



Obrázek č. 18: Příklad politiky
(Zdroj: interní dokumentace)

3.2.5 Náklady na současné řešení

Společnost při nasazení a provozu systému využila či stále využívá externí firmy. Ty plnily/plní v rámci nasazení DLP různé role. Při implementaci byla role implementátora zajištěna externí firmou. Podporu provozu kromě Trellix provádí i druhá externí firma, která je v roli integrátora řešení. Třetí externí firma asistuje při konzultaci a formulaci politik. Podpora je řízena SLA.

Zakoupená licence má permanentní formu (perpetual), společnost tedy zaplatila jednorázovou částku a licence k produktu má na dobu neurčitou.

Třetí částí nákladů je provoz serverů. Jak bylo zmíněno v předchozích kapitolách ePO server běží v cloudu. V tomto případě tedy odpadávají pořizovací náklady a zůstávají pouze provozní.

Jednorázovými náklady na pořízení tedy bylo zakoupení licencí a platba externímu subjektu za integraci. Provozními náklady, které společnost platí do dnes představují provoz serveru a podporu a konzultaci od třetích stran. Převážně náklady na podporu neustále rostou.

3.2.6 Další faktory

Soulad s předpisy a právní požadavky

Jak bylo zmíněno, DLP je nutné pro splnění regionálních směrnic, ale také zajišťuje lepší naplnění legislativních požadavků (GDPR) a lepší soulad se směrnicí NIS2. Někteří skupinoví manažeři a architekti kybernetické bezpečnosti nevidí benefity, které může DLP přinést. Kvůli možnosti lepšího souladu s právními požadavky ale nevylučují zařazení DLP do celoskupinových směrnic a tím i zavedení do celé nadnárodní skupiny.

Uživatelské zkušenosti a produktivita

Dopad DLP na práci běžného zaměstnance je převážně omezení využívání USB a vyměnitelných médií. Normální pracovní činnosti ani produktivitu ale nijak neomezuje. Oddělení informační bezpečnosti nezaregistrovalo žádný výrazný odpor ani nedostalo žádné stížnosti. Pro zaměstnance pracující s DLP nepřibývá při rutinním provozu mnoho činností. Jedná se převážně o monitorování fungování, občasné vytvoření reportu

a řešení incidentů, aktualizace či změny nastavení. Mezi jejich činnosti také spadá komunikace se zaměstnanci, u kterých byl odhalen nepovolený software (například audiovizuální materiály) a případná eskalace na liniového vedoucího či compliance.

Technické a integrační výzvy

V současnosti nejsou řešeny žádné problémy s výkonem, škálovatelností nebo kompatibilitou s jinými systémy či aplikacemi ve společnosti. Problémový je ale upgrade na nejnovější verzi produktu, který se zatím z neznámých důvodů nedaří provést. S tím souvisí problematická komunikace se společností Trellix, která často reaguje pomalu.

3.3 Popis zvažovaného řešení

Analyzovaná společnost zvažuje přechod na systém od společnosti Microsoft. Microsoft je nadnárodní společnost založená v Americe v roce 1975. Mezi produkty společnosti Microsoft patří operační systémy, aplikace pro produktivitu a spolupráci napříč zařízeními, serverové aplikace, aplikace pro podniková řešení, nástroje pro správu počítačů a serverů, nástroje pro vývoj softwaru a videohry. Společnost Microsoft také navrhuje a prodává zařízení, včetně počítačů, tabletů, herních a zábavních konzolí, dalších inteligentních zařízení a souvisejícího příslušenství. [24]

Nabízí produkty a služby pro podniky i spotřebitele prostřednictvím portfolia řešení pro kancelářskou produktivitu, zasílání zpráv, spolupráci a další. [23]

Obrázek č. 19: Logo Microsoft
(Zdroj: 24)

Jeho řešení Data Loss Prevention je součástí většího balíčku Microsoft Purview. Tento balíček je zaměřen na podniky a řeší rizika a dodržování předpisů pro služby Microsoft 365, včetně služeb Teams, SharePoint, OneDrive, Exchange a dalších. Purview spojuje dřívější řešení a služby Azure Purview a Microsoft 365 do jedné značky. Oproti Trellix DLP není dělen na více produktů, ale některé jeho funkcionality mohou být omezeny dle formy licence Microsoft 365. [23; 25]

Purview umožňuje organizacím implementovat strategii proti ztrátě dat definicí a uplatněním zásad DLP, které identifikují, monitorují a chrání citlivé informace napříč různými službami a nástroji, které zahrnují nejen řešení Microsoftu, jako jsou: [23; 25]

- Microsoft 365 (Teams, Exchange, SharePoint a OneDrive);
- Aplikace Office (Word, Excel, PowerPoint, …);
- Windows 10, Windows 11 a macOS koncové body;
- Lokální sdílení souborů a lokální služba SharePoint;

- Cloudové aplikace jiných výrobců. [23; 25]

Purview DLP detekuje citlivé položky pomocí hloubkové analýzy obsahu, která zahrnuje shodu primárních dat s klíčovými slovy, vyhodnocení regulárních výrazů, ověření interních funkcí, shodu sekundárních dat, která jsou v blízkosti shody primárních dat, algoritmy strojového učení a další metody pro detekci obsahu, který odpovídá stávajícím zásadám DLP. [23; 25]

Microsoft Purview Compliance Portal poskytuje centrální konzoli pro správu zásad, která správcům umožňuje definovat a spravovat zásady DLP v různých službách. Zásady DLP lze nastavit tak, aby monitorovaly akce uživatelů s citlivými položkami v klidovém stavu, při přenosu nebo při používání, a podle toho lze přijmout ochranná opatření. Všechny sledované aktivity DLP jsou zaznamenávány do auditního logu Microsoft 365, který lze prohlížet a prohledávat z portálu Microsoft Purview Compliance Portal, a jsou směrovány do průzkumníka aktivit, který poskytuje historický přehled aktivit prováděných na označeném obsahu. Pokud uživatel provede akci, která splňuje kritéria zásad DLP, a jsou nakonfigurovány výstrahy, DLP poskytuje výstrahy na panelu pro správu výstrah DLP. Řešení DLP pro lokální skenery rozšiřuje ochranu DLP na lokální sdílené soubory a knihovny dokumentů SharePoint. [23; 25]

Endpoint DLP umožňuje auditování a správu následujících akcí:

Nahrávání do cloudové služby nebo přístup přes nepovolené prohlížeče – lze kontrolovat a omezovat

- Odhalí pokus uživatele nahrát položku do domény služby s omezeným přístupem nebo když se pokusí získat přístup k položce prostřednictvím prohlížeče. Pokud používá nepovolený prohlížeč, aktivita odesílání je zablokována a uživatel je přesměrován na použití schváleného prohlížeče. Schválený prohlížeč pak na základě konfigurace zásad DLP buď povolí, nebo zablokuje odesílání nebo přístup. Na základě seznamu povolených a nepovolených domén v nastavení prevence ztráty dat lze blokovat, upozorňovat nebo kontrolovat, kdy lze chráněné soubory odesílat nebo kdy je možné zabránit jejich odesílání do cloudových služeb. Pokud je nakonfigurovaná akce nastavena na varování nebo blokování, je ostatním prohlížečům (definovaným v seznamu nepovolených prohlížečů v nastavení prevence ztráty dat) přístup k souboru zablokován. [25]

