Univerzita Pardubice

Fakulta ekonomicko-správní

Antivirová ochrana počítačů pro různé typy činností

Bakalářská práce

2025 Vladimír Machka

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Vladimír Machka**
Osobní číslo:	**E21794**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Antivirová ochrana počítačů pro různé typy činností**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je identifikovat cíle zneužití různými variantami virů ve třech vybraných typech využití počítače (např. programování, využívání webu, hraní her) a sestavit vhodná doporučení zabezpečení pro tyto cílové skupiny.

Osnova:

- Základní pojmy a definice.
- Specifikace modelových situací.
- Vypracování doporučení pro zabezpečení.
- Zhodnocení variant zabezpečení.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

Ethical hacking and countermeasures. Book 2 of 4, Threats and defense mechanisms. Second edition. Boston, MA: Cengage Learning, 2017. ISBN 978-1-305-88344-4.
JALŮVKA, Josef. Moderní počítačové viry: podstata, prevence, ochrana. 2., aktualiz. vyd. Praha: Computer Press, 2000. ISBN 80-7226-402-8.
KIM, Peter. Hacking: praktický průvodce penetračním testováním. Přeložil Jan POKORNÝ. Encyklopedie Zoner Press. Brno: Zoner Press, 2015. ISBN 978-80-7413-313-8.
KRÁL, Mojmír. Bezpečnost domácího počítače: prakticky a názorně. Průvodce. Praha: Grada, 2006. ISBN 80-247-1408-6.
SZOR, Peter. Počítačové viry: analýza útoku a obrana. Encyklopedie Zoner Press. Brno: Zoner Press, 2006. ISBN 80-86815-04-8.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2024**
Termín odevzdání bakalářské práce: **30. dubna 2025**

L.S.

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

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

V Pardubicích dne 1. září 2024

Prohlašuji:

Práci s názvem **Antivirová ochrana počítačů pro různé typy činností** jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

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

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

V Pardubicích dne 30. 4. 2025

Vladimír Machka v. r.

Poděkování:

Tímto bych rád poděkoval svému vedoucímu práce, RNDr. Ing. Oldřichu Horákovi, Ph.D., za jeho odbornou pomoc, cenné připomínky a rady, které mi významně pomohly při zpracování této bakalářské práce.

ANOTACE

Tato bakalářská práce se zaměřuje na problematiku antivirové ochrany v prostředí tří odlišných typů uživatelů: běžného uživatele, hráče počítačových her a programátora. Teoretická část popisuje základní druhy škodlivého softwaru a přehled antivirových programů. Praktická část obsahuje testování reálných scénářů, které simulují možné hrozby a vyhodnocují reakce antivirového systému. Výstupem práce je posoudit účinnost ochrany v různých uživatelských situacích a poukázat na limity běžně používaných bezpečnostních nástrojů.

KLÍČOVÁ SLOVA

antivirová ochrana, počítačové viry, kybernetická bezpečnost, běžný uživatel, hráč počítačových her, programátor, Windows Defender

TITLE

Computer Antivirus Protection for Various Types of User Activity

ANNOTATION

This bachelor's thesis focuses on the issue of antivirus protection in the context of three different types of users: a regular user, a computer game player, and a programmer. The theoretical part describes the main types of malicious software and provides an overview of antivirus programs. The practical part includes testing of real-life scenarios that simulate potential threats and evaluate the responses of the antivirus system. The outcome of the thesis is to assess the effectiveness of protection in various user situations and to highlight the limitations of commonly used security tools.

KEYWORDS

antivirus protection, computer viruses, cybersecurity, regular user, gamer, programmer, Windows Defender

OBSAH

Seznam obrázků

Seznam tabulek

Seznam zkratek

PUA	Potentially Unwanted Applications
SMS	Short message service
WAN	Wide Area Network
DDoS	Distributed denial-of-service
MS-DOS	Microsoft Disk Operating Systém
PC	Personal computer
APT	Advanced Persistent Threat
VPN	Virtual private network
EICAR	European Institute for Computer Antivirus Research

Úvod

Bezpečnost informací a ochrana počítačových systémů se v dnešní digitální době staly jedním z nejdiskutovanějších a nejvýznamnějších témat jak v odborné, tak i v laické veřejnosti. Vzhledem k tomu, že většina našich osobních i pracovních činností se přesouvá do digitálního prostoru, narůstá také množství dat, která jsou na našich zařízeních uchovávána – od důvěrné korespondence, přes bankovní přístupy až po pracovní dokumenty a osobní fotografie. Tato data jsou však neustále vystavena riziku útoků zvenčí, ať už formou klasických počítačových virů, ransomwaru, špionážního softwaru nebo stále častějších phishingových kampaní. Se zvyšující se technickou vyspělostí útočníků roste i potřeba vyspělých a důvěryhodných ochranných mechanismů, které budou schopny hrozby včas rozpoznat a účinně neutralizovat. Antivirové programy se v tomto směru staly nezbytnou součástí softwarové výbavy každého uživatele, avšak jejich efektivita se může lišit v závislosti na způsobu používání zařízení a celkovém chování uživatele při práci s internetem a softwarem.

Téma této bakalářské práce jsem si zvolil především kvůli osobní zkušenosti, která mi velmi jasně ukázala, jak snadné je stát se obětí digitálního útoku, i když člověk subjektivně nepovažuje své chování za rizikové. Během studia i osobního užívání počítače jsem se dostal do situace, kdy můj vlastní systém infikoval škodlivý kód. I když se nakonec nejednalo o vysoce destruktivní virus, došlo k poškození několika osobních souborů, zpomalení systému a nutnosti přeinstalace některých programů. Ztráta dat, především těch, která neměla zálohu, pro mě byla nepříjemným a zároveň poučným momentem. Právě tato zkušenost mě motivovala k hlubšímu zaměření na oblast antivirové ochrany a k přemýšlení o tom, jak odlišné mohou být bezpečnostní potřeby jednotlivých uživatelů. Někdo využívá počítač pouze ke čtení e-mailů a sledování zpráv, jiný k instalaci her z různých zdrojů a další třeba k vývoji softwaru – a každá z těchto činností s sebou nese jin bezpečnostní rizika a vyžaduje specifický přístup k ochraně systému.

Cílem této práce je identifikovat cíle zneužití různými variantami virů ve třech vybraných typech využití počítače (např. programování, využívání webu, hraná her) a sestavit vhodná doporučení zabezpečení pro tyto cílové skupiny.

1 Základní pojmy a definice

V této kapitole budou nejprve vysvětleny základní pojmy související s počítačovou bezpečností, se zaměřením na různé typy škodlivého softwaru (malwaru) a jejich charakteristiky. Následně budou představeny i hlavní druhy antivirových programů, jejich funkce a způsoby, jakými chrání uživatele před kybernetickými hrozbami.

1.1 Úvod do problemtiky počítačových virů

Počítačové viry jsou jedním z nejdéle známých a zároveň nejrozšířenějších typů škodlivého softwaru (malwaru), který představuje významné riziko pro informační bezpečnost. Od svého vzniku v 80. letech 20. století prošly viry výrazným vývojem – od jednoduchých programů schopných pouze zobrazit zprávu na obrazovce až po sofistikované a cílené útoky s cílem poškodit systém, odcizit data nebo ovládnout zařízení bez vědomí uživatele. Z hlediska bezpečnosti je porozumění fungování a šíření počítačových virů klíčové pro návrh efektivních obranných opatření a prevenci kybernetických hrozeb. (MICROSOFT Security documentation, 2025; NATIONAL INSTITUTE OF STANDARTS AND TCHNOLOGY,2025)

Pojem „počítačový virus“ byl inspirován biologickými viry, jelikož se podobně jako ty biologické šíří mezi hostitelskými systémy a potřebují nositele – infikovaný soubor, médium či připojení – k tomu, aby se mohly dále šířit. Základní vlastností počítačového viru je schopnost sebereplikace, tedy schopnost kopírovat svůj kód do jiných souborů nebo částí systému. Tímto způsobem se mohou viry šířit mezi počítači, často zcela nepozorovaně. (MICROSOFT Security documentation, 2025; NATIONAL INSTITUTE OF STANDARTS AND TCHNOLOGY,2025)

