UNIVERZITA PARDUBICE

Fakulta ekonomicko-správní

DIPLOMOVÁ PRÁCE

2025 Bc. Barbora Pecháčková

Univerzita Pardubice
Fakulta ekonomicko-správní

Ochrana firmy proti malwaru

Diplomová práce

2025 Bc. Barbora Pecháčková

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Barbora Pecháčková**
Osobní číslo:	**E22461**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Ochrana firmy proti malwaru**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout bezpečnostní politiku zvolené firmy proti malwaru.

Osnova:
- Popis stávajících hrozeb malwaru ve firmách.
- Analýza stávající ochrany vybrané firmy proti malwaru.
- Analýza rizik.
- Návrh bezpečnostní politiky zvolené firmy proti malwaru.

Rozsah pracovní zprávy: **Cca 55 stran.**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

FELDMAN, J., MISENAR, S., CONRAD, E. *CISSP Study Guide*. Syngress, 2023.
KOLOUCH, J. *CyberCrime*. CZ. NIC, 2016.
KOLOUCH, J., BAŠTA, P. *CyberSecurity*. CZ. NIC, zspo, 2019.

Vedoucí diplomové práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2024**
Termín odevzdání diplomové práce: **30. března 2025**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

Prohlašuji:

Práci s názvem Ochrana firmy proti malwaru jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30.03. 2025

Bc. Barbora Pecháčková

PODĚKOVÁNÍ

Ráda bych poděkovala své rodině za trpělivost, podporu a povzbuzení během celého studia i při psaní této diplomové práce. Zvláštní poděkování patří mému vedoucímu práce panu doc. Ing. Miloslavu Hubovi, Ph.D. za cenné rady a ochotu vždy pomoci. Poděkování patří také všem vyučujícím Fakulty ekonomicko-správní Univerzity Pardubice za znalosti a inspiraci, které mi poskytli během studia.

ANOTACE

Diplomová práce se zabývá problematikou ochrany firem proti malwaru. V teoretické části je popsána kybernetická bezpečnost, její význam pro organizace a základní legislativní rámce. Dále je zpracována typologie malwaru, jeho historický vývoj a specifika výskytu ve firemním prostředí. Praktická část je zaměřena na analýzu české společnosti Delta-M s.r.o. Byla provedena analýza stávajících bezpečnostních opatření, identifikace nedostatků a detailní analýza rizik s využitím modelového výpočtu potenciálních dopadů. Na základě výsledků byla navržena konkrétní organizační a technická opatření ke zvýšení úrovně zabezpečení. Přínosem práce je vytvoření praktického návodu pro malé a střední podniky, jak systematicky a efektivně posílit svou kybernetickou odolnost proti malwarovým hrozbám.

KLÍČOVÁ SLOVA

kybernetická bezpečnost, malware, ransomware, phishing, rootkit, spyware, firemní prostředí, analýza rizik, SLE, ALE, NIS2, ISO/IEC 27001, ochrana dat, bezpečnostní politika

TITLE

Corporate Protection Against Malware Attacks

ANNOTATION

This thesis deals with the issue of protecting companies against malware. The theoretical part describes cybersecurity, its importance for organizations, and the basic legislative frameworks. Furthermore, it presents the typology of malware, its historical development, and its specifics in the corporate environment. The practical part focuses on the analysis of the selected company Delta-M Ltd. The analysis of the current security measures, identification of shortcomings, and a detailed risk analysis using a model calculation of potential impacts were carried out. Based on the results, specific organizational and technical measures were proposed to increase the level of security. The main contribution of this thesis is the creation of a practical guideline for small and medium-sized enterprises on how to systematically and effectively strengthen their cyber resilience against malware threats.

KEYWORDS

cybersecurity, malware, ransomware, phishing, rootkit, spyware, corporate environment, risk analysis, SLE, ALE, NIS2, ISO/IEC 27001, data protection, security policy

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

MFA	Multi-Factor Authentication (vícefaktorová autentizace)
EDR	Endpoint Detection and Response
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NIS2	Směrnice EU o bezpečnosti sítí a informačních systémů (2. generace)
ISO/IEC 27001	Mezinárodní norma pro řízení informační bezpečnosti
GDPR	General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)
ROI	Return on Investment (návratnost investice)
VPN	Virtual Private Network (virtuální privátní síť)
COBIT	Control Objectives for Information and Related Technologies (rámec pro řízení IT)
CIA	Confidentiality, Integrity, Availability (triáda bezpečnosti)
SLE	Single Loss Expectancy (očekávaná jednorázová ztráta)
ALE	Annualized Loss Expectancy (roční očekávaná ztráta)
ARO	Annualized Rate of Occurrence (roční míra výskytu)
BYOD	Bring Your Own Device
DLP	Data Loss Prevention
APT	Advanced Persistent Threat
IT	Informační technologie
ENISA	European Union Agency for Cybersecurity (Agentura EU pro kybernetickou bezpečnost)

SLA	Service Level Agreement (dohoda o úrovni služeb)
AV	Antivirus (antivirový systém)

TERMINOLOGIE

V této kapitole jsou vysvětleny klíčové pojmy a zkratky, které se v práci objevují a které jsou nezbytné pro správné pochopení problematiky kybernetické bezpečnosti a ochrany firem proti malwaru.

- **Malware** – škodlivý software určený k narušení, poškození nebo neoprávněnému přístupu k informačním systémům (např. viry, trojské koně, ransomware, spyware). [11], [18]
- **Ransomware** – typ malwaru, který zašifruje data a požaduje výkupné za jejich zpřístupnění. [11], [18]
- **Phishing** – technika sociálního inženýrství, při níž útočník podvodně získává citlivé údaje (hesla, čísla karet) pomocí falešných e-mailů nebo webových stránek. [14], [22]
- **Insider threat (vnitřní hrozba)** – riziko vyplývající z činnosti vlastních zaměstnanců nebo spolupracovníků, kteří mohou vědomě či nevědomě způsobit únik nebo zneužití dat. [15], [22]
- **Supply chain útok** – útok vedený prostřednictvím dodavatelského řetězce, kdy útočník kompromituje dodavatele a zneužije jeho přístup k cílové organizaci. [15], [19]
- **Antivirus (AV)** – software určený k detekci, blokování a odstraňování známého škodlivého kódu. [12], [20]
- **Firewall** – zařízení nebo software, který filtruje síťový provoz mezi interní sítí a internetem a brání neoprávněnému přístupu. [12], [20]
- **VPN (Virtual Private Network)** – technologie umožňující šifrované a bezpečné spojení mezi vzdáleným uživatelem a firemní sítí přes veřejný internet. [12], [20]
- **CIA triáda** – základní princip informační bezpečnosti založený na důvěrnosti (Confidentiality), integritě (Integrity) a dostupnosti (Availability). [17], [21]
- **Vícevrstvá ochrana (defense in depth)** – strategie kombinující více vrstev technických, organizačních a procesních opatření tak, aby selhání jedné vrstvy nezpůsobilo úplný průlom. [17], [25]

- **Zero Trust Architecture (ZTA)** – bezpečnostní přístup založený na principu, že žádný uživatel ani zařízení není implicitně důvěryhodné a každý přístup musí být ověřen. [21], [25]
- **EDR (Endpoint Detection and Response)** – technologie pro detekci hrozeb a reakci na ně přímo na koncových zařízeních. [13], [19]
- **IDS/IPS (Intrusion Detection/Prevention System)** – systémy pro detekci a prevenci průniků do sítě; IDS hrozby pouze detekuje, IPS je aktivně blokuje. [13], [19]
- **DLP (Data Loss Prevention)** – technologie určené k monitorování a prevenci úniku citlivých dat mimo organizaci. [13], [23]
- **BYOD (Bring Your Own Device)** – politika umožňující zaměstnancům používat soukromá zařízení pro pracovní účely, což přináší flexibilitu, ale i rizika. [16], [24]
- **APT (Advanced Persistent Threat)** – dlouhodobý, cílený a sofistikovaný útok vedený často organizovanými skupinami. [16], [24]
- **Incident Response Plan (IRP)** – plán reakce na bezpečnostní incidenty, definující postupy a odpovědnosti při jejich řešení. [18], [22]
- **SLE (Single Loss Expectancy)** – očekávaná jednorázová ztráta při jednom incidentu. [14], [21]
- **ALE (Annualized Loss Expectancy)** – očekávaná roční ztráta vypočítaná jako součin SLE a pravděpodobnosti výskytu (ARO). [14], [21]
- **ARO (Annualized Rate of Occurrence)** – pravděpodobnost nebo četnost výskytu incidentu za rok. [14], [21]
- **ROI (Return on Investment)** – ukazatel návratnosti investic, využívaný k hodnocení efektivity bezpečnostních opatření. [14], [21]
- **GDPR (General Data Protection Regulation)** – obecné nařízení EU o ochraně osobních údajů. [15], [19]
- **NIS2** – evropská směrnice o bezpečnosti sítí a informačních systémů, která ukládá organizacím povinnosti v oblasti kybernetické bezpečnosti. [15], [19]
- **ISO/IEC 27001** – mezinárodní norma pro řízení informační bezpečnosti. [19], [25]

- **COBIT** – rámec pro řízení a správu IT, který propojuje IT cíle s obchodní strategií. [19], [25]
- **ENISA** – Agentura Evropské unie pro kybernetickou bezpečnost, která vydává metodiky a doporučení. [15], [19]
- **SLA (Service Level Agreement)** – dohoda o úrovni poskytovaných služeb, zahrnující i parametry dostupnosti a bezpečnosti. [15], [19]
- **IT (Informační technologie)** – souhrn technologií pro sběr, ukládání, zpracování a přenos informací. [11], [12]

ÚVOD

Rychlá digitalizace a s ní spojený růst využívání informačních technologií ve všech oblastech podnikání přináší organizacím bezpochyby řadu výhod, ale zároveň i nové hrozby.
V prostředí, kde se většina firemních procesů opírá o informační systémy, představuje kybernetická bezpečnost jednu z klíčových oblastí zajištění kontinuity podnikání. Moderní společnosti čelí útokům, které jsou stále sofistikovanější, finančně motivované a často vedené profesionálními zločineckými skupinami.

Jednou z nejvýznamnějších hrozeb současnosti je malware – škodlivý software, který může mít mnoho podob, od klasických virů až po ransomware či pokročilé botnety.

Důležitým aspektem kybernetické bezpečnosti je nejen zavádění technických opatření, ale také implementace vhodných procesů, pravidel a vzdělávání zaměstnanců. Bezpečnostní strategie by měla vycházet z mezinárodně uznávaných rámců, jako je ISO/IEC 27001, NIST Cybersecurity Framework či COBIT. Tyto metodiky pomáhají firmám identifikovat rizika, stanovit priority a efektivně reagovat na incidenty.

Cílem této diplomové práce je analyzovat ochranu vybrané společnosti proti malwaru, identifikovat slabá místa v jejím zabezpečení a navrhnout možná zlepšení. Teoretická část práce se zaměřuje na charakteristiku kybernetické bezpečnosti, definici a typologii malwaru a metody obrany proti těmto hrozbám. Praktická část práce je založena na detailní analýze vybrané firmy, jejích současných opatření a procesů v oblasti bezpečnosti, a na vyhodnocení rizik pomocí metodiky analýzy rizik. Na základě zjištěných výsledků jsou navržena konkrétní doporučení a postupy, které mohou přispět k posílení kybernetické odolnosti dané organizace.

Práce má nejen odborný, ale i praktický přínos. Poskytuje pohled na reálné slabiny, se kterými se mohou setkat podniky obdobné velikosti a zaměření, a nabízí návrhy opatření, která lze využít v praxi. Výsledky mohou sloužit nejen vedení dané společnosti, ale i širší odborné veřejnosti, která hledá inspiraci pro zlepšení kybernetické bezpečnosti v podnikových prostředích.

1 TEORETICKÁ ČÁST

Teoretická část práce je zaměřena na vymezení základních pojmů, souvislostí a rámců, které tvoří podklad pro porozumění problematice ochrany firem proti malwaru. Nejprve je popsána oblast kybernetické bezpečnosti, její historický vývoj a význam pro současné podnikové prostředí. Následně je definován samotný pojem malware, jeho jednotlivé druhy, způsoby šíření a specifika působení ve firemní sféře. Pozornost je věnována také organizačním a technickým metodám ochrany, také i aktuálním trendům, které přináší moderní přístupy k zabezpečení informačních systémů.