Vkládání do podporovaných prohlížečů – lze kontrolovat a omezovat

- Zjistí, když se uživatel pokusí vložit obsah do domény služby s omezeným přístupem. [25]

Kopírování na vyměnitelné médium USB – lze kontrolovat a omezovat

- Pokud je detekována tato činnost, je možno zablokovat kopírování nebo přesouvání chráněných souborů z koncového zařízení na vyměnitelné médium USB, nebo u činnosti varovat či provést kontrolu. [25]

Kopírování do sdílené síťové složky – lze kontrolovat a omezovat

- Při zjištění této činnosti lze zablokovat, varovat nebo provést kontrolu kopírování nebo přesouvání chráněných souborů z koncového zařízení do libovolné síťové sdílené složky, včetně přesměrovaných zařízení USB, která jsou zobrazena jako síťové sdílené složky na virtuální ploše Azure se systémem Windows 365. [25]

Tisk dokumentů – lze kontrolovat a omezovat

- Pokud je tato činnost zjištěna, můžete tisk chráněných souborů z koncového zařízení zablokovat, varovat nebo provést audit. Tato aktivita se vztahuje také na tiskárny přesměrované při používání Azure Virtual Desktop společně se systémem Windows 365. [25]

Kopírování do vzdálené relace – lze kontrolovat a omezovat

- Detekuje, když se uživatel pokusí zkopírovat položku do relace vzdálené plochy. [25]

Kopírování do Bluetooth zařízení – lze kontrolovat a omezovat

- Zjistí, když se uživatel pokusí zkopírovat položku do nepovolené aplikace Bluetooth (definované v seznamu nepovolených aplikací Bluetooth v nastavení DLP). [25]

Vytvoření a přejmenování položky – pouze kontrolovatelné, ne omezitelné

- Detekuje vytvoření nebo přejmenování položky. [25]

Kopírování do schránky – lze kontrolovat a omezovat

- Při zjištění této aktivity lze zablokovat, zablokovat s přepsáním nebo zkontrolovat kopírování chráněných souborů do schránky na koncovém zařízení. Pokud je pravidlo nastaveno na blokovat nebo blokovat s přepsáním, kopírování je blokováno, pokud je zdrojový obsah citlivý, s výjimkou případů, kdy je cílová stanice v rámci stejné aplikace Microsoft 365 Office. Tato činnost se vztahuje také na přesměrované schránky při použití Azure Virtual Desktop s Windows 365. [25]

Přístup nepovolenými aplikacemi

- Zjišťuje, když se aplikace, která je na seznamu nepovolených aplikací (definovaných v omezených aplikacích a jejich skupinách), pokusí získat přístup k chráněným souborům v koncovém zařízení. [25]

Všechny tyto činnosti jsou podporovány pro Windows 10 a 11, pro macOS je u posledních tří verzí podporována většina s výjimkou vkládání do podporovaných prohlížečů a kopírování do vzdálených relací. [25]

3.3.1 Shrnutí a licence

Silné stránky tohoto řešení zahrnují v posledních letech zvyšující se zaměření společnosti Microsoft na ochranu dat a dodržování předpisů a s tím zavádění bohaté sady funkcí a vlastností napříč celou nabídkou produktů Microsoft 365. Řešení od Microsoftu jsou tak často dobře promyšlená a pomáhají organizacím splnit požadavky na dodržování předpisů a také snížit riziko ztráty dat v důsledku exfiltrace nebo škodlivé manipulace. DLP je většinou do určité míry součástí podnikových plánů Microsoft 365. Tím je možné ušetřit náklady, pokud již společnost využívá řešení od Microsoftu a případný příplatek je obvykle malý. Další výhodou pro společnosti využívající MS produkty je možnost integrace s řadou dalších služeb MS Purview, jako například Purview eDiscovery, Data Governance, Insider Risk Management, nebo již zmiňovaný Purview Information Protection. [23; 25]

Mezi slabé stránky lze zařadit fakt, že DLP řešení Microsoftu se stále rychle vyvíjí a mění, což může ztížit plánování do budoucna a pochopení navázání nabízených funkcí na vlastní strategii ochrany dat. S tím souvisí i horší systém licencování, kde je nabízeno

mnoho DLP funkcí v různých plánech. Mnoho společností vidí Microsoft compliance a DLP řešení jako základní kámen k více komplexnímu řešení, které je doplněno produkty od jiných poskytovatelů. Na závěr stejně jako u řešení Trellix DLP nabízí Microsoft širokou škálu řešení, ale jejich správná integrace a údržba v průběhu používání může být pro organizace zbytečně náročné. [23; 25]

Licence

Jak bylo zmíněno, DLP je součástí balíčku Microsoft Purview, ten je zahrnut v licencích pro Microsoft 365. Dle licence se mohou lišit nabízené služby. Licence Microsoft 365 E3 zahrnuje pouze DLP pro e-maily a soubory. Pro Endpoint DLP a ochranu dat v Teams je vyžadována licence Microsoft 365 E5, či E5 Compliance. Konkrétní rozdělní popisuje následující tabulka. [24; 25]

Tabulka č. 10: Licenční balíčky Microsoft

DLP	**Microsoft 365**			
Licence	E3	E5	E5 Security	E5 Compliace
DLP e-maily a soubory	✓	✓		
DLP pro Teams		✓		✓
Endpoint DLP		✓		✓

(Zdroj: Vlastní zpracování dle 25)

Podmínkou je vždy vlastnictví licence E3, ke které lze poté dokoupit rozšíření E5 Compliance. Funkce a produkty tohoto rozšíření jsou již zahrnuty v E5. Pro firmy nevyužívající řešení od Microsoftu se tedy může jednat o značnou nevýhodu tohoto řešení, protože oba balíčky jsou značně rozsáhlé a zahrnují větší počet produktů, jako Windows, Office 365, OneDrive a další. Firmy by tak nakupovaly velké množství produktů, které nemusí využít.

3.4 Důvody pro přechod

Pro migraci na Microsoft řešení existuje řada důvodů.

Trellix představuje nestandartní řešení v rámci skupiny, přejitím na MS řešení by byl zajištěn lepší soulad se zbytkem organizace a tím i lepší integrace s ostatními systémy a lepší podpora.

Omezení licencí na počet, tedy pokud by počet zaměstnanců vzrostl nad počet zakoupených licencí, musely by se další licence dokupovat. To představuje další náklady, které u Microsoftu neexistují, protože je pro každého zaměstnance, k zajištění plnění pracovních činností, automaticky zařízena licence Microsoft 365 E5 obsahující i DLP.

S náklady souvisí také cena infrastruktury a neustále rostoucí cena externí podpory, které by byly po migraci nižší. Mohlo by se jednat o snížení ceny podpory a její celkové potřeby, z důvodu většího využití MS řešení. Část podpory by pak mohla být řešena interně a v případě externí podpory by byla společnost schopna vyjednat lepší ceny nebo částečně začlenit cenu infrastruktury do své aktuální smlouvy. Celková struktura nákladů na provoz by jinak byla velmi podobná současnému řešení, kde by nefigurovaly ceny za licence a společnost by tak hradila provoz infrastruktury a podporu/konzultaci od třetích stran.

