**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**

# Bakalářská práce

## Prevence, detekce a obnova dat v souvislosti s ransomwarem

**Kateřina Mlčochová**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Kateřina Mlčochová

Informatika

Název práce

**Prevence, detekce a obnova dat v souvislosti s ransomwarem**

Název anglicky

**Prevention, detection and data recovery in the context of ransomware**

---

**Cíle práce**

Cílem této bakalářské práce je shrnout existující strategie prevence, detekce a obnovy dat v souvislosti s ransomwarem a navrhnout doporučení pro zvýšení účinnosti ochrany uživatelů a minimalizaci dopadu ransomwarových útoků.

**Metodika**

V teoretické části se práce bude věnovat především prozkoumání odborné literatury, výzkumných článků a publikací týkajících se ransomwaru, programů, které jsou schopny detekovat ransomware a nástrojů pro obnovu dat. Dále na virtuálním stroji bude spuštěn ransomware a následně bude pomocí experimentu testována účinnost programů proti ransomwaru a nástrojů pro obnovu dat. Následná analýza výsledků experimentu by měla přinést doporučení v oblasti ochrany proti ransomwarovým útokům a minimalizaci jejich dopadu.

**Doporučený rozsah práce**

30 – 40 stran

**Klíčová slova**

ransomware, bezpečnost, počítačový virus, internetová kriminalita, kyberbezpečnost

---

**Doporučené zdroje informací**

JENKINSON, Andrew. Ransomware and Cybercrime. John Wiley & Sons, 2022. ISBN 9781032235509.
KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.
LISKA, Allan. Ransomware: Defending Against Digital Extortion. Oreilly Media, 2016. ISBN 9781491967881.
PETROWSKI, Thorsten a Tomáš KURKA. Bezpečí na internetu pro všechny. Liberec: Dialog, 2014. ISBN 978-80-7424-066-9.
SMEJKAL, Vladimír. Kybernetická kriminalita, 3. vydání. Vyd. 3. Plzeň: Aleš Čeněk s.r.o, 2022. ISBN 978-80-7380-849-5.

---

**Předběžný termín obhajoby**

2023/24 LS – PEF

**Vedoucí práce**

Ing. Václav Lohr, Ph.D.

**Garantující pracoviště**

Katedra informačních technologií

Elektronicky schváleno dne 4. 9. 2023

**doc. Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

**doc. Ing. Tomáš Šubrt, Ph.D.**

Děkan

V Praze dne 15. 03. 2024

**Čestné prohlášení**

Prohlašuji, že svou bakalářskou práci "Prevence, detekce a obnova dat v souvislosti s ransomwarem" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2024 _____

**Poděkování**

Ráda bych touto cestou poděkovala Ing. Václavu Lohrovi, Ph.D. za vedení mé práce a za jeho užitečné rady, které mi při vypracovávání poskytl.

# Prevence, detekce a obnova dat v souvislosti s ransomwarem

**Abstrakt**

Tato bakalářská práce se zaměřuje na stále se zvyšující hrozbu ransomwarových útoků a jejich dopady na podniky a jednotlivce. Cílem této práce je prozkoumat různé aspekty prevence, detekce a obnovy dat. V teoretické části práce jsou prozkoumány metody a techniky, které umožňují minimalizovat riziko infikace ransomwarem a snižovat dopady útoků.

V praktické části práce je proveden experiment, který zahrnuje testování různých programů na detekci ransomwaru a nástrojů na obnovu zašifrovaných dat. Tento experiment je klíčovým prvkem, který má poskytnout praktický náhled na efektivnost dostupných nástrojů v boji proti ransomwaru. Výsledky tohoto experimentu budou analyzovány s cílem identifikovat nejlepší produkty pro ochranu a obnovu dat.

Bakalářská práce má za cíl přispět k lepšímu porozumění o této aktuální hrozbě a poskytnout doporučení jak pro podniky, tak i jednotlivce.

**Klíčová slova:** ransomware, bezpečnost, počítačový virus, internetová kriminalita, kyberbezpečnost

# Prevention, detection and data recovery in the context of ransomware

**Abstract**

This bachelor thesis focuses on the ever-increasing threat of ransomware attacks and their impact on businesses and individuals. The aim of this thesis is to explore various aspects of data prevention, detection and recovery. In the theoretical part of the thesis, methods and techniques are explored to minimize the risk of ransomware infection and reduce the impact of attacks.

In the practical part of the thesis, an experiment is conducted which involves testing different ransomware detection programs and tools for recovering encrypted data. This experiment is a key element to provide a practical insight into the effectiveness of available tools in combating ransomware. The results of this experiment will be analysed to identify best practices for prevention, detection and data recovery.

The thesis aims to contribute to a better understanding of this current threat and provide recommendations for both businesses and individuals.

**Keywords**: ransomware, security, computer virus, cybercrime, cyber security

# Obsah

# 1. Úvod

Ve dnešní digitální éře, která je doprovázena neustálým pokrokem technologií a rychlým rozvojem digitálního prostředí, je zřejmé, že i kybernetické hrozby se stávají stále složitějšími a sofistikovanějšími. Ransomware zaujímá v tomto neustále se měnícím prostředí významné místo jako jedna z nejnaléhavějších a nejrozšířenějších hrozeb v oblasti kybernetické bezpečnosti, a to nejen kvůli ekonomickým škodám, které způsobuje, ale také kvůli rozsahu a dopadům, které postihují jak jednotlivce, tak podniky v různých oborech i velikostech.

Ransomware ovlivňuje nejen finanční stabilitu a kontinuitu provozu, ale i klíčové technologické systémy, narušuje integritu dat a ohrožuje důvěrnost citlivých informací. Prostřednictvím svévolného omezování přístupu k důležitým informacím, souborům, anebo dokonce celým systémům, způsobuje vážné problémy, které doprovází potřeba tento problém urgentně řešit.

Ve stále se rozšiřujícím spektru potenciálních cílů a při stále sofistikovanějších metodách útoků je třeba implementovat strategie, které by minimalizovaly rizika spojená s výskytem ransomwaru. Tyto strategie by měly umožnit efektivní detekci a rychlou reakci v případě úspěšného útoku. Je také důležité nezapomínat na znalost mechanismů a postupů pro obnovu dat po incidentu s ransomwarem, aby se nejen podniky, ale i jednotlivci, mohli po útoku co nejdříve zotavit.

# 2. Cíl práce a metodika

## 1.1 Cíl práce

Tato bakalářská práce má za cíl shrnout existující strategie prevence, jak se ransomware detekuje a způspby obnovy dat a navrhnout doporučení pro zlepšení účinnosti ochrany uživatelů a minimalizaci dopadů ransomwarových útoků.

## 1.2 Metodika

V teoretické části se práce zaměří především na prozkoumání odborné literatury, výzkumných článků a publikací zabývajících se ransomwarem, programy schopnými detekovat ransomware a nástroji pro obnovu dat. Dále bude na virtuálním stroji spouštěn ransomware a bude testována účinnost programů proti ransomwaru a nástrojů pro obnovu dat. Následná analýza výsledků experimentu by měla přinést doporučení v oblasti ochrany proti ransomwarovým útokům a minimalizaci jejich dopadů.

# 3. Teoretická východiska

## 3.1 Ransomware

Ransomware je typ škodlivého softwaru, jehož cílem je vydírat uživatele omezením přístupu k jejich datům nebo celému systému. (Liska, 2016) Termín ransomware vznikl spojením anglického slova „ransom“ (výkupné) a slova „malware“ (zkratka pro malicious software, tedy škodlivý software), což označuje jakýkoliv škodlivý software, jehož cílem je narušit činnost počítače, získat citlivé informace nebo získat přístup k systému. (Kolouch, 2016) Podrobněji by se dal popsat jako *„Typ malwaru, jehož prostřednictvím útočník vyžaduje pod různými výhružkami peníze, v lepším se může na počítači zobrazovat výzva k zaplacení „pokuty“ za údajné porušení autorských práv nebo používání nelegálního softwaru, v horším případě dojde k zašifrování dat na disku (přičemž není jisté, že po zaplacení útoční data opravdu odblokuje)“* (Král, 2015, s. 14). Tato forma kybernetické hrozby se vyskytuje ve dvou hlavních variantách, které se liší způsobem, jakým omezují přístup.

První varianta ransomwaru se zaměřuje na šifrování, maskování nebo blokování přístupu k jednotlivým souborům, čímž uživatelům brání v běžném používání jejich dat. Soubory jsou zašifrovány, a uživatelé tak nemohou své soubory otevřít nebo upravovat. Druhá varianta ransomwaru zasahuje na úrovni celých systémů, čímž omezuje uživatelům přístup k jejich zařízením.

Ransomware není omezen geograficky a ani se neváže pouze na konkrétní platformy, a proto se týká mnoha zařízení s různými operačními systémy. Všechna tato zařízení jsou vystavena riziku, přičemž metody útoku se mohou lišit. Nicméně útočníci často opakují známé vzorce chování, což usnadňuje detekci. (Kolouch, 2016)

### 3.1.1 Typy ransomwaru

Ransomwarové útoky se objevují v různých podobách, přičemž každá z nich má své specifické vlastnosti. Pochopení různorodých typů ransomwaru je klíčové pro zavedení cílených obranných strategií a snižování rizik spojených s tímto typem hrozby.

Kryptografický ransomware, známý také jako šifrovací ransomware nebo crypto-ransomware, je nejběžnější a nejznámější variantou ransomwaru. Jeho základním principem je šifrování souborů na cílovém zařízení a následné zablokování těchto souborů, dokud není

zaplaceno výkupné. Tento typ šifruje různé typy souborů, včetně dokumentů, fotografií, videí a databází, přičemž využívá silné a bezpečné šifrovací algoritmy. Zaměřuje se především na soubory, které jsou pro uživatele cenné nebo často používané. Součástí tohoto typu ransomwaru bývá často dialogové okno s odpočítávání času, které má za úkol přimět uživatele, aby rychle vyhověli požadavkům útočníků a zaplatili výkupné. Mezi známé příklady kryptografického ransomwaru patří CryptoLocker, WannaCry a Locky, které způsobily rozsáhlé finanční škody a vážně narušily činnost v mnoha odvětvích a sektorech. (Hermans, 2023)

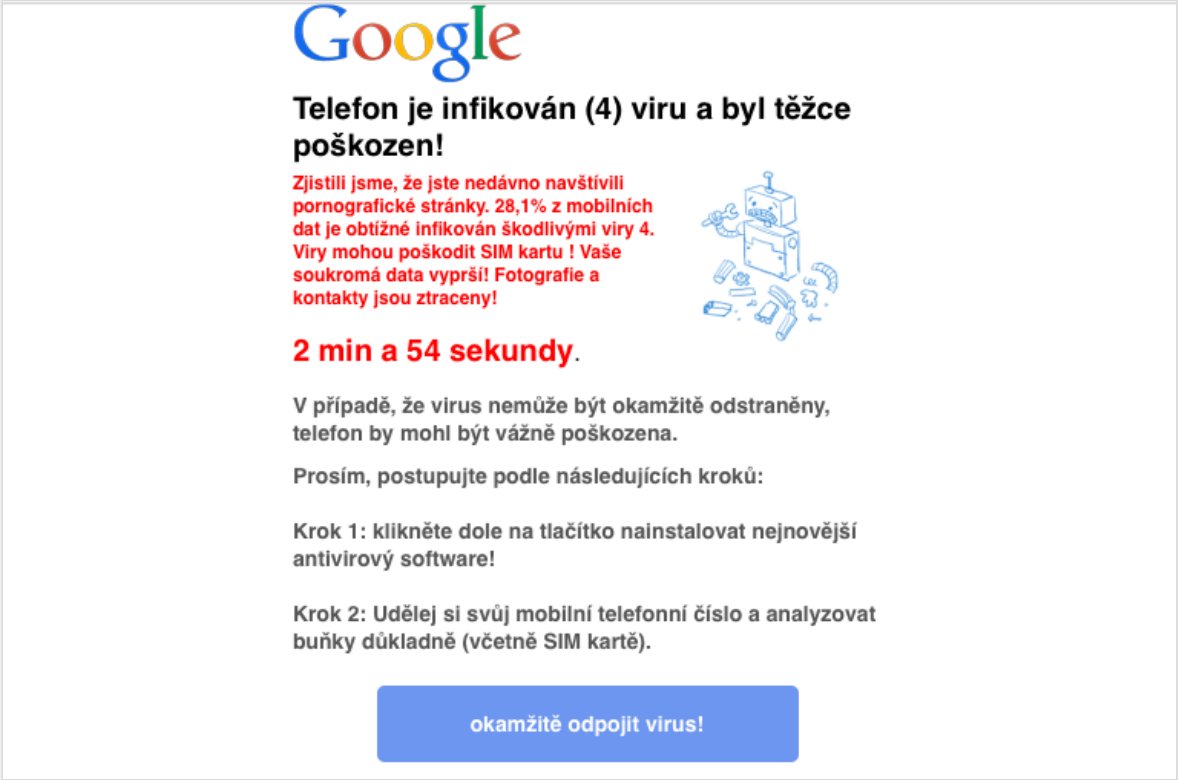

*Obrázek 1 Příklad ransomwaru WannaCry https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALPoheOGBqvpy1ztw0FuMbIFWyCOJQh1ZHRBh-izsSqeGt1fN68jtUUYHv3DAHvsikgMwyMoaSxOk7VXSm2LeYFgmd18AY8dvK-G86uANc_0hVMFjRL1Q7vQg9ekZqem0ysrgHYXXmAJoYwVwhP2c3h2l4__5ewVqo8gQlmNWwME*

Blokovací ransomware, známý také jako screen locker, je varianta ransomwaru, která se namísto šifrování souborů soustředí na zamčení napadeného zařízení nebo jeho částí, čímž zabraňuje uživatelům přístup k systémovým datům a funkcím. Zamčení se provádí tak, že útočník převezme kontrolu nad ovládacími mechanismy obrazovky a zobrazí okno s výzvou k zaplacení výkupného. I když uživatelé mohou vidět obsah své obrazovky, jejich možnosti interakce s ní jsou drasticky omezeny. To v praxi znamená, že uživatelé jsou často nuceni reagovat pouze na pokyny útočníka, zatímco normální funkce jejich zařízení zůstávají

zablokované. Útok může být zahájen využitím zranitelností operačního systému nebo prostřednictvím technik sociálního inženýrství, jež vedou uživatele k udělení přístupových práv, která ransomware následně využije k ovládnutí postiženého zařízení. (Wickramasinghe, 2023)


*Obrázek 2 Příklad blokovacího ransomwaru https://www.pcrisk.com/removal-guides/7291-sluzba-kriminalni-policie-virus*

Scareware, jak už název napovídá, používá jako hlavní taktiku vyvolání strachu u uživatelů, a to falešným informováním o tom, že jejich počítač je infikován škodlivým softwarem. Cílem je přimět uživatele, aby zaplatili za antivirový program, který by odstranil neexistující virus. Scareware se typicky objevuje ve formě vyskakovacích oken při prohlížení webových stránek nebo při instalaci softwaru. Klíčovým prvkem scarewaru je tedy, že i když se uživateli zobrazí varování, počítač ve skutečnosti není infikován a naopak, antivirový software, za který je v rámci scarewaru vyžadován poplatek, představuje pro uživatele skutečné nebezpečí. (Wickramasinghe, 2023)




*Obrázek 3 Příklad scarewaru https://www.lupa.cz/clanky/podvodne-reklamy-strasi-virovou-nakazou-siri-je-i-reklamni-sit-googlu/*

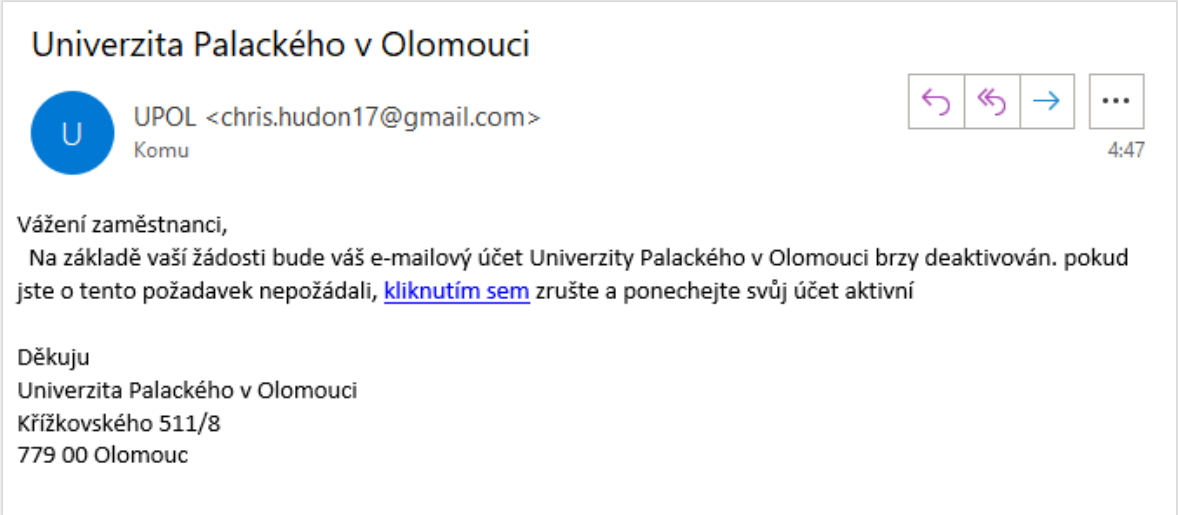
Leakware je varianta ransomwaru, který kombinuje proces šifrování souborů a současně únik dat, pokud nejsou splněny požadavky na zaplacení výkupného. Útočníci se často zaměřují na podniky nebo jednotlivce s klíčovými či citlivými informacemi, jako jsou osobní identifikační údaje, finanční informace nebo obchodní tajemství. Hrozba možného zveřejnění těchto informací přidává další rozměr naléhavosti k vyplacení výkupného, jelikož může vážně poškodit reputaci oběti a zároveň vést k vyšším právním rizikům. (Hermans, 2023)

## 3.2 Mechanismy infiltrace a šíření ransomwaru

### 3.2.1 Šíření ransomwaru

Ransomware se šíří různými způsoby, včetně známých phishingových e-mailů, které obsahují škodlivé odkazy nebo přílohy. (Cash, 2023) Bezpochyby platí, že kybernetičtí útočníci neustále nalézají nové přístupy a zranitelnosti, skrze které lze do systému proniknout. (Antal, 2023) Následuje popis několika z nejčastěji používaných metod:

- **Phishing** – Phishingové útoky představují formu kybernetických útoků, která se manifestuje skrze podvodné e-maily, textové zprávy, telefonní hovory či internetové stránky. Hlavním záměrem těchto útoků je manipulovat uživatele, aby vykonali určité akce, jako je stáhnutí škodlivého softwaru, sdílení důvěrných informací či osobních údajů. (What is phishing?, 2023) Jan Kolouch v rámci své literární práce specifikuje phishing jako: „*V širším slova smyslu se za phishing dá označit jakékoli podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem.*“ (Kolouch, 2016, s. 246). Kybernetičtí útočníci často systematicky provádějí rozsáhlý průzkum za účelem vytvoření rafinovaných e-mailových zpráv, které jsou schopny zaujmout a přesvědčit. Tyto e-maily často obsahují nebezpečné přílohy, jako jsou soubory ve formátu ZIP, PDF nebo tabulky, nebo obsahují odkazy směřující ke škodlivým webovým stránkám. (Cash, 2023)


Univerzita Palackého v Olomouci

U

UPOL <chris.hudon17@gmail.com>
Komu

4:47

Vážení zaměstnanci,
Na základě vaší žádosti bude váš e-mailový účet Univerzity Palackého v Olomouci brzy deaktivován. pokud jste o tento požadavek nepožádali, kliknutím sem zrušte a ponechejte svůj účet aktivní

Děkuju
Univerzita Palackého v Olomouci
Křížkovského 511/8
779 00 Olomouc

*Obrázek 4 Příklad phishingového e-mailu*

*https://www.facebook.com/itupol.cz/photos/a.905283816269634/2054435041354500/*

- **Protokol RDP (Remote Desktop Protocol)** – Protokol RDP představuje standard pro vzdálený přístup k zařízením, což zahrnuje schopnost spravovat uživatelská zařízení a řešit technické problémy. Paralelně s tím nabízí možnost k centralizaci zdrojů, například u stolních počítačů, které lze využívat pro náročné pracovní úkoly, spouštění aplikací, manipulaci s databázemi a dalšími prvky infrastruktury. Tímto mechanismem se optimalizuje rozdělení IT zdrojů a simultánně dochází ke zjednodušení procesů spojených se správou a údržbou zařízení. (Jak ochránit