V současnosti se pojem virus často používá jako obecné označení pro všechny typy malwaru, přestože se jedná o jednu konkrétní podkategorii. Moderní hrozby jsou rozmanité a zahrnují červy, trojské koně, ransomware, spyware a mnoho dalších forem škodlivého softwaru. Přesto je studium počítačových virů i nadále relevantní, neboť právě tyto útoky bývají často součástí větších škodlivých kampaní a kombinují se s dalšími typy útoků, čímž zvyšují svou účinnost a nebezpečnost. (MICROSOFT Security documentation, 2025; NATIONAL INSTITUTE OF STANDARTS AND TCHNOLOGY,2025)

Důsledky infekce virem mohou být velmi vážné – od zpomalení nebo zhroucení systému přes ztrátu dat až po zneužití osobních údajů nebo úplné převzetí kontroly nad zařízeními. Obzvláště

zranitelné jsou systémy bez pravidelných aktualizací, bez antivirové ochrany a s nedostatečně poučenými uživateli. Vzhledem k rostoucímu počtu útoků i škod způsobených viry je klíčové nejen využívat moderní bezpečnostní nástroje, ale také vzdělávat uživatele v oblasti digitální bezpečnosti. (MICROSOFT Security documentation, 2025; NATIONAL INSTITUTE OF STANDARTS AND TCHNOLOGY,2025)

Tato kapitola se dále bude věnovat přehledu hlavních druhů počítačových virů, jejich mechanismům šíření a způsobům, jakými mohou ovlivnit fungování systémů. (MICROSOFT Security documentation, 2025; NATIONAL INSTITUTE OF STANDARTS AND TCHNOLOGY,2025)

1.2 Druhy virů

Počítačové viry a obecně škodlivý software lze rozdělit do několika kategorií podle jejich chování, způsobu šíření a cíle útoku. Toto rozdělení je důležité pro pochopení strategie obrany proti jednotlivým hrozbám a pro výběr vhodných bezpečnostních opatření. Níže jsou uvedeny nejčastější typy malwaru. (MICROSOFT Security documentation, 2025)

1.2.1 Malware

Malware je považován za jakýkoli typ škodlivého softwaru, který je navržen k infikování počítačů nebo mobilních zařízení. Malware je používán hackery z různých důvodů, jako je získávání osobních údajů či hesel, krádeže peněz nebo blokování přístupu k zařízení. Před malwarem lze být chráněn pomocí antimalwarového softwaru. Malware, což je zkratka anglického výrazu „malicious software“, je typem škodlivého softwaru, jehož účelem je zajistit útočníkovi tajný přístup k zařízení. Do kategorie malwaru jsou zahrnuty typy jako spyware, adware, phishing, viry, trojské koně, červy, rootkity, ransomware a změny nastavení prohlížeče. (KRÁL, 2010; SZOR, 2005)

1.2.2 Počítačový virus

Počítačový virus je definován jako program, který je schopen infikovat jiný program tím, že do něj zkopíruje svou vlastní strukturu, čímž se infikovaný program stává prostředkem pro další šíření viru. Počítačový program je sled instrukcí procesoru, který je schopen vykonávat pouze to, k čemu byl naprogramován svým tvůrcem. Počítačový virus je však specifický tím, že potřebuje hostitele k tomu, aby mohl fungovat, podobně jako biologické viry. Dalším specifikem je, že čím je virus menší, tím je nenápadnější. Velikost virů se pohybuje od několika desítek bajtů po desítky kilobajtů. Je obecně známo, že počítačové viry jsou vždy vytvořeny

pro konkrétní typ operačního systému. Univerzální virus neexistuje. (JALŮVKA, 2000; KRÁL, 2010)

1.2.3 Trojský kůň

Trojský kůň je typ malwaru, který se maskuje jako legitimní software s cílem proniknout do systému uživatele. Obvykle se vydává za užitečnou aplikaci, která je stažena z nedůvěryhodného zdroje, jako jsou e-mailové přílohy nebo podezřelé webové stránky. (JALŮVKA, 2000; EC-COUNCIL, 2017; SZOR, 2005)

Po instalaci je útočníkovi poskytnut neautorizovaný přístup k zařízení, což může zahrnovat vzdálené ovládání, krádež citlivých informací nebo instalaci dalších škodlivých programů. Trojský kůň může provádět různé škodlivé akce, jako je monitorování aktivit uživatele, shromažďování přihlašovacích údajů nebo manipulace s uloženými daty. Vzhledem k tomu, že trojan často skrývá svou aktivitu mezi legitimními procesy a soubory, může být obtížné ho odhalit. (JALŮVKA, 2000; EC-COUNCIL, 2017; SZOR, 2005)

Identifikace trojského koně zahrnuje pravidelnou kontrolu systému aktuálním antivirovým softwarem a sledování neobvyklého chování, jako je zpomalení výkonu nebo podezřelé síťové aktivity. K detekci mohou být použity i specializované nástroje pro analýzu chování, které monitorují neobvyklé vzorce v síťové komunikaci nebo v souborových systémech. (JALŮVKA, 2000; EC-COUNCIL, 2017; SZOR, 2005)

1.2.4 Keylogger

Keylogger (klávesoví špióni) je typ škodlivého softwaru, jehož hlavním cílem je zaznamenávat stisky klávesna klávesnici infikovaného zařízení. Tento malware je navržen k tajnému sledování a shromažďování informací zadávaných uživateli, jako jsou text, přihlašovací údaje a hesla. Keylogger se obvykle dostává do systému prostřednictvím phishingových útoků nebo instalace nelegitimního softwaru a může využívat zranitelnosti v operačním systému nebo aplikacích. Jakmile je keylogger nainstalován, skrývá se, aby se vyhnul detekci. Může se maskovat pod neškodnými názvy souborů nebo se integrovat do legitimních aplikací. Jeho hlavní funkcí je zaznamenávat všechny stisky kláves, včetně textového vstupu a klávesových zkratek. Shromážděná data mohou být ukládána na místní disk nebo odesílána na vzdálený server. Keylogger může pravidelně synchronizovat data a přijímat příkazy od útočníka, což může zahrnovat aktualizace nebo instalaci dalšího malwaru. Přítomnost keyloggeru může ovlivnit výkon systému a vyvolat neobvyklé chování, což může signalizovat jeho přítomnost. (KRÁL, 2010; JALŮVKA, 2000; SZOR, 2005)

1.2.5 Ransomware

Ransomware je druh malwaru, který šifruje soubory na infikovaném zařízení a požaduje výkupné za jejich dešifrování. Obvykle vstupuje do systému prostřednictvím phishingových e-mailů s infikovanými přílohami nebo odkazy, stahováním škodlivého softwaru z nedůvěryhodných webových stránek, nebo zranitelností v operačním systému či aplikacích. Po aktivaci ransomware šifruje důležité soubory a zobrazuje výkupní zprávu s instrukcemi, jak zaplatit výkupné. Identifikace ransomware zahrnuje používání aktuálního antivirového a antimalwarového software a sledování neobvyklého chování systému, jako jsou změny v dostupnosti souborů nebo nové soubory s rozšířením souvisejícím s výkupným. (EC-COUNCIL, 2017)

1.2.6 Adware

Adware je typ malwaru, který narušuje uživatelský zážitek tím, že zobrazuje nechtěné reklamy a bannerové reklamy, čímž zpomaluje výkon počítače. Tento malware obvykle vstupuje do systému prostřednictvím softwaru staženého z nedůvěryhodných zdrojů nebo cracknutých verzí programů. Po instalaci adware začíná zobrazovat reklamy, vyskakovací okna a přesměrování na reklamní webové stránky, což výrazně narušuje pracovní a herní zážitek. Identifikace adware zahrnuje sledování neobvyklého nárůstu reklam, častých vyskakovacích oken a sníženého výkonu počítače. (SZOR, 2005; KRÁL, 2010)