1.1. Kybernetická bezpečnost a její význam pro firmy

1.1.1. Definice kybernetické bezpečnosti

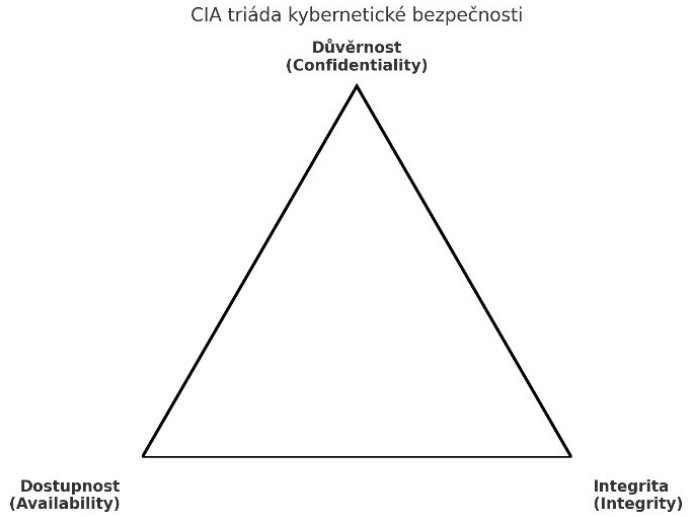
Kybernetická bezpečnost se v posledních desetiletích stala jedním z nejvýznamnějších témat, které ovlivňuje jak jednotlivce, tak i podniky a státní instituce. S rostoucí digitalizací a závislostí na informačních technologiích roste také množství hrozeb, kterým organizace čelí. Pro firmy představuje kybernetická bezpečnost nejen technickou otázku ochrany dat a systémů, ale především strategickou oblast, která ovlivňuje důvěru zákazníků, reputaci a ekonomickou stabilitu společnosti. [1], [3], [5], [6], [7], [16]

Zabezpečení firemních informačních aktiv je dnes nutnou podmínkou pro udržení konkurenceschopnosti i pro splnění právních požadavků. Nedostatečná ochrana může vést k únikům dat, finančním ztrátám a poškození dobrého jména. Proto je důležité chápat kybernetickou bezpečnost nejen jako soubor technologií, ale jako komplexní systém opatření zahrnující procesy, pravidla a lidský faktor. [2], [6], [7], [14], [16]

Existuje více definic kybernetické bezpečnosti, přičemž všechny zdůrazňují ochranu informačních aktiv před zneužitím, zničením nebo narušením.
Podle Mezinárodní telekomunikační unie (ITU, 2020) je kybernetická bezpečnost definována jako „shromažďování nástrojů, politik, konceptů bezpečnosti, záruk, pokynů, přístupů řízení rizik, činností, školení, osvědčených postupů, záruk a technologií, které lze použít k ochraně kyberprostoru, organizace a uživatelů“. [1], [3]

Často se kybernetická bezpečnost spojuje s pojmy jako důvěrnost, integrita a dostupnost (CIA triáda). Tyto tři principy (znázorněné na Obrázek *1* č.1) představují základní pilíře ochrany informací: [2]

- **Důvěrnost (Confidentiality):** zajistit, aby informace byly přístupné pouze oprávněným subjektům.
- **Integrita (Integrity):** chránit data před neoprávněnými změnami.
- **Dostupnost (Availability):** zaručit, že oprávnění uživatelé mají přístup k informacím a službám tehdy, kdy je potřebují.



Obrázek 1 - CIA triáda Zdroj: Vlastní zpracování

Pro firmy tak kybernetická bezpečnost znamená schopnost chránit své obchodní procesy, duševní vlastnictví a osobní údaje zákazníků před hrozbami a útoky, které mohou ohrozit jejich fungování a důvěryhodnost. [6], [7], [16]

1.1.2. Legislativní a normativní rámec

Kybernetická bezpečnost není pouze otázkou technologií, ale i dodržování právních a normativních požadavků. Firmy musí respektovat jak národní legislativu, tak mezinárodní normy a směrnice, které definují minimální standardy ochrany. [14], [15]

Směrnice Evropské unie NIS2 (Network and Information Security Directive 2), účinná od roku 2023, rozšiřuje povinnosti podniků v oblasti kybernetické bezpečnosti. Dotýká se zejména tzv. „zásadních“ a „důležitých“ subjektů, mezi něž patří například energetické, dopravní, zdravotnické či digitální služby. Firmy musí implementovat opatření k řízení rizik, hlásit incidenty a zajistit odolnost proti kybernetickým hrozbám. Nedodržení těchto povinností může vést k vysokým pokutám. [14], [15]

Jedním z nejvýznamnějších mezinárodních standardů je norma ISO/IEC 27001, která stanovuje požadavky na systém řízení bezpečnosti informací (ISMS). Norma je založena na systematickém přístupu k identifikaci rizik a zavádění odpovídajících kontrolních opatření. Certifikace podle ISO/IEC 27001 poskytuje firmám konkurenční výhodu, zvyšuje důvěru zákazníků a obchodních partnerů a zajišťuje soulad s legislativními požadavky. [11], [14]

Mezi další využívané metodiky patří například:

- **NIST Cybersecurity Framework** – americký rámec poskytující návod, jak hodnotit a zlepšovat úroveň kybernetické bezpečnosti. [9], [10]
- **COBIT (Control Objectives for Information and Related Technologies)** – rámec zaměřený na řízení a správu IT. [12]
- **ISO/IEC 27002** – doplňková norma s katalogem doporučených bezpečnostních opatření. [11]

Tyto rámce pomáhají firmám strukturovaně budovat své bezpečnostní programy, zlepšovat řízení rizik a plnit regulatorní požadavky. [9], [15]

1.2. Definice a typologie malwaru

1.2.1. Historický vývoj malwaru

Pojem **malware** vznikl spojením anglických slov „*malicious software*“ a označuje jakýkoliv škodlivý program nebo kód, jehož cílem je narušit chod počítačového systému, poškodit data nebo získat neoprávněný přístup k informacím. Malware může působit skrytě, aby se vyhnul odhalení, nebo naopak agresivně, kdy okamžitě způsobí viditelné škody. [1], [2], [3]

Malware představuje jednu z nejrozšířenějších forem kybernetických hrozeb a jeho podoby se neustále vyvíjejí. Útočníci využívají nové techniky a kombinují různé typy malwaru, aby zvýšili účinnost útoků a ztížili detekci. [6], [7]

Malware se tak posunul od individuálních experimentů k nástroji organizovaného zločinu a geopolitických konfliktů. Znalost historického vývoje je důležitá pro pochopení, jak se mění strategie útočníků i obranné technologie. [2], [6]

Vývoj škodlivého softwaru úzce souvisí s rozvojem výpočetní techniky a internetu. Malware se od svých počátků proměňoval od jednoduchých experimentálních kódů k dnešním vysoce sofistikovaným hrozbám. [1], [3]

Historický vývoj malwaru po dekádách:

- **70.–80. léta** – objevily se první koncepty samoreplikujícího se kódu. Programy jako *Creeper* (1971) na síti ARPANET nebo *Elk Cloner* (1982) na disketách byly spíše demonstrací možností než skutečnou hrozbou. Zároveň vznikaly první antivirové programy. [1], [2]
- **90. léta** – s masivním rozšířením osobních počítačů a internetu začala éra klasických počítačových virů a červů. Útoky se šířily disketami i e-maily (*Melissa*, 1999). Běžnými se staly antiviry a firewally. [2], [3]
- **2000–2010** – období exploze malwaru spojeného s internetem a e-mailem. Viry a červi (*ILOVEYOU*, *Conficker*) se šířily globálně během hodin. Objevily se první velké botnety a bankovní trojany (*Zeus*). [5], [6], [13]
- **2010–2020** – výrazný nárůst ransomware útoků (*CryptoLocker*, *WannaCry*, *NotPetya*), modulárního malwaru (*Emotet*) a špionážních kampaní (APT útoky). Malware se stává profesionálně provozovaným byznysem (tzv. Malware-as-a-Service). [4], [6], [18], [19]
- **Současnost** – útočníci využívají kombinace technik, zero-day zranitelnosti a pokročilé mechanismy obfuskace. Hrozby se často zaměřují na firmy a kritickou infrastrukturu, využívají cloud, IoT zařízení i dodavatelské řetězce. [3], [5], [6], [7], [20]

1.2.2. Typy malwaru

Malware není statickým fenoménem, jeho podoby se vyvíjejí společně s technologiemi. Porozumění jednotlivým druhům a historickým incidentům je zásadní pro návrh účinných metod obrany. [1], [2], [3]

Viry

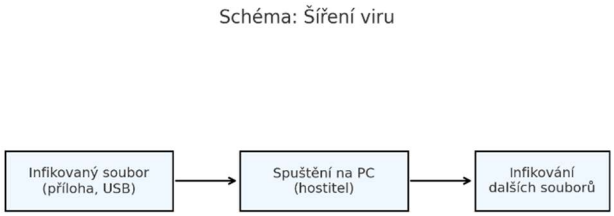
Počítačové viry se připojují k legitimním souborům nebo programům a šíří se při jejich spuštění. Často vyžadují interakci uživatele. [2]

Historické příklady:

- ***Melissa* (1999)** – makrovirus šířený e-mailem přes dokumenty MS Word. Způsobil masivní zahlcení e-mailových serverů. [2], [3]
- ***ILOVEYOU* (2000)** – e-mailový virus z Filipín, který se rozšířil do milionů počítačů během několika dní a způsobil škody v řádu miliard USD. [3], [6]

Tyto případy ukázaly, jak zneužití důvěry uživatelů a jednoduché sociální inženýrství mohou mít globální dopady. [5]

Postup šíření viru je znázorněn na Obrázek 22.



Obrázek 2 - Šíření viru Zdroj: Vlastní zpracování

Červi (worms)

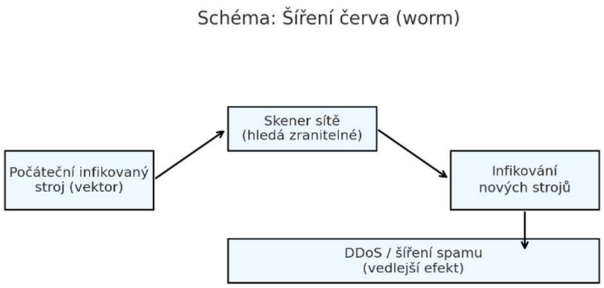
Samostatné programy schopné se šířit sítí bez nutnosti hostitelského souboru. Využívají síťové zranitelnosti. [1], [2]

Historické příklady:

- ***Morris worm* (1988)** – první velký internetový červ, který ochromil tehdejší síť ARPANET. [1]
- ***Conficker* (2008)** – využil chyby v OS Windows a vytvořil obrovský botnet s miliony nakažených zařízení. [6], [13]

Červi dokáží paralyzovat celé podnikové sítě během hodin. [7]

Postup šíření červa je znázorněn na Obrázek 3.



Obrázek 3 - Šíření červa Zdroj: Vlastní zpracování

Trojské koně (Trojans)

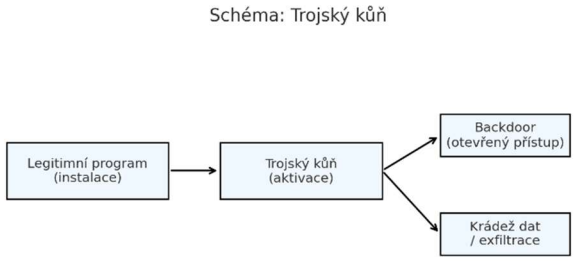
Malware tvářící se jako legitimní software, který po spuštění otevírá zadní vrátka nebo krade data. [2]

Historické příklady:

- ***Zeus* (2007)** – bankovní trojan, který kradl přihlašovací údaje a způsobil škody v řádu stovek milionů USD. [6], [13]
- ***Emotet* (2014–2021)** – modulární trojan, který sloužil jako nástroj pro šíření dalšího malwaru (např. ransomware). [4], [6]

Trojan je oblíbený pro svou schopnost skrytě ovládnout systém a sloužit jako vstupní bod pro další útoky. [5]

Postup šíření trojského koně je znázorněn na Obrázek 4.



Obrázek 4 - Šíření trojského koně Zdroj: Vlastní zpracování

Spyware a Adware

Spyware sleduje aktivity uživatele a sbírá citlivé údaje. Adware zobrazuje nevyžádanou reklamu a často také sleduje chování uživatele. [7]

Historické příklady:

- ***Pegasus*** – pokročilý spyware od NSO Group, který dokáže infikovat mobilní zařízení i bez interakce uživatele. [3], [6]
- ***Komerční adware balíčky*** *(např. Ask Toolbar, 2010+)* – obtěžující software, který zpomaloval počítače a zobrazoval nevyžádané reklamy. [7]

Spyware tedy představuje vážné riziko pro soukromí i obchodní tajemství. [16]

Postup šíření spywaru je znázorněn na Obrázek 5.

Obrázek 5 - Šíření spywaru Zdroj: Vlastní zpracování

Rootkity

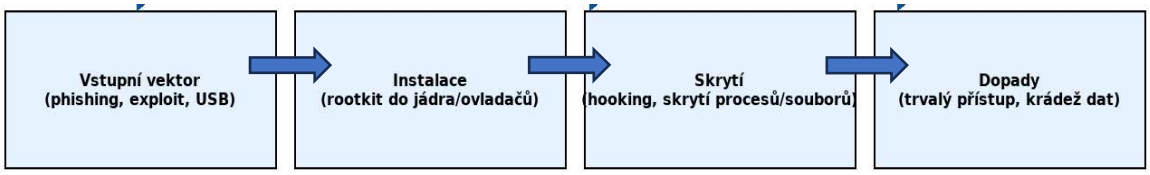
Software, který skrývá přítomnost malwaru a umožňuje útočníkovi trvalý přístup k systému. Často se instaluje na úrovni jádra OS. [13]

Historický příklad:

- ***Sony BMG rootkit* (2005)** – instalován na hudebních CD, skrytě měnil operační systém a ohrožoval bezpečnost uživatelů. [2], [3]

Rootkity jsou nebezpečné tím, že znesnadňují detekci a odstranění malwaru. [13]

Postup šíření rootkitu je znázorněn na Obrázek 6.