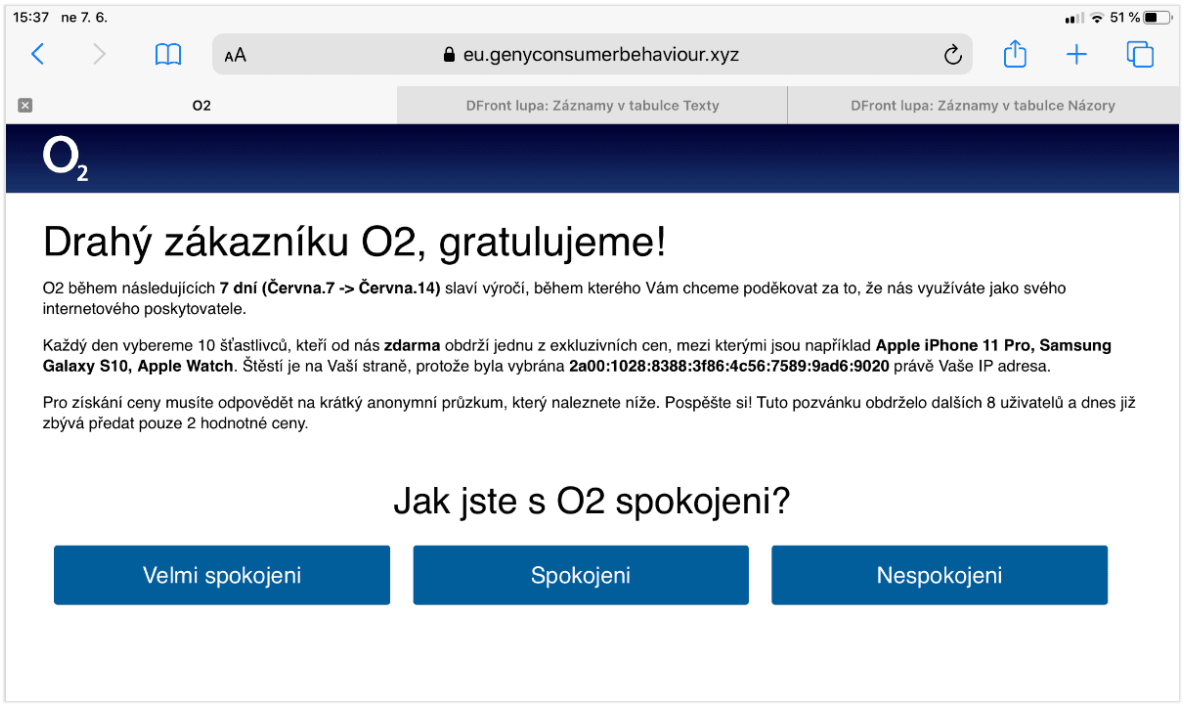
firmu před riziky spojenými s RDP?, 2023) Ransomware často zneužívá Remote Desktop Protocol (RDP) k provedení útoků na další síťové uzly. (Antal, 2023)

- **Poskytovatel spravovaných služeb (MSP) a vzdálené monitorování a správa (RMM)** – Poskytovatelé spravovaných služeb (MSP) nabízejí podnikům komplexní služby zaměřené na řízení a správu informačních technologií. Tyto služby usnadňují podnikům plnění úkolů spojených s IT oblastí. (Baker, 2023) Vzdálené monitorování a správa (RMM) představuje systematický proces, který umožňuje poskytovatelům spravovaných služeb (MSP) aktivně monitorovat a řídit koncová zařízení, sítě a počítačové systémy svých klientů na dálku. Tato metoda je proaktivní a umožňuje MSP reagovat na potenciální problémy ještě před tím, než by mohly způsobit větší komplikace. Termín RMM může být rovněž označován jako vzdálená správa IT nebo správa sítí. Útočníci zneužívají zranitelnosti v softwaru poskytovatelů spravovaných služeb (MSP), který se využívá pro vzdálené monitorování a správu (RMM), a tímto způsobem ohrožují integritu dat. Tato situace představuje významný bezpečnostní problém, neboť nejen citlivá data samotného poskytovatele jsou ohrožena, ale také mohou být narušeny data týkající se všech klientů tohoto podniku. Takovéto útoky umožňují útočníkům rovněž distribuovat ransomware napříč celou klientelou poskytovatelů spravovaných služeb (MSP), což vytváří silný nátlak na samotného poskytovatele, aby uvažoval o zaplacení výkupného. (Antal, 2023)

- **Malvertising** – Malvertising, známý též jako škodlivá reklama, reprezentuje relativně nový koncept, jenž využívá online reklamního prostoru k šíření ransomwaru. Většinou se jedná o začlenění škodlivých reklam do legitimních online reklamních sítí a webových stránek. Díky tomu, že reklamní obsah může být diskrétně zapracován do známých a důvěryhodných webů. Malvertising nabízí útočníkům optimální příležitost k rozšiřování svých útoků mezi uživateli, kteří by z bezpečnostních důvodů reklamy jinak neviděli – například díky firewallům a dalším bezpečnostním opatřením. (Din, 2022) Jakmile uživatel klikne na škodlivou reklamu, následuje průzkum zasaženého zařízení pomocí exploit kitu. (Cash, 2023) Exploit kity představují sady nástrojů, které byly vytvořeny za cílem provádět automatizované a tiché zneužívání identifikovaných zranitelností v počítačích obětí během jejich surfování na internetu. (What is an Exploit Kit?, 2023) Tyto sady nástrojů provádějí analýzu vašeho systému a shromažďují

informace o operačním systému, softwaru, prohlížeči a dalších relevantních údajích. Pokud exploit kit odhalí existenci nějaké zranitelnosti, pokusí se aktivně využít tuto nedostatečně zabezpečenou část a nainstalovat na váš počítač ransomware. (Cash, 2023)

*j*




*Obrázek 5 Příklad malvertisingu https://www.lupa.cz/aktuality/drahy-zakazniku-gratulujeme-reklamy-smerujici-na-podvodny-web-byly-i-v-siti-seznamu/*

- **Pirátský software** – Na internetu existuje nepřeberné množství pirátského softwaru, z nichž některý je obtížné rozeznat od legálních variant. Prostřednictvím těchto pirátských softwarů se často ransomware šíří. Zároveň když uživatel navštěvuje webové stránky, na nichž je pirátský software dostupný, výrazně se zvyšuje riziko, že se stane i obětí malvertisingu. (Baker, 2022) Uživatelé, kteří se uchylují k používání pirátského softwaru, se vystavují dalšímu nebezpečí tím, že nejsou schopni získávat nové aktualizace pro svůj software, včetně těch bezpečnostních. Absence těchto bezpečnostních aktualizací vytváří prostředí, v němž hrozí zvýšené nebezpečí využití existujících zranitelností, což také může vést k infikaci ransomwarem. (Cash, 2023)

- **Šíření sítí** – Při pohledu na několik raných verzí ransomwaru je patrné, že tyto varianty nebyly schopné se šířit po síti, na rozdíl od modernějších verzí. V

dnešní době jsou však varianty ransomwaru výrazně komplexnější a vybaveny mechanismy, které umožňují další šíření. Tato zdokonalení umožňují těmto variantám se šířit do dalších zařízení, jež jsou spojena se stejnou síťovou infrastrukturou. (Baker, 2022)

- **Přenosné počítače a disky USB** – Za účelem rozšíření ransomwaru se často využívají USB disky, neboť tyto zařízení jsou pohodlně přenosná a dá se je snadno připojit k různým počítačům. Notebooky se vzhledem k jejich častému využívání při pracovních úkolech a ukládání významného množství citlivých dat stávají zvlášť zranitelnými, kdy tyto zranitelnosti jsou výsledkem intenzivního používání právě přenosných zařízení. Po připojení do počítače se obsah uložený na disku USB automaticky spustí a spustí tak i potenciálně přítomný ransomware, který následně infikuje počítač. Tímto mechanismem má pak ransomware možnost se i šířit po celé síti a způsobit šifrování dat na všech zařízeních připojených k této síti. (Baker, 2022)

### 3.2.2 Mechanismus infiltrace cílového zařízení

Pro dosažení svých cílů musí ransomware nejprve úspěšně proniknout do cílového zařízení, což je zásadní krok pro jeho další rozvoj a působení. Pro tento účel využívá různé způsoby proniknutí do systému, jak bylo detailně popsáno v předchozí kapitole. Důraz je kladen na fakt, že tato variabilita metod neustále rozvíjí, aby byla schopna obejít různá ochranná opatření. Ačkoliv detaily šíření jednotlivých variant ransomwaru mohou být odlišné, všechny tyto varianty absolvují stejný základní postup, který se skládá z tří fází:

- **Fáze 1. infekce a distribuce –** Ransomware proniká do cílového zařízení skrze jednu z několika možných cest. Jakmile se dostane do systému, nainstaluje aplikaci pro vzdálený přístup, což útočníkům umožňuje získat kontrolu nad daným systémem. Cílem útočníků v této fázi není okamžité zašifrování dat, ale prvním krokem je získání nejvyššího oprávnění, za účelem nemožnosti přerušení procesu infiltrace. Následně se v systému ransomware pohybuje, provádí průzkum a hledá důležité údaje. (Poremba, 2023) Ransomware provede analýzu sítě a identifikuje zařízení, do kterých by mohl expandovat. V tomto procesu se zároveň snaží získat přístupové údaje k uživatelským účtům, aby je mohl následně

využít k dalšímu prolomení a infikaci dalších zařízení. Tímto způsobem se ransomware pokouší maximalizovat svou schopnost šíření a infikovat co největší počet zařízení v rámci sítě. (Merta, 2020)

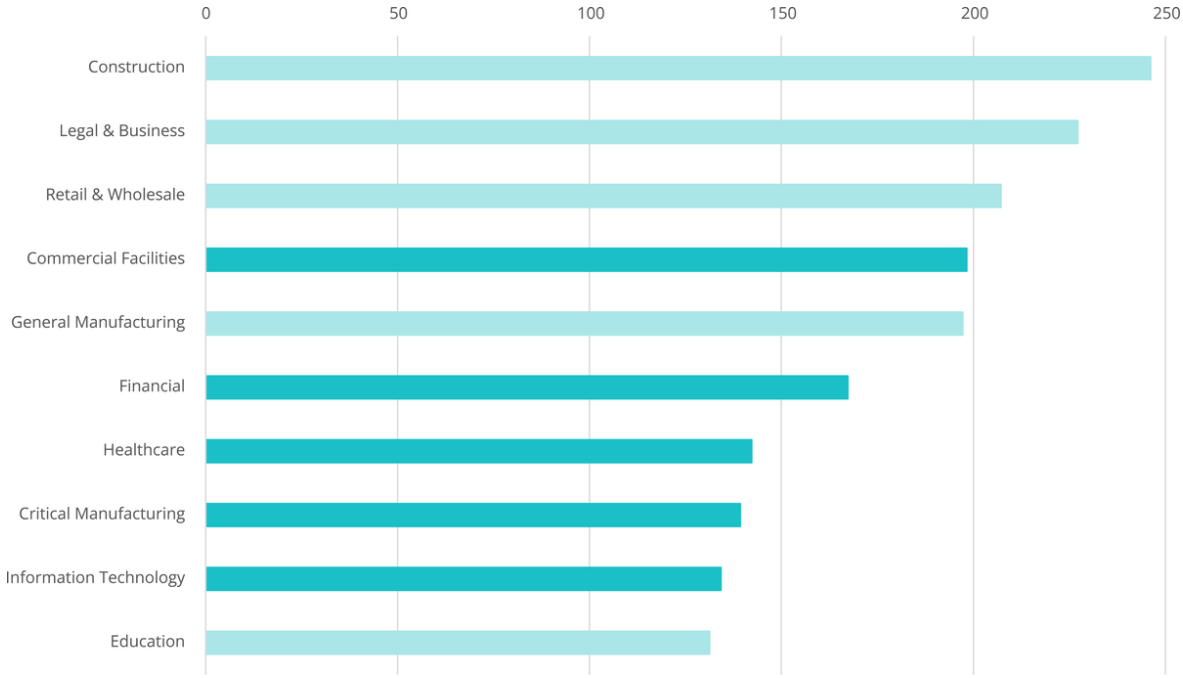
- **Fáze 2. zašifrování dat** – Jakmile ransomware získá přístup do systému, zahájí proces šifrování dat. Tato operace se provádí skrze integrovanou šifrovací funkci v operačním systému. Proces samotný zahrnuje přístup k datům, které jsou poté zašifrovány pomocí klíče, jenž je pod kontrolou útočníka. Po úspěšném zašifrování dat dochází k nahrazení původních nezašifrovaných verzí za nové, zašifrované kopie. Při výběru souborů k šifrování jsou většinou varianty ransomwaru obezřetné, aby udržely stabilitu systému. Některé varianty dokonce podniknou kroky směřující ke smazání záloh, což má za cíl ztížit možnost obnovy dat bez dešifrovacího klíče. Tímto způsobem ransomware maximalizuje svou moc nad daty a zvyšuje tlak na oběť k zaplacení výkupného. (What is Ransomware?, 2023)
- **Fáze 3. vyžadování výkupného –** Po dokončení procesu šifrování souborů se ransomware připravuje na požadování výkupného. Různé varianty ransomwaru používají různé metody, jak tento požadavek oběti sdělí. Často dochází k zobrazení výzvy k zaplacení výkupného prostřednictvím změny pozadí displeje nebo umístění textových souborů s instrukcemi do zašifrovaných adresářů. Tyto instrukce obvykle žádají oběť o zaplacení určité částky v kryptoměně výměnou za klíč k dešifrování dat. Po zaplacení výkupného může útočník poskytnout kopii soukromého klíče, který slouží k ochraně symetrického šifrovacího klíče, nebo přímo kopii samotného symetrického šifrovacího klíče. Tento klíč může být následně použit v dešifrovacím programu (také poskytnutém útočníkem), který umožní obnovit původní stav souborů a obnovit přístup k datům. (What is Ransomware?, 2023)

## 3.3 Hlavní cíle a motivace ransomwarových útoků

Zatímco někteří kybernetičtí útočníci využívají ransomware k narušení provozu, mnozí se rozhodnou tímto způsobem vymáhat finanční prostředky od konkrétních osob či subjektů. Pro dosažení tohoto cíle musí útočníci nejprve identifikovat své potenciální oběti a zde se

uplatňuje proces výběru. Útočníci pečlivě vybírají své cíle a následně na základě různých faktorů, jako jsou například úroveň zranitelnosti, důležitost cíle a jeho schopnost zaplatit, určují strategii, jakým způsobem bude cíl napaden. (Unveiling the Psychology Behind Ransomware Attacks and How to Avoid Them, 2023) Společným rysem mnoha cílových odvětví, jež lákají útočníky ransomwaru, spočívá v jejich přístupu k velkému množství citlivých dat. Tyto data nesou významnou hodnotu a často jde o informace, jež by měly být uchovávány s ohledem na bezpečnost a zachování důvěrnosti. Tato skutečnost výrazně zvyšuje pravděpodobnost, že subjekty budou ochotny zaplatit výkupné výměnou za obnovení přístupu. (Livingston, 2022)

Následný graf, který byl sestaven analytiky z Outpost24 KrakenLabs, názorně demonstruje, jaká odvětví byla nejvíce negativně ovlivněna útoky ransomwaru. Z této vizualizace je patrné, že sektory, které byly zasaženy nejvíce, zahrnují komerční zařízení, finanční sektor, stavebnictví, právní a obchodní sféru a také maloobchod a velkoobchod. (kritická odvětví jsou vyznačena tmavší modrou barvou) (Casas, 2023)



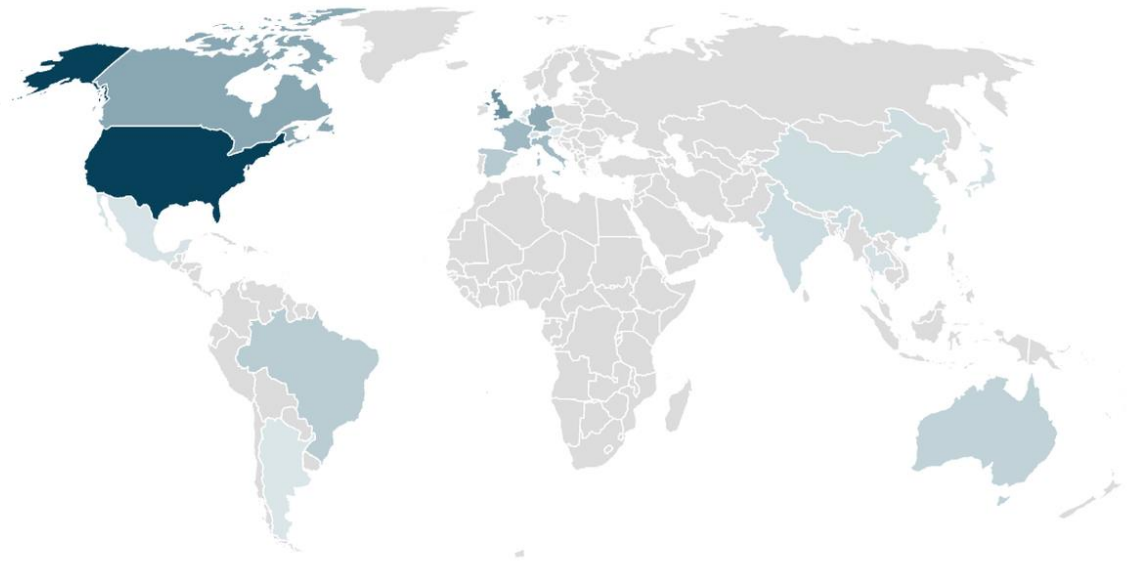

*Obrázek 6 Nejčastější zasažená odvětví https://outpost24.com/blog/ransomware-report-2023-targets-motives-and-trends/*

Útočníci také upřednostňují cílové odvětví, která jsou bohatší na cenný majetek a disponují rozsáhlejší zákaznickou základnou. Tato preference se odráží zejména ve finančním sektoru a sektoru komerčních zařízení. Podniky působící v těchto oblastech mají také tendenci mít vyšší počet zaměstnanců a spoléhají na služby třetích stran, což rozšiřuje spektrum

potenciálních vektorů útoku tj. způsobů, jakými může být zranitelnost zneužita (Čermák, 2023).

Analýza prováděná společností KrakenLabs také ukázala, že některé podniky jsou opakovaně terčem ransomwarových útoků ať už od stejných nebo různých skupin útočníků. Tato opakující se zranitelnost může být způsobena několika faktory, včetně nedostatečné reflexe a poučení se z předchozích útoků, nedostatečné segmentace sítě, což usnadňuje pohyb útočníků, a atraktivnosti cíle, kdy určité podniky lákají útočníky kvůli citlivým datům nebo schopnosti platit výkupné.

Při zkoumání geografického rozložení cílů ransomwarových útoků lze konstatovat, že jsou zejména zaměřeny na západní země. Ze 101 zemí, které byly zahrnuty v analýze, tvoří přibližně 42 % obětí Spojené státy a zhruba 28 % z tohoto celkového počtu pochází z různých evropských zemí. (Casas, 2023)



*Obrázek 7 Geologické rozložení útoků (tmavší modrá znamená vyšší počet) https://outpost24.com/blog/ransomware-report-2023-targets-motives-and-trends/*

Pro kybernetické útočníky bývá důležitá hodnota dat uložených v cílovém podniku. Jejich schopnost přistoupit k ukradení nebo zašifrování extrémně citlivých informací zvyšuje pravděpodobnost, že oběti budou ochotny uhradit vyšší výkupné. Dokonce i v případě, že by se jim nepodařilo výkupné získat, mají tato citlivá data stále vyšší cenu na dark webu, kde najdou potenciální zájemce.

Jak již bylo zmíněno útočníci obvykle selektují své cíle s ohledem na jejich schopnost uhradit vysokou částku výkupného. V tomto kontextu byl proveden průzkum od společnosti

Verizon v roce 2019 s názvem "Data Breach and Investigation Report," který prokázal, že zábavní průmysl, který se často zabývá velkorozpočtovými projekty, zaznamenal druhý nejvyšší počet kybernetických útoků. Úspěšný ransomwarový útok na finančně silné podniky může znamenat podstatně vyšší finanční zisky pro útočníky a přitáhnout jejich pozornost.