1.2.7 Spyware

Spyware se chová jako tajný monitorovací nástroj zaměřený na shromažďování citlivých informací o uživatelských aktivitách bez jejich vědomí. Infikuje zařízení prostřednictvím neověřených webových stránek, pirátských verzí softwaru nebo phishingových e-mailů. Po instalaci spyware tajně sbírá přihlašovací údaje, osobní a finanční informace, které mohou být zneužity. Identifikace zahrnuje sledování zpomalení výkonu, neobvyklé síťové aktivity a neznámé procesy běžící na pozadí. (SZOR, 2005; KRÁL, 2010)

1.2.8 Počítačoví červi

Počítačový červ, nazývaný anglicky "worm", je program, který na rozdíl od virů neinfikuje spustitelné soubory, ale infikuje systémy šířením kopií sebe sama pomocí počítačové sítě na připojené počítače. Tento způsob šíření způsobuje problémy, zejména neúměrným zatížením sítě a zahlcením diskového prostoru připojených počítačových stanic. Nejznámější případ červa pochází z listopadu 1988, kdy internetový červ infikoval během dvou dnů asi 6 000 počítačů

pracujících pod operačním systémem Unix. Hlavním rozdílem mezi virem a červem je skutečnost, že červ nepotřebuje ke své existenci žádného nositele. Zatímco počítačové viry jsou typicky spojovány s platformou operačního systému MS-DOS, červi se vyskytují především v rozlehlých sítích WAN a platformě internetového protokolu TCP/IP. V mnoha uživatelských operačních systémech nemají červi logické opodstatnění. Rozvoj internetu přinesl nový způsob šíření červů prostřednictvím elektronické pošty. Moderní definice červa zní: jedná se o program, který se šíří prostřednictvím e-mailové zprávy, ke které je připojen ve formě souboru. Častou podobou červů jsou skripty. (JALŮVKA, 2000; EC-COUNCIL, 2017)

1.2.9 Logické bomby

Logická bomba je termín používaný pro naprogramovanou chybu v běžném programu. Program může být navržen tak, aby se po určitém počtu spuštění smazal z disku jako součást ochrany proti kopírování, nebo aby po kopírování vykonal další škodlivý kód. Tyto scénáře jsou realistické v případech větších projektů s omezeným počtem revizí kódu. Populární hra Mosquitos, známá z mobilních telefonů Nokia série 30, je typickým příkladem výskytu logické bomby v praxi. Tato hra obsahovala funkci, která posílala SMS zprávy na zpoplatněné linky. Kód logické bomby je často skryt mezi zdrojovými kódy programu – takto skrytý zůstává aktivní. Častým příkladem skrytého kódu, který se dostane i do největších softwarových projektů, jsou takzvaná "velikonoční vajíčka". Programátoři je vytvářejí, aby uvedli údaje o všech členech týmu pracujícím na vývoji projektu. (JALŮVKA, 2000; SZOR, 2005)

Tabulka 1: Přehled typů škodlivého softwaru.

Typ malwaru	Způsob šíření	Hlavní účel/hrozba	Typické dopady na systém
Počítačový virus	Infikované soubory, e-mailové přílohy, výměnné disky	Samoreplikace, poškozování dat, šíření do dalších systémů	Zpomalení systému, ztráta dat, nestabilita
Počítačový červ	Síťová zranitelnost, e-maily, automatické šíření bez zásahu uživatel	Masové šíření po síti bez hostitelského souboru	Zatížení sítě, zahlcení systémových zdrojů
Trojský kůň	Skrytý v legitimním softwaru, přílohy e-mailů, download z neznámých zdrojů	Získání přístupu k systému, instalace dalšího malwaru	Únik dat, otevření zadních vrátek (backdoor), zpomalení PC
Spyware	Instalace spolu s freeware/shareware, skripty z webových stránek	Špehování aktivity uživatele, sběr osobních dat	Únik soukromí, cílená reklama, zpomalení systému
Adware	Instalace se softwarem, některé nechtěné aplikace	Zobrazování reklam, přesměrování webového provozu	Otravné reklamy, zpomalení systému
Keylogger	Infikované přílohy, trojské koně	Zaznamenávání stisknutých kláves, krádež přihlašovacích údajů	Krádež identity, neoprávněný přístup k účtům
Ransomware	Phishingové e-maily, exploitace zranitelností systému	Šifrování souborů a vydírání uživatele za dešifrovací klíč	Nedostupnost dat, finanční ztráty
Logická bomba	Skrytá v legitimním softwaru, aktivace při určité události	Sabotáž systému v předem daný čas nebo po určité akci	Náhlé smazání dat, poškození systému

Zdroj: vlastní zpracování

2 Antivirové programy

Antivirové programy představují základní prvek zabezpečení výpočetní techniky, jejichž úkolem je detekce, blokace a případné odstranění škodlivého softwaru, který může ohrozit integritu systému, citlivost dat nebo celkovou bezpečnost uživatele. S rozvojem internetu a nárůstem počtu připojených zařízení roste také množství hrozeb, které jsou na uživatele cíleny – od klasických počítačových virů přes trojské koně, ransomware až po pokročilé perzistentní hrozby (APT). Antivirové řešení se proto musí přizpůsobovat dynamicky se měnícímu prostředí, ve kterém působí, a to jak z hlediska rychlosti reakce na nové typy útoků, tak i v oblasti komplexnosti ochrany. (KASPERSKY, 2023)

Moderní antivirové programy se již dávno nesoustředí pouze na klasické skenování souborů – jejich funkce zahrnují behaviorální analýzu, monitorování síťové komunikace, ochranu proti phishingu, kontrolu e-mailových příloh a často také sandboxing podezřelých souborů. Většina známých antivirových řešení dnes využívá i cloudové databáze hrozeb a technologii strojového učení pro rychlejší identifikaci dosud neznámých vzorků malwaru. Díky těmto pokročilým nástrojům dokáže antivirový software efektivně čelit jak známým, tak i dosud neobjeveným hrozbám. (KASPERSKY, 2023)

Antivirové programy se staly nedílnou součástí operačních systémů – příkladem je Windows Defender, který je předinstalovaný v systémech Windows a zajišťuje základní úroveň ochrany ihned po instalaci systému. Vedle něj však existuje široká škála komerčních i bezplatných produktů, z nichž každý nabízí různou úroveň zabezpečení, výkonu a uživatelského komfortu. Při výběru konkrétního řešení je třeba zohlednit nejen technické parametry a rozsah funkcí, ale také individuální potřeby uživatele, včetně jeho typického chování při práci s počítačem. (KASPERSKY, 2023)

2.1.1 Microsoft Defender

Microsoft Defender, známý také jako Windows Defender, je integrovaný antivirový nástroj, který je součástí operačního systému Windows. Tento software nabízí širokou škálu funkcí pro ochranu před různými typy kybernetických hrozeb, jako jsou viry, malware, ransomware a další formy škodlivého softwaru. Je navržen tak, aby automaticky detekoval a eliminoval hrozby v reálném čase, čímž pomáhá chránit data a soukromí uživatele. Program je pravidelně

aktualizován, aby udržel krok s novými a vysoce sofistikovanými hrozbami. (MICROSOFT Zabezpečení Windows, 2025; KIM, 2015)

Mezi hlavní výhody Microsoft Defenderu patří jeho snadná integrace s operačním systémem Windows, což znamená, že uživatelé mají k dispozici spolehlivou ochranu bez nutnosti instalovat externí antivirové programy. Funkce jako ochrana při surfování na internetu, šifrování souborů a monitorování aktivit v reálném čase zajišťují, že program chrání zařízení nejen proti běžným hrozbám, ale také proti novým, vysoce cíleným útokům. Dalšími funkcemi jsou ochrana proti phishingu, přítomnost firewallu, a detekce neobvyklých aktivit na zařízeních. (MICROSOFT Zabezpečení Windows, 2025; KIM, 2015)