Obrázek 6 – Šíření rootkitu Zdroj: Vlastní zpracování

Ransomware

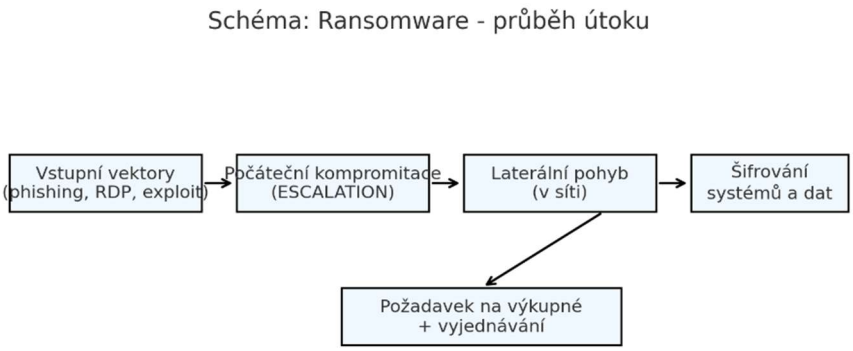
Malware, který zašifruje data a požaduje výkupné za jejich obnovení. Často kombinuje vydírání s únikem dat (*double extortion*). [4], [6]

Historické příklady:

- ***WannaCry* (2017)** – ransomware, který se šířil díky exploitu EternalBlue. Postihl více než 200 000 počítačů ve 150 zemích. [18]
- ***NotPetya* (2017)** – původně vydáván za ransomware, ve skutečnosti šlo o destruktivní malware. Způsobil miliardové škody globálním firmám. [19], [20]

Ransomware je dnes jednou z největších hrozeb pro firmy všech velikostí. [5], [6]

Postup šíření ransomwaru je znázorněn na Obrázek 7.



Obrázek 7 - Šíření ransomwaru Zdroj: Vlastní zpracování

Botnety

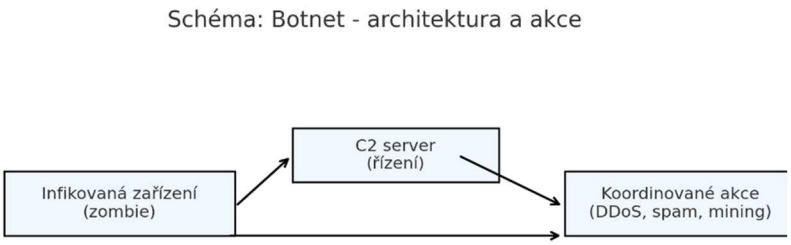
Sítě kompromitovaných zařízení („zombie“), které jsou ovládány útočníkem přes řídicí servery (C&C). [13]

Historický příklad:

- ***Mirai* (2016)** – botnet složený z IoT zařízení s výchozími hesly. Použit k masivním DDoS útokům, které odstavily velké části internetu. [3], [6]

Botnety dokazují, že mohou útočníci zneužít i běžná zařízení (kamery, routery) k rozsáhlým útokům. [7]

Postup šíření botnetu je znázorněn na Obrázek 8.



Obrázek 8 - Šíření botnetu Zdroj: Vlastní zpracování

Hybridní hrozby a nové trendy

Moderní malware kombinuje více technik najednou. Například ransomware může obsahovat funkce červa a šířit se napříč sítí, nebo trojský kůň může stahovat další škodlivé komponenty. [5]

Příklad:

- ***Maze* (2019)** – ransomware, který nejen šifroval data, ale i vyhrožoval jejich zveřejněním, pokud nebude zaplaceno výkupné. [6]

V Tabulka 1 - Typy malwaru jsou vypsány výše zmíněné typy malwaru pro lepší přehlednost.

Tabulka 1 - Typy malwaru

Typ malwaru	**Způsob šíření**	**Hlavní činnost**	**Příklad**
Virus	Připojuje se k infikovaným souborům, šíří se spuštěním hostitele	Poškozuje nebo mění data, zpomaluje systém	CIH („Černobyl“), Melissa
Červ (Worm)	Samostatně se šíří po síti bez zásahu uživatele	Rychlé zahlcení sítě, šíření dalších hrozeb	ILOVEYOU, WannaCry
Trojský kůň	Skryt v legitimním programu nebo příloze	Otevírá útočníkovi zadní vrátka, krade data	Zeus, Emotet
Ransomware	E-mailem, exploit zranitelnosti, RDP	Šifruje data, požaduje výkupné	CryptoLocker, Ryuk
Spyware	Instalace s jiným softwarem, phishing	Sběr dat uživatele, hesel, historie	DarkHotel, CoolWebSearch
Rootkit	Využití zranitelností, instalace útočníkem	Skrytí přítomnosti malwaru, správa systému	NTRootkit, Zeus rootkit
Adware	Balíček s freeware/shareware	Zobrazuje nechtěné reklamy, sleduje chování	Fireball, DollarRevenue
Botnet	Infekce zařízení a jeho vzdálené ovládání	Koordinované DDoS útoky, spam, těžba	Mirai, Storm botnet

Zdroj: Vlastní zpracování

1.2.3. Cíle a motivace útočníků

Motivace autorů malwaru jsou různé a často určují zvolenou taktiku, cíle a požadovanou úroveň sofistikovanosti útoku. Porozumění motivacím je důležité pro správné vyhodnocení rizik a návrh obranných opatření. Níže jsou shrnuty hlavní motivace spolu s typickými cíli a příklady útoků. [3], [9]

Finanční zisk

Nejčastější motivací je přímý finanční prospěch. Útočníci používají malware k vydírání (ransomware), krádeži platebních údajů, bankovních přihlašovacích údajů (bankovní trojské koně) nebo k provozování podvodu. [5], [6], [7]

- Typické cíle: firmy s kritickými daty, finanční instituce, ecommerce platformy.
- Příklad: útoky typu ransomware (WannaCry, NotPetya) nebo bankovní trojské koně jako Zeus, které byly zaměřené na získání finančních prostředků.

Průmyslová/korporátní špionáž

Státem sponzorované skupiny (APT) nebo konkurenčně motivované aktéry využívají malware k získání obchodních tajemství, výzkumu a vývoje nebo citlivých interních dokumentů. Tyto kampaně jsou často cílené, dlouhodobé a sofistikované. [3], [13]

- Typické cíle: výzkumné ústavy, technologické firmy, strategické podniky.
- Příklad: cílené APT kampaně, které zůstávají v síti dlouhou dobu, exfiltrují data a působí skrytě.

Politické a geopolitické motivace (sabotáž)

Útoky motivované politicky mohou směřovat k narušení kritické infrastruktury, destabilizaci organizací nebo zastrašení cílových skupin. Tyto útoky mohou mít rozsáhlé následky nad rámec finančních škod. [3], [16]

- Typické cíle: státní instituce, energetika, dopravní systémy, zdravotnictví.
- Příklad: destruktivní malware nebo útoky na infrastrukturu, které vedou k přerušení provozu.

Aktivismus a „hacktivismus“

Ideologicky motivované skupiny mohou používat malware jako nástroj protestu, k úniku informací nebo k narušení činnosti organizací, které považují za nežádoucí. Tyto útoky mohou být viditelnější, s cílem veřejného dopadu. [3], [20]

- Typické cíle: velké korporace, média, vládní instituce.
- Příklad: úmyslná úprava webu, únik interních dokumentů spojený s protestní kampaní.

Získání zdrojů pro další útoky (infrastruktura)

Útočníci mohou kompromitovat zařízení, aby je přidali do botnetu, sloužícího k DDoS útokům, rozesílání spamu nebo dalším útokům. Tato motivace je často spojena s opakovanými nebo automatizovanými kampaněmi. [3], [6]

- Typické cíle: neaktualizovaná IoT zařízení, domácí routery, zařízení se slabými hesly (Mirai).

Osobní motivace, zločin z „nudy“

Část útoků je dílem jednotlivců nebo skupin, které hledají uznání nebo chtějí jednoduše vyzkoušet své schopnosti. I když nemusí mít vysokou komplexnost, mohou způsobit škody (např. šíření viru pro „vzdělávací“ účely). [3], [5]

- Typické cíle: široké spektrum, často masové či náhodné útoky.

Insider threats (motivace zevnitř)

Motivace zaměstnanců nebo dodavatelů může zahrnovat finanční prospěch, pomstu, ideologii nebo neúmyslné chování (nedbalost). Vnitřní hrozba je často nejsilnějším vektorem, protože má legitimní přístup do systémů. [16], [13], [21]

- Typické cíle: interní databáze, intelektuální vlastnictví, přístupové informace.

1.3. Malware ve firemním prostředí

1.3.1. Specifická rizika pro organizace

Kybernetické útoky zaměřené na podniky se v posledních letech stávají čím dál častějšími a propracovanějšími. Firmy představují pro útočníky atraktivní cíl nejen kvůli finančnímu zisku, ale i kvůli možnosti paralyzovat kritické služby nebo získat přístup k cenným informacím. Malware je jedním z hlavních nástrojů, kterým útočníci tyto cíle realizují. V podnikových prostředích je proto nezbytné věnovat zvýšenou pozornost identifikaci hrozeb, pochopení způsobů jejich šíření a analýze reálných případů. [3], [6], [7], [9]

Organizace čelí specifickým hrozbám, které se liší od útoků zaměřených na jednotlivce. Útočníci cílí především na:

- Ransomware útoky: Paralyzují firemní infrastrukturu a vyřazují provoz. Firmy se často stávají obětí kvůli vysokému potenciálnímu výkupnému. [10]

- Supply chain útoky: Napadení dodavatelského řetězce může ohrozit stovky či tisíce organizací současně. Příkladem je incident SolarWinds (2020), kdy útočníci infikovali aktualizace softwaru, a tím získali přístup do sítí mnoha zákazníků včetně státních institucí. [11]
- Insider threats: Zaměstnanci či dodavatelé mohou úmyslně či neúmyslně přispět k šíření malwaru. Stačí otevření škodlivé přílohy, vložení infikovaného USB zařízení nebo zneužití přístupu. [12], [16]
- Cloudová prostředí a SaaS služby: Firmy využívající cloud čelí rizikům zranitelností konfigurace (např. špatně nastavené úložiště v Amazon S3) nebo zneužití přístupových údajů. [13]
- IoT zařízení ve firmách: Neaktualizované kamery, tiskárny či chytré senzory mohou být zneužity k šíření malwaru nebo vytvoření botnetu. [6], [14]

1.3.2. Nejčastější způsoby šíření ve firmách

Šíření malwaru ve firemním prostředí probíhá několika hlavními cestami. Mezi nejčastější patří:

- Phishing a spear phishing:
    - Útočníci rozesílají e-maily s podvodnými přílohami nebo odkazy.
    - Ve firemním prostředí se čím dál častěji využívá spear phishing – cílené útoky na konkrétní zaměstnance (např. finanční oddělení).
    - Podle zprávy Verizon *Data Breach Investigations Report 2022* byla phishingová kampaň součástí více než 80 % narušení bezpečnosti. [15]
- Infikovaná přenosná média (USB):
    - Stále častý způsob zavlečení malwaru, zejména ve výrobních podnicích.
    - Útočníci mohou fyzicky zanechat USB klíčenku na pracovišti – tzv. „baiting attack“. [16]

- Využití zranitelností softwaru:
    - Exploity cílí na neaktualizované systémy, servery nebo aplikace.
    - WannaCry (2017) se šířil prostřednictvím zranitelnosti protokolu SMB (EternalBlue).
    - Firmy často podceňují patch management. [10], [17]
- Útoky na vzdálený přístup (RDP, VPN):
    - Slabě zabezpečené nebo neaktualizované vzdálené přístupy jsou častým cílem.
    - RDP brute-force útoky jsou běžnou metodou pro zavedení ransomwaru do firemní sítě. [18]
- Dodavatelské aktualizace a legitimní nástroje:
    - Malware se může šířit prostřednictvím infikovaných aktualizací softwaru (supply chain útoky).
    - Útočníci využívají i legitimní administrační nástroje („living off the land“ techniky), aby se vyhnuli detekci. [11], [19]

1.3.3. Reálné případy útoků na firmy

Analýza reálných případů pomáhá pochopit, jakým způsobem útočníci využívají malware v praxi.