Trellix DLP vyžaduje lokální externí podporu z důvodu složitější instalace a upgradování produktu. Lepší integrace a synergie s prostředím společnosti by teoreticky mohla tuto složitost zmenšit a přispět tak k výše zmíněné redukci potřeby podpory.

V neposlední řadě tu je možnost být „pilotním“ projektem pro případ, že by se vedení rozhodlo o nasazení Purview DLP v dalších regionálních jednotkách. Pro ty by poté provedený projekt implementace Purview DLP mohl pomoci k odhalení částí, které by mohly být problematické a také k nasdílení best practices při provozu a nasazení DLP (např. nastavení politik).

3.5 Požadavky

Ze současného nasazení v obou regionálních jednotkách lze vyvodit požadavky společnosti na DLP systém. Je třeba posoudit potřeby obou jednotek (Rumunsko a Česká republika), protože případná migrace by probíhala obou jednotkách. Důvodem je vysoká pravděpodobnost růstu nákladů pro jednotku, která by zůstala na řešení od Trellix a také zachování celistvosti používaných systémů napříč celou skupinou.

Požadavky lze rozdělit do jednotlivých oblastích týkajících se využití DLP, tedy na management, monitoring a funkční a technické. Konkrétní požadavky jsou uvedeny v následujících tabulkách.

Tyto požadavky bude nutné důsledně porovnat s nabízenými funkcemi MS Purview, ideálně za asistence konzultanta s detailními znalostmi produktů firmy Microsoft. Některé požadované funkce mohou být pokryty jinými produkty, a to buď v rámci MS Purview (např. MIP), nebo jinými již implementovanými systémy. V případě, že MS řešení nebude vyhovovat velké části klíčových požadavků, bude nutné pečlivě zvážit, jestli migraci uskutečnit.

Tabulka č. 11: Požadavky na správu

Management					
Požadavek		Požadované	Nasazeno		Komentář
			CZ	RO	
1	Podpora Active Directory pro synchronizaci systémů – použití specifických kontejnerů	✓	✓	✓	Pro zajištění, že v rozsahu jsou pouze pracovní stanice CZ a RO. Správa uživatelů
2	Nastavení maximálního zatížení pracovní stanice	✓	✓	✓	Nastavení zásad konfigurace klienta systému Windows
3	Podpora a kompatibilita s Office 365, SharePointem a OneDrivem	✓	✓	✓	Aby bylo možné povolit funkci klasifikace pro nově vytvořené dokumenty. Podpora funkcionality MIP. Použití klasifikace od jiných dodavatelů (importované do nástroje).
4	Nastavení politik pro ochranu dat. Přiřazování a vynucování politik na konkrétních skupinách. Hierarchické dědění zásad.	✓	✓	✓	Vytváření a úpravy nových politik. Přiřazení politik. Kompletní úpravy zásad.
5	Hromadná instalace na pracovištích (prostřednictvím GPO, SCCM, centrální správou nebo jiným způsobem)	✓	✓	✓	Instalace a kontrola, zda mají všechny stanice nainstalované funkční produkty, totéž platí pro odinstalaci.
6	Hromadná aktualizace a instalace/odinstalace produktových rozšířeních a doplňkových řešeních na všech nebo na vybraných stanicích	✓	✓	✓	V případě výjimek i samostatná instalace produktu.
7	Podpora Windows 10 a 11	✓	✓	✓	

(Zdroj: Vlastní zpracování)

Tabulka č. 12: Požadavky na monitorování

Monitoring					
Požadavek		Požadované	Nasazeno		Komentář
			CZ	RO	
1	Centrální správa, nastavení zásad pro monitorování. Možnost rozdělení stanic do skupin, správa skupin.	✓	✓	✓	Centrální správa, správa a distribuce DLP politik dle organizační struktury v AD. Řízení je založeno na uživatelské úrovni.
2	Skenování citlivých dat na fyzických úložištích	✓	✓	✓	
3	Skenování citlivých dat na cloudových úložištích	×	×	×	Online skenování dat na úložištích (např. DLP Discover).
4	Označování souborů na základě discovery skenování	×	×	×	Záleží na konkrétním požadavku na discover.
5	Analýza archivů rar, zip atd..	✓	✓	✓	Řešení je schopno nahlédnout dovnitř archivu.
6	Vytvoření logu po zablokování jakékoliv akce (na základě politik, kterou chtěl uživatel provést	✓	Částečně	✓	Logování
7	Zasílání oznámení o incidentech/událostech operátorům DLP (v reálném čase).	✓	×	✓	Upozornění prostřednictvím e-mailu se všemi nebo vybranými detaily.
8	Monitorování a blokování těchto vektorů: USB; e-mail; web/cloud; tiskárny	✓	USB	✓	Sledování názvu souboru, obsahu a dalších detailů dokumentů.
9	Možnost vytvoření vlastního vzoru pro sledování přenosu/využití citlivých dat. Klasifikace informací založena na: klíčových slovech; slovnících; regulárních výrazech; uživateli (ruční klasifikace).	✓	Částečně	✓	Vyhledávání důvěrných údajů (např. rodných čísel) pomocí definovaných klíčů. Úplná úprava a import/export těchto klasifikátorů pro obsah/kontext je povinná

10	Správa zařízení (autorizace médií, takže je možné používat pouze autorizovaná média)	✓	Částečně	✓	
11	Další požadavky Použití DLP Incident manageru Použití dotazů a sestav Tvorba reportů/dotazů na základě obchodních potřeb Automatizovaný export reportů Přístup ke sdílené složce, ve které se vytvářejí sestavy Ruční export reportů Přístup ke sdílené složce, ve které se vytvářejí sestavy	✓	✓	✓	Může být specifické pro konkrétní řešení.

(Zdroj: Vlastní zpracování)

Tabulka č. 13: Funkční a technické požadavky

Funkční a technické					
Požadavek		**Požadované**	**Nasazeno**		**Komentář**
			CZ	**RO**	
1	Aplikace na pracovní stanici s tichým provozem	✓	✓	✓	Možnost skrýt ikony nebo deaktivovat konfigurační pole. Dokud nejsou splněna pravidla ochrany, není nutná interakce s uživatelem.
2	Vynucení šifrování e-mailů v případě práce s citlivými daty	×	×	×	
3	Blokování „Print screen" v případě práce s citlivými daty	×	×	×	
4	Sledování nahrávání dokumentů přes webový prohlížeč	✓	×	Částečně	V případě citlivých následuje vyskakovací okno pro odůvodnění.
5	Automaticky otevírané okno pro odůvodnění akce uživatele při porušení zásad	✓	Částečně	✓	
6	Možnost přizpůsobení vyskakovacích oznámení	✓	✓	✓	tj. změnit textaci
7	Automatické označování nově vytvořených dat na základě jejich DLP klasifikace meta-tagem, vodoznakem	×	×	×	Doplněk pro aplikace Office 365 - stejný jako MIP
8	Tvorba reportu o DLP událostech/incidentech dle business požadavků. Podpora různých formátů (PDF, HTML, XML, CSV)	✓	✓	✓	
9	Funkčnost DLP na koncovém bodu v případě, že stanice nebude připojena k síti (offline režim)	✓	✓	✓	
10	Automatická aktualizace politik a odesílání dat o událostech/incidentech do databáze ihned po připojení stanice do provozu	✓	✓	✓	