Pro domácí uživatele Windows je Microsoft Defender ideálním řešením pro základní úroveň ochrany. V případě složitějších požadavků nebo u firemního nasazení je doporučeno přejít na verzi Microsoft Defender for Endpoint, která nabízí pokročilou detekci hrozeb, centralizované řízení bezpečnosti a reakci na incidenty. Tato verze je určená pro organizace, které potřebují pokročilé nástroje pro ochranu citlivých dat a správu zařízení ve větším měřítku. (MICROSOFT Zabezpečení Windows, 2025; KIM, 2015)

Microsoft Defender má oproti jiným antivirovým programům také výhodu v tom, že je pravidelně aktualizován bez nutnosti zásahů ze strany uživatele. Tyto aktualizace zajišťují, že program poskytuje účinnou ochranu proti novým formám malware, které se objevují na internetu. Vzhledem k tomu, že je součástí operačního systému, je také optimalizován pro výkon a minimální zásah do uživatelského prostředí, což přispívá k hladkému chodu systému. Pro firmy a pokročilé uživatele, kteří potřebují větší kontrolu nad bezpečností, je k dispozici více funkcí v rámci rozšířené verze Defenderu. (MICROSOFT Zabezpečení Windows, 2025; KIM, 2015)

2.1.2 Kaspersky

Kaspersky je vysoce ceněný antivirový software, který poskytuje komplexní ochranu proti širokému spektru kybernetických hrozeb, včetně virů, ransomware, phishingu a spywaru. Kaspersky nabízí jak základní antivirovou ochranu, tak pokročilé funkce, jako je ochrana v reálném čase, VPN pro zajištění bezpečné internetové komunikace, správce hesel a nástroje pro detekci malwaru. Tento software je kompatibilní s operačními systémy Windows, macOS, Android a iOS, což zajišťuje širokou dostupnost pro domácí i firemní uživatele. (KASPERSKY Antivirová ochrana a kybernetická bezpečnost, 2025)

Kaspersky je pravidelně aktualizován a využívá pokročilé cloudové technologie pro detekci nových hrozeb a optimalizaci ochrany před neustále se vyvíjejícími kybernetickými útoky. Jeho antivirová ochrana je doplněna o funkce, které chrání před phishingovými útoky, blokují nebezpečné webové stránky a monitorují síťovou komunikaci, což zajišťuje ucelenou ochranu na všech frontách. Dále nabízí různé úrovně zabezpečení, přičemž pokročilí uživatelé mohou mít přístup k detailním nastavením pro přizpůsobení ochrany svým konkrétním potřebám. Kaspersky nadále zůstává jedním z nejdůvěryhodnějších antivirových programů na trhu. (KASPERSKY Antivirová ochrana a kybernetická bezpečnost, 2025)

2.1.3 AVAST

Avast je renomovaný antivirový program, který poskytuje širokou škálu funkcí pro ochranu před kybernetickými hrozbami. Tento software zahrnuje nástroje pro detekci a odstranění malwaru, ochranu před ransomwarem, ochranu soukromí, VPN, správce hesel a další bezpečnostní funkce. Avast je navržen pro ochranu zařízení se systémy Windows, macOS, Android a iOS. Je známý svou schopností detekovat nejen známý malware, ale i novější a neznámé hrozby díky pokročilým metodám analýzy a strojového učení. (AVAST, 2025)

Program je dostupný v různých verzích, které vyhovují potřebám jednotlivců i firemních uživatelů. Avast Free Antivirus poskytuje základní ochranu, zatímco Avast Premium Security nabízí pokročilejší funkce, včetně ochrany před ransomwarem, šifrování souborů a firewallem. Avast Business Security se zaměřuje na poskytování komplexní ochrany pro firemní prostředí, zahrnující nástroje pro správu více zařízení a ochranu citlivých dat. (AVAST, 2025)

Významným prvkem Avast je jeho pravidelná aktualizace databáze hrozeb, což zajišťuje aktuálnost ochrany před novými a vysoce sofistikovanými kybernetickými útoky. Avast rovněž využívá cloudové technologie k detekci nových hrozeb v reálném čase a nabízí různé přizpůsobitelné možnosti ochrany, které vyhovují specifickým potřebám uživatelů. (AVAST, 2025)

2.1.4 ESET

ESET nabízí různé produkty, které jsou zaměřeny nejen na ochranu před tradičními hrozbami, ale i na prevenci proti moderním typům malwaru, jako je ransomware, phishing nebo DDoS útoky. Program využívá pokročilou detekci na bázi strojového učení, což mu umožňuje identifikovat i dosud neznámé hrozby. Pro zajištění maximální bezpečnosti je ESET vybaven funkcí pro ochranu před škodlivým softwarem při online bankovnictví a nakupování. ESET

také pravidelně aktualizuje své databáze a algoritmy, aby uživatelům poskytoval aktuální ochranu proti novým hrozbám. (ESET, 2025)

Pro firemní uživatele ESET poskytuje nástroje pro centrální správu bezpečnosti na více zařízeních. Díky tomu mohou administrátoři snadno monitorovat a spravovat antivirovou ochranu napříč celou organizací. K dispozici je také podpora pro vzdálenou správu a ochranu zařízení napříč různými platformami, včetně Windows, macOS, Android a Linux. ESET zároveň umožňuje implementaci pokročilých analytických nástrojů pro odhalování a reakci na bezpečnostní incidenty. (ESET, 2025)

Díky těmto funkcím je ESET doporučován pro domácí uživatele, malé a střední firmy, ale i pro velké organizace, které potřebují komplexní a flexibilní řešení pro ochranu všech svých zařízení. (ESET, 2025)

2.1.5 AVG

AVG je populární antivirový program, který poskytuje komplexní ochranu pro domácí uživatele i malé firmy. Je známý svou schopností detekovat a chránit před širokým spektrem hrozeb, včetně virů, malwaru, spyware, ransomware a phishingu. AVG využívá moderní technologie detekce, které zahrnují analýzu chování souborů a programů, což mu umožňuje rozpoznat i nové, dosud neznámé hrozby. Jeho ochrana v reálném čase je klíčová pro bezpečnost uživatele, protože monitoruje veškeré aktivity na zařízení a okamžitě zasáhne při podezřelé aktivitě. (AVG TECHNOLOGIES, 2025)

Kromě standardní antivirové ochrany AVG poskytuje také další nástroje, které zlepšují celkovou bezpečnost a výkon zařízení. Program obsahuje funkce pro ochranu soukromí online, jako je zabezpečení Wi-Fi připojení a blokování nebezpečných webových stránek, které by mohly obsahovat malware nebo phishingové pokusy. AVG rovněž nabízí nástroje pro správu hesel, což umožňuje bezpečné ukládání a generování silných hesel, které zajišťují lepší ochranu účtů uživatelů. Mezi další funkce patří optimalizace výkonu systému a odstranění nepotřebných souborů pro zlepšení rychlosti a efektivity zařízení. (AVG TECHNOLOGIES, 2025)

AVG je k dispozici ve dvou hlavních verzích: bezplatná verze, která nabízí základní ochranu, a plně funkční verze s pokročilými funkcemi, jako je VPN pro šifrování internetového připojení a rozšířená ochrana před ransomwarem. Tento antivirový program je kompatibilní s operačními systémy Windows, macOS, Android a iOS, což znamená, že může být používán na široké škále zařízení, od počítačů po mobilní telefony. Díky pravidelným aktualizacím a neustálému

vylepšování je AVG silným nástrojem pro ochranu před novými hrozbami a zajištění bezpečnosti online aktivit. (AVG TECHNOLOGIES, 2025)

Tabulka 2: Srovnání antivirových programů.