- **Sony Pictures (2014):** Útok zničil data na tisících počítačů a vedl k úniku citlivých informací. Za útokem stáli pravděpodobně státem podporovaní útočníci. [20]
- **Maersk (2017):** Rejdařská společnost Maersk byla zasažena útokem NotPetya, který ochromil její globální logistické operace. Firma odhadla škody na více než 300 milionů USD. [21]
- **Colonial Pipeline (2021):** Ransomware útok na amerického provozovatele ropovodu vedl k dočasnému zastavení dodávek paliva a způsobil rozsáhlé ekonomické dopady. [22]
- **SolarWinds (2020):** Supply chain útok umožnil útočníkům přístup do sítí více než 18 000 organizací po celém světě. [11]

- **Česká republika - Fakultní nemocnice Brno (2020):** Ransomware paralyzoval nemocniční systémy, omezil provoz a způsobil přerušení plánovaných operací. [23]

1.4. Metody ochrany proti malwaru

1.4.1. Organizační opatření

Ochrana před malwarem musí být vícevrstvá a kombinovat organizační i technická opatření. Pouhé nasazení antivirového softwaru již není dostačující, protože útočníci využívají sofistikované techniky, které dokážou tradiční detekci obejít. Moderní přístup k obraně proto zahrnuje lidský faktor, procesní pravidla, technické prostředky i inovativní bezpečnostní trendy. [9], [12], [13], [14]

Organizační opatření tvoří základní pilíř obrany proti malwaru. I sebelepší technické řešení selže, pokud zaměstnanci nebudou proškoleni nebo nebudou existovat jasně stanovená pravidla. [7]

- **Bezpečnostní politika podniku:**
    - Dokument, který definuje zásady nakládání s IT prostředky, pravidla přístupů, klasifikaci dat a reakci na incidenty.
    - Politika by měla být pravidelně revidována a přizpůsobována novým hrozbám. [14]
- **Školení a zvyšování povědomí:**
    - Zaměstnanci patří k nejčastějším vektorům útoků, tzn., že phishing je úspěšný hlavně díky lidské chybě.
    - Firmy by měly provádět pravidelná školení, simulace phishingu a interní kampaně zvyšující povědomí. [18]
- **Pravidla používání IT:**
    - Stanovení zásad pro práci se služebními zařízeními, USB médii, vzdáleným přístupem a cloudovými službami.
    - Zakázání nebo omezení neautorizovaného softwaru (tzv. „shadow IT“). [15]

Organizační opatření vytvářejí prostředí, v němž je uživatel informovaný, zodpovědný a stává se aktivní součástí obrany. [13]

1.4.2. Technická opatření

Technické prostředky poskytují praktickou obranu proti škodlivému kódu a umožňují včasnou detekci i reakci. [4], [10]

- Antivirové systémy:
    - Stále základní nástroj, i když jejich schopnost odhalit nové a neznámé hrozby je omezená.
    - Moderní antivirová řešení kombinují signatury s heuristickou a behaviorální analýzou. [19]
- EDR (Endpoint Detection and Response):
    - Pokročilejší nástroj, který monitoruje chování koncových stanic a umožňuje rychlou reakci na incidenty.
    - Umí izolovat napadené zařízení a zabránit šíření malwaru. [20]
- Firewall a IDS/IPS:
    - Firewall reguluje síťovou komunikaci a blokuje neautorizované přístupy.
    - Systémy IDS/IPS (Intrusion Detection/Prevention) detekují a blokují pokusy o útok v síťovém provozu. [14]
- Šifrování:
    - Zajišťuje ochranu dat při přenosu i v klidu. I pokud dojde k úniku, útočník nemůže data využít.
    - Nutné zejména u přenosných zařízení a cloudových služeb. [9]
- Zálohování a obnova dat:
    - Poslední linie obrany proti ransomwaru.
    - Zálohy musí být oddělené od produkční sítě (např. offline nebo v izolovaném cloudu).
    - Důležité je pravidelně testovat obnovu, nejen samotné ukládání záloh. [7], [16]

Technická opatření musí být nasazena na více úrovních, tedy od koncových zařízení přes síť až po servery a cloud. [13]

1.4.3. Trendy v ochraně

Kybernetická bezpečnost se dynamicky vyvíjí a reaguje na nové techniky útočníků. Firmy dnes čím dál častěji využívají inovativní přístupy: [3], [6]

- Zero Trust Security:
    - Princip „nevěř nikomu, ověřuj vše“.
    - Každý přístup (i zevnitř sítě) se musí autentizovat a autorizovat.
    - Minimalizuje dopady kompromitace účtu nebo zařízení. [9], [12], [22]
- Umělá inteligence a strojové učení:
    - AI pomáhá v detekci anomálií a predikci útoků.
    - Umožňuje odhalit dosud neznámé hrozby na základě chování, nikoliv signatur. [20], [23]
- Behaviorální analýza:
    - Sleduje aktivity uživatelů a zařízení, hledá neobvyklé vzory chování.
    - Například hromadné šifrování souborů je indikátor ransomwaru. [5], [17]
- Sandboxing:
    - Spouštění podezřelých souborů v izolovaném prostředí, kde se vyhodnocuje jejich chování.
    - Chrání produkční systémy před přímým zavlečením malwaru. [6], [19]

Trendy ukazují, že budoucnost ochrany před malwarem bude stát na kombinaci automatizace, strojového učení a adaptivních politik, které reagují na kontext přístupu. [23]

2 PRAKTICKÁ ČÁST

2.1 Charakteristika vybrané společnosti

2.1.1. Základní údaje o společnosti

Společnost Delta-M s.r.o. je firma sídlící v Chrudimi, která se specializuje na prodej nářadí a zahradní techniky. Kromě samotného prodeje nabízí zákazníkům také servis zakoupených produktů a dlouhodobě působí jako stabilní partner v oblasti péče o zahradní techniku. Podnik kombinuje tradiční kamennou prodejnu se servisním zázemím, čímž cílí především na regionální klientelu, pro kterou je důležitá možnost osobního kontaktu a rychlé opravy či údržby zařízení.

V roce 2022 se podnikatelská činnost společnosti Delta-M rozšířila o e-shop zaměřený na online prodej nářadí a zahradní techniky. Díky této kombinaci se podařilo rozšířit působnost firmy na celorepublikovou úroveň a oslovit širší skupinu zákazníků prostřednictvím digitálního kanálu. E-shop tak tvoří významnou část obchodního modelu, která zajišťuje diverzifikaci příjmů a posiluje konkurenceschopnost firmy. [26], [27]

2.1.2. IT infrastruktura a používané systémy

IT infrastruktura společnosti Delta-M s.r.o. je tvořena především kancelářskými a prodejními počítači, které slouží pro běžnou administrativu, účetnictví, správu skladových zásob a provoz pokladního systému. Provozovna je dále vybavena síťovým připojením a lokálním serverem, který uchovává interní dokumentaci a databázi zákazníků. V rámci servisu zahradní techniky se používají specializované aplikace pro evidenci zakázek a servisních úkonů.

Společnost provozuje taktéž e-shop, který běží na externím hostingu u poskytovatele cloudových služeb. E-shop je napojen na platební bránu a databázi zákazníků, což zvyšuje důležitost zajištění dostupnosti a zabezpečení tohoto systému. Vzhledem k tomu, že online prodej tvoří významnou část příjmů, výpadek e-shopu by mohl mít okamžitý dopad na ekonomické výsledky.

Společnost využívá e-mailovou komunikaci, cloudová úložiště pro sdílení dokumentů a účetní software propojený s databází zákazníků a dodavatelů. IT prostředí je tedy kombinací lokálních systémů a cloudových služeb, což s sebou přináší specifické bezpečnostní výzvy, zejména v oblasti správy přístupů, pravidelného zálohování a aktualizací.

2.1.3. Význam informačních technologií pro podnikání

Pro společnost Delta-M mají informační technologie zásadní význam. E-shop představuje klíčový zdroj příjmů a jeho nepřetržitá dostupnost je nutnou podmínkou pro zachování obchodní kontinuity. Jakýkoli výpadek by znamenal nejen okamžité ztráty z neuskutečněných prodejů, ale i riziko poškození pověsti v očích zákazníků.

Interní systémy společnosti jsou zase nezbytné pro zajištění chodu prodejny, správu skladů a účetnictví. Bez jejich správného fungování by bylo výrazně narušeno řízení provozu, což by se negativně promítlo do spokojenosti zákazníků i finanční stability společnosti.

Zvláštní pozornost si zaslouží také oblast zpracování osobních údajů, které firma získává od svých zákazníků. Jedná se především o jména, adresy, kontaktní údaje a u e-shopu také o platební informace. Správné nakládání s těmito daty je nejen zákonnou povinností vyplývající z GDPR, ale i klíčovým faktorem pro budování důvěry zákazníků.

2.1.4. Specifika a rizika prostředí

Charakter firmy přináší i určitá specifická rizika:

- Sezónní závislost: V období jara a léta je poptávka po zahradní technice nejvyšší. Případný kybernetický incident v této době by měl mnohonásobně vyšší ekonomické dopady.
- Omezené IT kapacity: Firma nedisponuje rozsáhlým IT oddělením, bezpečnost je spíše v kompetenci jednoho správce či externího dodavatele. To zvyšuje riziko podcenění aktualizací a bezpečnostních opatření.
- Napojení na externí služby: Provoz e-shopu, platební brány a cloudových aplikací znamená závislost na třetích stranách. Útok na dodavatelský řetězec nebo chyba poskytovatele může mít přímý dopad na fungování firmy.
- Lidský faktor: Zaměstnanci, kteří nejsou odborníky na kybernetickou bezpečnost, mohou neúmyslně přispět k zavlečení malwaru do systému (otevření phishingového e-mailu, připojení infikovaného USB zařízení).

2.2. Analýza současného stavu

2.2.1. Organizační opatření

V rámci organizační bezpečnosti lze ve společnosti identifikovat základní pravidla, avšak jejich úroveň není dostatečná ve vztahu k současným hrozbám. Firma Delta-M s.r.o. disponuje základními interními směrnicemi týkajícími se práce s IT technikou, nicméně komplexní bezpečnostní politika chybí. Zaměstnanci jsou sice průběžně informováni o obecných zásadách práce s počítači, ale pravidelná školení zaměřená na kybernetickou bezpečnost nejsou prováděna. To zvyšuje riziko, že zaměstnanec neúmyslně otevře phishingový e-mail nebo připojí infikované zařízení.

E-shop má zavedená základní pravidla pro správu zákaznických dat a dodržuje požadavky GDPR. I zde ale chybí systematické vzdělávání pracovníků a definovaný postup pro reakci na incidenty (incident response plán).

2.2.2. Technická opatření

Technická úroveň zabezpečení se liší podle povahy provozu ve společnosti:

- **Antivirová ochrana:** Na většině koncových zařízení je nainstalován běžně dostupný antivirový software, který je aktualizován. Jedná se však o základní ochranu, která nemusí být schopná detekovat více propracované hrozby.
- **Firewall a síťová ochrana:** Společnost využívá běžný firemní router s integrovaným firewallem. V síti není nasazen pokročilejší systém IDS/IPS, který by dokázal aktivně detekovat útoky.
- **Zálohování:** Zálohování účetních a skladových dat je realizováno, ale chybí jasně definovaná pravidla zálohování (např. pravidelné testy obnovy). V případě e-shopu jsou zálohy zajištěny externím poskytovatelem hostingu, což snižuje nároky na správu, ale zvyšuje závislost na třetí straně.
- **Šifrování:** Běžná pracovní zařízení nejsou plošně šifrována, což představuje riziko zejména u notebooků používaných mimo firmu. Komunikace e-shopu s uživateli je chráněna protokolem HTTPS, což je ale standardem.
- **Správa přístupů:** Přístupy do interních systémů jsou chráněny uživatelským jménem a heslem, avšak více faktorová autentizace (MFA) není plošně implementována.

- **Aktualizace a patch management:** Aktualizace softwaru a operačních systémů probíhají nepravidelně a spíše až ve chvíli, kdy je to nutně potřeba.

2.2.3. Personální a provozní zajištění

Společnost disponuje pouze omezenými personálními kapacitami v oblasti IT. Firma má k dispozici správce IT na částečný úvazek, který se stará především o provozuschopnost infrastruktury. Bezpečnostní aspekty nejsou jeho hlavní náplní. Co se týče e-shopu, ten spoléhá na podporu poskytovatele hostingu, což znamená, že část odpovědnosti je přenesena na externího dodavatele, avšak kontrola nad detailním nastavením bezpečnosti je omezená. [26]

2.2.4. Identifikovaná slabá místa

Na základě analýzy současného stavu lze shrnout hlavní slabiny zabezpečení následovně:

- absence komplexní bezpečnostní politiky, pravidelných školení a incident response plánu,
- základní antivirová ochrana bez pokročilejší detekce hrozeb (EDR),
- chybějící IDS/IPS a segmentace sítě,
- neexistence systematické správy aktualizací,
- nedostatečně řešené šifrování dat na koncových zařízeních,
- závislost na třetích stranách (hosting, platební brána) bez plné kontroly nad bezpečností,
- omezené personální kapacity pro řešení bezpečnosti.

Pro souhrn zjištěných nedostatků slouží Tabulka 2 - Současná opatření a jejich nedostatky.

Tabulka 2 - Současná opatření a jejich nedostatky

Oblast	Stávající stav	Nedostatky / rizika
Organizační opatření	Základní pravidla pro práci s IT, dodržování GDPR u e-shopu	Chybí komplexní bezpečnostní politika, pravidelná školení zaměstnanců a incident response plán
Antivirová ochrana	Nainstalován běžný antivirový software na koncových zařízeních	Omezená detekce nových a sofistikovaných hrozeb, absence EDR
Firewall a síťová ochrana	Základní firewall v rámci routeru	Chybí IDS/IPS, nedostatečná segmentace sítě
Zálohování	Zálohy účetních a skladových dat, e-shop zálohován poskytovatelem	Chybí testy obnovy, nejasná politika zálohování, riziko závislosti na poskytovateli
Šifrování	HTTPS pro e-shop, částečné šifrování dat	Koncová zařízení nejsou plošně šifrována
Správa přístupů	Hesla pro interní systémy, MFA u administrace e-shopu	MFA není plošně implementována, slabší zabezpečení interních přístupů
Aktualizace (patch management)	Aktualizace probíhají nepravidelně, spíše ad hoc	Chybí systematický proces patch managementu
Personální zajištění	IT správce na částečný úvazek, podpora poskytovatele hostingu	Omezené kapacity, bezpečnost není hlavní náplní, malá kontrola nad hostingem

Zdroj: Vlastní zpracování

2.3. Analýza rizik

2.3.1. Identifikace hrozeb

Analýza rizik představuje klíčový krok při zajišťování kybernetické bezpečnosti. Umožňuje identifikovat nejpravděpodobnější hrozby, zhodnotit jejich dopady a určit, na které oblasti by se měla firma Delta-M s.r.o. zaměřit v rámci ochrany proti malwaru. [9], [11], [16]

Na základě charakteristik firmy a současného zabezpečení lze definovat následující hrozby:

- **Ransomware útoky:** Mohou ochromit e-shop i interní systémy prodejen a servisu.
- **Phishing a spear phishing:** Riziko otevření škodlivé přílohy nebo vyplnění přihlašovacích údajů.
- **Využití zranitelností softwaru:** Nedostatečný patch management zvyšuje riziko zneužití známých chyb.
- **Útoky na vzdálený přístup (RDP, VPN):** Slabě chráněné vzdálené přístupy mohou být kompromitovány např. opakovaným zadáváním hesel pro prolomení.