Je třeba si uvědomit, že motivace za ransomwarovými útoky není omezena pouze na finanční zisk. Existuje také kategorie kyberzločinců, kde jejich motivací je dosáhnout maximálního poškození dat. Tyto útoky mohou být motivovány ideologickými důvody nebo touhou po vyvolání chaosu a destabilizaci. Útočníci tak hledají cíle s vysokým potenciálem pro devastaci, bez ohledu na finanční výhody. (Livingston, 2022)

## 3.4 Prevence ransomwarových útoků

### 3.4.1 Identifikace klíčových bezpečnostních zranitelností

Rozpoznání zranitelností je klíčovým prvkem kybernetické bezpečnosti, který podnikům umožňuje identifikovat potenciální slabiny v jejich IT prostředí a systémech. Tento proces je rozsáhlý a zahrnuje systematické zkoumání technických systémů, infrastruktury a softwarových aplikací podniku. Cílem je identifikovat potenciálně rizikové oblasti, které by mohly být zneužity. To zahrnuje jak zranitelnosti ve vlastních systémech podniku, tak i ve spojení s dodavatelským řetězcem a obchodními partnery. (Ward Security Consulting Group, 2023)

K identifikaci zranitelností lze využít několik postupů. Například penetrační testy jsou nástrojem, který podnikům umožňuje simulovat útoky a ověřit, jakým způsobem by se systém choval při skutečném útoku. Monitorování integrity souborů je též klíčové pro rychlou detekci neoprávněného přístupu a narušení systému. Tímto způsobem lze rychle reagovat na bezpečnostní incidenty a minimalizovat jejich dopad. (Yacono, 2023)

Existuje mnoho strategií a opatření, která lze implementovat pro ochranu před ransomwarem. Vzhledem k neustálému vývoji kybernetických hrozeb je kritické dodržovat základní principy kybernetické bezpečnosti a udržovat proaktivní postoj. Tímto způsobem lze minimalizovat riziko nákazy ransomwarem jak pro jednotlivce, tak i pro podniky. (Chin, 2023)

### 3.4.2 Aktualizace softwaru

Software patches, často označované jako záplaty, představují aktualizace softwaru a operačního systému, jejichž hlavním účelem je eliminovat bezpečnostní chyby ve specifickém softwarovém produktu. Vývojáři softwaru se obvykle snaží vydávat tyto aktualizace pravidelně, aby tak zajišťovali bezpečnost svých uživatelů. Tyto aktualizace jsou obvykle dostupné prostřednictvím oficiálních webových stránek daného výrobce nebo přímo v aplikaci. (Understanding Patches and Software Updates, 2023) Například Microsoft rozděluje své aktualizace Windows do dvou základních kategorií, a to důležitých a volitelných. Mezi aktualizace označené jako důležité spadají zejména ty, které se týkají bezpečnosti. (Petrowski, 2014)

Je třeba zajistit, aby všechny operační systémy, aplikace a softwarové produkty byly pravidelně aktualizovány, a to nejlépe ihned po vydání. Tyto aktualizace nejenže zvyšují efektivitu systému, ale také likvidují potenciální bezpečnostní mezery, které by mohly být zneužity kybernetickými útočníky. (7 Steps to Help Prevent & Limit the Impact of Ransomware, 2023)

Doporučuje se i aktivace automatických aktualizací pro rychlý přístup k nejnovějším bezpečnostním aktualizacím. Hlavním důvodem jsou incidenty, které vznikly v důsledku zanedbaných aktualizací softwaru, kdy se ukázalo, že podniky, které tyto aktualizace neprováděly, jsou výrazně náchylnější k útokům ransomwarem. (Ransomware protection: How to keep your data safe in 2023, 2023)

### 3.4.3 Efektivní zálohování dat

Při implementaci efektivního zálohování s ohledem na odolnost proti ransomwaru je klíčové si uvědomit, že útočníci se často zaměřují na online zálohy ještě před tím, než ransomware spustí v cílovém prostředí. Proto je nejspolehlivějším způsobem ochrany dat před útokem ransomwaru udržování off-line záloh. (Baker, 2023)

Je nutné zálohy provádět pravidelně a pečlivě ověřovat jejich integritu. Pokud dojde k útoku ransomwarem, lze pomocí těchto off-line záloh obnovit svůj systém do předchozího stavu. (Protecting Against Ransomware, 2019) Off-line zálohy by se měly udržovat buďto na externím pevném disku nebo cloudovém úložišti. Zálohování klíčových dat by mělo být prováděno alespoň jednou denně.

Jednou z doporučených metod zálohování je tzv. pravidlo 3-2-1. To znamená uchovávání tří samostatných kopií dat na dvou různých typech úložišť a jednu kopii uchovávat off-line. Navíc lze do tohoto procesu začlenit ještě další krok, a to ukládání jedné kopie na nesmazatelný a nezměnitelný server v cloudovém úložišti.

Při vytváření efektivního zálohování je potřeba se řídit několika pravidly:

- Off-line zálohy by měly být zcela odděleny od zbytku infrastruktury
- Přístup k těmto zálohám by měla být řízen pomocí přísných seznamů řízení přístupu (ACL) a ověřování by mělo probíhat pomocí více faktorového ověřování
- Správci by se měli vyvarovat opakovaného používání hesel k účtům
- Připojení off-line záloh k síti, by mělo nastat jen při krizové situaci, do které spadá ransomwarový útok (Chin, 2023)

### 3.4.4 Plán reakce na incidenty a rozšíření povědomí o rizicích ransomwaru

Vzhledem k tomu, že koncoví uživatelé nebo zaměstnanci představují hlavní bod vstupu pro kybernetické útoky, je třeba zajistit, aby tito uživatelé měli základní znalosti v oblasti kybernetické bezpečnosti a ohledně ransomwaru samotného. Díky těmto znalostem mohou výrazně snížit riziko útoků na samém počátku, a dokonce jim předcházet. Některé základní principy, které by měly být součástí povědomí o kybernetické bezpečnosti, zahrnují následující:

- Bezpečné surfování po internetu
- Vytváření silných a bezpečných hesel
- Používání bezpečných sítí VPN (žádné veřejné Wi-Fi)
- Rozpoznávání podezřelých e-mailů nebo příloh
- Udržování aktualizovaných systémů a softwaru (Chin, 2023)

Plán reakce na incidenty představuje užitečný nástroj pro usnadnění rychlých rozhodnutí. Zároveň vymezuje pravomoce bezpečnostního týmu pro přijímání rozhodujících opatření, jako je například odstavení kritických podnikových služeb, v případě akutního hrozícího ransomwarového útoku. (Baker, 2023) Plán by měl jasně stanovit postupy pro komunikaci během incidentu a obsahovat seznam kontaktů na interní týmy, externí partnery a regulační orgány, kteří by měli být informováni. Tato připravenost a strukturovaný přístup

jsou klíčové pro efektivní reakci na ransomware útoky a minimalizaci jejich dopadů. (7 Steps to Help Prevent & Limit the Impact of Ransomware, 2023)

### 3.4.5 Zvýšení zabezpečení e-mailu

Phishingové útoky prostřednictvím e-mailů představují historicky nejčastější způsob infikování systémů. (Chin, 2023) Tyto podezřelé e-maily často obsahují škodlivý odkaz nebo URL adresu, která jakmile je otevřena na počítači příjemce, spustí instalaci ransomwaru. Pro ochranu proti takovýmto útokům se doporučuje nasadit bezpečnostní řešení pro e-mailovou komunikaci, která aktivně provádí analýzu, filtrování URL adres a provádí izolaci (sandboxování) potenciálně rizikových příloh. Aby se těmto hrozbám zabránilo ještě před tím, než uživatelé vůbec interagují s e-mailem, je užitečné používat automatizované přesunutí podezřelých e-mailů do karantény. Lze také implementovat omezení příjmu určitých typů příloh, jako jsou například archivy ve formátu ZIP, spustitelné soubory, skripty JavaScript nebo instalátory systému Windows chráněné heslem. Kromě toho může být užitečné označovat e-maily, které mají externího odesílatele, značkou "[Externí]" a umísťovat varovnou zprávu v horní části e-mailu, což pomůže uživatelům lépe rozpoznat potenciální rizika při práci s těmito e-maily. (Baker, 2023)

Lze přijmout i další preventivní opatření prostřednictvím následujících praktik:

- Zdrženlivost při interakci s přílohami, soubory nebo odkazy, které pocházejí z neznámých zdrojů nebo nejsou autorizovány
- Pravidelná aktualizace emailových aplikací pro zachování bezpečnosti a funkčnosti
- Sender Policy Framework (SPF) - metoda e-mailové autentizace, která identifikuje specifické e-mailové servery, jež jsou oprávněny zasílat odchozí elektronickou poštu.
- DomainKeys Identified Mail (DKIM) - nabízí šifrovací klíč a digitální podpis pro autentizaci e-mailových zpráv a zajištění integrity dat, což slouží k verifikaci, že e-mail nebyl padělán, zfalšován nebo modifikován
- Domain Message Authentication Reporting & Conformance (DMARC) - autentizace e-mailových zpráv prostřednictvím porovnání protokolů SPF a DKIM. (Chin, 2023)

### 3.4.6 Architektura nulové důvěryhodnosti

Architektura nulové důvěryhodnosti (Zero Trust Architecture, ZTA) představuje bezpečnostní koncept, který se stal standardem v oblasti kybernetické bezpečnosti. Jedná se o soubor bezpečnostních zásad a postupů, které představují přístup k zabezpečení IT prostředí. Jedním z hlavních principů nulové důvěryhodnosti je posun od tradičního modelu, kde se služby a uživatelé implicitně považují za důvěryhodné, směrem k nastavení, kde výchozím předpokladem je nedůvěra. Jinými slovy, žádný uživatel ani služba není automaticky považován za důvěryhodný, což klade zvýšený důraz na prevenci neoprávněného přístupu k důležitým datům a službám. (Sandbu, 2023) Při každé žádosti o přístup k určitým systémům se zavádí důkladný proces kontroly. Tento proces zahrnuje plné ověření identity žadatele, což zahrnuje například kontrolu uživatelských údajů a hesel. Následuje autorizační fáze, kdy se prověřuje, zda má žadatel dostatečná oprávnění k žádanému přístupu. Aby byla zajištěna bezpečnost datové komunikace, probíhá následně šifrování komunikace mezi žadatelem a systémem. Teprve po úspěšném provedení těchto kroků může být žádost o přístup schválena a realizována. (Osvojte si proaktivní zabezpečení s modelem nulové důvěry (Zero Trust), 2023) Mnoho starších systémů ale stále spoléhá na implicitní důvěru, což představuje významné bezpečnostní riziko. (Sandbu, 2023)

Architektura s nulovou důvěryhodností je koncipována a implementována s následujícími principy:

- Veškerá komunikace je zabezpečena bez ohledu na umístění sítě
- Přístup k jednotlivým podnikovým prostředkům je udělován na základě jednotlivých relací
- Přístup ke zdrojům je určen dynamickými zásadami – včetně pozorovatelného stavu identity klienta, aplikace/služby a požadujícího prostředku
- Podnik sleduje a měří integritu a bezpečnostní stav všech vlastněných a přidružených prostředků
- Veškeré ověřování a autorizace prostředků jsou dynamické a přísně vynucované před povolením přístupu
- Podnik shromažďuje co nejvíce informací o aktuálním stavu aktiv, síťové infrastruktury a komunikace a využívá je ke zlepšení svého zabezpečení (Rose, 2020)

### 3.4.7 Zabezpečení koncových bodů

Rozšířením podnikatelských aktivit a nárůstem počtu koncových uživatelů, jako jsou notebooky, chytré telefony, servery atd., se zvyšuje počet koncových bodů, které je třeba zabezpečit. (Chin, 2023) Správná konfigurace koncových bodů může výrazně snížit rizika a eliminovat potenciální bezpečnostní mezery, které mohou vzniknout v důsledku výchozích nastavení. (7 Steps to Help Prevent & Limit the Impact of Ransomware, 2023) Jako příklad lze uvést nastavení antivirového softwaru, který vykazuje schopnost detekce a blokování škodlivých souborů a zároveň upozorňuje uživatele na potenciálně rizikovou návštěvu podezřelých webových stránek (Jones, 2022). Podniky by měly zvážit i implementaci platforem pro ochranu koncových bodů (Endpoint Protection Platforms, EPP) nebo detekci a ochranu koncových bodů (Endpoint Detection and Response, EDR) pro všechny uživatele v síti. EDR je pokročilejší než EPP a zaměřuje se na reakci a potlačení hrozeb, které mohou proniknout do sítě.

Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) představují klíčové komponenty pro celkovou kybernetickou bezpečnost. Tyto platformy spojují komplexní soubor obranných mechanismů, které zahrnují klasickou ochranu proti virům, šifrování citlivých dat, systémy pro prevenci ztráty dat a také schopnost detekovat a rychle reagovat na potenciální proniknutí do systému. Dále poskytují robustní bezpečnostní opatření pro zabezpečení webového prohlížeče a umožňují sledovat události v reálném čase, což zahrnuje okamžitá bezpečnostní upozornění a oznámení, což umožňuje rychlou reakci na hrozby. (Chin, 2023)

## 3.5 Principy detekce ransomwaru

Principem detekce ransomwaru je identifikovat neobvyklou aktivitu a okamžitě upozornit uživatele na možnou hrozbu. Díky tomu mají uživatelé možnost zastavit šíření viru před tím, než dojde k zašifrování důležitých nebo citlivých souborů. (What is Ransomware Detection?, 2023) Detekce ransomwaru využívá sofistikované metody, které zahrnují automatizaci a analýzu škodlivého softwaru pro odhalení potenciálně nebezpečných souborů v rané fázi infekce. Je třeba poznamenat, že nalezení těchto souborů není vždy snadným úkolem, neboť útočníci často používají různé techniky pro skrytí ransomwaru v legitimním softwaru, například využití skriptů jako PowerShell, VBScript, Mimikatz a PsExec, což zvyšuje náročnost jeho identifikace. (Johnson, 2023)

Obvykle se používají čtyři primární metody pro detekci ransomwaru – metoda založená na charakteristických vlastnostech, metoda založená na chování, metoda založená na neobvyklém síťovém provozu a metoda heuristické detekce. Tyto charakteristiky říkají, co ransomware dělá a jak ho rozpoznat.

Metoda detekce na základě charakteristických vlastností provádí analýzu vzorku ransomwaru s použitím hash hodnoty a porovnává ji se známými charakteristikami. Tato metoda umožňuje rychlou statickou analýzu souborů v systému. Bezpečnostní platformy a antivirový software analyzují data z těchto spustitelných souborů a vytvářejí pravděpodobnostní hodnocení, zda se jedná o ransomware nebo o legitimní spustitelný soubor. Většina antivirového softwaru provádí tuto analýzu během procesu skenování souborů na případné viry. (Johnson, 2023)

Ransomware především vykazuje atypické chování tím, že systematicky provádí zásahy do desítek souborů, které následně nahrazuje jejich zašifrovanými variantami. Metody detekce ransomwaru založené na analýze chování jsou schopny sledovat tuto neobvyklou aktivitu a včas upozornit uživatele. Tento druh detekčního přístupu může efektivně přispět k ochraně uživatelů nejen před samotným ransomwarem, ale také před dalšími běžnými formami kybernetických útoků. (What is Ransomware Detection?, 2023)

Ransomware lze identifikovat i prostřednictvím analýzy síťového provozu, což zahrnuje podrobné zkoumání datových toků mezi koncovými body. Tato metoda se zaměřuje na sledování objemů přenášených dat a odhalování jakýchkoli anomálií, které by mohly poukazovat na potenciální útok ransomwarem. V případě zaznamenání podezřelé aktivity může být systém rychle izolován. Jednou z výhod této metody je schopnost odvracet ransomwarové útoky bez nutnosti detailní znalosti specifických charakteristik těchto útoků. Je však třeba poznamenat, že tato metoda má tendenci generovat falešně pozitivní výsledky, což může vést k blokování legitimního provozu, snížení produktivity a způsobit například nákladné výpadky služeb. (Robinson, 2023)

Zmiňovaná detekční metoda, která využívá charakteristické vlastnosti a analýzu chování, nese také určité nedostatky. (Bazrafshan, 2013) Problém u metody založené na charakteristických vlastnostech spočívá v extrakci charakteristik a v tom, že tyto rysy lze snadno obejít. (Ye, 2008) V reakci na tyto problémy byly vyvinuty heuristické metody pro detekci ransomwaru, jež se snaží tyto nedostatky překonat. Heuristické přístupy k detekci malwaru zahrnují techniky strojového učení, které slouží k analýze chování spustitelných souborů. (Bazrafshan, 2013) Rozpoznávání založené na heuristice má potenciál poskytovat

ochranu i proti novým a neznámým hrozbám, ale je obvykle časově náročné a stále ještě nedokáže odhalit tyto hrozby se stoprocentní úspěšností. (Ye, 2008)

### 3.5.1 Automatizovaná detekce ransomwaru

Moderní postupy pro detekci ransomwaru jsou zaměřeny především na pečlivé sledování chování počítačového systému na úrovni jeho souborového systému. V rámci automatizovaných přístupů k detekci ransomwaru se rozlišují dvě hlavní skupiny metod – ty, které využívají technologie umělé inteligence, a ty, které na umělé inteligenci založeny nejsou. Přístupy založené na umělé inteligenci (artificial intelligence, AI) obvykle využívají metody strojového učení (machine learning), hlubokého učení (deep learning) a umělých neuronových sítí (artificial neural network). Existují také hybridní metody, které kombinují více technik. Na druhé straně metody, které nevyužívají umělou inteligenci, se zaměřují na analýzu síťového provozu a kontrolu datových paketů. Jednou z klíčových výhod automatizovaných přístupů je schopnost odhalit, zablokovat a obnovit systém po ransomwarovém útoku bez potřeby lidského zásahu. Tyto nástroje se vyznačují vysokou přesností a spolehlivostí při detekci, prevenci a následném zotavení po útoku ransomwarem.

Detekce založená na strojovém učení představuje pokročilý přístup, kdy je strojový model vyškolený pro rozpoznávání ransomwaru na základě jeho charakteristického chování a vlastností. Tento postup vyžaduje shromáždění rozsáhlého souboru dat obsahujícího neškodné a škodlivé vzorky, extrakci relevantních atributů z těchto vzorků a následné vyškolení strojového modelu. Tento model následně na základě svého naučeného chování klasifikuje nové vzorky jako buď bezpečné nebo potenciálně škodlivé.

Techniky hlubokého učení byly vyvinuty jako nástroje pro překonání omezení, která tradiční metody detekce ransomwaru přinášejí, a to s cílem zvýšit přesnost a spolehlivost ve věci identifikace ransomwarových hrozeb. Je však třeba poznamenat, že pro trénink těchto hlubokých učení je nezbytné dostatečné množství dat. To může být omezením pro jejich použití v situacích s omezeným objemem datových souborů, zejména v případě malých souborů nebo datových sad s nízkým objemem. Dalším významným faktorem je potřeba vysokého výpočetního výkonu pro účinný provoz těchto algoritmů. Zároveň mohou nastat obtíže s adaptací těchto algoritmů na reálná data, což vyžaduje další úsilí a odbornost v oblasti hlubokého učení.

Přístupy založené na umělých neuronových sítích představují perspektivní metodu pro detekci různorodých forem ransomwaru. Umělé neuronové sítě nabízejí významnou

flexibilitu a adaptabilitu, což je klíčové pro úspěšné zvládnutí nových podob ransomwaru a odhalení útoků, které dosud nebyly známé, tzv. útoků nultého dne. Jejich všestrannost umožňuje efektivní identifikaci různých projevů ransomwaru a rychlou adaptaci na nové hrozby. Nicméně, tato metoda je náročná na výpočetní výkon a může být citlivá na dostupnost aktuálních dat. Dále, kvůli povaze umělých neuronových sítí jako takzvaných "black-box" modelů, může být obtížné pro lidské analytiky sledovat a pochopit vnitřní mechanismy těchto sítí a identifikovat anomálie v procesu detekce ransomwaru.