Antivirový program	Výrobce	Typ licence	Funkce ochrany	Zátěž systému	Výhody
ESET NOD32 Antivirus	ESET (Slovensko)	Placená, zkušební verze	Ochrana v reálném čase, antispyware, anti-phishing	Nízká	Rychlý, nenáročný, vhodný pro hráče i běžné uživatele
AVG Antivirus Free	Avast Software	Zdarma (Free), placená	Reálný čas, webová ochrana, e-mailový štít	Střední	Dobrá základní ochrana, jednoduché rozhraní
Avast Free Antivirus	Avast Software	Zdarma (Free), placená	Behaviorální analýza, sandbox, síťová kontrola	Střední	Bohatá výbava i v bezplatné verzi
Kaspersky Anti-Virus	Kaspersky Lab	Placená, zkušební verze	Ochrana proti virům, spyware, ransomware	Nízká až střední	Vysoká úspěšnost detekce, uživatelsky přívětivý
Microsoft Defender	Microsoft (USA)	Zdarma (integrován)	Integrovaná ochrana, cloudová analýza, firewall, reputační analýza	Nízká	Bez nutnosti instalace, solidní ochrana zdarma

Zdroj: vlastní zpracování

3 Scénáře

3.1 Úvod ke scénářům testování

V předchozí teoretické části této práce byla podrobně analyzována problematika antivirové ochrany, včetně principů fungování antivirových programů, jednotlivých druhů hrozeb, kterým může být uživatel vystaven, a specifik zabezpečení různých typů uživatelů. Teoretický základ položil důležité poznatky, které jsou nezbytné pro správné pochopení významu antivirové ochrany v dnešním digitálním světě.

S ohledem na tyto teoretické poznatky je nyní cílem praktické části práce ověřit účinnost antivirové ochrany v reálných podmínkách. Praktická část je zaměřena na tři odlišné typy uživatelů – běžného uživatele počítače, hráče počítačových her a programátora. Každý z těchto uživatelů má specifické návyky, potřeby i rizika, která se odrážejí v jejich způsobu používání počítače, a tím i v požadavcích na úroveň a typ antivirové ochrany. Tato praktická simulace umožní získat lepší představu o tom, jak různé bezpečnostní nástroje reagují na typické hrozby, se kterými se jednotlivé skupiny mohou setkat.

V rámci praktického testování bylo využito simulovaných scénářů, které odpovídají reálnému chování uživatelů a potenciálním rizikům. Testování bylo provedeno přímo na fyzickém zařízení, bez použití virtuálního prostředí, aby byly výsledky co nejvíce autentické a odpovídaly skutečným podmínkám. Každý scénář byl navržen tak, aby prověřil schopnost antivirového systému detekovat a neutralizovat různé typy hrozeb, ať už se jedná o stažení škodlivého souboru, instalaci potenciálně nežádoucí aplikace, pokus o spuštění neověřeného softwaru nebo simulaci vlastní tvorby potenciálně škodlivého kódu.

Důraz byl kladen nejen na samotné výsledky detekce, ale také na komfort uživatele během zásahu antivirového programu, na míru informovanosti o hrozbě a na schopnost antivirové ochrany správně reagovat bez nutnosti složitých uživatelských zásahů. Zvláštní pozornost byla věnována i situacím, kdy ochrana selhala nebo nebyla dostatečně efektivní, což umožňuje identifikovat slabá místa v zabezpečení a formulovat doporučení pro zlepšení.

Všechny testy byly provedeny v souladu s předem stanovenou metodikou, aby bylo možné jednotlivé výsledky porovnat a vyhodnotit objektivně. Praktická část tak nejen ověří poznatky získané v teoretické části, ale zároveň přinese cenné informace o skutečné funkčnosti antivirové ochrany v prostředí různých typů uživatelů.

3.2 Testování scénářů

V rámci praktické části této bakalářské práce byla provedena série testů, které měly za cíl simulovat reálné situace, se kterými se mohou setkat různé typy uživatelů počítačů – od běžných uživatelů, přes hráče počítačových her až po programátory a technicky pokročilé uživatele. Tyto modelové scénáře byly navrženy tak, aby co nejvíce odpovídaly běžnému chování daných uživatelů a současně odhalily silné a slabé stránky antivirové ochrany v prostředí systému Windows 10 s aktivním řešením Microsoft Defender.

Zvolená metoda testování kombinuje simulace skutečných hrozeb s využitím testovacích nástrojů a bezpečných skriptů, které nereprezentují reálné útoky, ale napodobují jejich chování. Takový přístup je bezpečný, přesto dostatečně názorný pro zhodnocení účinnosti antivirové ochrany. Všechny testy byly prováděny na fyzickém zařízení mimo virtuální prostředí, čímž se maximalizovala věrohodnost podmínek, za nichž běžní uživatelé pracují.

3.3 Metodika

Každý scénář byl navržen pro konkrétní typ uživatele a obsahoval čtyři jednotlivé testy, které reprezentují různé úrovně rizik a hrozeb. Uživatelé byli zastoupeni následujícími kategoriemi:

Běžný uživatel PC – minimální technické znalosti, běžná každodenní práce.

Hráč počítačových her – orientace na výkon, instalace z neoficiálních zdrojů, občasné obcházení licencí.

Programátor – pokročilá práce se skripty, testování kódu, používání externích nástrojů.

Pro každý scénář byly sledovány tyto aspekty: reakce antivirového systému, možnosti zásahu uživatele, reálné dopady na systém, ochrana bez nutnosti zásahu uživatele a zajištění aktuálnosti zabezpečení.

Testování probíhalo na zařízení s operačním systémem Windows 10 Pro, s aktuálními aktualizacemi a zapnutým a aktualizovaným řešením Microsoft Defender. V žádném případě nebyly používány skutečně škodlivé kódy, pouze simulace a testovací nástroje.

3.4 Modelový scénář 1 – Běžný uživatel internetu

První modelový scénář je zaměřen na běžného uživatele, který využívá počítač primárně k prohlížení webových stránek, práci s e-mailem, sledování videí, online nakupování

a využívání cloudových služeb. Tento typ uživatele patří mezi nejčastější a zároveň nejzranitelnější skupinu, neboť při běžném procházení internetu dochází k interakci s velkým množstvím dat, webových domén a často i s podvodnými nebo neověřenými zdroji informací.

V rámci plánované simulace bude testováno, jak antivirový software reaguje na nejběžnější bezpečnostní rizika spojená s webovým prostředím. Součástí simulace bude například pokus o přístup na známé phishingové nebo podvodné weby (blokované např. Googlem či ESETem), stažení infikovaného e-mailového přílohového souboru (např. makro dokumentu v Excelu nebo Wordu) nebo interakce s falešnými reklamními bannery. Bude rovněž zkoumáno, jak se antivir a prohlížeč chovají v situaci, kdy uživatel nevědomky stáhne zavádějící instalační soubor, který může obsahovat nežádoucí doplňky, adware nebo spyware.

Cílem této simulace je zjistit, zda bezpečnostní software dokáže těmto útokům předejít a jakým způsobem informuje uživatele o případném riziku. Současně bude sledováno, jak dobře je uživatel chráněn i v případě, že používá pouze základní ochranu (např. Windows Defender bez rozšíření), a nakolik může situaci zlepšit použití pokročilých nástrojů – například rozšíření do prohlížeče, VPN nebo filtrování obsahu.

Výsledky této části pomohou stanovit srozumitelná a efektivní doporučení pro běžné uživatele internetu, kteří chtějí zvýšit svoji digitální bezpečnost, aniž by museli investovat do složitých nebo nákladných řešení.

3.5 Modelový scénář 2 – Hráč počítačových her

Druhý modelový scénář je zaměřen na uživatele, kteří počítač využívají převážně k hraní her. Tato uživatelská skupina se často pohybuje v prostředí, kde dochází ke stahování herních souborů, aktualizací, modifikací (modů), a v některých případech i nelegálních kopií her (tzv. cracků). Z hlediska bezpečnosti se jedná o rizikovou činnost, neboť spustitelné soubory (.exe, .dll aj.), které pocházejí z neoficiálních nebo neověřených zdrojů, bývají častým nositelem škodlivého kódu.