- **Insider threats:** Neúmyslné zavlečení malwaru zaměstnanci (USB, neznalost).
- **Supply chain útoky:** Závislost na poskytovateli hostingu a platební brány znamená riziko kompromitace z externího prostředí.
- **Ztráta nebo odcizení zařízení:** Notebooky bez šifrování mohou vést k úniku citlivých dat.

2.3.2. Hodnocení pravděpodobnosti a dopadu

Každá hrozba byla posouzena z hlediska pravděpodobnosti (nízká, střední, vysoká) a dopadu (nízký, střední, vysoký). Hodnocení slouží k identifikaci prioritních oblastí, na které by se měla společnost zaměřit v rámci zavádění bezpečnostních opatření. Rizika s vysokou pravděpodobností a současně vysokým dopadem představují kritické hrozby, které je nutné řešit okamžitě a systematicky. Naopak hrozby s nižší pravděpodobností a nižším dopadem je vhodné sledovat, ale není nutné jim věnovat stejnou míru zdrojů. Vše je zobrazeno v Tabulka 3 - Hodnocení pravděpodobnosti a dopadu. [9], [11]

Tabulka 3 - Hodnocení pravděpodobnosti a dopadu

Hrozba	Pravděpodobnost	Dopad	Hodnocení rizika
Ransomware útok	**Vysoká**	**Vysoký**	**Kritické**
Phishing a spear phishing	**Vysoká**	**Střední**	**Vysoké**
Využití zranitelností softwaru	**Střední**	**Vysoký**	**Vysoké**
Útoky na vzdálený přístup	**Střední**	**Vysoký**	**Vysoké**
Insider threats	**Střední**	**Střední**	**Střední**
Supply chain útok	**Nízká/střední**	**Vysoký**	**Vysoké**
Ztráta / odcizení zařízení	**Střední**	**Střední**	**Střední**

Zdroj: Vlastní zpracování, metodika podle [9], [11]

Z tabulky je patrné, že nejzávažnějším rizikem pro společnost jsou ransomware útoky, které mají vysokou pravděpodobnost výskytu a zároveň velmi vážný dopad na chod firmy. Tyto útoky mohou vést k úplné paralýze podnikových procesů a značným finančním ztrátám, a proto je jejich prevence a připravenost na incident klíčová.

Významná hrozba je také phishing a spear phishing, jejichž úspěšnost je založena především na lidském faktoru. Pravděpodobnost útoku je vysoká, a i když dopad nemusí být vždy kritický, může vést k odcizení přístupových údajů a otevření dveří k dalšímu útoku.

Využití zranitelností softwaru a útoky na vzdálený přístup představují technické hrozby, které mohou mít vysoký dopad, zejména pokud útočník získá přístup do interních systémů. Tyto hrozby ukazují na nutnost pravidelného záplatování softwaru, implementace více faktorové autentizace a omezení vzdálených přístupů pouze na nezbytné uživatele.

Insider threats a ztráta či odcizení zařízení se řadí mezi střední rizika. Jejich dopad je omezenější, ale i přesto mohou vést k úniku citlivých informací. Řešením je zavedení přísnějších přístupových práv, školení zaměstnanců nebo také použití nástrojů pro správu a šifrování mobilních zařízení.

Supply chain útoky jsou sice méně pravděpodobné, ale jejich potenciální dopad je vysoký. Firmy se stávají stále více závislé na externích dodavatelích a službách, a proto je nutné zohledňovat bezpečnostní standardy dodavatelů a zahrnovat je do celkové strategie řízení rizik.

Hodnocení lze shrnout tak, že společnost by měla věnovat největší pozornost hrozbám, které kombinují vysokou pravděpodobnost a vysoký dopad, a současně nepodceňovat ani méně pravděpodobné útoky s kritickým dopadem, které mohou mít dlouhodobý vliv na reputaci a ekonomickou stabilitu firmy.

2.3.3. Riziková matice

Riziková matice je jedním z nejpoužívanějších nástrojů pro vizualizaci a vyhodnocení rizik. Jejím cílem je poskytnout jednoduchý a přehledný pohled na to, jak se jednotlivé hrozby liší z hlediska pravděpodobnosti výskytu a závažnosti dopadů. Díky grafickému zobrazení je možné rychle identifikovat, které hrozby představují pro organizaci největší nebezpečí, a měly by být prioritně řešeny. [9], [11]

Metodický postup sestavení matice:

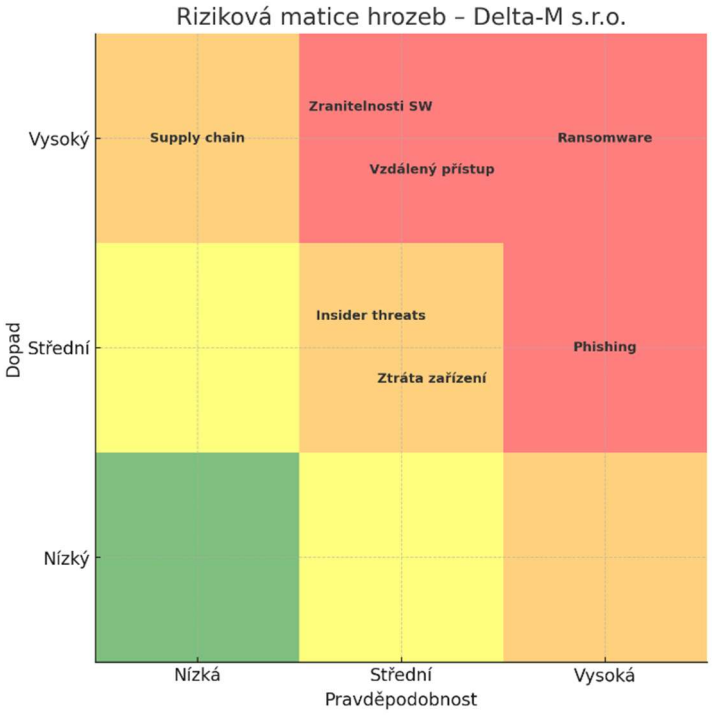
- **Identifikace hrozeb** – nejprve byly shromážděny a popsány relevantní hrozby, které mohou ovlivnit bezpečnost informačních aktiv firmy. [9]
- **Stanovení kritérií hodnocení** – pro každou hrozbu byla určena její pravděpodobnost (nízká, střední, vysoká) a dopad (nízký, střední, vysoký). [9]

- **Kombinace výsledků** – jednotlivé hrozby byly zakresleny do matice, kde osa X představuje pravděpodobnost a osa Y dopad. [9]
- **Barevné odlišení** – každá kombinace byla přiřazena do barevné zóny: zelená (nízké riziko), žlutá (střední riziko), oranžová (vysoké riziko), červená (kritické riziko). [9]
- **Vyhodnocení** – výsledky byly interpretovány a porovnány s cílem určit nejkritičtější hrozby, které vyžadují okamžité řešení. [9]

Riziková matice není pouze analytický nástroj, ale i prostředek pro komunikaci výsledků směrem k vedení společnosti. Poskytuje vizuálně srozumitelný přehled, díky kterému lze:

- stanovit priority při zavádění bezpečnostních opatření,
- efektivně alokovat zdroje na zmírnění nejzávažnějších rizik,
- podporovat rozhodování vedení při plánování strategie informační bezpečnosti,
- sledovat vývoj rizik v čase a vyhodnocovat účinnost zavedených opatření. [9], [11]

Matice rizik vytvořená konkrétně pro společnost Delta-M s.r.o. je zobrazena na Obrázek 9.



Obrázek 9 - Riziková matice Zdroj: Vlastní zpracování, metodika podle [9], [11]

2.4. Modelové scénáře útoků

Pro lepší ilustraci reálných dopadů kybernetických hrozeb na podnikové prostředí byly vytvořeny dva modelové scénáře, které vycházejí z podmínek společnosti Delta-M s.r.o. První scénář simuluje útok typu ransomware, který cílí na e-shop a interní systémy, a ukazuje přímé finanční ztráty i vliv na provoz. Druhý scénář se zaměřuje na vnitřní hrozbu v podobě neúmyslného úniku dat (exfiltrace) zaměstnancem, kde se kromě finančních nákladů hodnotí i reputační a regulatorní rizika. Tyto scénáře slouží jako praktická demonstrace metodiky výpočtu SLE a ALE a zároveň umožňují porovnat účinnost navrhovaných bezpečnostních opatření.

2.4.1. Ransomware útok

Ransomware patří mezi největší hrozby, kterým malé a střední firmy čelí. Útočníci dokáží během několika hodin zablokovat přístup k datům a ochromit e-shop i vnitřní systémy. V následujícím scénáři se proto zaměříme na to, jak by takový útok mohl dopadnout na firmu Delta-M s.r.o., jaké by způsobil škody a jak by je bylo možné omezit pomocí bezpečnostních opatření. [3], [5], [6], [7], [16]

2.4.1.1. Definice a metodika (SLE a ALE)

Pro výpočet rizik se využívají dva základní ukazatele: **SLE** (Single Loss Expectancy) a **ALE** (Annualized Loss Expectancy). [9], [11], [12]

- **SLE – jednorázová očekávaná ztráta:** představuje finanční dopad jediného incidentu. Vypočítává se jako součet všech přímých i nepřímých nákladů (ušlá marže, provozní náklady během výpadku, náklady na obnovu systémů, očekávané sankce).

Vzorec pro výpočet SLE:
SLE = ztracená hrubá marže + provozní náklady výpadku + náklady na obnovu + očekávaná pokuta (pravděpodobnost × výše pokuty)

- **ALE – očekávaná roční ztráta:** vyjadřuje průměrnou roční ztrátu, kterou lze očekávat s ohledem na pravděpodobnost výskytu incidentu.

Vzorec pro výpočet ALE:
ALE = SLE × ARO
kde **ARO** (Annualized Rate of Occurrence) označuje četnost incidentů za rok.

2.4.1.2. Vstupní předpoklady scénáře

Vstupní předpoklady pro tuto modelovou situaci jsou smyšlené hodnoty, které nekorespondují s hodnotami společnosti Delta-M s.r.o., jedná se pouze o simulaci, aby bylo na příkladu jasné, jak se řádnou ochranou proti malwarovému útoku lze zajistit lepších výsledků.

- **E-shop:** průměrný denní obrat 150 000 Kč, hrubá marže 25 %, během výpadku trvale zanikne 70 % objednávek.
- **Doba výpadku (před/po opatřeních):** 3 dny / 0,5 dne (e-shop), 2 dny / 0,5 dne (prodejna/servis).
- **Provozní náklady během výpadku:** 15 000 Kč/den.
- **Externí obnova systémů:** 100 000 Kč před, 40 000 Kč po opatřeních.
- **Riziko úniku osobních údajů (GDPR):** 40 % před, 10 % po; modelovaná pokuta 200 000 Kč.
- **ARO:** 0,40 před, 0,15 po.
- **Opatření (roční náklady):** MFA 20 000 Kč, EDR 120 000 Kč, zálohy 60 000 Kč, školení 40 000 Kč, IDS/segmentace 80 000 Kč → celkem 320 000 Kč/rok. [8], [29], [31]

Tabulka 4 - Výsledky výpočtu

Ukazatel	**Před opatřeními**	**Po opatřeních**
SLE (jednorázová ztráta)	327 750 Kč	86 625 Kč
ALE (roční očekávaná ztráta)	131 100 Kč/rok	12 994 Kč/rok
Roční náklady na opatření	–	320 000 Kč
Roční úspora rizika (ALE_před − ALE_po)	–	118 106 Kč/rok
Čistý přínos (úspora − náklady)	–	−201 894 Kč/rok

Zdroj: Vlastní zpracování

2.4.1.3. Interpretace výsledků

Z výpočtů (Tabulka 4 - Výsledky výpočtu) vyplývá, že opatření významně snižují riziko, jelikož ALE klesá přibližně desetinásobně. Nicméně při ročních nákladech 320 000 Kč je čistý finanční přínos záporný. Náklady na opatření převyšují vyčíslenou roční úsporu rizika. To ale

neznamená, že by opatření neměla smysl, jelikož model pracuje s konzervativními čísly. V praxi by se mohlo stát, že by pravděpodobnost útoku byla vyšší, což by mohlo konečný výsledek změnit.