K identifikaci ransomwaru mohou být využity i techniky, které nevyužívají umělou inteligenci, jako je analýza provozu a kontrola síťových paketů. Jedním z efektivních algoritmů, který se používá pro detekci ransomwaru, je metoda detekce anomálií. Tato metoda provádí analýzu síťového provozu a identifikuje vzory, které se odchylují od normálního chování. Například neobvyklé vzory, jako je rychlý nárůst šifrování souborů nebo vysoký počet odchozích síťových spojení směřujících k podezřelým IP adresám, mohou být indikátorem ransomwarové aktivity. Algoritmy pro detekci anomálií jsou schopny rychle identifikovat takové odchylky od běžného síťového provozu a tím upozornit bezpečnostní týmy na potenciální hrozby spojené s ransomwarem. (Raizza, 2023)

### 3.5.2 Manuální detekce ransomwaru

Manuální identifikace ransomwaru zahrnuje systematický proces, kde odborník na kybernetickou bezpečnost analyzuje a zasahuje do systému ručně, místo použití automatizovaných nástrojů. Tento přístup vyžaduje důkladnou analýzu systémových záznamů, síťového provozu a dalších indikátorů kompromitace s cílem rozpoznat charakteristické vzory a chování, které jsou spojeny s ransomwarem. I když ruční detekce může být náročná na čas a lidské zdroje, může být užitečná jako doplňkový nástroj k automatizovaným metodám detekce, protože může pomoci odhalit nové nebo neznámé varianty ransomwaru, které by automatizované systémy mohly přehlédnout.

I přes svou efektivitu vykazuje ruční detekce ransomwaru několik omezení. Tento postup může být časově náročný a vyžaduje vysokou kvalifikaci pracovníků, kteří provádějí analýzu systémových protokolů a monitorují síťový provoz. Kromě toho, ruční detekce nemusí být optimální pro velké podniky nebo rozsáhlé sítě, kde by se mohly ukázat účinnější automatizované metody detekce.

Metoda pro detekci ransomwaru, která se u tohoto typu detekce často uplatňuje, je známá jako skenování. Tato metoda vyžaduje přítomnost vyškoleného odborníka, který

provádí důkladnou manuální analýzu jednotlivých souborů a systémů s cílem identifikovat potenciální známky ransomwarové aktivity, jako jsou zašifrované soubory nebo anomální síťový provoz. Manuální skenování má své výhody, ale současně nese riziko falešných pozitivních výsledků, což může negativně ovlivnit normální provoz systému. Je důležité, aby pracovníci provádějící toto skenování byli dostatečně školeni a měli hluboké pochopení ransomwarových hrozeb, aby byli schopni rozpoznat reálné hrozby od benigních anomálií. (Raizza, 2023)

## 3.6 Detekce pomocí detekčních programů

### 3.6.1 Antivirové programy

Antivirový software (antivirový program) je bezpečnostní program určený k prevenci, detekci, vyhledávání a odstraňování virů a jiných typů škodlivého softwaru z počítačů, sítí a dalších zařízení. Antivirový program, který se obvykle instaluje do počítače jako proaktivní přístup ke kybernetické bezpečnosti, může pomoci zmírnit různé kybernetické hrozby. (Rosencrance, 2024)

Antivirový software kontinuálně provádí skenování aplikací a souborů a následně analyzuje tato data na základě databáze známých variant virů. Pro detekci virů využívají antivirové programy obvykle tři metody:

- **Skenování** – skenování spočívá v porovnání analyzovaných dat s databází známých charakteristických vlastností nebo znaků, které jsou pro viry typické. Tato metoda je základní a široce používaná. Nicméně útočníci mohou efektivně tuto detekci obcházet prostřednictvím úprav kódu, jeho šifrování či modifikací charakteristik, což snižuje účinnost tohoto typu detekce. Další omezení spočívá v tom, že tato metoda identifikuje pouze viry, které mají již známé charakteristiky, což znamená, že nové typy virů mohou být přehlédnuty.
- **Generická detekce** – za účelem překonání omezení detekce založené na skenování, se generická detekce zaměřuje na identifikaci společných charakteristik populárních typů virů. Generická detekce může být rozsáhlá – jako například skenování známých kódů exploitů – nebo specifická; například skenování konkrétních "packerů"(nástroj, který zabalí dohromady spustitelný kód souboru, data a obsahuje také kód pro rozbalení programu). (Poonia, 2022)

- **Heuristická detekce** – Jedná se o sofistikovanější metodu detekce, která využívá identifikaci podezřelých vzorců chování nebo struktur v souborech. Vývojáři antivirových programů vypracovávají sadu pravidel určených k detekci virů na základě odchylek od normálního chování a následně podrobují segmenty kódu testům podle těchto pravidel, s cílem identifikovat, zda se jedná o virus či nikoliv. (Mixon, 2021)

### 3.6.2 Anti-ransomwarové programy

Anti-Ransomware software je specializovaný software proti boji s ransomwarem, který detekuje a blokuje škodlivý software ještě předtím, než může zašifrovat data uživatele. Poskytuje také další bezpečnostní opatření, včetně zálohování dat, aby se minimalizovala možnost ztráty dat v případě útoku. Tento software je k dispozici jako samostatný produkt nebo součást komplexních bezpečnostních řešení.

Mnohé programy provádějí detekci škodlivého softwaru na základě analýzy databáze známých charakteristik, obdobně jako antivirové programy. V případě identifikace souboru odpovídajícího daným definicím je označen jako potenciální hrozba. Tento přístup je účinný při detekci známých variant ransomwaru, nicméně vyžaduje pravidelné aktualizace pro zachycení nově vytvořených ransomwarových hrozeb a minimalizaci rizika jejich přehlédnutí.

Dalším způsobem detekce škodlivého softwaru, využívaným též antivirovými programy, je heuristická detekce. Tato metoda představuje alternativu ke statickému skenování databází a umožňuje anti-ransomwarovým programům identifikovat i potenciální hrozby, které nebyly dosud známy. Heuristika provádí analýzu chování a charakteristik podezřelých souborů s cílem detekovat škodlivý software, aniž by se spoléhala na porovnání s konkrétním seznamem známých škodlivých kódů.

Třetí metodou, jíž anti-ransomwarový software detekuje škodlivý kód, je spouštění potenciálně škodlivého programu v tzv. sandboxu, což představuje izolovaný prostor v operačním systému. V tomto prostředí je potenciálně škodlivý software mylně veden k přesvědčení, že má neomezený přístup k systému, avšak ve skutečnosti běží v izolovaném kontejneru, kde je sledováno jeho chování. Pokud se projeví jakékoli indikace škodlivého chování, anti-ransomwarový program okamžitě zasáhne a ukončí běh programu. V případě, že program nevykazuje žádné nebezpečné chování, je mu povoleno běžet mimo sandbox.

Po detekci škodlivého softwaru v systému je nezbytné provést jeho odstranění. Ačkoliv většina hrozeb může být odstraněna anti-ransomwarovým programem okamžitě po

identifikaci, některé varianty škodlivého softwaru jsou navrženy tak, aby po svém odstranění způsobily další škody na cílovém zařízení. V případě podezření, že se jedná o takový případ, program obvykle izoluje soubor do karantény v bezpečné oblasti úložiště počítače. Tato izolace škodlivého souboru v karanténě brání jeho aktivaci a umožňuje následné manuální odstranění bez rizika poškození systému. (Zamora, 2015)

## 3.7 Obnova dat po ransomwarovém útoku

Jak zdůraznil Král ve své knize, zaplacení výkupného není doporučeným postupem a neposkytuje záruku na obnovení dat. Podle průzkumu provedeného společností Kaspersky, bez ohledu na to, zda byly oběti útoku ochotny zaplatit výkupné či nikoli, pouze 29 % zasažených jednotek bylo schopno zcela obnovit všechny své soubory, které byly buď zašifrovány nebo zablokovány v důsledku útoku. Polovina těchto obětí (50 %) utrpěla ztrátu alespoň některých svých souborů, 32 % přišlo o významné množství dat a 18 % zaznamenalo ztrátu malého počtu souborů. 13 %, které zažily útok ransomwarem, utrpělo téměř úplnou ztrátu svých dat. (Over half of ransomware victims pay the ransom, but only a quarter see their full data returned, 2021)

### 3.7.1 Obnovení dat ze zálohy

Jednou z nejúčinnějších metod obnovy zašifrovaných souborů je obnova ze zálohy. Záloha je kopie souborů uložená odděleně od počítače, obvykle na externím pevném disku nebo v cloudu. (Ransomware Data Recovery: How to Save Your Data, 2023)

Proces obnovy záloh zahrnuje několik klíčových fází. Po fyzickém připojení externího zařízení, obvykle USB disku, je třeba upravit bootovací konfiguraci systému, aby bylo umožněno spouštět systém z tohoto externího zařízení. Tato úprava probíhá v prostředí BIOS/UEFI, kde má uživatel možnost vybrat preferovaný zdroj pro bootování. Po nastavení správného bootovacího média systém načte speciální prostředí pro obnovu dat. V tomto prostředí jsou k dispozici různé volby, včetně možnosti odstranění problémů, upřesnění parametrů obnovy a obnovy zálohy z bitové kopie operačního systému. Pokud je k dispozici více verzí zálohy, systém automaticky vybere nejnovější, ale uživatel má také možnost ručně vybrat konkrétní zálohu. Před samotným spuštěním procesu obnovy systém zobrazí uživateli souhrn, který obsahuje klíčové informace o obnově. Tento souhrn musí být uživatelem

potvrzen. Po potvrzení začne systém provádět samotný proces obnovy dat a systémových souborů z vybrané zálohy. (Bitová kopie Windows od vytvoření po obnovu, 2022)

### 3.7.2 Použití vestavěných nástrojů obnovy

Některé operační systémy, jako je například Windows 10, disponují vestavěnými utilitami pro provádění obnovy. Konkrétně nástroj pro obnovu systému Windows umožňuje navrátit systémové nastavení do předem vytvořeného bodu obnovení, což je užitečný postup pro obnovu stability a spolehlivosti operačního systému. (Baker, 2023)

V případě, že se systém nepodaří načíst normálním způsobem, je možné spustit nouzový režim. Tento režim zapne systém bez spouštění všech programů, které by mohly bránit jeho správnému spuštění. Nouzový režim se spouští v prostředí pro opravu systému, které se obvykle spustí automaticky, pokud je zjištěna chyba, která by zabránila běžnému startu systému, ale lze tento režim vyvolat i klávesovou zkratkou. (Spuštění Nástroje Obnovení systému, 2020)

Tato možnost bývá v mnoha případech úspěšná, ale některé současné varianty ransomwaru mají schopnost cíleně poškodit tyto nástroje pro obnovu systému, čímž narušují jejich funkcionalitu. (Ransomware Data Recovery: How to Recover Files From an Attack, 2023)

### 3.7.3 Nástroje pro dešifrování

Dešifrovací nástroje představují specializovaný software, který je navržen s cílem rozšifrovat soubory, jež byly zašifrovány konkrétními variantami ransomwaru. Tyto aplikace jsou většinou vyvíjeny kybernetickými odborníky a mohou sloužit jako účinný prostředek pro obnovu zašifrovaných dat, aniž by bylo nutné platit výkupné. Jejich účinnost spočívá v tom, že dokáží prolomit šifrování a navrátit data do původního stavu, což umožňuje obětem minimalizovat ztrátu důležitých informací a finančních prostředků. (Ransomware Data Recovery: How to Save Your Data, 2023) Při dešifrování systém extrahuje a převádí zašifrovaná data a transformuje je na texty a obrázky, které jsou snadno srozumitelné nejen pro čtenáře, ale i pro systém. (Rouse, 2023)

V oblasti dešifrování ransomwaru existuje několik online zdrojů a webových platforem, které poskytují specializované nástroje a řešení. Při výběru konkrétního nástroje pro

dešifrování je klíčové dbát na důvěryhodnost zdroje. Stahování těchto nástrojů z nedůvěryhodných zdrojů může představovat vážné bezpečnostní riziko a hrozbu nové infekce.

Efektivita dešifrovacích nástrojů může variabilně záviset na konkrétním podtypu ransomwaru a na použité metodě šifrování. Toto je zkomplikováno i kontinuálním vývojem nových variant ransomwaru, což může omezovat dostupnost relevantních dešifrovacích nástrojů. (Ransomware Data Recovery: How to Save Your Data, 2023)

# 4. Vlastní práce

Ve vlastní práci bude popsán proces přípravy virtuálního prostředí, vybrané vzorky ransomwaru, kritéria použitá při testování antivirových a anti-ransomwarových programů a nástrojů na obnovu dat a následná analýza dat experimentu. Finální část práce pak obsáhne komplexní srovnání testovaných produktů na základě vybraných kritérií.

## 4.1 Příprava virtuálního prostředí

Jako virtualizační nástroj byl použit program Oracle VM VirtualBox z důvodu jeho jednoduché použitelnosti a možnosti vytváření izolované virtuální stroje a možnosti mít spuštěných více virtuálních strojů najednou.

Na VirtualBox je naistalován systém Windows 10. Po úspěšné instalaci je potřeba virtuální stroj správně nastavit, aby bylo toto prostředí bezpečné při testování různých variant ransomwaru. Prvním krokem v nastavení bylo nastavení sdílených složek z fyzického počítače, kdy toto sdílení představuje riziko, kterým se ransomware může šířit. V tomto případě byla celá sdílená složka odebrána, což zaručuje nejvyšší stupeň ochrany. V případě, že je potřeba do složky stále nahlížet, je třeba změnit typ přístupu na „Read only“. Dalším krokem je nastavení síťové karty, kde bylo virtuálně nastaveno, že není připojena k síti a virtuálně by odpojen i síťový kabel. Jedině takto bude virtuální stroj s plnou jistotou odpojen od sítě a bude zaručeno, že toto prostředí bude bezpečné.

## 4.2 Získání reálných vzorků ransomwaru

Vzorky ransomwaru, které byly využity k testování, byly získány z veřejně dostupné platformy GitHub. Získané vzorky jsou rozděleny podle specifických typů ransomwaru. Rozdělení vzorků podle těchto typů umožní provést důkladné a diferencované testy, které poskytnou užitečné informace o schopnostech a omezeních testovaných programů.

Mezi konkrétní typy ransomwaru, které byly při testu využity, patří například Cerber, Cryptowall, Jigsaw, Locky, Mamba, Matsnu, Petrwrap, Petya, Radamant, RedBoot, Rex, Satana, TeslaCrypt, Thanos, Unnamed0, Vipasana, WannaCry, WannaCryPlus a další. Tato variabilita umožnila pokrýt širokou škálu variant a strategií, které tyto ransomwary využívají k infikaci a šifrování cílových systémů. Právě tyto rozdílné strategie mohou ovlivnit účinnost antivirových a anti-ransomwarových programů při jejich detekci a eliminaci. Získané vzorky

tak slouží jako reprezentativní soubor pro testování a hodnocení účinnosti anti-ransomwarových řešení.

## 4.3 Hodnocená kritéria u antivirových a anti-ransomwarových programů

Kritéria posuzovaná při hodnocení antivirových a anti-ransomwarových programů byla následující:

- Spolehlivost detekce
- Cena licence
- Průměrná rychlost blokace hrozby
- Průměrné zatížení procesoru
- Průměrné využití paměti RAM
- Potřebné uložiště

Spolehlivost detekce je klíčovým kritériem, které hodnotí schopnost antivirových programů a anti-ransomwarových programů úspěšně identifikovat ransomware. Toto kritérium hodnotí efektivitu a přesnost detekce ransomwaru v systému a následné potlačení jeho škodlivých aktivit. Spolehlivost detekce představuje zásadní faktor pro posouzení účinnosti a spolehlivosti těchto programů. Tento výsledek je vyjádřen v procentech a počítá se jako poměr počtu správně detekovaných vzorků ransomwaru k celkovému počtu vzorků, které byly testovány. Spolehlivost detekce byla tedy vypočtena pomocí následujícího vzorce:

$$Spolehlivost\ detekce\ (\%) = \frac{\text{Počet správně detekovaných ransomwarových vzorků}}{\text{Celkový počet testovaných ranomwarových vzorků}} \times 100$$

Cena licence je klíčovým aspektem při hodnocení finanční dostupnosti antivirových a anti-ransomwarových programů. Toto kritérium vyjadřuje cenu licence na software v českých korunách za jedno roční období. Pokud nebyla cena uvedena v českých korunách, byl proveden převod měny dle aktuálního kurzu na české koruny. Ceny byly vždy převzaty z oficiálních stránek poskytovatelů.

Kritérium „Průměrná rychlost blokace hrozby“ se zaměřuje na časový interval, který program potřebuje k identifikaci a následnému zablokování ransomwaru v systému. Rychlá reakce na detekci hrozby je klíčová pro minimalizaci škod způsobených v systémech nebo na

datech. Průměrná rychlost blokace hrozby byla měřena v sekundách a zahrnuje čas od okamžiku, kdy se ransomware v systému spustil, až po dobu, během které byl úspěšně identifikován a zastaven antivirovým programem. Sledování rychlosti blokace bylo měřeno pro každý vzorek ransomwaru, který byl součástí testování. Následně jsou výsledky rychlosti blokace pro každý typ antiviru přepočítány na průměrnou hodnotu, což umožnilo získat údaj o tom, jak rychle antivirový program reaguje na různé typy ransomwaru.

Průměrné zatížení procesoru zahrnuje průměrnou míru zatížení v procentech během dvou konkrétních stavů:

- **Aktivní činnost** – Stav, kdy program provádí činnosti jako jsou skenování systému nebo analýza souborů v reálném čase
- **Klidový režim** – Tento stav nastává, kdy program nevykonává žádnou aktivní činnost a je v klidovém režimu

K měření bude využit vestavěný nástroj Správce úloh, který zaznamenává přesná data o využití procesu danou aplikací. Tento přístup umožňuje lepší porovnání z hlediska jejich dopadu na výkon procesoru v různých situacích.

Průměrné využití paměti RAM je dalším klíčovým kritériem, které se zabývá mírou, jakou antivirové programy využívají operační paměť (RAM) v různých provozních situacích. Toto kritérium umožňuje zhodnotit, jak antivirové programy interagují s pamětí systému a jakým způsobem ovlivňují celkový výkon počítače. Využití paměti RAM bylo měřeno během aktivní činnosti a klidového režimu pomocí Správce úloh, jak bylo již popsáno u kritéria „Zatížení procesoru“.

Kritérium "potřebné úložiště" se zaměřuje na velikost místa na pevném disku, které program zabíral po dokončení jeho instalace a konfigurace. Kritérium je vyjádřeno v megabytech (MB). Měření tohoto kritéria bylo provedeno zjištěním velikosti všech souborů, které byly na disku nainstalovány.

## 4.4 Hodnocená kritéria u nástrojů na obnovu dat

Hodnocená kritéria pro nástroje na obnovu dat byla následující:

- Úspěšnost obnovy
- Podporované typy ransomwaru
- Průměrná rychlost obnovy
- Průměrné zatížení procesoru

- Průměrné využití paměti RAM
- Potřebné uložiště

Úspěšnost obnovy se zaměřuje na schopnost nástrojů na obnovu dat úspěšně obnovit data, která byla ztracena nebo poškozena v důsledku útoku ransomwaru. Úspěšnost obnovy byla vyjádřena jako procentuální podíl obnovených dat z celkového počtu zašifrovaných nebo poškozených souborů. Pro vyhodnocení úspěšnosti obnovy dat se provedl proces obnovy dat pomocí daného nástroje. Po dokončení obnovy se zaznamenal počet úspěšně obnovených dat. Pokud obnova souboru proběhla jen částečně, například pouze na 50 %, bude tato částečná obnova zaznamenána jako úspěšně obnovený soubor s hodnotou 0,5 místo hodnoty 1, která by vyjadřovala úplnou obnovu souboru. Výpočet byl proveden dle následujícího vzorce:

$$Úspěšnost\ obnovy\ (\%) = \frac{\text{počet úspěšně obnovených souborů}}{\text{Celkový počet zašifrovaných či poškozených dat}} \times 100$$

Kritérium „Podporované typy ransomwaru“ se zaměřuje na schopnost nástroje obnovit data, zašifrované různými typy ransomwaru. Toto kritérium je vyjádřeno pomocí čísla, které udává počet typů ransomwaru, které nástroj dokáže úspěšně dešifrovat. Například pokus nástroj podporuje 10 typů ransomwaru, bude toto kritérium vyjádřeno číslem 10.

Průměrná rychlost obnovy hodnotí časový interval, který nástroj na obnovu dat potřebuje k úspěšné obnově dat po detekci ransomwaru v systému. Kritérium zahrnuje časový úsek od okamžiku, kdy nástroj na obnovu začal s procesem dešifrování, až po ohlášení nástrojem o dokončení obnovy.