11	Zálohování konfigurace, zásad, dat událostí/incidentů a všech relevantních informací na straně správy DLP	✓	✓	✓	
12	Možnost vytvářet nezávislé administrátorské účty. Rozdělení rolí a rozdělení povinností. Protokolování jejich činnosti				
13	Správa RSD – možnost povolit použití pouze registrovaných výměnných médií (blacklisting, whitelist), rozdílné nastavení podle použité politiky (pro různé skupiny)	✓	Částečně	✓	RSD jsou zařízení jako USB port, Bluetooth, čtečky paměťových karet a smartphony.
14	Po vložení neregistrovaného zařízení – zobrazí uživateli přizpůsobitelné vyskakovací okno. Uživatelské rozhraní pro přizpůsobení automaticky otevíraných oken musí podporovat značky html	✓	Částečně	✓	
15	Nouzové řešení pro naléhavé potřeby	✓	✓	✓	Znamená, že pokud by uživatel chtěl provést zakázanou funkci, může kontaktovat operátora DLP a ten může uživateli umožnit splnit jeho naléhavé potřeby. Obcházení zásad.

(Zdroj: Vlastní zpracování)

3.6 Migrace Trellix na Microsoft

Tato část práce představuje popis průběhu migrace z Trellix na MS DLP.

Před samotným zahájením procesu migrace by bylo vhodné provést určité kroky a odpovědět na otevřené otázky, toto lze zařadit do předprojektové fáze projektu . Jde převážně o poskytnutí informací od centrály, jako kdy bude kompletně dokončeno nasazení MWP (managed workplace) klientů (včetně MS Intune), které se zatím očekává někdy uprostřed roku 2024. Kromě ujištění, že požadované licence na Endpoint DLP jsou skutečně dostupné ve skupinové smlouvě, jde také o potvrzení budoucích plánů týkajících se DLP, zda jsou plány na zavádění ve větším rozsahu v budoucnosti. Pokud ano, je dobré mít informace, jak budou skupinové procesy provázány s lokálními DLP požadavky.

Dalšími činnostmi by mělo být provedení GAP analýzy pro zhodnocení oblastí, které pokrývá MS Purview a zda je technicky možné provést migraci při zachování současných požadavků na funkce. Podle výsledku by mělo být provedeno rozhodnutí o proveditelnosti migrace. V tom případě by následoval POC (Proof of Concept) pro Purview DLP, tedy otestování systému v testovacím prostředí. Pro POC je vhodné, z důvodu rozdílnosti UI a definice politik v ePO konzoli a MS Purview portálu, zpracovat politiky na obecná pravidla, podobně jako v kapitole 3.2.4 a také připravit základní scénáře na otestování. Podle zhodnocení výsledků testu a přechozích analýz by mělo být provedeno konečné rozhodnutí o provedení implementace, v tom případě by mohla začít projektová fáze. Konkrétní činnosti jsou spolu s jejich trváním uvedeny v následujících kapitolách.

3.6.1 Intervenční oblasti a klíčové role

Pro úspěšné provedení změny je důležité identifikovat intervenční oblasti, kterých by se provedená změna mohla dotknout a klíčové role, které budou mít vliv na změnu.

Intervenční oblasti

- **Lidské zdroje a jejich řízení** – Běžných zaměstnanců se změna výrazně nedotkne, agenta na koncové stanici lze odinstalovat i instalovat bez nutnosti jejich zásahu. Změna je ale může ovlivnit tím, že se rozhodne o zavádění nových

funkcionalit DLP a jejich činnosti tak budou více monitorovány. Pracovníci, kteří s DLP budou aktivně pracovat budou vyžadovat školení.

- **Organizační struktura firmy** – Změna nebude pravděpodobně vyžadovat větší organizační změny. Možné jsou drobné úpravy odpovědností a rolí v rámci IT/bezpečnostních oddělení za správu nového DLP. Rozdělení rolí by mohlo zůstat stejné jako současné (uvedeno v kapitole 3.2.2) s tím, že zaměstnanci zodpovědní za současné DLP budou mít zachovanou odpovědnost za nové řešení.
- **Technologie firmy** – Změna DLP řešení nabídne nové funkcionality, přičemž některé mohou chybět. Nabízí se ale možnost lepší integrace s ostatními MS produkty, jako například Microsoft Information Protection (MIP) nebo MS Edge.
- **Komunikační a organizační toky a procesy firmy** – Stejně jako u organizační struktury, nebude změna vyžadovat větší změny. Bude třeba provést aktualizace bezpečnostní dokumentace, politik a směrnic pro nový DLP systém. Stejně tak zavedení nových nebo úprava stávající procesů pro správu, monitoring a reporting DLP v Microsoft prostředí.

Klíčové role pro úspěšnou změnu

- **Agent změny –** Hlavní roli by pravděpodobně zastával externí implementátor s podporou z vnitřního prostředí společnosti. V rámci společnosti vybere zaměstnance zodpovědné za změnu ze svého oddělení vedoucí informační bezpečnosti. IT podpora bude zajištěna jak interně, tak externě.
- **Sponzor změny –** Sponzorem změny bude vedoucí a ostatní pracovníci oddělení informační bezpečnosti a také vedení regionální jednoty a skupinový architekt bezpečnosti společnosti.
- **Advokát změny–** Roli advokáta změny zle přiřadit IT týmu, ostatním zaměstnancům v oblasti kybernetické bezpečnosti a skupinovým manažerům a architektům bezpečnosti.

3.6.2 Činnosti migrace

V následující tabulce jsou vyobrazeny činnosti, které by bylo potřeba provést pro úspěšnou migraci DLP systému. Je nutně zmínit, že tabulka, hlavně doby trvání jednotlivých fází, je spíše orientační. Jedním z důvodů je stálá nejistota uskutečnění

projektu a korporátní prostředí, které může značně ovlivnit doby trvání jednotlivých činností. Z tohoto důvodu nemá smysl provádět časovou analýzu, tabulka tedy rozděluje projekt na jednotlivé hrubé fáze a odhaduje jejich přibližné trvání. Návaznost těchto fází je lineární, stejně jako v tabulce. Konkrétní činnosti, jejich návaznosti a doby trvání by bylo vhodné určit až v předprojektové fázi migrace, kdy bude rozhodnuto o konkrétním rozsahu.

Pro úspěšné provedení procesu migrace je vhodné řídit se zásadami projektového řízení, vytvořit RACI matici, stanovit vhodnou časovou i finanční rezervu a celkově dodržovat systematický přístup k řízení změn.