Možné cesty k pozitivnímu čistému přínosu:

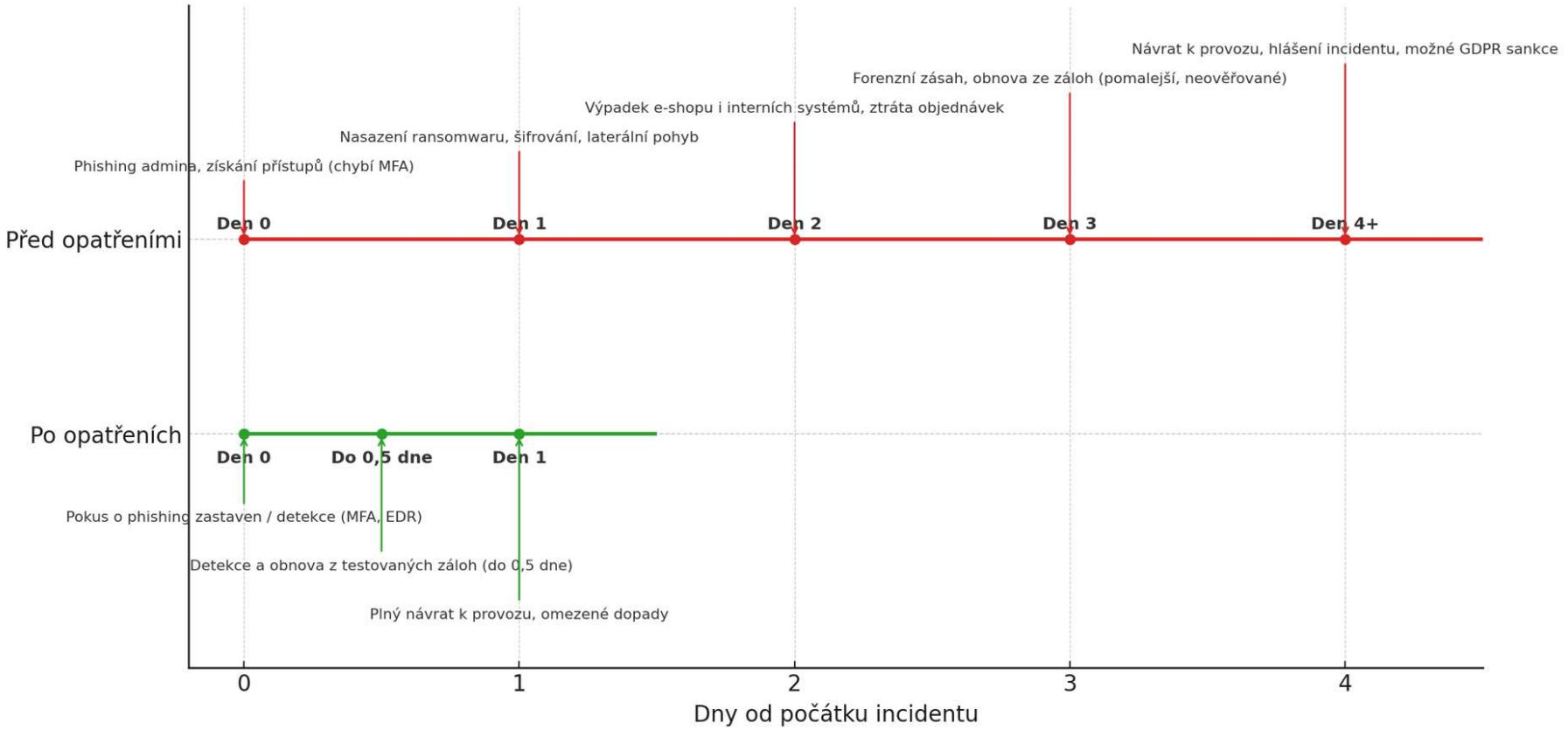
- **Kalibrace ARO a dopadů:** reálné ARO může být vyšší (alespoň 0,6), což by zvýšilo ALE_před a tím i úsporu rizika. [9]
- **Optimalizace nákladů:** využít levnější EDR, MSP balíčky, část IDS/segmentace řešit jako jednorázovou investici do vybavení.
- **High-impact minimum:** MFA, zálohy, školení a základní EDR poskytují nejlepší poměr ceny a efektu.

2.4.1.4. Časová osa incidentu

Časová osa modelového scénáře (Obrázek 10) zobrazuje průběh ransomware útoku v jednotlivých dnech a zároveň ukazuje rozdíl mezi situací před zavedením opatření a po jejich implementaci. Slouží tak jako názorná ilustrace, jak konkrétní bezpečnostní kroky ovlivňují průběh incidentu, jeho dopady i délku trvání.

Před zavedením opatření se útok rozvíjí bez větší detekce či omezení. Již v den 0 dojde k získání přístupových údajů prostřednictvím phishingového e-mailu, protože chybí více faktorová autentizace. Následující den je nasazen ransomware do pozadí e-shopu a útočník díky slabé segmentaci proniká i do interní sítě Delta-M. V důsledku toho jsou e-shop i interní systémy zcela mimo provoz po dobu dvou dnů, což přináší ztrátu objednávek a reputační problémy. Analýza a obnova ze záloh probíhají až během dnů 2–3, přičemž obnova je pomalá, a ne zcela spolehlivá. Celý incident je zakončen až čtvrtý den, kdy je obnova dokončena a incident je hlášen, přičemž hrozí sankce z titulu GDPR.

Po zavedení opatření je průběh incidentu zásadně odlišný. Zavedení MFA, EDR a segmentace výrazně snižuje možnosti útočníka v pohybu po síti a zvyšuje pravděpodobnost včasné detekce útoku. V případě, že by k útoku i přes tato opatření došlo, testované zálohy a nástroje EDR umožňují rychlou obnovu systému, obvykle do půl dne. Pravděpodobnost úniku dat i riziko šíření ransomwaru do celé sítě je výrazně nižší, a tím se minimalizují nejen finanční ztráty, ale i reputační škody společnosti.



Obrázek 10 - Časová osa incidentu

Zdroj: Vlastní zpracování

2.4.2. Neúmyslná exfiltrace dat

Insider hrozby představují významné riziko, protože k citlivým informacím mají přístup právě zaměstnanci nebo spolupracovníci organizace. Tento scénář modeluje případ, kdy interní pracovník (servisní technik nebo administrativní zaměstnanec) omylem zkopíruje zákaznickou databázi či servisní dokumentaci a tyto informace se dostanou do nepovolaných rukou.

Cílem je určit přímé i nepřímé finanční dopady takového incidentu (včetně reputačních škod a regulatorních sankcí) pomocí metrik SLE a ALE a navrhnout opatření, která riziko sníží.

Tento model obsahuje několik faktorů, které jsou založeny na předpokladech (reputace, pravděpodobnost sankcí). [7], [30]

2.4.2.1. Vstupní předpoklady

- **Přímé finanční ztráty z podvodů / zneužití dat:** 80 000 Kč
- **Vyšetřování a právní náklady:** 30 000 Kč
- **Smluvní pokuty / kompenzace partnerům:** 40 000 Kč
- **ARO:** 0,25 (25 % ročně)
- **E-shop** – roční obrat (použit jako základ pro odhad reputační ztráty): 150 000 Kč/den × 365 ≈ 54 750 000 Kč/rok (převzato ze scénáře I).
- **Hrubá marže e-shopu:** 25 % → roční hrubá marže ≈ 13 687 500 Kč/rok.
- **Předpokládaný podíl zákazníků ztracených v důsledku úniku dat (reputace):** 5 % před opatřeními, 0,5 % po opatřeních (silné snížení díky rychlému zjištění a komunikaci). [6], [31]
- **Modelovaná pokuta GDPR:** 200 000 Kč; pravděpodobnost pokuty: 0,40 před, 0,10 po → EV(GDPR) = p × 200 000. [14], [30]
- **Opatření a orientační roční náklady (DLP, IAM, monitoring, školení, HR procesy):** 190 000 Kč/rok
- **Odhad snížení přímé SLE díky opatřením (DLP + auditing):** pokles z 150 000 Kč → 60 000 Kč (konzervativní odhad díky omezení úniku dat a rychlejší detekci).

Tabulka 5 - Výsledky výpočtů MS II.

Položka	**Před opatřeními**	**Po opatřeních**
Přímé náklady (podvody, vyšetřování, smluvní pokuty)	150 000 Kč	60 000 Kč
EV(GDPR) (pravděpodobnost × pokuta)	80 000 Kč	20 000 Kč
Reputační ztráta (5 % vs 0,5 % z hrubé marže)	684 375 Kč	68 438 Kč
SLE (součet)	**914 375 Kč**	**148 438 Kč**
ARO	0,25	0,08
ALE (SLE × ARO)	**228 594 Kč/rok**	**11 875 Kč/rok**
Roční náklady opatření	–	190 000 Kč/rok
Roční úspora rizika	–	216 719 Kč/rok
Čistý přínos (úspora − náklady)	–	**26 719 Kč/rok**

Zdroj: Vlastní zpracování

2.4.2.2. Interpretace výsledků

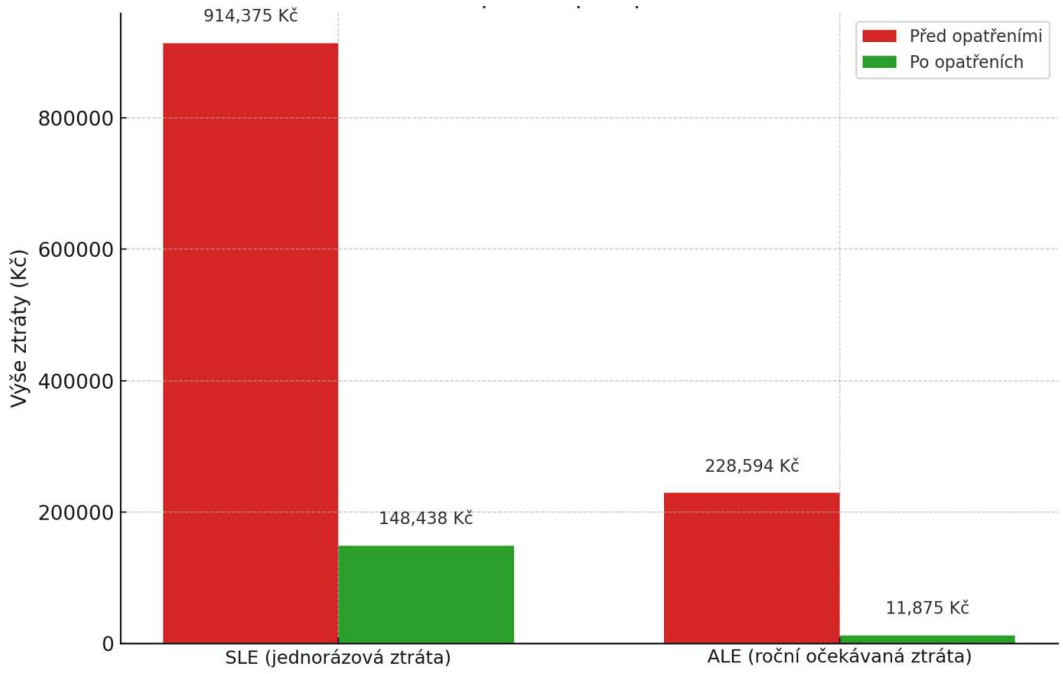
Z Tabulka 5 i grafického znázornění (Obrázek 11 - Grafické znázornění navržených opatření

Zdroj: Vlastní zpracování) je patrné, že zavedení navrhovaných opatření má zásadní vliv na snížení rizik spojených s vnitřními hrozbami. Jednorázová ztráta (SLE) klesá z původních 914 375 Kč na 148 438 Kč, což představuje více než šestinásobné snížení. Největší podíl na SLE před opatřeními tvoří reputační ztráta, vyčíslená na základě odhadu 5% ztráty zákazníků, která sama o sobě činí přes 680 tisíc Kč. Po implementaci opatření se tento odhad snižuje na méně než 70 tisíc Kč díky rychlejší detekci a lepší komunikaci incidentu.

Také očekávaná roční ztráta (ALE) výrazně klesá – z hodnoty 228 594 Kč/rok na pouhých 11 875 Kč/rok. Tento pokles je způsoben nejen nižší jednorázovou ztrátou, ale také snížením pravděpodobnosti výskytu (ARO) z 0,25 na 0,08. Z ekonomického pohledu tak roční úspora rizika činí přibližně 216 719 Kč.

Pokud jsou brány v úvahu i roční náklady na opatření (cca 190 000 Kč), vychází čistý přínos ve výši 26 719 Kč/rok. Investice do prevence je tedy ekonomicky smysluplná, protože nejen pokrývá náklady, ale navíc přináší finanční přínos a zároveň výrazně redukuje reputační a regulatorní rizika, která mají potenciál ohrozit dlouhodobou stabilitu a důvěryhodnost firmy.

Z hlediska řízení rizik lze proto konstatovat, že opatření jsou opodstatněná, a to i v případě, že by přímý finanční přínos nebyl vysoký, neboť hlavním benefitem je omezení těžko vyčíslitelných, ale pro firmu kritických dopadů na reputaci a vztahy se zákazníky.



Obrázek 11 - Grafické znázornění navržených opatření Zdroj: Vlastní zpracování

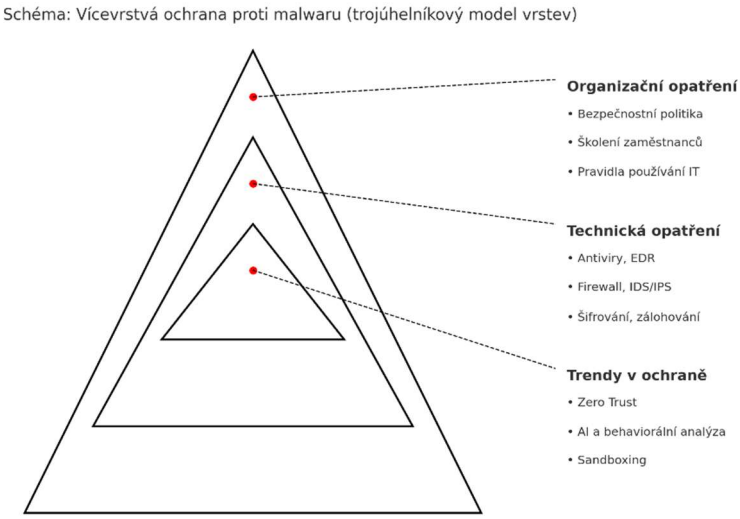
2.4.3. Shrnutí výsledků

Modelová situace I. (ransomware útok) ukázala, že i když bezpečnostní opatření významně snižují očekávané roční ztráty (ALE) z více než 130 000 Kč na zhruba 13 000 Kč, jejich vysoké roční náklady znamenají záporný čistý přínos. Naopak Modelová situace II (vnitřní hrozba – exfiltrace dat) po započtení reputačních škod a regulatorních sankcí prokázala, že opatření nejen dramaticky redukují SLE i ALE, ale zároveň mají pozitivní ekonomický efekt s čistým přínosem přibližně 27 000 Kč ročně. Oba scénáře potvrzují, že správná kombinace technických a organizačních opatření dokáže zásadně snížit rizika, přičemž u některých hrozeb je investice návratná i čistě z ekonomického hlediska, zatímco u jiných je nutné zohlednit především nefinanční přínosy, jako je ochrana reputace a důvěry zákazníků.