V rámci plánované simulace bude analyzována typická situace, kdy hráč stáhne instalační balíček herního obsahu z neoficiálního webu. Bude sledováno, jakým způsobem na tento zásah zareaguje antivirový systém – zda bude soubor ihned blokován, detekován jako potenciálně nebezpečný, nebo zda bude umožněno jeho spuštění bez upozornění. Dále bude zkoumáno, zda je antivir schopen identifikovat tzv. trojské koně, které se mohou maskovat jako herní utility,

cheaty nebo pomocné nástroje, a zároveň bude ověřena schopnost detekce méně závažného, avšak rušivého adwaru, který bývá distribuován formou tzv. bundle softwaru.

Součástí simulace bude rovněž testování tzv. herních režimů antivirových programů – tedy nastavení, která mají za úkol minimalizovat dopad bezpečnostního softwaru na výkon počítače během hraní. Cílem této části bude ověřit, zda je možné dosáhnout kompromisu mezi plynulým chodem her a účinnou ochranou proti bezpečnostním hrozbám.

Na základě výsledků budou formulována doporučení pro optimální nastavení zabezpečení pro hráče. Ta budou zahrnovat vhodné postupy pro bezpečné stahování herního obsahu, doporučená nastavení antivirového softwaru, a zásady digitální hygieny specifické pro prostředí herních komunit a platforem.

3.6 Modelový scénář 3 – Hráč počítačových her

Třetím modelovým scénářem bude prostředí běžného hráče počítačových her. Tato uživatelská skupina se pravidelně pohybuje v online prostředí, kde často dochází ke stahování herních souborů, aktualizací, modifikací (modů) a v některých případech i nelegálních kopií her (tzv. cracků). Z bezpečnostního hlediska se jedná o vysoce rizikovou činnost, neboť instalační nebo spustitelné soubory (např. s příponou .exe) se často stávají nositelem škodlivého kódu, zejména v případech, kdy pocházejí z neoficiálních nebo neověřených zdrojů.

V rámci této simulace bude analyzována modelová situace, kdy hráč stáhne instalační balíček s neověřeným obsahem – např. herní mod, crack nebo instalační soubor z neoficiálního webu. Bude sledováno, jakým způsobem na takovou situaci zareaguje antivirový software nainstalovaný v systému. Zjišťováno bude, zda je detekováno potenciálně nebezpečné chování, zda dojde k automatickému zablokování přístupu k souboru, přesunu do karantény nebo zda je spuštění povoleno bez upozornění.

Dále bude ověřováno, jak antivirový systém chrání uživatele před tzv. trojskými koni, které se často vydávají za herní utility, cheaty nebo zrychlovací nástroje, a zda dokáže identifikovat také méně závažné, ale obtěžující typy škodlivého softwaru, jako je adware distribuovaný v rámci tzv. bundle instalátorů. Součástí testování bude i ověření přítomnosti tzv. *silent install*, kdy je do systému bez vědomí uživatele nainstalován doplňkový software, často měnící nastavení prohlížeče nebo sbírající uživatelská data.

Zvláštní pozornost bude věnována funkcím herních režimů, které některé antivirové programy nabízejí. Bude zkoumáno, zda je během hraní skutečně zachována potřebná míra ochrany

v reálném čase i při snížení zátěže systému. Cílem bude ověřit, jakou míru bezpečnosti lze při používání těchto funkcí udržet a jaký dopad mají na výkon počítače během hraní.

Na základě výsledků simulace budou vyhodnocena doporučení pro hráče, jak si udržet vysokou úroveň zabezpečení při stahování a spouštění herního obsahu. Zohledněna budou jak nastavení antivirového softwaru, tak zásady bezpečného chování v online prostředí, s důrazem na prevenci infekce škodlivým softwarem bez omezení uživatelského komfortu a herního výkonu.

4 Vyhodnocení a porovnání testovacích scénářů

4.1 Porovnání testovaných uživatelských scénářů

Cílem této kapitoly je shrnout a porovnat výsledky získané při testování antivirové ochrany u tří odlišných typů uživatelů – běžného uživatele počítače, hráče počítačových her a programátora. Každý z těchto modelových uživatelů byl vystaven čtyřem typickým bezpečnostním situacím, které simulují reálné hrozby, s nimiž se mohou ve své každodenní praxi setkat. Porovnání se zaměřuje nejen na samotnou reakci antivirového řešení (konkrétně Windows Defender), ale i na míru zásahu uživatele, úroveň informování o potenciálním nebezpečí a případné selhání ochrany. Důležitou součástí analýzy je také zhodnocení míry rizika, které dané situace představují, a interpretace výsledků z hlediska typického chování daného uživatele.

Tato srovnávací část navazuje na praktické scénáře a přináší komplexnější pohled na efektivitu antivirové ochrany v různých podmínkách používání počítače. Výsledky testování ukazují, že ačkoliv základní bezpečnostní nástroje v systému Windows dokážou odhalit a zablokovat některé typy hrozeb, v mnoha případech zůstává rozhodující úroveň informovanosti a opatrnosti samotného uživatele. Kapitola se proto rovněž zaměřuje na možná rizika spojená s jednotlivými přístupy k používání počítače a navrhuje vhodná opatření, která mohou přispět ke zvýšení celkové bezpečnosti.

4.2 Úroveň rizika a typické chování

Každá skupina uživatelů se vyznačuje odlišným způsobem práce s počítačem, což se přímo promítá do toho, jakým hrozbám je nejčastěji vystavena. Z výsledků testů vyplývá, že **běžný uživatel** často čelí hrozbám, které přicházejí skrze neúmyslné stažení škodlivého souboru, spuštění přílohy e-mailu nebo instalaci „neškodně vypadajících“ aplikací. Tito uživatelé často nemají hlubší technické znalosti, spoléhají se na výchozí nastavení systému a očekávají, že je ochrání automatické mechanismy. Antivirová ochrana zde musí být co nejvíce automatizovaná a nenáročná na rozhodování ze strany uživatele.

Naproti tomu **hráči počítačových her** častěji stahují obsah z méně důvěryhodných zdrojů, ať už se jedná o modifikace, herní utility nebo cracky. Často kvůli výkonu deaktivují antivirovou ochranu, případně ignorují varování systému, pokud jim brání ve spuštění požadovaného obsahu. Riziko tedy spočívá v kombinaci snížené ostražitosti a záměrného obcházení ochrany systému. Antivirový software musí být v tomto případě dostatečně robustní,

aby detekoval hrozby i v méně viditelných formách – například ve spustitelných souborech nebo knihovnách.

Programátoři se pohybují v ještě komplexnějším prostředí. Pracují s vývojovými nástroji, testují skripty, knihovny nebo emulátory. Typickou hrozbou v tomto prostředí nejsou jen viry, ale také potenciálně škodlivé skripty nebo komponenty, které mohou být součástí otevřených repozitářů. Často se zde používají i síťové nástroje pro testování zranitelností (např. PowerShell skripty, reverzní shelly), což může být běžným antivirem označeno jako hrozba, ačkoliv jde o legitimní testování. Programátor tedy často potřebuje vyšší míru kontroly nad bezpečností a zároveň jasnou informovanost o rizicích každého zásahu.

4.3 Reakce antivirové ochrany

Testování ukázalo, že ve všech třech scénářích byl systém Windows Defender funkční a aktivní, nicméně jeho reakce se lišila v závislosti na typu hrozby. Na klasické EICAR soubory reagoval ihned ve všech případech. U PUA aplikací (např. YouPlay) však většinou nezasáhl, i když tyto programy představují potenciální riziko.

Nejzajímavější rozdíly byly patrné při testování chování v méně zjevně nebezpečných situacích. Zatímco u běžného uživatele byl například zachycen pokus o otevření poznámkového bloku s EICAR řetězcem, u programátora se podařilo bez jakékoli reakce systému spustit skript přejmenovávající soubory v systému. Hráč pak mohl bez potíží stáhnout crack nebo hru ze zdroje mimo oficiální platformy.

Z toho vyplývá, že účinnost antivirového softwaru ve výchozím nastavení je dostačující pouze proti základním hrozbám, ale selhává u méně tradičních nebo skrytých hrozeb, typických právě pro hráče a vývojáře.