Tabulka č. 14: Činnosti migrace

Činnost	Výstup	Doba trvání
A. Iniciační fáze 1. Ustanovení projektového týmu a cílů projektu 2. Analýza stávajícího stavu a rozsahu využití Trellix DLP 3. Kontrola skupinové smlouvy s MS	Analýza současného stavu, projektový tým a potvrzení dostupnosti licencí	2 týdny
B. Přípravná fáze 1. Průběžné sledování stavu nasazení MWP klientů a MS Intune 2. Zmapování lokálních a skupinových procesů s ohledem na migraci a zavádění DLP 3. Detailní zmapování aktuálních DLP politik a procesů v Trellix 4. GAP analýza a konzultace s expertem na MS Purview 5. Proof of Concept (POC) 6. Případné doplnění/úprava požadavků a návrh kompenzačních opatření pro řešení nedostatků Purview DLP	Rozhodnutí o proveditelnosti migrace. Zdokumentování DLP politik. Seznam požadavků.	2 až 3 měsíce
C. Návrh cílového stavu 1. Návrh nasazení a architektury MS Purview DLP	Návrh cílového stavu MS Purview DLP pokrývající architekturu, rozsah,	5 týdnů

2. Definice rozsahu a přístupu k migraci (uživatelsky nebo počítačově centrický) 3. Návrh transformace stávajících DLP politik 4. Specifikace požadovaných oprávnění a rolí pro správu a používání 5. Vyjednání a smluvní zajištění externí podpory pro provozní fázi MS Purview DLP	transformaci politik a oprávnění. Včetně zajištění podpory provozu.	
D. Testovací prostředí 1. Příprava testovacího prostředí 2. Instalace a konfigurace v testovacím prostředí 3. Testování funkcí a úpravy nastavení	Systém a politiky otestovány a přizpůsobeny k nasazení.	3 týdny
E. Realizace migrace 1. Příprava prostředí pro nasazení do produkce 2. Školení klíčových uživatelů 3. Pilotní implementace a průběžné doladění 4. Migrace a úprava politik, historických dat a nastavení 5. Plná implementace (ve vlnách)	MS Purview DLP plně implementované v produkčním prostředí.	2 až 3 měsíce
F. Finalizace migrace 1. Ladění v produkčním prostředí 2. Zpřísnění bezpečnostních politik 3. Finální školení uživatelů a konečné přiřazení rolí a odpovědností 4. Odstranění agentů Trellix a ukončení relevantních smluv	Aplikované finální nastavení a politiky systému. Klíčoví uživatelé plně proškoleni.	4 týdny
G. Ukončení a vyhodnocení 1. Kontrola dosažení cílů a zhodnocení migrace 2. Ukončení migrace, schválení současného stavu	Závěrečná zpráva projektu hodnotící úspěšnost migrace.	2 týdny

(Zdroj: Vlastní zpracování)

3.6.3 Rizika migrace

Již nyní lze zevrubně identifikovat rizika, se kterými by se projekt migrace mohl potýkat. Je nutné zmínit, že se nejedná o bezpečností rizika, ale rizika týkající se provedení změny. Tato rizika by mohla značně ohrozit úspěch projektu, způsobit prodlevy, navýšení nákladů nebo nedostatečné pokrytí DLP funkcemi po změně.

Tabulka č. 15: Identifikace rizik

Č.	Hrozba	Scénář
1	Nekompatibilita nebo nedostatečná funkcionalita MS Purview DLP ve srovnání s požadavky společnosti	Zpoždění nebo zrušení migrace. Chybějící funkce.
2	Problémy s migrací existujících dat a politik z Trellix	Nové DLP nelze rychle plnohodnotně použít. Narušení kontinuity ochrany dat.
3	Nedostatečné znalosti	Prodlevy instalace, konfigurace a testování. Komplikace s integrací.
4	Nedostatečné proškolení administrátorů a koncových uživatelů	Provozní problémy – nesprávná obsluha a správa nového DLP řešení snižující jeho účinnost a tvorba chyb
5	Nedostatečná koordinace mezi klíčovými skupinami zaměstnanců nebo mezi odděleními	Zpoždění a konfliktní požadavky
6	Riziko výpadků nebo narušení ochrany dat během přechodné fáze	Během migrace nebyly správně pokryty požadavky na ochranu dat. Únik citlivých dat.
7	Prodlevy a zpoždění v harmonogramu projektu. Nečekané výdaje	Nedařilo se splnit termíny dílčích činností, zpoždění projektu. Vyčerpání rozpočtu projektu.
8	Problémy se škálovatelností nebo výkonností	Problémy při testování či implementaci – zpoždění projektu. Provozní problémy
9	Odchod klíčových členů projektového týmu během realizace	Absence klíčového člena zhoršila anebo zastavila postup migrace

(Zdroj: Vlastní zpracování)

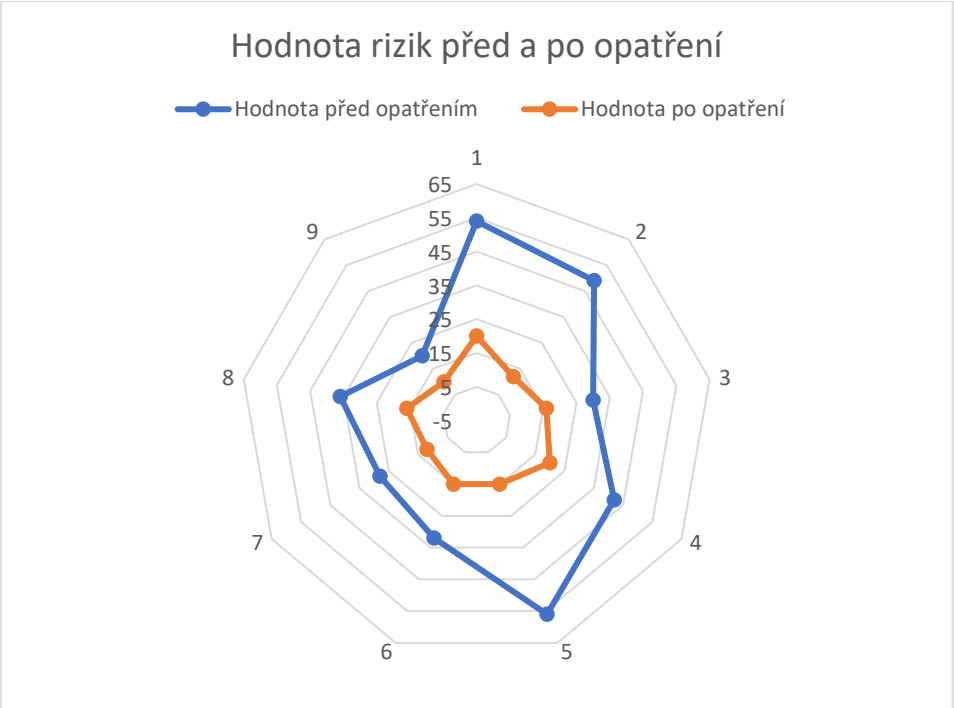
Pomocí kvantitativního odhadu lze určit hodnotu pro jednotlivá rizika. Hodnota představuje násobek pravděpodobnosti a dopadu (na škále 1-10). Jak lze vidět, největší rizika se týkají technických a organizačních aspektů projektu.

Ke snížení hodnot rizik jsou dále navržena opatření, která snižují pravděpodobnost či dopad rizika a tím i jeho hodnotu na akceptovatelnou úroveň.