2.5. Návrh opatření a doporučení

Návrh opatření je založen na principu vícevrstvé obrany (Obrázek 12), která kombinuje organizační, technická a procesní opatření. Tento přístup je pro firmu velikosti Delta-M s.r.o. optimální, neboť umožňuje zvýšit odolnost proti malwarovým hrozbám bez nutnosti zásadních investic do složitých bezpečnostních řešení. [3], [8], [11]

Výhodou vícevrstvé obrany je její odolnost a flexibilita. Znamená to, že pokud útočník obejde jednu vrstvu (například phishingem získá heslo), další vrstvy (MFA, monitoring, segmentace) mohou útok zastavit nebo alespoň výrazně omezit jeho dopady. Tento přístup je proto považován za standardní a osvědčenou praxi v oblasti kybernetické bezpečnosti, a to jak u velkých korporací, tak i u malých a středních podniků. [5], [29], [31]



Obrázek 12 - Vícevrstvá obrana Zdroj: Vlastní zpracování

2.5.1. Organizační opatření

- **Zavedení bezpečnostní politiky:**
  - Vytvořit interní směrnici, která bude definovat pravidla práce s IT prostředky, nakládání s daty a povinnosti zaměstnanců.
  - Politika by měla zahrnovat i postup při bezpečnostních incidentech.
- **Pravidelná školení zaměstnanců:**
  - Minimálně 1× ročně provádět školení o kybernetických hrozbách.
  - Využívat praktické testy (např. simulované phishingové e-maily).

- **Incident response plán:**
    - Vypracovat plán, který jasně určí postupy při kybernetickém incidentu (od detekce až po obnovu provozu).
    - Definovat kontaktní osoby a jejich kompetence. [10]

2.5.2. Technické opatření

- **Pokročilá antivirová ochrana (EDR):**
    - Nasadit Endpoint Detection and Response systém, který dokáže odhalit i neznámé hrozby a podezřelé chování. [3], [5]
- **IDS/IPS a segmentace sítě:**
    - Doplnit stávající síť o systém pro detekci a prevenci útoků.
    - Rozdělit síť na zóny (kanceláře, servery, e-shop), aby případný útok neohrozil všechny systémy současně. [3], [8]
- **Více faktorová autentizace (MFA):**
    - Zavést MFA nejen u administrátorských účtů, ale i pro přístup k e-mailům, VPN a cloudovým službám. [8], [24]
- **Šifrování koncových zařízení:**
    - Zavést plošné šifrování disků u notebooků a počítačů.
    - Využít standardní nástroje (např. BitLocker, FileVault).
- **Zálohování a testy obnovy:**
    - Nastavit pravidelnou politiku zálohování s uchováváním záloh mimo hlavní síť.
    - Minimálně 2× ročně testovat obnovu dat.

2.5.3. Procesní opatření

- **Patch management:**
    - Zavést systematický proces aktualizací, včetně pravidelného vyhodnocování zranitelností.
    - Využít automatizované nástroje pro distribuci aktualizací. [9], [11]
- **Smluvní zajištění s dodavateli:**
    - Požadovat od poskytovatele hostingu a platební brány doložení bezpečnostních opatření (SLA, certifikace).
    - Zajistit pravidelnou komunikaci ohledně bezpečnostních incidentů. [29]
- **Externí bezpečnostní audit:**
    - 1× ročně provést základní audit (interně či externím specialistou), aby bylo možné zhodnotit efektivitu zavedených opatření. [31]

2.5.4. Prioritizace opatření

S ohledem na dostupné kapacity a rozpočet se doporučuje následující pořadí implementace:

- **Okamžité zavedení MFA a aktualizace bezpečnostních politik**
  Více faktorová autentizace (MFA) patří k nejúčinnějším a zároveň finančně nenáročným opatřením. Spolu s aktualizovanými bezpečnostními politikami (např. pravidla pro práci s hesly) představuje základní obrannou linii, která dokáže zabránit velkému množství útoků vedených přes kompromitované účty.
- **Pravidelná školení zaměstnanců a incident response plán**
  Lidský faktor zůstává jednou z nejčastějších slabin v oblasti kybernetické bezpečnosti. Pravidelná školení zvyšují povědomí zaměstnanců o hrozbách, jako je phishing nebo sociální inženýrství. Současně by měla být vytvořena a nacvičena procedura reakce na incident (incident response plan), aby byla organizace schopna reagovat rychle a koordinovaně.
- **Implementace EDR a segmentace sítě**
  Endpoint Detection and Response (EDR) systémy umožňují včasnou detekci útoků a jejich blokaci na koncových zařízeních. Segmentace sítě zajišťuje, že se případný útočník nemůže volně pohybovat mezi jednotlivými částmi infrastruktury. Kombinace těchto opatření výrazně omezuje rozsah a dopad případného útoku.

- **Zálohování s testy obnovy a plošné šifrování zařízení**
  Pravidelné zálohování dat je nezbytné pro obnovení chodu společnosti po útoku, zejména v případě ransomwaru. Zálohy však musí být nejen vytvářeny, ale také pravidelně testovány, aby byla zajištěna jejich funkčnost. Plošné šifrování zařízení pak chrání citlivá data před zneužitím v případě ztráty či krádeže notebooku nebo mobilního telefonu.
- **Audit bezpečnosti a smluvní zajištění s dodavateli**
  Po zavedení základních opatření by měl následovat audit, který ověří jejich funkčnost a identifikuje případné mezery. Neméně důležité je smluvně ošetřit spolupráci s dodavateli, zejména pokud mají přístup k systémům nebo zpracovávají citlivá data.

2.6. Přínos navržených opatření

Implementace navržených organizačních, technických a procesních opatření přinese firmě Delta-M s.r.o. řadu konkrétních přínosů, které lze rozdělit do několika oblastí.

2.6.1. Zvýšení úrovně kybernetické bezpečnosti

Zavedení vícevrstvé ochrany významně snižuje pravděpodobnost úspěšného malwarového útoku. Každá jednotlivá vrstva přitom představuje samostatnou bariéru – i pokud útočník překoná jednu z nich, další opatření mu v postupu zabrání nebo útok alespoň zpomalí. Nasazení technologií jako EDR (Endpoint Detection and Response) umožňuje včasnou detekci neobvyklého chování koncových zařízení a jejich izolaci. IDS/IPS systémy zajišťují monitoring síťového provozu a blokaci podezřelých aktivit v reálném čase. Segmentace sítě omezuje možnost laterálního pohybu útočníka napříč infrastrukturou, čímž brání plošnému rozšíření infekce. Plošné šifrování disků a zařízení pak chrání data i v případě ztráty notebooku či mobilu. Zavedení MFA (více faktorové autentizace) výrazně komplikuje zneužití přístupových údajů, což je jeden z nejčastějších vstupních vektorů útoku.

2.6.2. Zajištění kontinuity provozu

Schopnost udržet provoz nebo jej rychle obnovit je pro společnost klíčová. Pravidelné zálohování spolu s testy obnovy poskytuje jistotu, že data budou dostupná i v případě ransomwarového útoku nebo hardwarového selhání. Zkušenosti ukazují, že samotná existence záloh nestačí, je tedy nutné jejich funkčnost průběžně ověřovat. Incident response plán určuje jasné postupy při odhalení incidentu: kdo má jaké pravomoci, jak probíhá eskalace problému, jak se komunikuje dovnitř firmy i směrem k zákazníkům a partnerům. Díky tomu se zkrátí doba

potřebná k vyřešení incidentu, sníží se chaos a minimalizuje se negativní dopad na každodenní činnost firem.

2.6.3. Ochrana citlivých dat a důvěry zákazníků

Ochrana osobních údajů zákazníků a citlivých firemních informací je nejen právní povinností, ale i zásadním faktorem důvěryhodnosti společnosti. Šifrování koncových zařízení brání zneužití dat v případě jejich ztráty nebo krádeže. MFA zase zajišťuje, že ani kompromitované heslo samo o sobě nestačí k neoprávněnému přístupu do systémů. Implementace těchto opatření pomáhá splnit požadavky GDPR a minimalizovat riziko sankcí. Zákazníci i obchodní partneři přitom vnímají úroveň ochrany dat jako jeden z klíčových ukazatelů důvěry, lze tedy bezpečnost považovat konkurenční výhodou.

2.6.4. Ekonomické přínosy

Ekonomické dopady kybernetických incidentů bývají zásadní. Náklady spojené s výkupným, dlouhodobým výpadkem e-shopu, obnovou systémů nebo reputačními škodami mohou dosahovat velmi vysokých částek. Investice do preventivních opatření (např. EDR, školení, segmentace, zálohování) jsou ve srovnání s těmito náklady relativně nízké. Analýza modelových scénářů ukázala, že dobře nastavená opatření mohou snížit ALE (Annualized Loss Expectancy) o desítky až stovky tisíc korun ročně. I když některá opatření nemusí přinášet okamžitě pozitivní čistý přínos v přímém finančním vyjádření, jejich skutečný přínos spočívá ve snížení rizika katastrofických dopadů a ochraně dlouhodobé stability firmy.

2.6.5. Soulad s legislativou a normami

Evropská legislativa, zejména směrnice NIS2 a nařízení GDPR, klade stále vyšší požadavky na úroveň kybernetické bezpečnosti. Organizace, které se jim aktivně přizpůsobí, nejen že minimalizují riziko sankcí, ale také zvyšují svou konkurenceschopnost. V praxi to znamená, že splnění požadavků na bezpečnostní opatření je často podmínkou pro spolupráci s většími partnery nebo pro účast ve výběrových řízeních. Implementace vícevrstvé ochrany, pravidelné audity a dokumentované procesy řízení bezpečnosti tak přinášejí i strategické obchodní výhody.

2.6.6. Posílení firemní kultury

Technologie sama o sobě nestačí, rozhodující roli hrají zaměstnanci. Pravidelná školení, jasná pravidla používání IT prostředků a otevřená komunikace o rizicích posilují povědomí o kybernetické bezpečnosti v celé organizaci. Zaměstnanci se stávají aktivní součástí obrany, rozpoznávají podezřelé situace a dokážou včas nahlásit možné incidenty. To vede ke snížení počtu událostí způsobených lidskou chybou, které tvoří významnou část všech bezpečnostních

incidentů. Z dlouhodobého hlediska pak tato opatření přispívají k budování kultury důvěry, odpovědnosti a profesionálního přístupu k ochraně dat.

3 VYHODNOCENÍ VÝSLEDKŮ

3.1. Porovnání teorie a praxe

V teoretické části práce byla popsána základní východiska kybernetické bezpečnosti, současné trendy v ochraně proti malwaru a rámce, které firmám doporučují systematický přístup k řízení rizik (např. ISO/IEC 27001, NIST Cybersecurity Framework, COBIT či směrnice NIS2). Tyto dokumenty představují obecně uznávaný teoretický základ, na němž lze budovat efektivní bezpečnostní politiku a dlouhodobě řídit kybernetická rizika. Jejich výhodou je univerzálnost a strukturovaný pohled, který pomáhá organizacím postupovat metodicky a neopomenout žádnou klíčovou oblast.

Praktická část práce však ukázala, že realita malých a středních podniků, jako je Delta-M s.r.o., je odlišná. Tato firma má sice zavedené základní bezpečnostní prvky (antivirovou ochranu, pravidelné zálohování, firewall), avšak postrádá pokročilejší opatření, která by dokázala čelit současným sofistikovaným hrozbám (např. EDR systémy, segmentace sítě, více faktorová autentizace, pravidelná školení zaměstnanců). Ukázalo se tedy, že zatímco teorie směřuje k úplnému pokrytí všech vrstev ochrany, praxe v menších firmách se často omezuje na minimum dané kapacitami a financemi.

Porovnání teorie a praxe ukazuje, že i když je plná implementace bezpečnostních rámců pro menší podniky často nerealistická, existuje prostor pro zavedení levných a relativně jednoduchých opatření. I základní kroky, jako je MFA, školení zaměstnanců nebo pravidelné testy záloh, mají potenciál významně snížit úroveň rizika a posílit odolnost dané společnosti.

3.2. Vyhodnocení efektivity navržených opatření

Na základě provedené analýzy rizik lze hodnotit přínos jednotlivých bezpečnostních opatření jak kvantitativně, tak kvalitativně.

Kvantitativní vyhodnocení

Modelový scénář ransomware útoku ukázal, že očekávaná roční ztráta (ALE) klesne po implementaci opatření z 131 100 Kč na 12 994 Kč, což představuje snížení rizika o přibližně 90 %. Podobně i u phishingového scénáře by kombinace školení zaměstnanců a MFA mohla snížit pravděpodobnost incidentu (ARO) ze 60 % na 20 %, čímž by se ALE snížilo ze 120 000 Kč na přibližně 40 000 Kč. Tyto výsledky jasně ukazují, že i relativně levná opatření mohou mít výrazný vliv na úroveň rizika.

Kvalitativní vyhodnocení

Implementovaná opatření přinášejí firmě schopnost reagovat na incidenty rychleji a efektivněji. Významným přínosem je i posílení důvěry zákazníků, například u e-shopu je důvěra zákazníků klíčovým faktorem pro udržení loajality a schopnosti konkurovat na trhu. Součástí efektivity je rovněž lepší připravenost na legislativní požadavky (NIS2, GDPR). Tyto faktory sice nejsou vždy snadno kvantifikovatelné, ale mají zásadní význam pro dlouhodobou udržitelnost podnikání.