4.4 Doporučení pro jednotlivé skupiny

Z porovnání lze vyvodit konkrétní doporučení pro každou cílovou skupinu:

- **Běžný uživatel** by měl mít zapnutý real-time antivirus, aktualizovaný systém a využívat rozšíření do prohlížeče pro blokaci škodlivých webů. Měl by se vyhnout instalaci softwaru z neznámých zdrojů. Doporučuje se využít i kontrolu příloh v e-mailu a naučit se základy rozpoznání phishingu.
- **Hráč** by měl být obzvlášť opatrný při stahování herních souborů, módů nebo cracků. Ideální je provozovat hlavní antivirus v kombinaci s antimalwarovým nástrojem.

Vhodné je využít herního režimu antiviru, který neomezuje výkon, ale zároveň zachová základní ochranu. Nikdy by neměl zcela vypínat bezpečnostní funkce kvůli výkonu.

- **Programátor** by měl používat virtualizaci (např. Windows Sandbox nebo virtuální stroje) při testování neznámých skriptů. Vhodné je používat nástroje s vyšší granularitou (např. ESET, Kaspersky s pokročilým režimem) a konfigurovat vlastní výjimky a pravidla. Měl by mít přehled o síťových spojeních a logování procesů v systému.

4.5 Celkové shrnutí

Z výsledků testování je zřejmé, že antivirová ochrana není univerzálně účinná pro všechny typy uživatelů stejně. V základním nastavení funguje dobře proti známým hrozbám a klasickým virům, ale může selhávat v situacích, které vyžadují hlubší kontext nebo pokročilou detekci.

Každý typ uživatele si vyžaduje jinou úroveň zabezpečení a jiné návyky. Běžný uživatel potřebuje jednoduché řešení s minimálními zásahy, hráč zase vyváženost mezi výkonem a bezpečností, a programátor musí být schopen bezpečně testovat potenciálně nebezpečný kód. To ukazuje, že kybernetická bezpečnost je komplexní oblast a žádné jediné řešení není univerzálně použitelné.

Tabulka 3: Přehled a vyhodnocení scénářů.

Kritérium	Běžný uživatel PC	Hráč PC her	Programátor
Technická znalost	Nízká	Střední	Vysoká
Typické riziko	Nechtěné stažení malware/ PUA	Cracky, módy, neoficiální zdroje	Neověřené knihovny, skripty
Chování při instalaci softwaru	Instaluje bez ověření	Ignoruje varování kvůli hře nebo výkonu	Vytváří a testuje vlastní skripty/ nástroje
Reakce na hrozbu	Spoléhá na antivir	Může vypínat ochranu	Vytváří výjimky, případně antivir vypíná
Detekce EICAR testu	Úspěšná	Úspěšná	Úspěšná
Reakce na podezřelý obsah	Blokování spuštění skriptu v Poznámkovém bloku	Varování při pokusu o spouštění cracku	Instalace PUA bez reakce
Doporučená ochrana	Automatická, nenáročná, se zapnutými výchozími funkcemi	Kombinace výkonného antiviru s herním režimem	Pokročilý antivir, virtualizace, logování

Zdroj: vlastní zpracování

5 Případová studie

5.1 Testování antivirové ochrany u běžného uživatele osobního počítače

V dnešní době je osobní počítač součástí života téměř každého člověka. Běžný uživatel ho využívá k široké škále činností – od prohlížení internetu, práce s dokumenty, sledování videí až po komunikaci přes sociální sítě nebo online nakupování. Většina uživatelů však při své činnosti není plně obeznámena s riziky, která na ně při těchto aktivitách číhají. Právě tato neznalost, kombinovaná s nízkou mírou obezřetnosti, vytváří ideální prostředí pro šíření malwaru, potenciálně nežádoucích aplikací (PUA) a dalších typů hrozeb.

Cílem této části praktického testování bylo simulovat nejběžnější situace, se kterými se běžný uživatel může setkat, a ověřit, jak na tyto situace reaguje antivirová ochrana integrovaná ve Windows (Windows Defender). Současně bylo cílem zjistit, zda je standardní ochrana dostatečná pro ochranu dat a soukromí běžného uživatele, a jaké další kroky by bylo vhodné doporučit pro zvýšení úrovně zabezpečení.

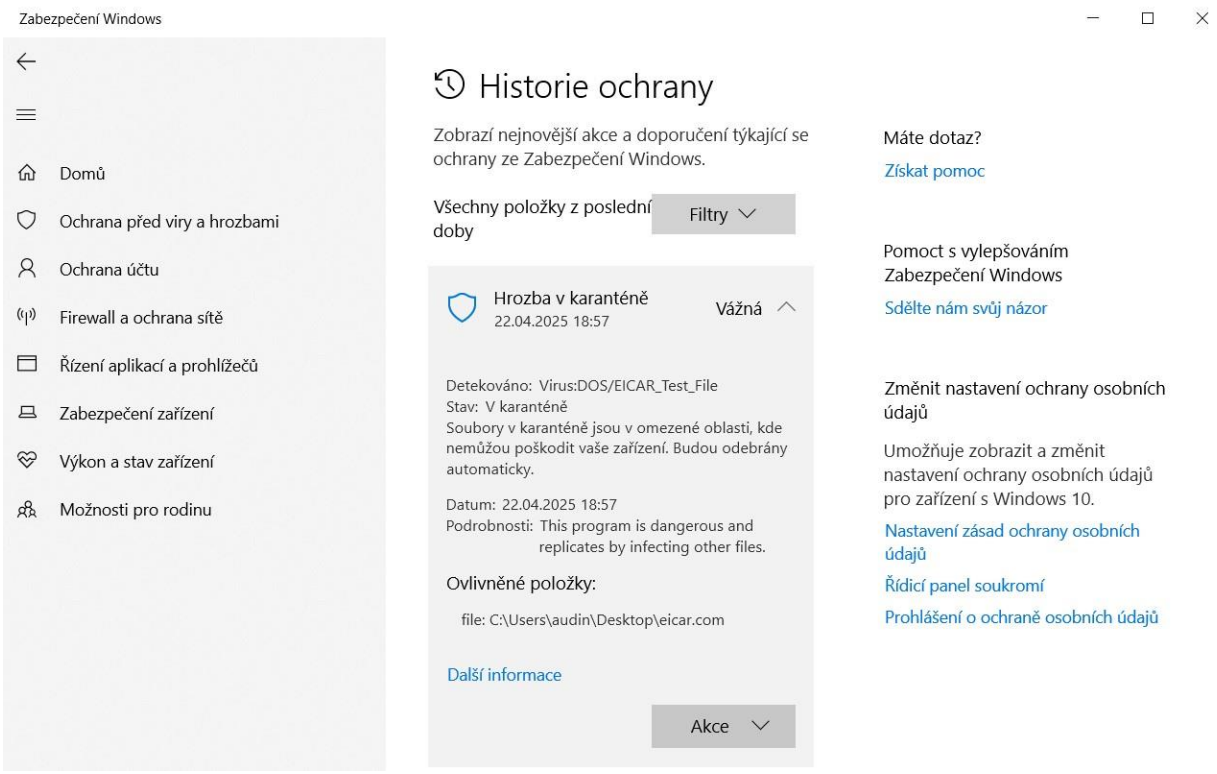
5.2 Průběh testování

1. Test s EICAR souborem

První test spočíval ve stažení EICAR testovacího souboru z oficiálních stránek European Institute for Computer Antivirus Research. Tento soubor je mezinárodně uznávaným standardem pro testování antivirových řešení a není skutečně škodlivý, pouze simuluje infekci.

Po kliknutí na odkaz ke stažení a potvrzení uložení souboru na disk reagoval Windows Defender okamžitě. Soubor byl ihned zablokován a přesunut do karantény, přičemž uživatel byl upozorněn prostřednictvím notifikace. Tento test potvrdil, že Defender správně identifikuje známé vzorky a základní detekční schopnosti fungují bezchybně.

Důležité je zmínit, že reakce byla automatická a uživatel nebyl nucen činit žádné složité rozhodnutí, což je v případě nezkušených uživatelů velmi zásadní.