Tabulka č. 16: Kvantifikace rizik a návrhy na opatření

Č.	P	Dopad	Hodnota	Opatření	P	Dopad	Hodnota
1	6	9	**54**	Důkladná analýza požadavků ve fázi přípravy za asistence externího konzultanta MS. Zvážit možnosti doplnění funkcí jinými MS nástroji.	4	5	**20**
2	7	7	**49**	Detailní zmapování existujících politik a nastavení DLP. Robustní zálohy .	3	4	**12**
3	5	6	**30**	Zajištění odpovídajících schopností prostřednictvím školení nebo externích konzultantů. Důsledné testování v přípravné fázi.	4	4	**16**
4	6	7	**42**	Pečlivá příprava školících materiálů a plánů. Proškolení klíčových osob s předstihem před ostrým nasazením.	4	5	**20**
5	7	8	**56**	Ustanovení řídícího výboru projektu se zástupci všech dotčených oddělení. Pravidelné statusy a komunikace.	5	3	**15**
6	4	8	**32**	Průběžné monitorování stavu obou DLP řešení, redundance po dobu souběžného provozu, postupné zavádění nového řešení po částech	3	5	**15**
7	7	4	**28**	Realistické stanovení délky činností. Detailní kalkulace nákladů. Stanovení finanční a časové rezervy. Průběžné sledování čerpání a plnění harmonogramu. Eskalace odchylek.	4	3	**12**
8	6	6	**36**	Naddimenzování infrastruktury, sledování vytížení v rané fázi produkčního provozu a příprava rozšíření kapacit	4	4	**16**
9	2	10	**20**	Zajištění zastupitelnosti mezi klíčovými členy projektového týmu	2	5	**10**

(Zdroj: Vlastní zpracování)



Obrázek č. 20: Pavučinový graf rizik
(Zdroj: Vlastní zpracování)

3.7 Časté problémy

Organizace se při nasazování a používání DLP systémů setkávají s řadou problémů. Tyto problémy je potřeba odhalit a adresovat v případě migrace na MS Purview, tak i v případě setrvání u současného řešení Trellix pro zajištění hladkého provozu. [1; 13]

3.7.1 Administrativní náročnost řešení DLP incidentů

DLP systémy mohou generovat mnoho incidentů a nutit tak jejich uživatele procházet citlivá interní data, která mohou obsahovat osobní údaje zaměstnanců, údaje o kontraktech apod. DLP systémy mohou vytvářet desítky až stovky incidentů týdně, kde řešení každého incidentu představuje komplexní a časově náročný proces. To vede u většiny velkých podnikových implementací k upuštění od restriktivních politik a přesunu systému do monitorovacího módu, kde pouze sbírá informace pro potřeby pozdější analýzy. [1; 13]

Možností je zapojení uživatelů do rozhodovacího procesu, zda se skutečně jedná o DLP incident. Tím lze omezit vystavení klíčových uživatelů DLP systému citlivým datům, ale také snížit počet celkových i false positive incidentů. Toto zapojení bývá realizováno vyskakovacím oknem při podezření na incident, kde je uživatel upozorněn a také mu může být nabídnuta možnost odůvodnění prováděné akce. Takové zapojení uživatelů umožňuje zabránit omylům (např. chybně zadaná e-mailová adresa) a také má školící účinek, protože zaměstnanci si nejsou vědomi citlivosti dat, se kterými pracují, a že jejich jednání není v souladu s firemní politikou. [1; 13]

Společnost v současnosti tato vyskakovací okna příliš nepoužívá, při rozšíření/migraci systému by bylo vhodné zvážit začlenění této funkcionality do více nových či stávajících politik.

3.7.2 Náročnost implementace

Jelikož jsou DLP systémy dodávány ve formě rámcového řešení (framework), bez definovaných bezpečnostních politik, musí si organizace sama navrhnout pravidla a definovat a nasadit bezpečností politiky. Takové řešení je nevhodné pro malé

organizace bez bezpečnostních týmů. I u velkých organizací je integrace do podnikového prostředí časově i finančně náročná a probíhá za využití externího integrátora. [1; 13]

Pro řešení tohoto problému je možné zvážit pořízení systému s předdefinovanými politikami na bázi best practises, standardů a právních předpisů. Flexibilita při tvorbě slovníků a politik také přináší usnadnění implementace a větší nezávislost na dodavateli technologie a externích integrátorech.

Tento problém se týká společnosti v případě, že proběhne migrace na Purview DLP, které sice nenabízí předdefinované politiky, ale společnost má k dispozici rámec pro jejich tvorbu ve formě aktuálně používaných politik. K dispozici jsou také současně používané slovníky. Využití externího integrátora a časová náročnost implementace jsou ale vzhledem k velikosti společnosti nevyhnutelné.

3.7.3 Velké množství false positive incidentů

Falešně pozitivní incident je situace, kdy DLP systém označí činnost za incident, ale ve skutečnosti se o bezpečnostní incident nejedená. False negative (falešně negativní) incident je opakem, kdy se uskutečnil bezpečnostní incident, ale DLP systém ho nezachytil. V případě, že DLP systémy generují velké množství false positive událostí, zbytečně rostou nároky na správu. Protože často dochází k blokování legitimní komunikace běžných uživatelů, končí takové systémy často ve stavu monitoringu, ve kterém také nejsou příliš užitečné. Pokud mají tento problém, tak často celkově generují velké množství událostí, klíčový uživatel takového systému pak případně musí tyto události procházet a identifikovat skutečné a false positive události. [1; 13]

Řešením je správné nastavení a definice pravidel pro analýzu dat, a to především volba techniky analýzy obsahu a její řádná konfigurace. Společnost nemá v dohledné době plány na rozsáhlé využití žádné z komplexnějších technik, uvedených v podkapitole 1.4.1, které jsou často náročnější na false positives i negatives. Do budoucna je ale dobré si na tento problém dávat pozor při nastavování nových politik.

3.8 Posouzení DLP systému

Současný systém Trellix je funkční, nepotýká se žádnými výraznými technickými či organizačními problémy a splňuje požadavky společnosti na monitoring a ochranu dat. Systém je v provozu od roku 2020, ale nejsou plně využity jeho možnosti – nabízí řadu funkcí, které společnost nevyužívá. Pokud by společnost chtěla zlepšit svoji ochranu dat, tak může rozšířit současný systém o nové politiky, nebo provést migraci na jiné řešení. Existují důvody pro zvážení migrace na Microsoft Purview DLP. Mezi hlavní patří:

- Zajištění lepšího souladu se zbytkem organizace a lepší integrace s jinými systémy Microsoft.
- Potenciální snížení nákladů na provoz a podporu díky využití stávajících licencí Microsoft 365 E5.

Pokud by se rozhodlo o zavádění DLP v rámci celého nadnárodního koncernu, jednalo by se s nejvyšší pravděpodobností o MS Purview DLP, migrace by poté mohla být zároveň vyžadována od vedení. V tomto ohledu by mohla lokální jednotka provést de facto pilotní projekt nasazení tohoto systému v rámci skupiny. Licence pravděpodobně pokrývá všechny potřebné prvky pro nasazení MS DLP bez nutnosti dokoupení rozšíření. Technicky je migrace také proveditelná, Microsoft Purview nabízí širokou řadu funkcí mimo DLP a měl by být schopen pokrýt všechny klíčové požadavky, v této oblasti je nutné provést důkladnou analýzu. Dále v rámci studie proveditelnosti migrace je potřeba otestovat Purview DLP formou POC. Pokud bude shledán vyhovujícím a migrace bude odsouhlasena, lze přistoupit k projektové fázi.