Průměrné zatížení procesoru je kritérium, které hodnotí míru, do které nástroj na obnovu dat ovlivňuje výkon procesoru během procesu obnovy. Toto kritérium je vyjádřeno v procentech a představuje úroveň zátěže, kterou nástroj klade na procesor za účelem provádění svých operací. Tak jako u antivirových programů a anti-ransomwarových programů, i u nástrojů na obnovu dat k měření probíhalo během aktivní činnosti a klidového režimu.

Průměrné využití paměti RAM umožňuje posoudit, jak nástroje na obnovu dat využívají paměť systému a jakým způsobem ovlivňují celkový výkon počítače. V průběhu testování byly nástroje na obnovu dat monitorovány při aktivní činnosti, tj. při procesu obnovy a při klidovém režimu, kdy není prováděna žádná aktivní činnost. K měření využití paměti RAM i průměrného zatížení procesoru byl využit nástroj Správce úloh, který zaznamenává údaje o využití paměti i procesoru daným nástrojem. Tento přístup umožňuje

srovnání nástrojů na obnovu dat z hlediska jejich vlivu na hardware v různých provozních situacích.

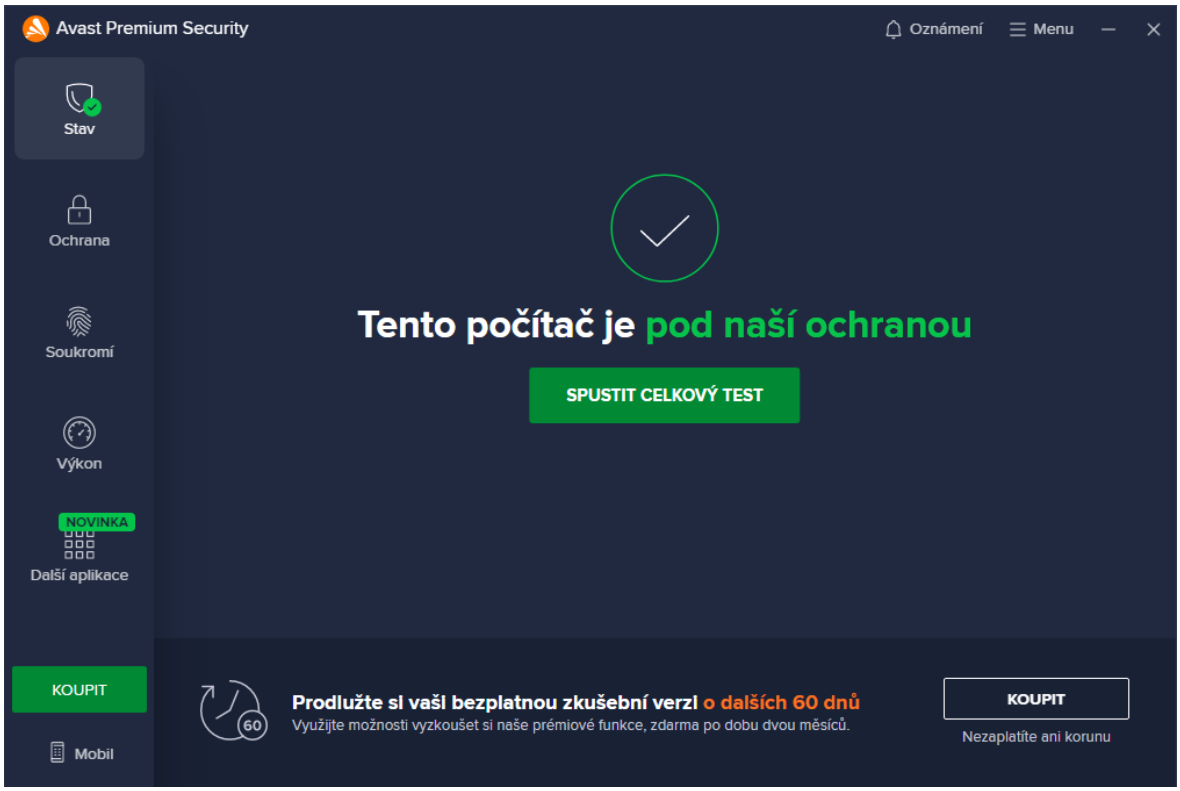
Velikost potřebného úložiště je dalším kritériem, které je nezbytné zohlednit při hodnocení nástrojů na obnovu dat. Toto kritérium se zaměřuje na množství prostoru na pevném disku, které je vyžadováno pro instalaci a následného provozu nástroje na obnovu dat. Velikost potřebného úložiště bylo hodnoceno v megabytech (MB).

## 4.5 Testované antivirové programy

Pro výběr testovaných antivirových programů byla použita data z webu antivirovecentrum.cz, který poskytuje přehledný seznam antivirových programů spolu s jejich hodnocením a oceněními. Na základě těchto informací bylo vybráno pět nejlepších antivirových programů, které excelují v ochraně před škodlivým softwarem.

### 4.5.1 Avast Premium Security

Avast Premium Security dosáhl v testu vysoké spolehlivosti detekce ransomwaru, která dosáhla hodnoty 99,61 %, čímž se stal antivirovým programem s nejlepší detekcí ze všech testovaných. Roční licence pro tento produkt je k dispozici za částku 690 Kč. Avast je schopen blokovat ransomware s průměrnou rychlostí 9,0224 sekundy. Nicméně, v porovnání s ostatními antivirovými programy, Avast vykazuje vyšší zatížení procesoru, a to 32,97 %, což může negativně ovlivnit starší zařízení. Průměrné využití paměti RAM Avastu činí 131,083 MB. Ze všech testovaných antivirových programů zabírá Avast největší místo na úložišti, a to celkových 1680 MB.




*Obrázek 8 Avast Premium Security UI*

### 4.5.2 AVG internet security

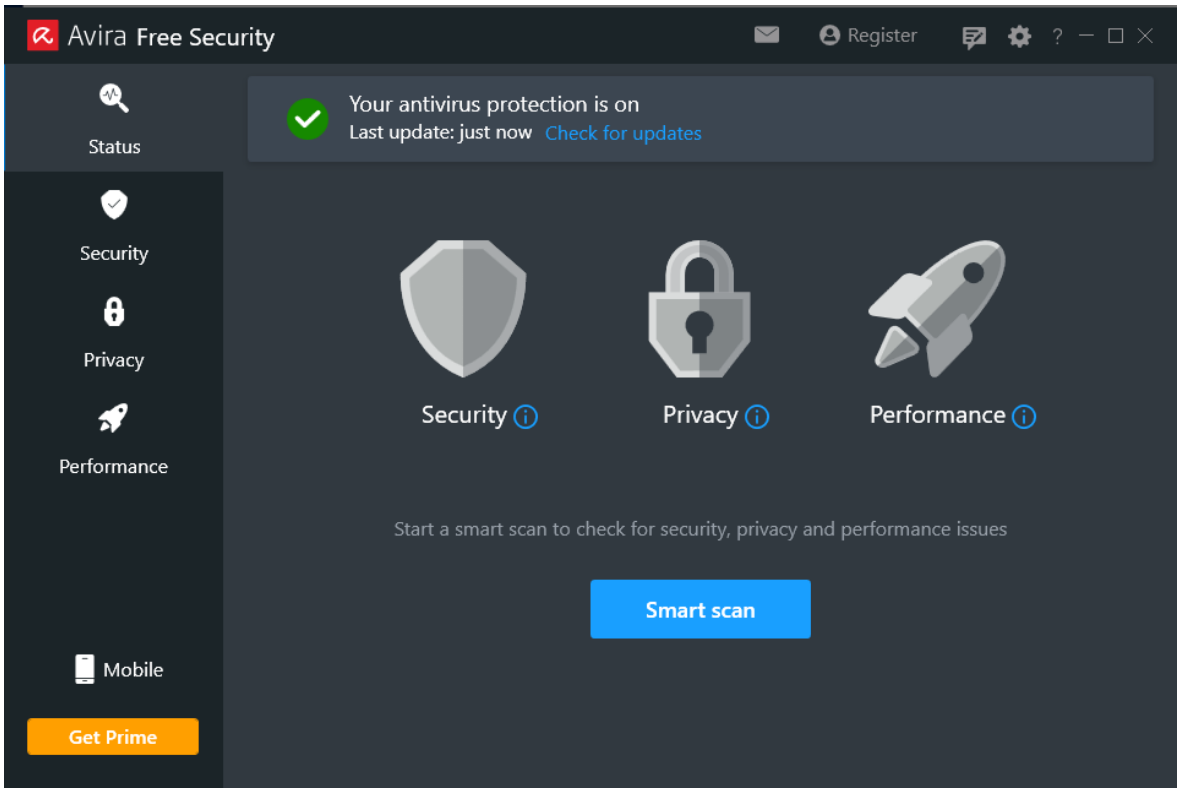
AVG Internet Security si ve spolehlivosti detekce ransomwaru vedl jako druhý nejlepší, přičemž dosáhl úctyhodných 99,23 %. Roční licence pro tento produkt je dostupná za částku 1091,15 Kč. AVG Internet Security dosahuje blokování ransomwaru s průměrnou rychlostí 10,32934 sekund. V porovnání s ostatními antivirovými programy, AVG zatěžuje procesor průměrně, přičemž jeho zatížení dosahuje 31,25 %. Co se týče paměti RAM, AVG

Internet Security průměrně využívá 83,6484127 %. Pro svou činnost vyžaduje AVG Internet Security celkově 678 MB úložiště.


*Obrázek 9 AVG Internet Security UI*

### 4.5.3 Avira Free Security

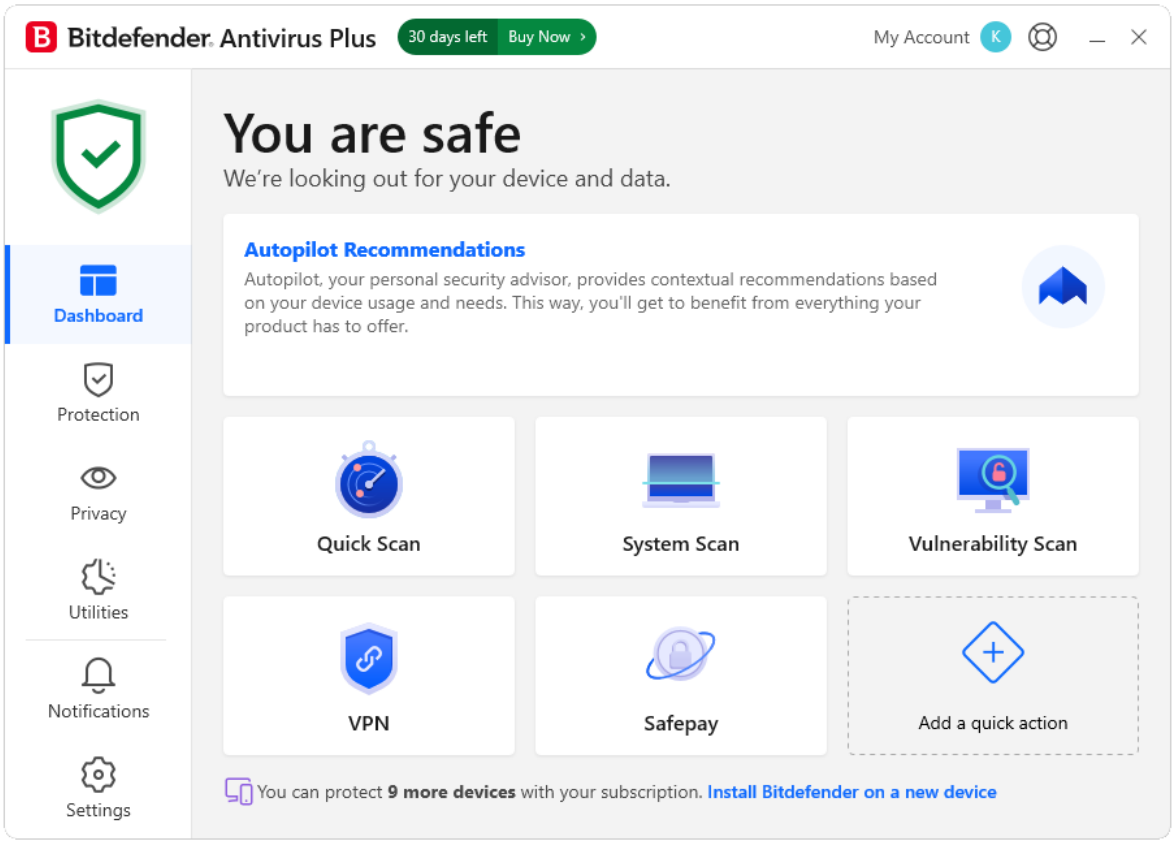
Avira, s účinností detekce ransomwaru 95 %, se umístila jako nejméně účinný antivirový program mezi všemi testovanými. Na druhou stranu nabízí licenci zdarma a dosáhla průměrné rychlosti blokování ransomwaru 2,1142 sekundy, což zaručuje poměrně rychlou reakci na identifikaci škodlivého softwaru a je nejrychlejší ze všech testovyných. Avira dosahovala zatížení procesoru průměrně na úrovni 26,55 % a využití paměti RAM činilo 68,5942 MB. Potřebných 1001 MB úložiště je průměrným požadavkem, což Aviru řadí mezi středně náročné antivirové programy z hlediska potřeby diskového prostoru.




*Obrázek 10 Avira Free Security UI*

### 4.5.4 Bitdefender Antivirus Plus

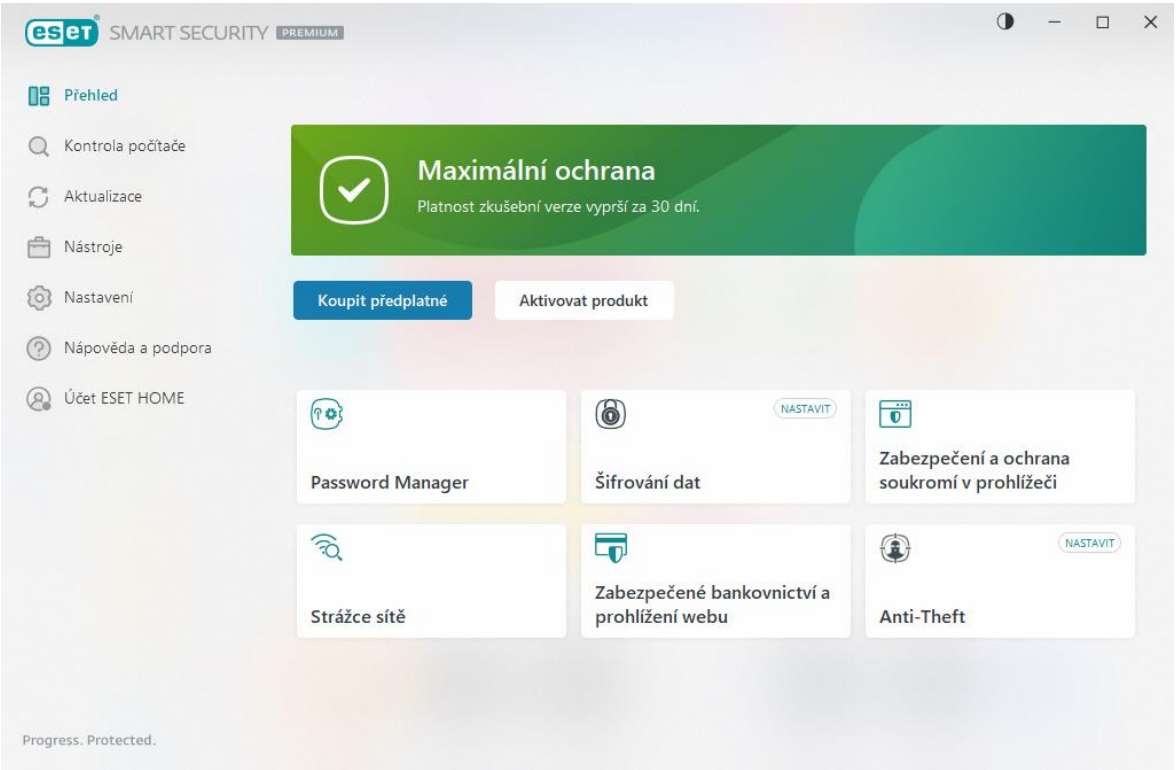
Bitdefender Antivirus Plus v testu skončil s vysokou spolehlivostí detekce ransomwaru dosahující hodnoty 99,615 %. Tímto výsledkem dosáhl stejné úrovně spolehlivosti detekce jako Avast Premium Security. Cena roční licence tohoto produktu činí 549 Kč. Bitdefender dokázal blokovat ransomware s průměrnou rychlostí 3,0923 sekund. V porovnání s jinými antivirovými programy Bitdefender vykazuje třetí nejnižší průměrné zatížení procesoru, konkrétně 27,236 %. Průměrné využití paměti RAM činí 144,44 MB. Celkově Bitdefender Antivirus Plus vyžaduje 1121 MB úložného prostoru na disku.




*Obrázek 11 Bitdefender Antivirus Plus UI*

### 4.5.5 ESET Premium

ESET Antivirus Premium dosáhl ve srovnání s ostatními testovanými antivirovými programy nižších výsledků. Jeho spolehlivost detekce ransomwaru činila 98,846 %. Roční licence tohoto produktu je k dispozici za částku 1490 Kč. Průměrná rychlost blokace ransomwaru u ESETu dosáhla hodnoty 16,7653 sekund. V porovnání s jinými antivirovými programy je ESET méně náročný na výkon procesoru, s průměrným zatížením procesoru dosahujícím hodnoty 19,75 %. Průměrné využití paměti RAM u tohoto antiviru činí 19,3704 MB. ESET Antivirus Premium vyžaduje pro svůj provoz celkové úložiště o velikosti 624 MB.




*Obrázek 12 ESET Premium UI*

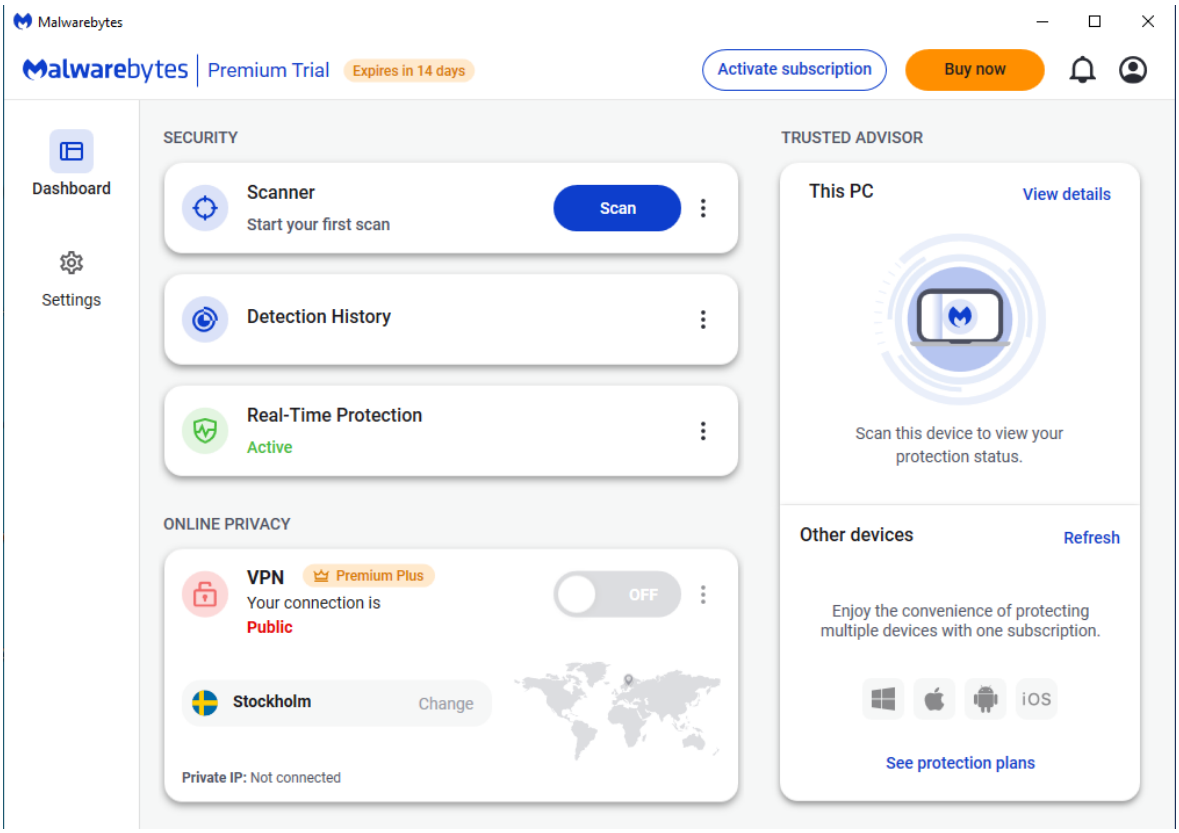
## 4.6 Testované antiransomwarové programy

Pro výběr testovaných antiransomwarových programů byla využita data z webu geckoandfly.com, který poskytuje přehledný seznam nejlepších antiransomwarových programů. Na základě těchto informací bylo vybráno pět programů, které vynikají v ochraně proti ransomwaru.