Celkově lze říci, že navržená opatření významně zvyšují bezpečnostní úroveň společnosti, a to i přesto, že představují určitou finanční zátěž. Návrh zároveň respektuje omezený rozpočet malých firem a doporučuje prioritizaci opatření podle poměru ceny ku výkonu, což činí přístup realistickým a aplikovatelným.

3.3. Přínos pro firmu

Navržená opatření mají několik konkrétních přínosů, které se dají rozdělit do více dimenzí.

- **Technický přínos:** Zavedení vícevrstvé ochrany (firewall, EDR, IDS/IPS, zálohy, MFA) významně snižuje pravděpodobnost úspěšného útoku a zkracuje dobu potřebnou k obnově provozu. Opatření navíc umožňují rychlejší detekci útoků, a tedy i menší škody.
- **Organizační přínos:** Vytvoření bezpečnostní politiky a pravidelných školení zaměstnanců zvyšuje jejich povědomí o hrozbách a aktivně je zapojuje do procesu obrany. Díky tomu se zaměstnanci stávají nejen potenciální slabinou, ale i aktivní součástí ochrany firmy.
- **Ekonomický přínos:** I když opatření znamenají roční investici, předejdou potenciálním ztrátám, které mohou přesáhnout mnohdy i milionové částky (např. při úspěšném ransomware útoku nebo velkém úniku dat). Náklady na prevenci jsou tedy ve srovnání s možnými ztrátami zanedbatelné.
- **Strategický přínos:** Firma je připravena na legislativní změny (např. implementaci směrnice NIS2) a může díky tomu posílit svou pozici při jednání s obchodními partnery. Splnění bezpečnostních požadavků se stává konkurenční výhodou.

Pro firmu Delta-M s.r.o. tedy práce představuje konkrétní a praktický návod, jak systematicky a realisticky posílit svou odolnost proti malwaru a jiným kybernetickým hrozbám.

3.4. Přínos pro širší oblast kybernetické bezpečnosti

Výsledky této práce mají potenciální přínos i nad rámec vybrané společnosti.

- **Metodický přínos:** Práce ukazuje, jak lze provést analýzu rizik v prostředí menší firmy pomocí jednoduchého modelu SLE/ALE a scénářů, což může být inspirací pro další podniky v ČR.
- **Aplikační přínos:** Vytvořený modelový příklad (ransomware i insider scénář) s reálnými čísly demonstruje, že i menší firmy mohou kvantifikovat kybernetická rizika a vyhodnocovat návratnost investic do ochrany.
- **Edukační přínos:** Díky schématům, časové ose útoku a přehledným tabulkám lze práci využít i jako studijní materiál pro školení zaměstnanců menších firem.
- **Strategický přínos:** Diplomová práce dokládá, že systematická kybernetická bezpečnost se netýká pouze velkých korporací, ale je dosažitelná i pro malé a střední podniky, pokud se zvolí vhodná a ekonomicky přiměřená strategie.

Tato část diplomové práce tedy ukazuje, že i relativně malá firma může významně zvýšit svou kybernetickou odolnost prostřednictvím cílených a ekonomicky udržitelných opatření. Praktický přínos spočívá zejména v detailních modelových příkladech a doporučeních, která lze okamžitě aplikovat. Přínos pro širší oblast pak spočívá v prezentaci metodiky, která může být inspirací pro další malé a střední podniky v České republice.

ZÁVĚR

Tato diplomová práce se zaměřila na problematiku ochrany firem proti malwaru a na konkrétní případ společnosti Delta-M s.r.o. Práce byla rozdělena na část teoretickou a praktickou, které se vzájemně doplňovaly a společně poskytly ucelený pohled na zajištění kybernetické bezpečnosti.

V teoretické části byly nejprve popsány základy kybernetické bezpečnosti, historie a současný vývoj malwaru i jeho nejrozšířenější typy. Součástí byla také analýza specifik firemního prostředí, nejčastějších způsobů šíření hrozeb a přehled metod ochrany, které zahrnují jak technická, tak organizační a procesní opatření. Tyto poznatky vytvořily rámec, jenž umožnil lépe porozumět aktuálním rizikům a připravit se na jejich hodnocení v praktické části.

Praktická část se zaměřila na reálné prostředí firmy Delta-M. Byla provedena charakteristika společnosti, zhodnocení současného zabezpečení a detailní analýza rizik. Modelový scénář ransomware útoku ukázal, že potenciální jednorázová ztráta by se mohla pohybovat ve stovkách tisíc korun a že dlouhodobé roční ztráty způsobené incidenty by mohly významně zatěžovat rozpočet. Druhá modelová situace (vnitřní hrozba) pak ukázala, že i zdánlivě méně pravděpodobné incidenty mohou mít pro firmu citelné následky. Kvantifikace pomocí SLE a ALE prokázala, že únik citlivých dat zaměstnancem může znamenat nejen přímé finanční ztráty a smluvní sankce, ale i významné reputační dopady. Zároveň se ukázalo, že v tomto případě navržená opatření (princip nejmenších práv, DLP systémy, školení, jasná HR politika) mají pozitivní ekonomickou návratnost (ROI), a tedy jsou přínosná i z pohledu investic.

Na základě této analýzy byla navržena sada opatření založená na principu vícevrstvé ochrany. Do návrhu byla zahrnuta technická opatření (EDR, IDS/IPS, segmentace sítě, šifrování), organizační kroky (bezpečnostní politika, školení zaměstnanců, pravidla pro práci s IT prostředky) i procesní prvky (incident response plán, pravidelné testy záloh). Vyhodnocení ukázalo, že tato opatření mohou snížit očekávané roční ztráty (ALE) až o 90 %, zajistit rychlejší obnovu provozu a zvýšit úroveň souladu s legislativními požadavky, zejména GDPR a NIS2.

Cíle práce byly tímto naplněny, práce popsala současné hrozby malwaru a jejich dopady na firmy, analyzovala stav zabezpečení konkrétních společností, identifikovala nedostatky a navrhla praktická opatření. Součástí bylo také modelové vyčíslení rizik a ekonomické zhodnocení přínosů jednotlivých opatření, což poskytlo firmám jasný argumentační rámec pro rozhodování o investicích do bezpečnosti.

Možnosti dalšího rozvoje vidím především v oblasti dlouhodobého měření efektivity zavedených opatření a pravidelných auditů kybernetické bezpečnosti. Do budoucna by bylo vhodné posílit také aktivní zapojení zaměstnanců do prevence a zvážit certifikaci podle standardu ISO/IEC 27001, která by společnosti přinesla nejen vyšší úroveň zabezpečení, ale i konkurenční výhodu při jednání s obchodními partnery.

Z mé analýzy vyplývá, že i menší firma, jakou je Delta-M s.r.o., dokáže díky rozumně nastaveným a finančně dostupným opatřením výrazně posílit svou odolnost vůči malwaru. V praxi to znamená, že i když nemá rozpočet jako velká korporace, může díky nástrojům jako MFA, EDR nebo pravidelnému školení zaměstnanců výrazně snížit riziko vážného incidentu. Při psaní práce jsem se přesvědčila, že teorie z rámců typu ISO 27001 nebo NIS2 se dá přenést i do prostředí menších firem, jen je potřeba ji přizpůsobit jejich možnostem. Práce tak může sloužit nejen jako shrnutí současných hrozeb, ale také jako praktický návod pro firmy, které řeší podobné problémy.

POUŽITÁ LITERATURA

[1] NÚKIB. *Výkladový slovník kybernetické bezpečnosti*. Brno: NÚKIB, 2022 [online; cit. 2025-09-19]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf

[2] JIRÁSEK, P. a kol. *Výkladový slovník kybernetické bezpečnosti (verze 5)*. Praha: Policejní akademie ČR & AFCEA, 2022 [online; cit. 2025-09-19]. Dostupné z: https://nukib.gov.cz

[3] ENISA. *ENISA Threat Landscape 2024*. Heraklion: ENISA, 2024 [online; cit. 2025-09-19]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[4] ENISA. *ENISA Threat Landscape 2024 (PDF edition)*. Heraklion: ENISA, 2024 [online; cit. 2025-09-19]. Dostupné z: https://securitydelta.nl/media/com_eventbooking/ENISA-Threat-Landscape-2024.pdf

[5] VERIZON. *2024 Data Breach Investigations Report (DBIR)*. Verizon, 2024 [online; cit. 2025-09-19]. Dostupné z: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[6] IBM SECURITY; PONEMON INSTITUTE. *Cost of a Data Breach Report 2024*. IBM, 2024 [online; cit. 2025-09-19]. Dostupné z: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

[7] IBM SECURITY; PONEMON INSTITUTE. *Cost of a Data Breach Report 2025*. IBM, 2025 [online; cit. 2025-09-19]. Dostupné z: https://www.ibm.com/reports/data-breach

[8] NIST. *Special Publication 800-207: Zero Trust Architecture*. Gaithersburg: NIST, 2020 [online; cit. 2025-09-19]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[9] NIST. *Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments*. Gaithersburg: NIST, 2012 [online; cit. 2025-09-19]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[10] NIST. *Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems*. Gaithersburg: NIST, 2010 [online; cit. 2025-09-19]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[11] ISO. *ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks*. Ženeva: ISO, 2022 [online; cit. 2025-09-19]. Dostupné z: https://www.iso.org/standard/80585.html

[12] ISO. *ISO 31000: Risk management – Guidelines*. Ženeva: ISO, 2018 [online; cit. 2025-09-19]. Dostupné z: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf

[13] MITRE. *ATT&CK® for Enterprise – Matrix & Techniques*. MITRE, 2025 [online; cit. 2025-09-19]. Dostupné z: https://attack.mitre.org/matrices/

[14] EVROPSKÁ UNIE. *Nařízení (EU) 2016/679 (GDPR)*. Úřední věstník Evropské unie, 2016 [online; cit. 2025-09-19]. Dostupné z: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[15] EVROPSKÁ UNIE. *Směrnice (EU) 2022/2555 (NIS2)*. Úřední věstník Evropské unie, 2022 [online; cit. 2025-09-19]. Dostupné z: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[16] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti ČR za rok 2023*. Brno: NÚKIB, 2024 [online; cit. 2025-09-19]. Dostupné z: https://nukib.gov.cz/download/uredni-deska/zpravy/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf

[17] NÚKIB. *FN Brno nahlásila kybernetický bezpečnostní incident* [tisková zpráva]. Brno: NÚKIB, 13. 3. 2020 [online; cit. 2025-09-19]. Dostupné z: https://nukib.gov.cz/cs/infoservis/tiskove-zpravy/1972-fn-v-brne-bohunicich-dnes-nahlasila-nukibu-kyberneticky-bezpecnostni-incident/

[18] ČT24. *Útok na benešovskou nemocnici způsobil škodu přes 59 milionů korun*. Praha: Česká televize, 18. 8. 2020 [online; cit. 2025-09-19]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/utok-na-benesovskou-nemocnici-zpusobil-skodu-pres-59-mil-kc

[19] IROZHLAS. *Benešovskou nemocnici napadl ransomware Ryuk*. Praha: Český rozhlas, 14. 1. 2020 [online; cit. 2025-09-19]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware_2001140600_pj

[20] ZDRAVOTNICKÝ DENÍK. *FN Brno se stala terčem kybernetického útoku*. Praha: Zdravotnický deník, 14. 3. 2020 [online; cit. 2025-09-19]. Dostupné z: https://www.zdravotnickydenik.cz/2020/03/fn-brno-se-stala-tercem-kybernetickeho-utoku/

[21] CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ za rok 2023*. Praha: CZ.NIC, 2024 [online; cit. 2025-09-19]. Dostupné z: https://csirt.cz/public/media/1711540396/501/

[22] CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ za rok 2024*. Praha: CZ.NIC, 2025 [online; cit. 2025-09-19]. Dostupné z: https://csirt.cz/public/media/1743090507/756/

[23] CZ.NIC. *Domain Report 2024 – tisková zpráva*. Praha: CZ.NIC, 30. 1. 2025 [online; cit. 2025-09-19]. Dostupné z: https://www.nic.cz/page/4507/

[24] NIST. *Special Publication 800-207A (draft): A Zero Trust Architecture Model for Access Control in Cloud-Native Applications*. Gaithersburg: NIST, 2023 [online; cit. 2025-09-19]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.ipd.pdf

[25] PALO ALTO NETWORKS. *What is the MITRE ATT&CK Matrix?* Palo Alto Networks, 2025 [online; cit. 2025-09-19]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-matrix

[26] ČESKÝ STATISTICKÝ ÚŘAD. *E-commerce v České republice 2022*. Praha: ČSÚ, 2023.

[27] MINISTERSTVO PRŮMYSLU A OBCHODU. *Digitální ekonomika a společnost v ČR*. Praha: MPO, 2022.

[28] MICROSOFT. *Security risks of cloud services*. Whitepaper. Redmond: Microsoft, 2022.

[29] ENISA. *Cloud Security for SMEs*. European Union Agency for Cybersecurity, 2021.

[30] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Handbook on European data protection law*. Luxembourg: Publications Office of the EU, 2021.

[31] JIRÁSEK, Jakub. *Kybernetická bezpečnost v malých a středních podnicích*. Praha: CZ.NIC, 2020. ISBN 978-80-88168-47-2.

[32] VERIZON. *Data Breach Investigations Report 2022*. Verizon Enterprise, 2022.

[33] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zpráva o stavu kybernetické bezpečnosti České republiky 2021*. Brno: NÚKIB, 2022.