Na základě výše uvedeného by bylo vhodné v současné době pokračovat s řešením Trellix DLP během roku 2024. Zároveň provést příslušné analýzy a případně POC pro Microsoft Purview DLP, také zjistit všechny další potřebné informace a provést důležitá rozhodnutí, jako například zda nové řešení bude fungovat a monitorovat události na základě AD (uživatelů) nebo pracovních stanic. Pokud budou výsledky uspokojivé, může se v roce 2024 přistoupit k samotné migraci na nové řešení. Případná migrace by měla být řízena podle zásad projektového řízení a měla by zohlednit intervenční oblasti i klíčové role popsané v dokumentu.

3.8 Finanční zhodnocení

Tato část práce zhodnocuje přibližné finanční zhodnocení přechodu na jiného dodavatele DLP řešení. Jak bylo zmíněno v kapitolách 3.2.4 a 3.4, struktura nákladů je velmi podobná pro obě řešení.

Perpetual licence Trellix DLP Endpoint se pohybuje kolem $120. Společnost má v současné době 3 500 ks licencí, původní pořízení licencí by tedy dnes stálo téměř 10 000 000 Kč. Licence má permanentní formu (perpetual), zákazník zaplatí jednorázově a licenci má na dobu neurčitou. Upuštěním od tohoto řešení tedy společnost neušetří žádné náklady týkající se licencí, jako by bylo možné u modelu předplatného (subscription). [18]

Cena licence Microsoft 365 E5 Compliance je €57.70 na uživatele na jeden měsíc. Na rok je to tedy €692,4 za uživatele. Dostáváme se tak na částku €2 423 400, po přepočtu 61 324 137 Kč. Tuto částku ale společnost nemusí uhradit, jelikož již hojně používá různá řešení od Microsoftu, má skupina pořízeny velké licenční balíčky, včetně balíčku Microsoft 365 E5, tento balíček totiž zahrnuje i Windows, aplikace Office 365 a další. [26]

Otázkou jsou tedy náklady implementace, podpory a provozu řešení. Velká část systémů společnosti funguje v cloudovém prostředí, včetně současného DLP řešení, budoucí DLP řešení by fungovalo obdobně, není teda potřeba měnit či pořizovat nový hardware. Architektura nebude potřeba nová ani nebude vyžadovat rozsáhlé změny, jen úpravu či rozšíření.

Budoucí cenu podpory lze jen těžce odhadnout, vzhledem k většímu využití Microsoft řešení společností je ale možné odhadnou, že cena podpory Purview DLP bude nižší než ta současná. Další náklady představují po-implementační konzultace, které se týkají používaných politik atd. Tyto konzultace jsou v rozsahu jednotek MD (man-day) za měsíc a společnost je také využívá i v současnosti.

Největší položku nákladů tedy představuje samotná práce na procesu přechodu. Velké množství činností ze všech fází změny je společnost schopna si zajistit sama. Bude ovšem potřebovat zajistit některé činnosti i externě, jako například konzultanta na testy Microsoft řešení či systémového integrátora. Cena se může vyšplhat až na 2000 Kč za hodinu. Rozsah této práce je odhadnut na přibližně 20 MD.

Tabulka č. 17: Náklady

Položka	Odhad náročnosti	Odhad ceny	Celkem
Implementační práce	20 MD	16 000 Kč / MD	320 000 Kč

(Zdroj: Vlastní zpracování)

ZÁVĚR

V této diplomové práci byla představena energetická společnost, která působí na nadnárodním trhu. Cílem práce bylo posouzení nasazení DLP ve zmíněné společnosti se zhodnocením přechodu k jinému dodavateli.

Problematice bezpečnosti a ochrany dat se věnovala teoretická část. V analytické části byly vedle popisu společnosti, jejího oboru podnikání a struktury, uvedeny i klíčové body současného systému řízení bezpečnosti informací.

Současné i zvažované řešení bylo popsáno v návrhové části, včetně aktuálního nasazení řešení a používaných politik. Na základě těchto informací a analýzy současného stavu byla zpracována problematika migrace DLP systému. Zmiňovanou změnou je přechod z řešení Trellix DLP na Microsoft Purview Data Loss Prevention. Byly stanoveny důvody pro přechod a požadavky na DLP řešení, následně identifikovány dopady do intervenčních oblastí, klíčové role pro změnu a činnosti pro úspěšné provedení migrace. Migrace a její uskutečnění se jako každý jiný projekt potýká s různými riziky, proto byla identifikována a kvantifikována klíčová rizika ohrožující průběh a návrh opatření k jejich zmírnění. Závěrem bylo provedeno zhodnocení současného systému a jeho případné změny.

Trellix DLP je funkční, správně zařazený do organizace s přidělenými rolemi a souvisejícími odpovědnostmi a stanovenými procesy, není však zcela efektivně využitý. Nicméně existují důvody pro zvážení migrace na systém Microsoft Purview DLP, který by mohl přinést lepší integraci s ostatními systémy společnosti, snížení nákladů a sjednocení řešení v rámci celé skupiny.

Z těchto důvodů lze doporučit provedení přechodu na jiného dodavatele, nicméně konkrétní úsporu nákladů lze jen velmi obtížně kvantifikovat, protože oba systémy mají velmi podobnou strukturu nákladů na vlastnictví a licence do finančního zhodnocení nevstupují. Hlavní úspora by spočívala ve snížení nákladů na podporu a systémového integrátora, které by si společnost mohla pokrýt interními zdroji nebo by byla schopná vyjednat lepší cenu. Zjištění míry a cena zajištění podpory a role integrátora externími firmami by mělo být vedle studie proveditelnosti a POC dalším kritériem k odsouhlasení migrace, jejíž projekt může být finančně i časově náročný a při malých úsporách by se

nemusel vyplatit vůbec anebo s velmi dlouhou dobou návratnosti investice. V případě upuštění od záměru provedení přechodu na Purview DLP, z jakéhokoliv důvodu, lze doporučit rozšiřování současného systému implementací nových politit, které pokryjí další komunikační kanály a tím sníží riziko úniku dat. Ať už bude společnost pokračovat se stávajícím nebo přejde na nové řešení, je zásadní pravidelně revidovat a aktualizovat bezpečnostní politiky a postupy v souladu s nejnovějšími hrozbami a trendy v oblasti ochrany dat.

V neposlední řadě byla provedena krátká finanční zhodnocení změny, která je shrnuta na předchozích řádcích.

Řízení provozu a změny DLP systému je komplexním procesem, který vyžaduje důkladnou přípravu a aktivní zapojení odborníků z různých oblastí od IT, přes bezpečnost až po řízení zdrojů. Práce poukazuje na nutnost systematického postupu při zhodnocování a realizování takových změn systémů organizace v kontextu neustále se zvyšujících kybernetických rizik.

SEZNAM POUŽITÝCH ZDROJŮ

[1] SEDLÁK, Petr a KONEČNÝ, Martin. *Přeměna ISMS v manažerské informatice*. Brno: CERM, akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.

[2] [SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-068-2.

[3] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[4] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN EN ISO/IEC 27000, *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Praha,2020.

[5] NELSON, *Daniel. Structured vs. Unstructured Data*. Online. Unite.ai. 23. 8. 2020. Dostupné z: https://www.unite.ai/structured-vs-unstructured-data/ [cit.2023-03-24].

[6] IBM. *X-Force Threat Intelligence Index*. Online. 2024. Dostupné z: https://www.ibm.com/reports/threat-intelligence. [cit. 2024-05-02].