### 4.6.1 MalwareBytes Anti-Ransomware

MalwareBytes Anti-Ransomware, jako první testovaný antiransomwarový program, dosáhl v testu spolehlivosti detekce hodnoty 90 %, což je výsledek, který není na úrovni

nejlepších v porovnání s ostatními testovanými produkty. Roční licence pro tento produkt je k dispozici za částku 1400,29 Kč. MalwareBytes Anti-Ransomware se vyznačoval nižším zatížením procesoru ve srovnání s ostatními nástroji, a to pouze 16,9790 %. Průměrné využití paměti RAM dosahovalo hodnoty 76,3726 MB. Pro své správné fungování potřebuje 375 MB volného místa na disku.




*Obrázek 13 Malwarebytes UI*

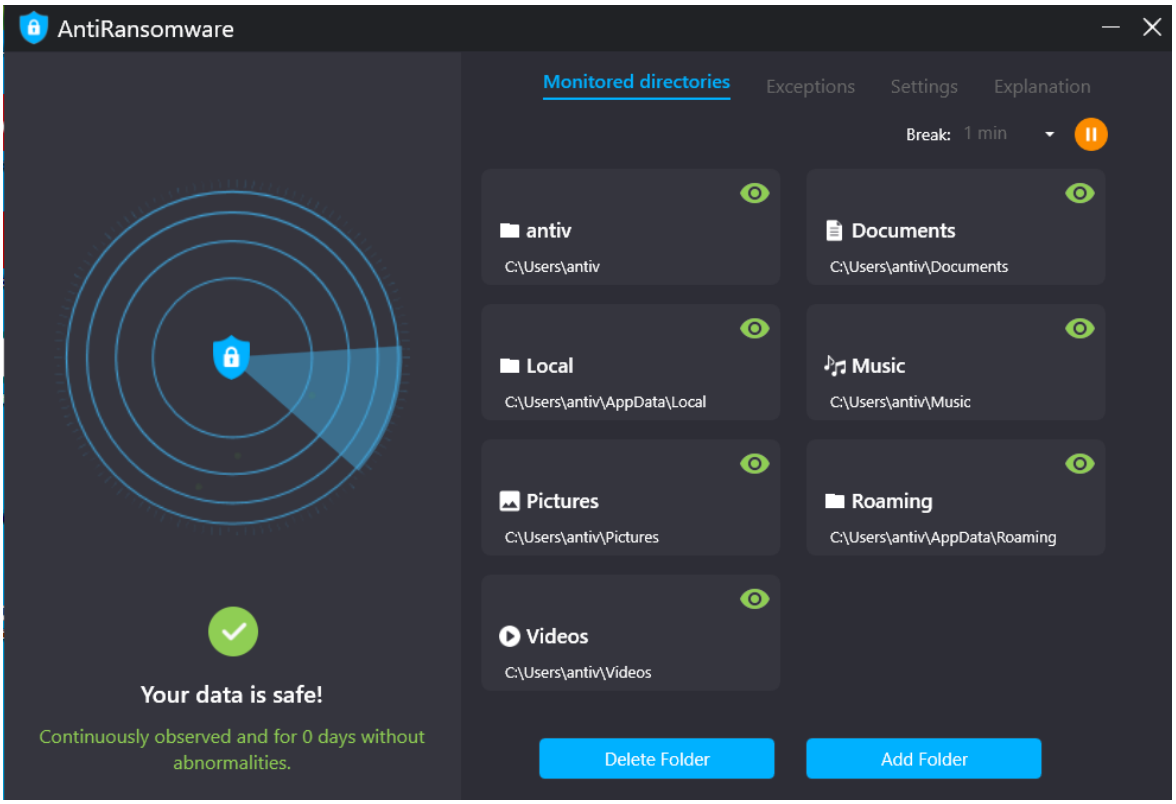
### 4.6.2 CryptoPrevent

V testu dosáhl CryptoPrevent spolehlivosti detekce ransomwaru ve výši 77,6923 %, což je oproti konkurečním produktům horší výsledek. Cena roční licence činí 466,74 Kč, což je relativně dostupná částka v porovnání s ostatními. Průměrná rychlost blokace hrozeb u CryptoPrevent byla 13,2067 sekund. Během testování byl procesor zatížen průměrně na úrovni 44,9059 %. Průměrné využití paměti RAM dosahovalo hodnoty 78,2882 MB. CryptoPrevent pro své fungování vyžadoval pouze 52,4 MB úložného prostoru.


*Obrázek 14 CryptoPrevent UI*

### 4.6.3 Acronis Anti-Ransomware

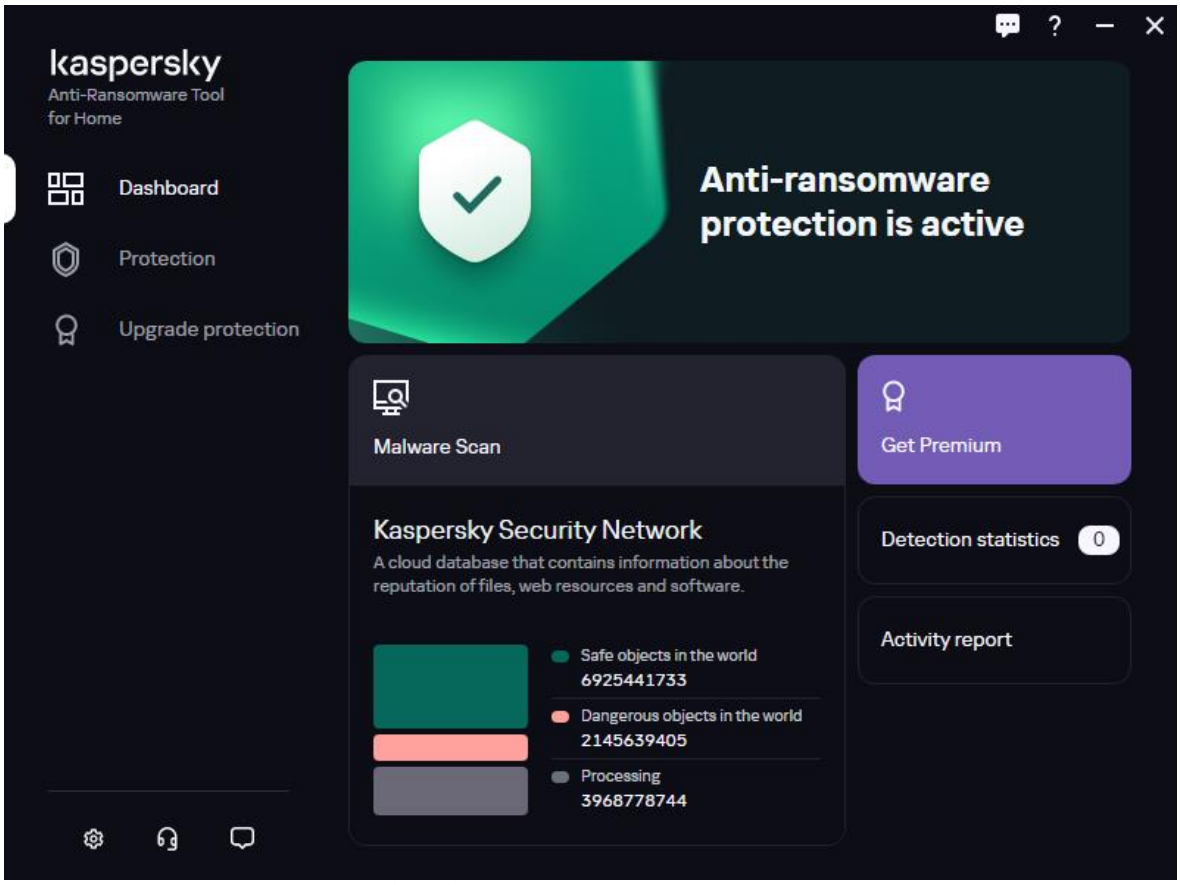
Acronis Anti-Ransomware v testu prokázal spolehlivost detekce ransomwaru na úrovni 77,6923 %. Cena licence tohoto produktu činí 1 158,68 Kč. Průměrná rychlost blokace hrozby byla 10,7514 sekund, což značí mírně nadprůměrnou reakční dobu. Zatížení procesoru dosahovalo průměrné hodnoty 11,18 %, což je relativně nízká hodnota v porovnání s konkurenčními produkty. Průměrné využití paměti RAM činilo 73,87 MB, což odpovídá průměru mezi testovanými nástroji. Potřebné úložiště pro tento program je nejmenší ze všech, pouze 15,4 MB.




*Obrázek 15 Acronis Anti-Ransomware UI*

### 4.6.4 Kaspersky Anti-Ransomware Tool

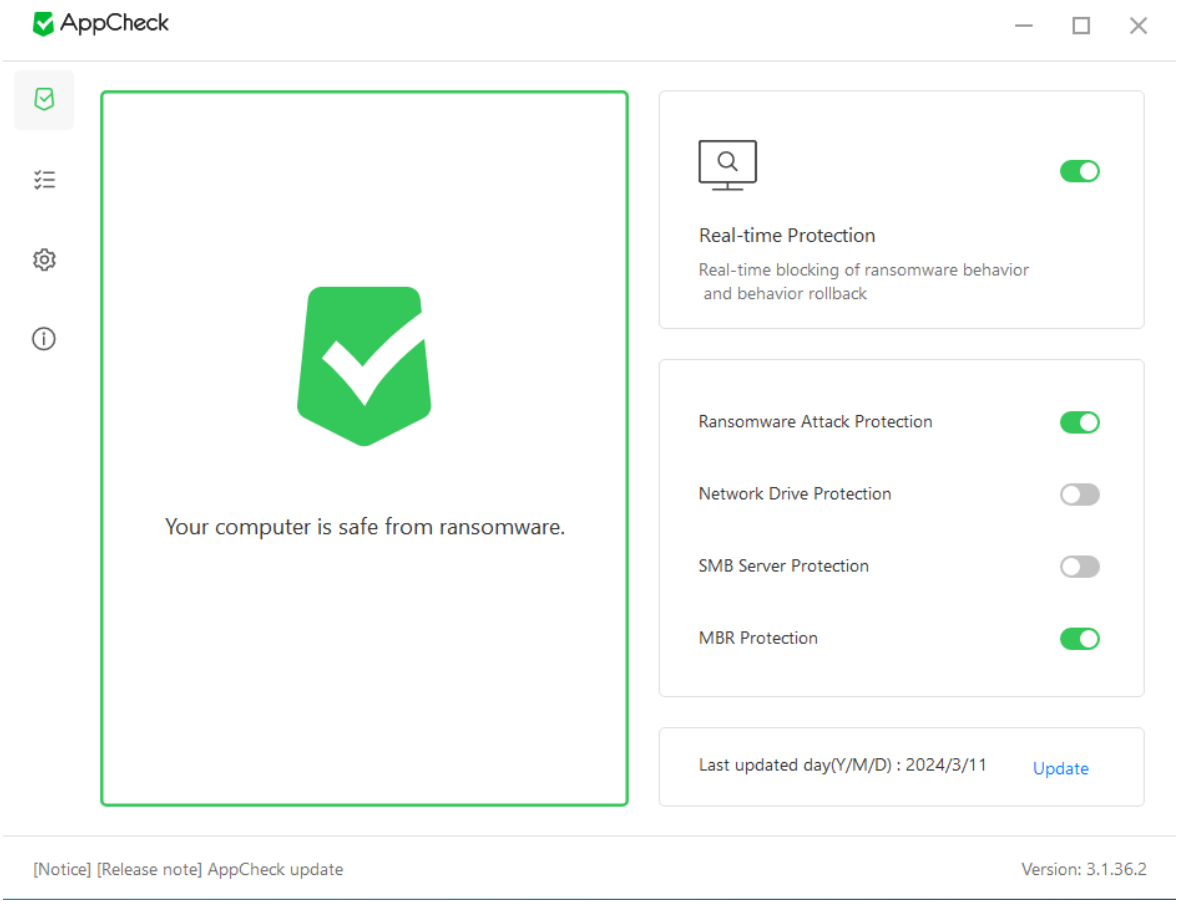
Kaspersky Anti-Ransomware Tool se ve zde uvedeném testu ukázal jako spolehlivý nástroj s úrovní detekce ransomwaru dosahující 89,2307 %. Co se týče ceny licence, uživatelé mohou získat tuto ochranu bezplatně. Průměrná rychlost blokace hrozby u Kaspersky Anti-Ransomware Tool dosáhla hodnoty 13,37 sekundy, což je mírně vyšší hodnota ve srovnání s některými jinými testovanými programy. Zatížení procesoru během provozu nástroje dosahovalo průměrné hodnoty 35,3081 % a průměrné využití paměti RAM nástroje bylo 68,0581 MB. Potřebné úložiště pro tento program činí 277 MB.




*Obrázek 16 Kaspersky Anti-Ransomware Tool UI*

### 4.6.5 AppCheck

Výsledky testu pro antivirový program AppCheck ukázaly spolehlivost detekce ransomwaru na úrovni 82,3076 %. Tato hodnota je nejnižší ze všech testovaných konkurenčních nástrojů. Cena licence pro tento program činí 579,07 Kč. Průměrná rychlost blokace hrozby u AppChecku dosáhla hodnoty 28,53 sekund, což je vyšší hodnota než u většiny ostatních testovaných produktů. Avšak, AppCheck má výhodu v nižším průměrném zatížení procesoru, které činí 15,5882 %. Průměrné využití paměti RAM u tohoto produktu je velmi nízké, pouze 5,8 MB. I potřebné uložiště pro AppCheck činí pouze 20,5 MB, což je opět nejnižší hodnota ve srovnání s ostatními produkty.




*Obrázek 17 AppCheck UI*

## 4.7 Testované nástroje pro obnovu dat

Testované nástroje na obnovu dat byly získány z několika doporučení různých webů, z důvodu nedostupnosti instalačního balíčku, nebo že některé uváděné nástroje na těchto webech již neexistují. Mezi tyto weby patřily zenarmor.com, geckoandfly.com nebo comparitech.com.

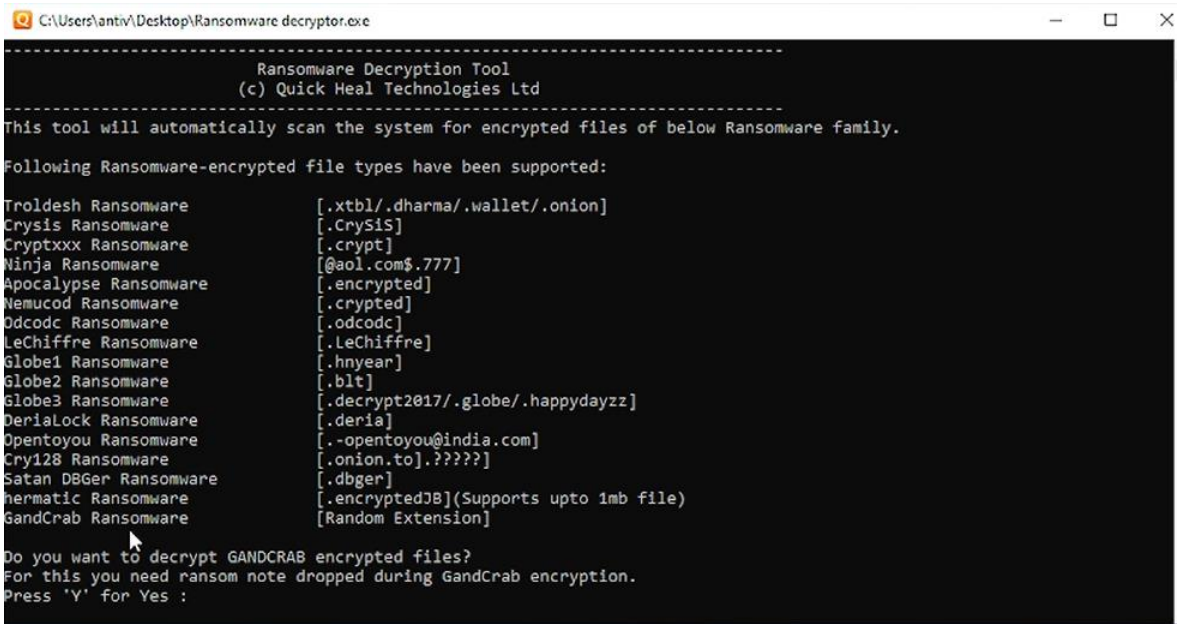
### 4.7.1 Trend Micro Ransomware File Decryptor

Trend Micro Ransomware File Decryptor navzdory podporovaným typům ransomwaru, kterých bylo celkem 23, nedosáhl žádné úspěšné obnovy dat. Rychlost obnovy byla 32 minut a 41 sekund. Během procesu obnovy dat Trend Micro Ransomware File Decryptor vykazoval průměrné zatížení procesoru ve výši 23,15 % a průměrné využití paměti RAM bylo 29,3 MB, což jsou relativně nízké hodnoty. Potřebné úložiště činilo 12,2 MB.


*Obrázek 18 Trend Micro Ransomware File Decryptor UI*

### 4.7.2 QuickHeal Decryption Tool

QuickHeal Decryption Tool dosáhl v testu úspěšnosti obnovy dat velmi nízkého výsledku, a to 9,0909 %. I když se jedná o mírné zlepšení ve srovnání s nástrojem Trend Micro Ransomware File Decryptor, stále je tento výsledek velice tristní. QuickHeal podporuje celkem 17 typů ransomwaru. Rychlost obnovy dat u QuickHeal Decryption Tool dosáhla hodnoty 6 hodin, 51 minut a 5 sekund. Tento čas je výrazně delší ve srovnání s ostatními testovanými nástroji. Během provádění obnovy dat QuickHeal Decryption Tool vykazoval průměrné zatížení procesoru ve výši 6,9 % a průměrné využití paměti RAM bylo 56,5 MB. Pro své fungování potřebuje 27 MB volného místa na disku.




*Obrázek 19 QuickHeal Decryption Tool*

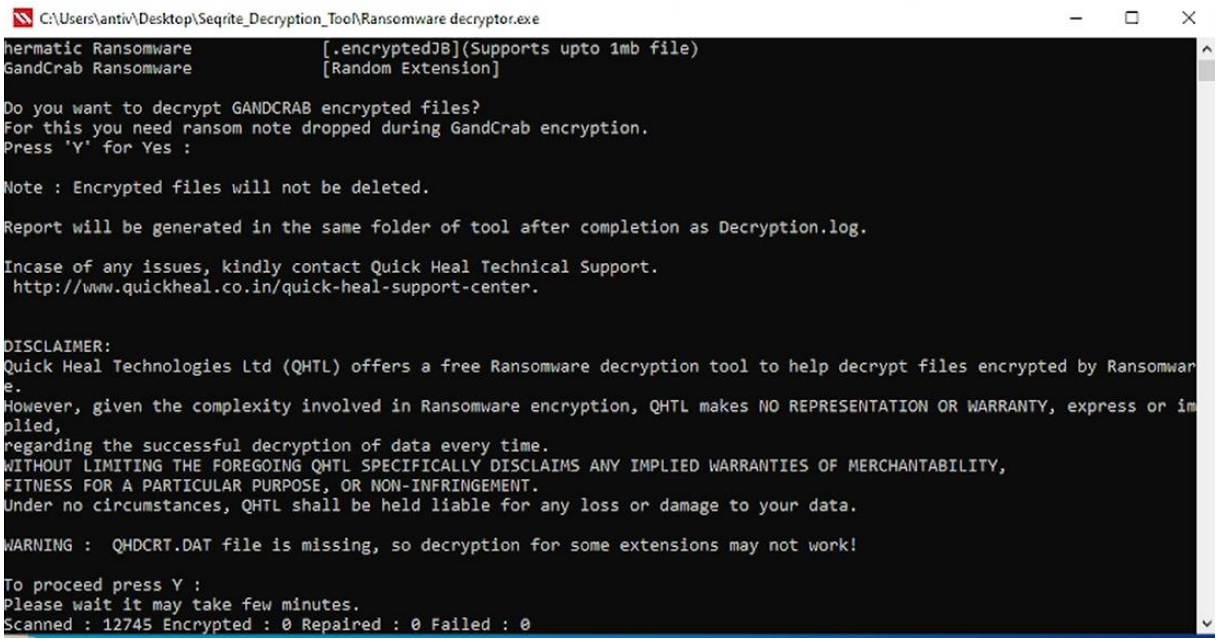
### 4.7.3 360 Ransomware Decryption Tool

Přestože QuickHeal Decryption Tool podporuje rozsáhlý počet 80 typů ransomwaru, nedokázal úspěšně obnovit žádná data. Rychlost obnovy byla 5 minut a 10 sekund, což je sice kratší doba než u ostatních nástrojů, ale možná právě proto nepřinesla žádné úspěšné výsledky. Během procesu obnovy dat QuickHeal Decryption Tool vykazoval průměrné zatížení procesoru ve výši 9,7 %. Průměrné využití paměti RAM bylo zaznamenáno na hodnotě 30,45 MB. Potřebné uložiště pro QuickHeal Decryption Tool činilo 9,78 MB.


*Obrázek 20 360 Ransomware Decryption Tool*

### 4.7.4 Seqrite Decryptor

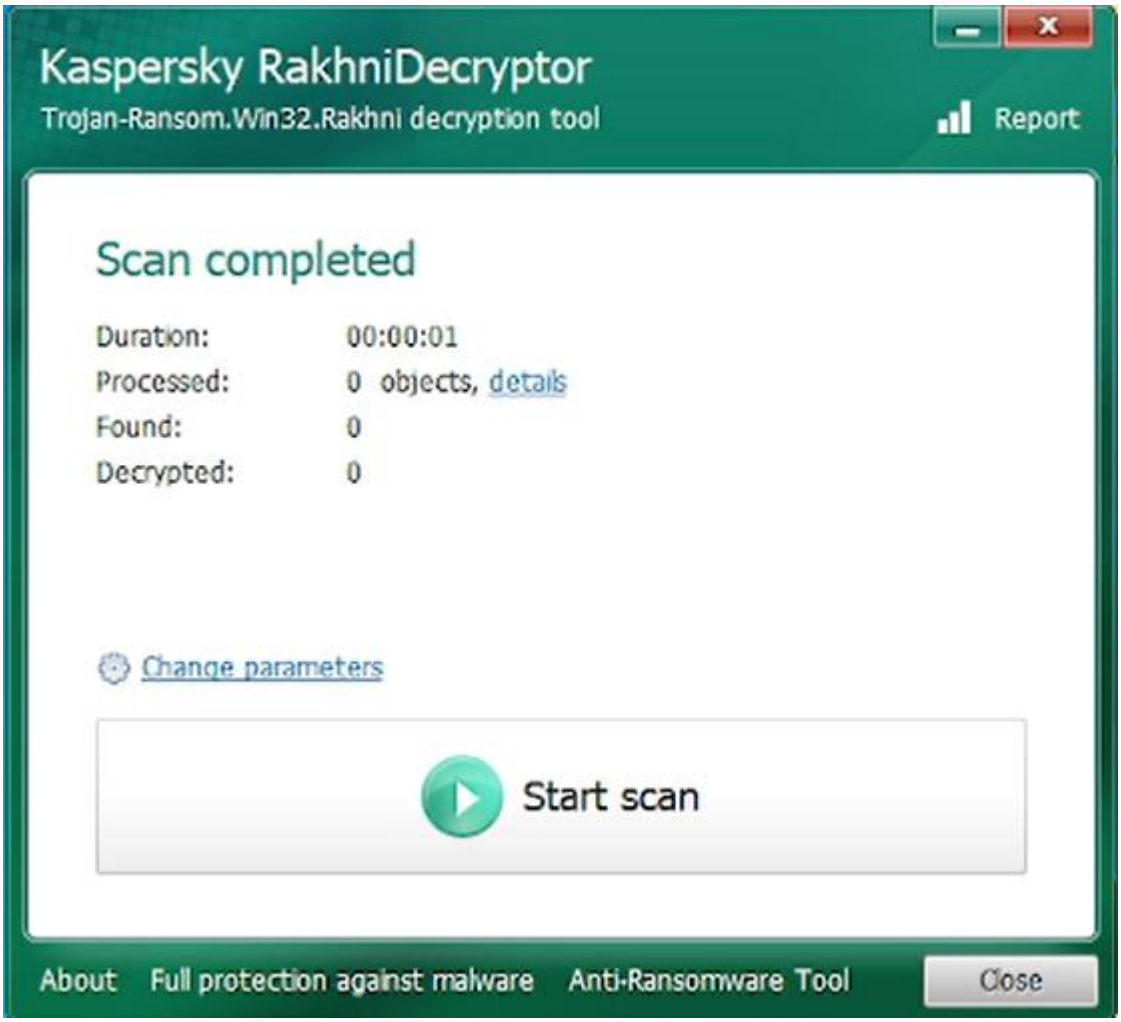
Seqrite Decryptor se v testu ukázal jako efektivní nástroj s úspěšností obnovy dat dosahující 72,7272 %. S podporou 16 typů ransomwaru poskytuje širokou škálu možností pro obnovu po útoku. Průměrná rychlost obnovy, která dosáhla hodnoty 10 minut a 19 sekund. Během procesu obnovy dat má Seqrite Decryptor průměrné zatížení procesoru ve výši 16,85 % a průměrné využití paměti RAM bylo 6,75 MB. Potřebné uložiště pro Seqrite Decryptor činilo 26,9 MB, což je vyšší hodnota než u některých konkurenčních nástrojů, ale stále dostatečně nízká pro bezproblémové použití.




*Obrázek 21 Seqrite Decryptor UI*

### 4.7.5 Kaspersky Rakhni Decryptor

Kaspersky Rakhni Decryptor byl hodnocen v testu a dosáhl úspěšnosti obnovy dat ve výši 54,5454 %, což ho řadí na druhé místo v úspěšnosti obnovy dat. Podporované typy ransomwaru, které nástroj zvládá dešifrovat, činí celkem 35. Průměrná rychlost obnovy dat pomocí Kaspersky Rakhni Decryptor byla zaznamenána na hodnotě 6 minut a 21 sekund. Zatížení procesoru se průměrně pohybovalo kolem 17 %, což má minimální vliv na celkový výkon systému. Průměrné využití paměti RAM činilo 19,35 MB. Potřebné uložiště pro instalaci a provoz nástroje činilo 19,35 MB.




*Obrázek 22 Kaspersky Rakhni Decryptor UI*

## 4.8 Výpočet vah kritérií

### 4.8.1 Stanovení vah pro antivirové a antiransomwarové programy

Pro určení důležitosti jednotlivých kritérií byla použita Saatyho metoda. Nejprve byla vytvořena tabulka porovnání mezi jednotlivými kritérii. Poté byl vypočten geometrický průměr pro každou variantu zvlášť.

| | *Spolehlivost detekce* | *Průměrná rychlost blokace hrozby* | *Cena licence* | *Průměrné zatížení procesoru* | *Průměrné využití paměti RAM* | *Potřebné uložiště* |
|---|---|---|---|---|---|---|
| ***Spolehlivost detekce*** | 1 | 2 | 4 | 5 | 5 | 7 |
| ***Průměrná rychlost blokace hrozby*** | 1/2 | 1 | 3 | 4 | 4 | 6 |
| ***Cena licence*** | 1/4 | 1/3 | 1 | 3 | 3 | 5 |
| ***Průměrné zatížení procesoru*** | 1/5 | 1/4 | 1/3 | 1 | 1 | 3 |
| ***Průměrné využití paměti RAM*** | 1/5 | 1/4 | 1/3 | 1 | 1 | 3 |
| ***Potřebné uložiště*** | 1/7 | 1/6 | 1/5 | 1/3 | 1/3 | 1 |

*Tabulka 1 Saatyho matice pro antivirové a antiransomwarové programy*

Váha každé varianty byla poté získána podílem součtu všech geometrických průměrů a geometrického průměru dané varianty. Tyto váhy pak odrážejí důležitost jednotlivých kritérií při výběru antivirového programu.

| | *Geometrický průměr* | *Váha* |
|---|---|---|
| *Spolehlivost detekce* | 3,344681 | 0,399 |
| **Průměrná rychlost blokace hrozby** | 2,289428 | 0,273 |
| **Cena licence** | 1,246441 | 0,149 |
| **Průměrné zatížení procesoru** | 0,606962 | 0,072 |
| **Průměrné využití paměti RAM** | 0,606962 | 0,072 |
| **Potřebné uložiště** | 0,284396 | 0,034 |
| **Suma** | 8,378871 | 1,0 |

*Tabulka 2 Preference kritérií pro antivirové a antiransomwarové programy*

### 4.8.2 Stanovení vah pro nástroje na obnovu dat

Stejný postup byl aplikován i při stanovení vah u nástrojů pro obnovu dat. Stejným způsobem byly provedeny porovnání mezi jednotlivými kritérii a následně byl vypočten geometrický průměr pro každou variantu. Váhy jednotlivých kritérií byly poté získány pomocí podílu součtu všech geometrických průměrů a geometrického průměru dané varianty.

| | *Úspěšnost obnovy* | *Podporované typy ransomwaru* | *Průměrná rychlost obnovy* | *Průměrné zatížení procesoru* | *Průměrné využití paměti RAM* | *Potřebné uložiště* |
|---|---|---|---|---|---|---|
| ***Úspěšnost obnovy*** | 1 | 3 | 4 | 5 | 5 | 6 |
| ***Podporované typy ransomwaru*** | 1/2 | 1 | 3 | 4 | 4 | 5 |
| ***Průměrná rychlost obnovy*** | 1/4 | 1/3 | 1 | 3 | 3 | 4 |
| ***Průměrné zatížení procesoru*** | 1/5 | 1/4 | 1/3 | 1 | 1 | 3 |
| ***Průměrné využití paměti RAM*** | 1/5 | 1/4 | 1/3 | 1 | 1 | 3 |
| ***Potřebné uložiště*** | 1/6 | 1/5 | 1/4 | 1/3 | 1/3 | 1 |

*Tabulka 3 Saatyho matice pro nástroje na obnovu dat*

| | *Geometrický průměr* | *Váha* |
|---|---|---|
| *Spolehlivost detekce* | 3,259844428 | 0,397 |
| **Průměrná rychlost blokace hrozby** | 2,220906155 | 0,271 |
| **Cena licence** | 1,200936955 | 0,146 |
| **Průměrné zatížení procesoru** | 0,606962231 | 0,074 |
| **Průměrné využití paměti RAM** | 0,606962231 | 0,074 |
| **Potřebné uložiště** | 0,312197466 | 0,038 |
| **Suma** | 8,207809466 | 1,0 |

*Tabulka 4 Preference kritérií pro nástroje na obnovu dat*

## 4.9 Vícekriteriální analýza variant

Pro posouzení a porovnání různých antivirových programů byla využita vícekriteriální analýza variant. Tento přístup umožňuje systematicky zhodnotit a srovnat více aspektů najednou, což pomáhá nalézt optimální volbu antivirového řešení. Místo jednoduchého srovnání jednotlivých programů podle jednoho kritéria, bodovací metoda s váhami, která byla využita, umožňuje zkoumat různé faktory, jako je právě spolehlivost, rychlost, cena a další, a najít tak komplexní a vyvážené řešení.

Každé zkoumané kritérium bylo klasifikováno jako minimalizační nebo maximalizační, aby výsledky mohly být správně obodovány a šlo tak dosáhnout objektivního srovnání mezi jednotlivými programy.

| | *Avast Premium Security* | *AVG Internet Security* | *Avira Free Security* | *Bitdefender Antivirus Plus* | *ESET Antivirus Premium* | *Charakter kritéria* |
|---|---|---|---|---|---|---|
| ***Spolehlivost detekce (%)*** | 99,615 | 99,23 | 95 | 99,615 | 98,846 | Max |
| ***Průměrná rychlost blokace hrozby (s)*** | 9,0224 | 10,3293 | 2,1142 | 3,0923 | 16,7653 | Min |
| ***Cena licence (Kč)*** | 690 | 1091,15 | 0 | 549 | 1490 | Min |
| ***Průměrné zatížení procesoru (%)*** | 32,97016129 | 31,25 | 26,55 | 27,236 | 19,75 | Min |
| ***Průměrné využití paměti RAM (MB)*** | 131,0830645 | 83,6484127 | 68,59423077 | 144,44 | 19,37037 | Min |
| ***Potřebné uložiště (MB)*** | 1680 | 678 | 1001 | 1121 | 624 | Min |

*Tabulka 5 Vícekriteriální analýza variant antivirových programů – výsledná data z testování s přiřazenými charaktery*

Pro úplné zhodnocení každého antivirového programu byla tabulka s daty obodována. Pomocí skalárního součinu jednotlivých kritérií s jejich váhami bylo dosaženo bodového výsledku, který určil konečné hodnocení.

| | *Avast Premium Security* | *AVG Internet Security* | *Avira* | *Bitdefender Antivirus Plus* | *ESET Antivirus Premium* | *Charakter kritéria* | *Váha* |
|---|---|---|---|---|---|---|---|
| ***Spolehlivost detekce (%)*** | 10 | 9 | 6 | 10 | 8 | Max | 0,399 |
| ***Průměrná rychlost blokace hrozby (s)*** | 6 | 5 | 10 | 9 | 4 | Min | 0,273 |
| ***Cena licence (Kč)*** | 7 | 5 | 10 | 8 | 4 | Min | 0,149 |
| ***Průměrné zatížení procesoru (%)*** | 5 | 6 | 8 | 7 | 10 | Min | 0,072 |
| ***Průměrné využití paměti RAM (MB)*** | 5 | 7 | 8 | 4 | 10 | Min | 0,072 |
| ***Potřebné uložiště (MB)*** | 4 | 9 | 6 | 5 | 9 | Min | 0,034 |

*Tabulka 6 Vícekriteriální analýza variant antivirových programů – bodové ohodnocení s přiřazenými váhami*

Stejný postup byl uplatněn i u antiransomwarových programů, kdy data nejprve byla přenesena do tabulky a byly určeny charaktery jednotlivých kritérií.

| | *MalwareBytes Anti-Ransomware* | *CryptoPrevent* | *Acronis Anti-Ransomware* | *Kaspersky Anti-Ransomware Tool* | *AppCheck* | *Charakter kritéria* |
|---|---|---|---|---|---|---|
| ***Spolehlivost detekce (%)*** | 90 | 77,6923 | 80,7692 | 89,2307 | 82,3076 | Max |
| ***Průměrná rychlost blokace hrozby (s)*** | 6,48889 | 13,2067 | 10,7514 | 13,37 | 28,53 | Min |
| ***Cena licence (Kč)*** | 1400,29 | 466,74 | 1 158,68 | 0 | 579,07 | Min |
| ***Zatížení procesoru (%)*** | 16,9790 | 44,9059 | 11,18 | 35,3081 | 15,5882 | Min |
| ***Využití paměti RAM (MB)*** | 76,3726 | 78,2882 | 73,87 | 68,0581 | 5,8 | Min |
| ***Potřebné uložiště (MB)*** | 375 | 52,4 | 15,4 | 277 | 20,5 | Min |

*Tabulka 7 Vícekriteriální analýza variant antiransomwarových programů – výsledná data z testování s přiřazenými charaktery*

Tabulka bylo obodována a poté pomocí skalárního součinu kritérií s jejich váhami bylo vypočítáno bodové hodnocení, přičemž váhy zůstaly stejné jako u antivirových programů.

| | *MalwareBytes Anti-Ransomware* | *CryptoPrevent* | *Acronis Anti-Ransomware* | *Kaspersky Anti-Ransomware Tool* | *AppCheck* | *Charakter kritéria* | *Váha* |
|---|---|---|---|---|---|---|---|
| ***Spolehlivost detekce (%)*** | 9 | 6 | 7 | 9 | 8 | Max | 0,397 |
| ***Průměrná rychlost blokace hrozby (s)*** | 9 | 6 | 7 | 6 | 4 | Min | 0,271 |
| ***Cena licence (Kč)*** | 4 | 9 | 5 | 10 | 8 | Min | 0,146 |
| ***Průměrné zatížení procesoru (%)*** | 8 | 5 | 10 | 6 | 9 | Min | 0,074 |
| ***Průměrné využití paměti RAM (MB)*** | 7 | 7 | 8 | 8 | 10 | Min | 0,074 |
| ***Potřebné uložiště (MB)*** | 5 | 8 | 10 | 6 | 9 | Min | 0,038 |

*Tabulka 8 Vícekriteriální analýza variant antiransomwarových programů – bodové ohodnocení s přiřazenými váhami*

Na závěr byla provedena analýza nástrojů na obnovu dat. Stejným způsobem jsme data získaná z testu převedli do tabulky a jednotlivým kritériím byl přiřazen charakter.

| | *Trend Micro Ransomware File Decryptor* | *QuickHeal Decryption Tool* | *360 Ransomware Decryption Tool* | *Seqrite Decryptor* | *Kaspersky Rakhni Decryptor* | *Charakter kritéria* |
|---|---|---|---|---|---|---|
| ***Úspěšnost obnovy (%)*** | 0 | 9,0909 | 0 | 72,7272 | 54,5454 | Max |
| ***Podporované typy ransomwaru*** | 23 | 17 | 80 | 16 | 35 | Max |
| ***Průměrná rychlost obnovy (h:m:s)*** | 0:32:41 | 6:51:05 | 0:05:10 | 0:10:19 | 0:06:21 | Min |
| ***Průměrné zatížení procesoru (%)*** | 23,15 | 6,9 | 9,7 | 16,85 | 17 | Min |
| ***Průměrné využití paměti RAM (MB)*** | 29,3 | 56,5 | 30,45 | 6,75 | 19,35 | Min |
| ***Potřebné uložiště (MB)*** | 12,2 | 27 | 9,78 | 26,9 | 6,19 | Min |

*Tabulka 9 Vícekriteriální analýza variant nástrojů na obnovu dat – výsledná data z testování s přiřazenými charaktery*

Tabulka byla opět obodována a každému kritériu byly přiřazeny adekvátní váhy. Poté byl využit skalární součin kritérií s jejich váhami k výpočtu konečného bodového ohodnocení.

| | *Trend Micro Ransomware File Decryptor* | *QuickHeal Decryption Tool* | *360 Ransomware Decryption Tool* | *Seqrite Decryptor* | *Kaspersky Rakhni Decryptor* | *Charakter kritéria* | *Váha* |
|---|---|---|---|---|---|---|---|
| ***Úspěšnost obnovy (%)*** | 0 | 1 | 0 | 8 | 6 | Max | 0,397 |
| ***Podporované typy ransomwaru*** | 5 | 4 | 9 | 4 | 6 | Max | 0,271 |
| ***Průměrná rychlost obnovy (s)*** | 5 | 1 | 10 | 7 | 9 | Min | 0,146 |
| ***Průměrné zatížení procesoru (%)*** | 6 | 10 | 9 | 7 | 7 | Min | 0,074 |
| ***Průměrné využití paměti RAM (MB)*** | 8 | 6 | 8 | 10 | 9 | Min | 0,074 |
| ***Potřebné uložiště (MB)*** | 8 | 7 | 9 | 7 | 10 | Min | 0,038 |

*Tabulka 10 Vícekriteriální analýza variant nástrojů na obnovu dat – bodové ohodnocení s přiřazenými váhami*

# 5. Výsledky a doporučení

Výsledky byly hodnoceny pomocí bodovací metody vícekriteriální analýzy variant, přičemž byla zohledněna váha jednotlivých kritérií. Konečné hodnocení a seřazení antivirových programů jsou uvedeny v Tabulka 11 Výsledky antivirových programů.

| *Pořadí* | *Antivirový program* | *Vážený součet bodů* |
|---|---|---|
| *1.* | Bitdefender Antivirus Plus | 8,601 |
| *2.* | Avira | 7,97 |
| *3.* | Avast Premium Security | 7,527 |
| *4.* | AVG Internet Security | 6,943 |
| *5.* | ESET Antivirus Premium | 6,626 |

*Tabulka 11 Výsledky antivirových programů*

Na základě vypočtených bodů a porovnání jednotlivých programů bylo zjištěno, že Bitdefender Antivirus Plus dosáhl nejvyššího počtu bodů (8,601), tudíž lze o něm konstatovat, že má vysokou úroveň ochrany a je spolehlivý. Avira a Avast Premium Security rovněž prokázaly vysokou efektivitu při ochraně proti ransomwaru, s bodovým ohodnocením 7,97 a 7,527 bodů. AVG Internet Security a ESET Antivirus Premium také poskytují určitou úroveň ochrany, avšak s výrazně nižšími výsledky ve srovnání s ostatními programy,

Doporučení se vztahuje na první tři nejlépe hodnocené antivirové programy, zejména na Bitdefender Antivirus Plus, který je z nich nejlépe hodnocený. Tyto programy se vyznačují vysokou úrovní ochrany a spolehlivosti v boji proti ransomwaru. Jejich efektivita a spolehlivost při detekci a odstraňování hrozeb by se dala označit za více než dostačující.

| *Pořadí* | *Antiransomwarový program* | *Vážený součet bodů* |
|---|---|---|
| *1.* | Kaspersky Anti-Ransomware Tool | 7,923 |
| *2.* | MalwareBytes Anti-Ransomware | 7,896 |
| *3.* | AppCheck | 7,176 |
| *4.* | Acronis Anti-Ransomware | 7,118 |
| *5.* | CryptoPrevent | 6,514 |

*Tabulka 12 Výsledky antiransomwarových programů*

Po provedeném hodnocení antiransomwarových programů byli získány následující výsledky zobrazené v Tabulka 12 Výsledky antiransomwarových programů. Kaspersky Anti-Ransomware Tool se umístil na prvním místě s váženým součtem bodů 7,923. MalwareBytes Anti-Ransomware následuje na druhém místě s bodovým skóre 7,896. AppCheck obsadil třetí

místo s bodovým součtem 7,176, zatímco Acronis Anti-Ransomware se umístil na čtvrtém místě s 7,118 body. Posledním programem v naší tabulce je CryptoPrevent s bodovým skóre 6,514.