[7] IBM. *Cost of a Data Breach Report 2023*. Online. IBM. 2023. Dostupné z: https://www.ibm.com/reports/data-breach. [cit. 2024-03-20].

[8] BRULÍK, Richard. *Moderní kyberbezpečností software ochrání data i před záškodníkem uvnitř firmy*. Online. SystemOnLine. Dostupné z: https://www.systemonline.cz/it-security/jak-ochranit-data-pred-zaskodnikem-uvnitr-firmy.htm. [cit. 2024-05-02].

[9] PONEMON INSTITUTE. *2022 Cost of Insider Threats Global Report*. Online. 2022. Dostupné z: https://www.proofpoint.com/au/resources/threat-reports/cost-of-insider-threats. [cit. 2024-05-02].

[10] CODE42. *2021 Data Exposure Report*. Online. 2021. Dostupné z: https://www.code42.com/resources/reports/2021-data-exposure. [cit. 2024-05-02].

[11] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN EN ISO/IEC 27002, *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti*. Praha; 2023.

[12] RONEY, Chris. *Data Leak Prevention vs Data Loss Prevention: A Comprehensive Guide to Secure Your Data*. Online. Endpoint Protector. 19. 12. 2023. Dostupné z: https://www.endpointprotector.com/blog/data-leak-prevention-vs-data-loss-prevention-guide/. [cit. 2024-05-02].

[13] KADRMAS, Petr. *Ochrana před ztrátou dat – systémy DLP*. Online. SystemOnLine. 2010. Dostupné z: https://www.systemonline.cz/it-security/ochrana-pred-ztratou-dat-systemy-dlp.htm. [cit. 2024-05-03].

[14] ROTHMAN, Mike a MOGULL, Rich. *Understanding and Selecting a Data Loss Prevention Solution*. Online. Securosis. 31. 11. 2017. Dostupné z: https://cdn.securosis.com/assets/library/reports/Understanding_and_Selecting_DLP.v3_FINAL_.pdf. [cit. 2024-05-02].

[15] DIGITAL GUARDIAN. *The Definitive Guide to Data Loss Prevention*. Online. Digital Guardian. 2016. Dostupné z: https://www.infosecpartners.com/images/pdf/Definitive-Guide-Data-Loss-Prevention.pdf. [cit. 2024-05-02].

[16] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN EN ISO/IEC 27001, *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky*. Praha; 2023.

[17] SEDLÁK, Petr**.** *Management informační bezpečnosti.* (přednáška) Brno: VUT v Brně, Fakulta podnikatelská, 2022.

[18] *Dolar, Americký dolar USD, kurzy měn*. Online. Kurzy.cz. Dostupné z: https://www.kurzy.cz/kurzy-men/nejlepsi-kurzy/USD-americky-dolar/. [cit. 2024-03-28].

[19] STG. *Symphony Technology Group Announces the Launch of Extended Detection and Response Provider, Trellix.* Online. STG. 2022. Dostupné z: https://stg.com/news/symphony-technology-group-announces-the-launch-of-extended-detection-and-response-provider-trellix/. [cit. 2024-03-28].

[20] STG. *McAfee Announces Sale of Enterprise Business to Symphony Technology Group for $4.0 Billion*. Online. STG. 2021. Dostupné z: https://stgpartners.com/news/mcafee-announces-sale-of-enterprise-business-to-symphony-technology-group-for-4-0-billion/. [cit. 2024-03-28].

[21] TRELLIX. *Data Loss Prevention*. Online. Trellix. Dostupné z: https://www.trellix.com/products/dlp/. [cit. 2024-04-01].

[22] TRELLIX. *Trellix Data Loss Prevention 11.11.x Product Guide*. Online. Trellix. 2024. Dostupné z: https://docs.trellix.com/bundle/data-loss-prevention-landing-page/page/UUID-d99a9913-80b8-d1b9-e030-9186ad9648ff.html. [cit. 2024-04-01].

[23] THE RADICATI GROUP, INC. *Data Loss Prevention - Market Quadrant 2024*. Online. Radicanti. 2024. Dostupné z: https://www.forcepoint.com/sites/default/files/resources/industry_analyst_reports/report-2024-radicati-dlp-market-quadrant-en_0.pdf. [cit. 2024-04-01].

[24] MICROSOFT. *Ochrana před únikem informací Microsoft Purview*. Online. Microsoft.. Dostupné z: https://www.microsoft.com/cs-cz/security/business/information-protection/microsoft-purview-data-loss-prevention. [cit. 2024-04-05].

[25] MICROSOFT. *Learn about data loss prevention*. Online. Microsoft. 2024. Dostupné z: https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp. [cit. 2024-04-05].

[26] *Kurz Eura, Euro EUR, aktuální kurzy koruny a měn*. Kurzy.cz. Online. Dostupné z: https://www.kurzy.cz/kurzy-men/nejlepsi-kurzy/EUR-euro/. [cit. 2024-03].

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

AD	Active Directory
ČSN	Česká technická norma
DC	Device Control
DLP	Data Loss (Leak) Prevention
FRP	File and Removable Media Protection
GDPR	General Data Protection Regulation
ICT	Informační a komunikační technologie (Information and Communication technology)
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systém
IS	Informační systém
ISM	Information Security Management
ISMS	Information Security Management System
IT	Informační technologie (Information Technology)
MS	Microsoft
OS	Operační systém
PII	Personally Identifiable Information
POC	Proof of Concept
RegEx	Regular Expression
SLA	Service Level Agreement
ZB	Zetta Bajt
ZKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha č. 1: Klasifikační schéma hodnocení dopadu

Lokální stupnice hodnocení dopadu						
Kritérium ---- Klasifikační stupeň	**Finanční ztráta (čistá ztráta)**	**Poškození dobrého jména**	**Narušení práv a předpisů**	**Narušení obchodních aktivit**	**Dopad na bezpečnost osob**	**Únik osobních dat; dopad na ochranu soukromí osob**
Nízká	Do 500 000 Kč	Poškození dobrého jména v určité zájmové skupině nebo na regionální úrovni	Následky jsou omezené na část společnosti	Přípustná doba výpadku je mezi 5 a 20 pracovními dny	Lehká zranění osob	Malé sociální nebo finanční dopady
Střední	Mezi 500 000 a 5 000 000 Kč	Poškození dobrého jména na národní úrovni s předpokládaným trváním následků kratším než 6 měsíců	Následky nese jediná společnost	Přípustná doba výpadku mezi 24 hodinami a 5 pracovními dny	Zranění nevyžadující okamžitou lékařskou péči	Postřehnutelné sociální nebo finanční dopady
Vysoká	Mezi 5 000 000 a 10 000 000 Kč	Poškození dobrého jména na národní úrovni s předpokládaným trváním následků víc než 6 měsíců	Následky pro všechny regionální společnosti	Přípustná doba výpadku je mezi 4 a 24 hodinami	Těžká zranění vyžadující okamžitou lékařskou péči	Vážné sociální nebo finanční dopady
Velmi vysoká	Nad 10 000 000 Kč*	Poškození dobrého jména na mezinárodní úrovni	Následky přesahující lokální národní úroveň	Přípustná doba výpadku je menší než 4 hodiny	Smrtelné úrazy	Ničivé sociální nebo finanční dopady

(Zdroj: vlastní zpracování dle interní dokumentace)