Na základě těchto výsledků jsou doporučeny programy Kaspersky Anti-Ransomware Tool a MalwareBytes Anti-Ransomware jako hlavní volby pro ochranu proti ransomwaru. Ostatní programy, jako je AppCheck, Acronis Anti-Ransomware a CryptoPrevent, nevykazují dostatečnou spolehlivost a účinnost a není doporučeno jejich použití.

| *Pořadí* | *Nástroj pro obnovu dat* | *Vážený součet bodů* |
|---|---|---|
| *1.* | Kaspersky Rakhni Decryptor | 6,886 |
| *2.* | Seqrite Decryptor | 6,806 |
| *3.* | 360 Ransomware Decryption Tool | 5,499 |
| *4.* | Trend Micro Ransomware File Decryptor | 3,425 |
| *5.* | QuickHeal Decryption Tool | 3,077 |

*Tabulka 13 Výsledky nástrojů na obnovu dat*

Po porovnání jednotlivých nástrojů bylo zjištěno, že Kaspersky Rakhni Decryptor dosáhl nejvyššího hodnocení s bodovým ohodnocením 6,886. Seqrite Decryptor rovněž dosáhl podobně vysokého hodnocení, konkrétně 6,806 bodů. Nicméně, je nutné zdůraznit, že i přes tato vcelku vysoké hodnocení, tyto nástroje dokázaly obnovit maximálně 72 % ztracených dat, což je stále relativně malé procento. Nástroj 360 Ransomware Decryption Tool dosáhl bodového hodnocení 5,499 a umístil se tak na třetím místě, nicméně dokázal účinně obnovit přibližně pouze 9 % dat. Následující nástroje, Trend Micro Ransomware File Decryptor a QuickHeal Decryption Tool, nedosáhly žádné úspěšnosti při obnově dat, což významně ovlivnilo jejich bodové hodnocení.

Vzhledem k výsledkům doporučujeme zejména první dva nejlépe hodnocené nástroje pro obnovu dat, především Kaspersky Rakhni Decryptor, který dosáhl nejvyššího hodnocení. Tyto nástroje mají schopnost alespoň částečné obnovy dat po ransomwaru a dokáží tak alespoň nějakým způsobem minimalizovat jeho negativní dopady.

# 6. Diskuse

V bakalářské práci byli testovány antivirové programy, antiransomwarové programy a nástroje na obnovu dat za účelem posouzení jejich schopnosti detekovat a zastavit ransomware a obnovit data po útoku. Výsledky ukázaly, že antivirové programy jako Bitdefender Antivirus Plus, Avira a Avast Premium Security, antiransomwarové programy Kaspersky Anti-Ransomware Tool a MalwareBytes Anti-Ransomware a nástroje na obnovu dat Kaspersky Rakhni Decryptor či Seqrite Decryptor dosáhly vysoké úspěšnosti detekce a obnovy dat a byly tak doporučeny jako vhodná ochrana proti ransomwaru.

Nicméně, je třeba vzít v úvahu, že výsledky bakalářské práce se mohou lišit od jiných testů provedených jinými subjekty. Například, v testu prováděném webovým portálem testy-spotrebicu.cz bylo nejvyšší hodnocení uděleno antivirovým programům ESET Mobile Security a Avast Premium Security. Tato odlišná hodnocení mohou být způsobena různými metodologiemi testování, použitými testovacími scénáři nebo dokonce různými verzemi testovaného softwaru.

Hodnocení antiransomwarových programů se také liší, a to s žebříčkem uvedeném na webu geckoandfly.com. Například, podle hodnocení na webu se na prvním místě umístil MalwareBytes Anti-Ransomware, zatímco ve výsledcích práce se tento program umístil na druhém místě. Největší rozdíl v hodnoceních nastává v případě programu CryptoPrevent. Na webu geckoandfly.com se umístil na druhém místě, zatímco v naší studii se umístil na posledním.

I výsledky nástrojů na obnovu dat jsou odlišné. Hodnocení publikované na webu zenarmor.com uvádí, že na druhém místě se umístil Trend Micro Ransomware File Decryptor, zatímco výsledky bakalářské práce ho umisťují až na čtvrté místo. Zajímavé je také srovnání výsledků pro nástroj QuickHeal. Na webu zenarmor.com se tento nástroj umístil na posledním místě, což je shodné i s výsledky práce.

# 7. Závěr

Tato práce se zabývala problematikou ransomwaru a metodami prevence, detekce a obnovy dat po ransomwarových útocích. Na základě provedeného experimentu a vícekriteriální analýzy variant byly získány důležité poznatky o účinnosti různých bezpečnostních programů a nástrojů na obnovu dat.

V teoretické části byly shrnuty různé typy ransomwaru, mechanismy infiltrace a šíření, hlavní cíle a motivace útoků, prevence, principy detekce a obnovy dat. Tato teoretická východiska poskytla základní povědomí o ransomwaru a důležité strategie pro ochranu a obnovu dat.

Vlastní práce se zaměřila na testování antivirových, antiransomwarových programů a nástrojů pro obnovu dat. Na základě vícekriteriální analýzy variant byly vyhodnoceny nejlepší produkty pro ochranu a obnovu dat. Výsledky ukázaly, že některé programy a nástroje dosahují vysoké úrovně ochrany a spolehlivosti, zatímco jiné vykazují účinnost nižší.

Tato práce přináší hlubší porozumění problematice ransomwaru. Její výsledky a doporučení jsou cenným zdrojem informací pro uživatele i podniky, které hledají efektivní způsoby, jak chránit svá data.

# 8. Seznam použitých zdrojů

LISKA, Allan, 2016. Ransomware: Defending Against Digital Extortion. Oreilly Media. ISBN 9781491967881.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

What is Ransomware?, 2023. KnowBe4 [online]. Clearwater, Florida: KnowBe4 [cit. 2023-08-07]. Dostupné z: https://www.knowbe4.com/ransomware

DRAKE, Veronica, 2023. The History and Evolution of Ransomware Attacks. Flashpoint [online]. Washington: Flashpoint [cit. 2023-08-07]. Dostupné z: https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/

FAWKES, Guy, 2023. Historie ransomware hrozeb: jak to bylo, je a bude. VpnMentor [online]. vpnMentor [cit. 2023-08-07]. Dostupné z: https://cs.vpnmentor.com/blog/historie-ransomware-hrozeb-minulost-soucasnost-budoucnost/

THREAT INTEL REPORT: History of Ransomware, 2023. Kivu [online]. Berkeley: Kivu [cit. 2023-08-07]. Dostupné z: https://kivuconsulting.com/wp-content/uploads/2021/06/Kivu-Cyber-Report_The-History-of-Ransomware_May2020.pdf

HARFORD, Isabella, SHARON, Shea, ed., 2023. The history and evolution of ransomware. TechTarget [online]. New York: TechTarget [cit. 2023-08-08]. Dostupné z: https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware

Cyber threat bulletin: The ransomware threat in 2021, 2023. Government of Canada [online]. Canada: Government of Canada [cit. 2023-08-08]. Dostupné z: https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021

2023 SonicWall Cyber Threat Report, 2023. SonicWall [online]. Milpitas: SonicWall [cit. 2023-08-08]. Dostupné z: https://www.sonicwall.com/2023-cyber-threat-report/

CASH, Lauryn, 2023. How Does Ransomware Spread? Armorblox [online]. Sunnyvale: Armorblox [cit. 2023-08-09]. Dostupné z: https://www.armorblox.com/blog/how-does-ransomware-spread/

ANTAL, Gabriella, 2023. How Does Ransomware Spread? Here's What You Need to Know. Heimdal [online]. København: Heimdal [cit. 2023-08-09]. Dostupné z: https://heimdalsecurity.com/blog/how-ransomware-spreads/

BAKER, Kurt, 2023. HOW DOES RANSOMWARE SPREAD? 10 MOST COMMON INFECTION METHODS. Crowdstrike [online]. [cit. 2023-08-09]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/how-ransomware-spreads/

What is phishing?, 2023. IBM [online]. New York: IBM [cit. 2023-08-09]. Dostupné z: https://www.ibm.com/topics/phishing

Jak ochránit firmu před riziky spojenými s RDP?, 2023. Eset Digital Security Guide [online]. Praha: Eset [cit. 2023-08-09]. Dostupné z: https://digitalsecurityguide.eset.com/cz/jak-ochranit-firmu-pred-riziky-spojenymi-s-rdp

DIN, Antonia, 2022. What Is Malvertising? Heimdal [online]. København: Heimdal [cit. 2023-08-10]. Dostupné z: https://heimdalsecurity.com/blog/what-is-malvertising-and-how-to-protect/

What is an Exploit Kit?, 2023. Paloalto networks [online]. Kalifornie: Paloalto networks [cit. 2023-08-10]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

What is Ransomware?, 2023. Check Point [online]. Tel Aviv: Check Point [cit. 2023-08-10]. Dostupné z: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

POREMBA, Sue, 2023. Understanding the Progression of a Ransomware Attack. Security Boulevard [online]. Security Boulevard [cit. 2023-08-10]. Dostupné z:

https://securityboulevard.com/2023/05/understanding-the-progression-of-a-ransomware-attack/

MERTA, Michal, 2020. Jak útočí ransomware a jak snížit rizika napadení. System online [online]. Brno: System online [cit. 2023-08-10]. Dostupné z: https://m.systemonline.cz/it-security/jak-utoci-ransomware-a-jak-snizit-rizika-napadeni.htm

Unveiling the Psychology Behind Ransomware Attacks and How to Avoid Them, 2023. Vinca Cyber [online]. Bengalúru: Vinca Cyber [cit. 2023-08-11]. Dostupné z: https://www.vincacyber.com/unveiling-the-psychology-behind-ransomware-attacks-and-how-to-avoid-them/

LIVINGSTON, Zephin, 2022. Main Targets of Ransomware Attacks & What They Look For. ESecurity Planet [online]. Nashville: eSecurity Planet [cit. 2023-08-11]. Dostupné z: https://www.esecurityplanet.com/threats/what-ransomware-attackers-look-for/

CASAS, Pol, Jacobo BLANCAS a Alejandro VILLANUEVA, 2023. Ransomware Report 2023: targets, motives, and trends. Outpost24 [online]. Outpost24 [cit. 2023-08-11]. Dostupné z: https://outpost24.com/blog/ransomware-report-2023-targets-motives-and-trends/

ČERMÁK, Miroslav, 2023. Přečtěte si, co je to vektor útoku, zranitelnost, exploit a payload. Clever and smart [online]. Zálepy: clever and smart [cit. 2023-08-11]. Dostupné z: https://www.cleverandsmart.cz/prectete-si-co-je-to-vektor-utoku-zranitelnost-exploit-a-payload/

KRÁL, Mojmír, 2015. Bezpečný internet - Chraňte sebe i svůj počítač. Praha: Grada. ISBN 978-80-247-5453-6.

VULNERABILITY IDENTIFICATION, 2023. Ward Security Consulting Group [online]. [cit. 2023-09-22]. Dostupné z: https://warditsecurity.com/vulnerability-identification/

YACONO, Lauren, 2023. How To Identify Security Vulnerabilities: 5 Tips to Keep Your Network Secure. *Cimcor* [online]. 09.03.2023 [cit. 2023-09-22]. Dostupné z: https://www.cimcor.com/blog/5-ways-to-help-fix-security-vulnerabilities

CHIN, Kyle, 2023. How to Prevent Ransomware Attacks: Top 10 Best Practices in 2023. *UpGuard* [online]. 25.07.2023 [cit. 2023-09-22]. Dostupné z: https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks

Understanding Patches and Software Updates, 2023. *Cybersecurity and infrastructure security agency* [online]. [cit. 2023-09-22]. Dostupné z: https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates

Protecting Against Ransomware, 2019. *Cybersecurity and infrastructure security agency* [online]. 11.04.2019, 02.09.2021 [cit. 2023-09-22]. Dostupné z: https://www.cisa.gov/news-events/news/protecting-against-ransomware

7 Steps to Help Prevent & Limit the Impact of Ransomware, 2023. *Center for internet security* [online]. [cit. 2023-09-22]. Dostupné z: https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

Ransomware protection: How to keep your data safe in 2023, 2023. *Kaspersky* [online]. [cit. 2023-09-22]. Dostupné z: https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

BAKER, Kurt, 2023. How to Prevent Ransomware: 10 Pro Tips. *Crowdstrike* [online]. 30.01.2023 [cit. 2023-09-22]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/how-to-prevent-ransomware/

JOHNSON, Kyle, 2023. 3 ransomware detection techniques to catch an attack. *TechTarget* [online]. srpen 2023 [cit. 2023-09-22]. Dostupné z: https://www.techtarget.com/searchsecurity/feature/3-ransomware-detection-techniques-to-catch-an-attack

Protecting Against Ransomware, 2019. Cybersecurity and infrastructure security agency [online]. 11.04.2019, 02.09.2021 [cit. 2023-09-22]. Dostupné z: https://www.cisa.gov/news-events/news/protecting-against-ransomware

What is Ransomware Detection?, 2023. *Crowdstrike* [online]. [cit. 2023-09-22]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-detection/

RAIZZA, Amjad a Abdulmohsen ALGARNI, 2023. Ransomware Detection Using Machine Learning: A Survey. *MDPI* [online]. [cit. 2023-09-22]. Dostupné z: https://www.mdpi.com/2504-2289/7/3/143

YE, Yanfang, Dingding WANG, Tao LI a Dongyi YE, 2008. An intelligent PE-malware detection system based on association mining. *ReasearchGate* [online]. [cit. 2023-09-22]. Dostupné z: https://www.researchgate.net/publication/238420750_An_intelligent_PE-malware_detection_system_based_on_association_mining

ROSE, Scott, Oliver BOERCHERT, Stu MITCHELL a Sean CONELLY, 2020. Zero Trust Architecture. *National Institute of Standarts and Technology* [online]. [cit. 2023-09-22]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

MIXON, Erica, 2021. Why Antivirus Is Not Enough To Prevent Ransomware. BLUMIRA. Blumira.com [online]. [cit. 2024-03-03]. Dostupné z: https://www.blumira.com/does-antivirus-prevent-ransomware/

ZAMORA, Wendy, 2015. How does anti-malware work? MALWAREBYTES. Malwarebytes.com [online]. [cit. 2024-03-03]. Dostupné z: https://www.malwarebytes.com/blog/news/2015/12/how-does-anti-malware-work

SANDBU, Marius, 2023. *c*. Packt Publishing. ISBN 978-1-80324-634-5.

Osvojte si proaktivní zabezpečení s modelem nulové důvěry (Zero Trust), 2023. *Microsoft* [online]. [cit. 2023-09-22]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/zero-trust

Over half of ransomware victims pay the ransom, but only a quarter see their full data returned, 2021. *Kaspersky* [online]. 30.03.2021 [cit. 2023-09-22]. Dostupné z: https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned

BAZRAFSHAN, Zahra, Hashem HASHEMI, Seyed MEHDI HAZRATI FARD a Ali HAMZEH, 2013. A survey on heuristic malware detection techniques. *ReasearchGate* [online]. [cit. 2023-09-22]. Dostupné z: https://www.researchgate.net/publication/260729684_A_survey_on_heuristic_malware_detection_techniques

HASSAN, Nihad A. a Rami HIJAZI, 2019. Ransomware revealed. New York: Apress. ISBN 9781484242551.

JONES, Caitlin, 2022. How To Recover From A Ransomware Attack. Expert Insights [online]. 24.11.2022 [cit. 2023-09-22]. Dostupné z: https://expertinsights.com/insights/how-to-recover-from-a-ransomware-attack/

Ransomware Data Recovery: How to Save Your Data, 2023. *Cloudian* [online]. [cit. 2023-09-27]. Dostupné z: https://cloudian.com/guides/ransomware-backup/ransomware-data-recovery-5-ways-to-save-your-data/

Bitová kopie Windows od vytvoření po obnovu, 2022. *Levná PC* [online]. [cit. 2023-09-27]. Dostupné z: https://www.levnapc.cz/bitova-kopie-windows-od-vytvoreni-po-obnovu.html

BAKER, Kurt, 2023. Ransonware Recovery: 5 Steps To Recover Your Data. *Crowdstrike* [online]. [cit. 2023-09-27]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-recovery/

Spuštění Nástroje Obnovení systému, 2020. *Servis PC Kupka* [online]. [cit. 2023-09-27]. Dostupné z: http://servispckupka.cz/nastroj_obnoveni_systemu_windows_10.php#nastroj_obnoveni_systemu

Ransomware Data Recovery: How to Recover Files From an Attack, 2023. *DiskInternals* [online]. Jun 27, 2023 [cit. 2023-09-27]. Dostupné z: https://www.diskinternals.com/partition-recovery/recover-ransomware-encrypted-deleted-files/

ROUSE, Margaret, 2023. Decryption. *Techopedia* [online]. 8 September, 2023 [cit. 2023-09-27]. Dostupné z: https://www.techopedia.com/definition/1773/decryption

PETROWSKI, Thorsten a Tomáš KURKA, 2014. *Bezpečí na internetu pro všechny*. Liberec: Dialog. ISBN 978-80-7424-066-9.

HERMANS, Kris, 2023. Mastering Ransomware. Cybellium. ISBN 9798397868303.

NARULA, Jitender a Atul NARULA, 2023. Breaking Ransomware: Explore ways to find and exploit flaws in a ransomware attack. BPB Publications. ISBN 9355513623.

ROSENCRANCE, Linda, 2024. DEFINITION antivirus software (antivirus program). TECHTARGET. TechTarget [online]. [cit. 2024-03-03]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/antivirus-software

POONIA, Ravi, 2022. Malware analysis tutorial livello 3 Intermediate. HACKERHOOD. HackerHood [online]. [cit. 2024-03-15]. Dostupné z: https://hackerhood.redhotcyber.com/tutorial-di-malware-analysis-2/

# 9. Seznam obrázků, tabulek a zkratek

## 9.10 Seznam obrázků



## 9.11 Seznam tabulek

## 9.12 Seznam použitých zkratek

RAM – Random Access Memory
UI – User Interface
BIOS – Basic Input-Output System
UEFI – Unified Extensible Firmware Interface
RMM – Managed Service Provider
MSP – Remote Monitoring and Management
RDP – Remote Desktop Protocol
USB – Universal Serial Bus
URL – Uniform Resource Locator
SPF – Sender Policy Framewor
DKIM – DomainKeys Identified Mail
DMARC – Domain Message Authentication Reporting & Conformance
EPP – Endpoint Protection Platforms
EDR – Endpoint Detection and Respons
AI – Artificial Intelligence
ACL – Access Control List