Obrázek 1: Test EICAR souboru.

Zdroj: vlastní zpracování

2. Instalace potenciálně nežádoucí aplikace (PUA)

Ve druhém testu jsem simuloval běžnou situaci, kdy si uživatel stáhne software z méně známého zdroje. Stáhnul jsem program YouPlay z webu filehippo.com. Tento software je často označován jako potenciálně nežádoucí aplikace, protože může zobrazovat reklamy nebo shromažďovat údaje o uživateli bez jeho vědomí.

Samotné stažení proběhlo bez zásahu antiviru. Ani během instalace nebyl zobrazen žádný varovný dialog nebo notifikace. Program se nainstaloval a spustil zcela bez omezení. Po nainstalování byl aktivní na pozadí a bylo obtížné zjistit, jaké konkrétní procesy vykonává.

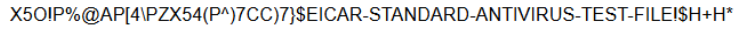
Tento test ukázal, že antivirová ochrana v základním nastavení nemusí odhalit méně zjevné hrozby, které sice nejsou přímo škodlivé, ale mohou nepřímo ovlivnit bezpečnost a soukromí uživatele.

3. Test: Ruční vytvoření EICAR souboru v Poznámkovém bloku

Třetí test byl zaměřen na simulaci situace, kdy si uživatel nevědomky vytvoří škodlivý soubor. V Poznámkovém bloku (Notepad) jsem ručně napsal známý EICAR testovací řetězec:

Následně jsem se pokusil soubor uložit pod příponou .txt. V momentě uložení souboru zasáhl Microsoft Defender a okamžitě upozornil na nalezení hrozby. Soubor byl automaticky přesunut do karantény a uživatel byl upozorněn na pokus vytvoření nebezpečného obsahu.

Tento test ukázal, že antivirová ochrana reaguje nejen na stažení či otevření souboru, ale i na samotnou tvorbu nebezpečného obsahu přímo v systému uživatele.

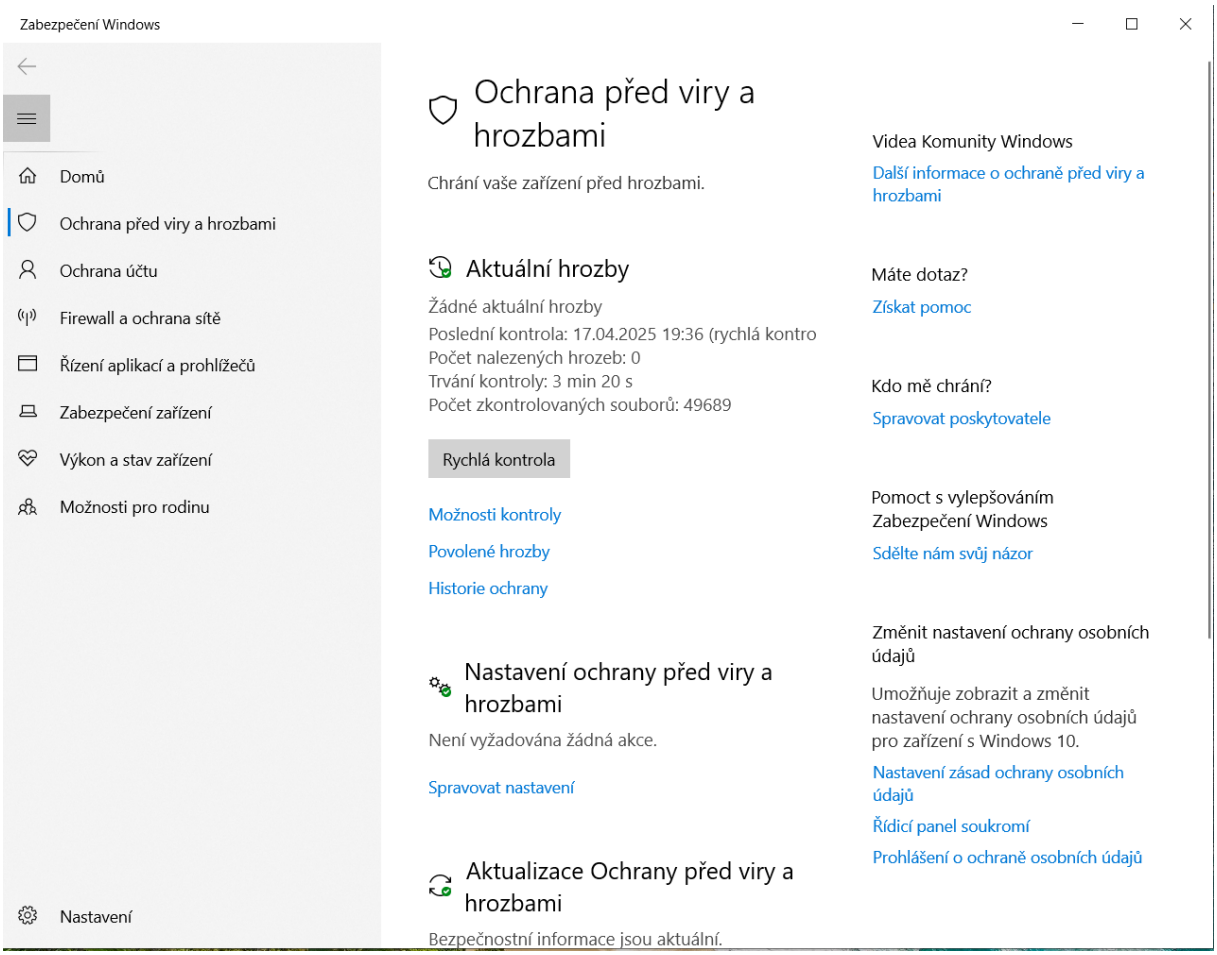


Obrázek 2: Blokace nebezpečného souboru.

Zdroj: vlastní zpracování

4. Kontrola aktuální úrovně zabezpečení systému

Na závěr testování byla provedena ruční kontrola aktuálnosti antivirového systému. Byla ověřena funkčnost Windows Defenderu, aktualizovanost virové databáze a zapnutí systémového firewallu. Kontrola prokázala, že všechny bezpečnostní funkce fungují správně a jsou aktuální, což je důležité z hlediska prevence před hrozbami, na které běžný uživatel nemusí být připraven.



Obrázek 3: Kontrola aktivního zabezpečení.

Zdroj: vlastní zpracování

5.3 Vyhodnocení testování

Výsledky testování ukazují, že antivirová ochrana Windows Defender si bez problémů poradí s klasickými hrozbami, které jsou dobře známé a běžně detekované. V případě EICAR souboru proběhla detekce okamžitě a systém uživatele efektivně ochránil.

Oproti tomu v případě potenciálně nežádoucího softwaru a aplikací stažených z neověřených zdrojů je Defender poměrně pasivní. Nezaznamenal žádnou podezřelou aktivitu a uživatel tak zůstává plně odkázán na svou vlastní obezřetnost. Tento fakt může být zvlášť problematický u méně zkušených uživatelů, kteří nemusí tušit, že jejich zařízení je vystaveno riziku.

5.4 Návrh vlastních doporučení

Na základě výsledků praktických testů doporučuji implementaci následujících bezpečnostních opatření:

1. **Aktivace ochrany proti potenciálně nežádoucím aplikacím (PUA):** Windows Defender nabízí možnost detekce a blokace PUA, tato funkce však není ve výchozím nastavení aktivní. Doporučuji ji ručně zapnout přes pokročilá nastavení Zabezpečení Windows.
2. **Důsledné používání ověřených zdrojů pro stahování softwaru:** Softwarové produkty by měly být stahovány výhradně ze stránek výrobců nebo z oficiálních obchodů (Microsoft Store, Steam apod.). Tím se minimalizuje riziko zavlečení škodlivého softwaru.
3. **Instalace doplňkových antimalwarových nástrojů:** Doporučuji využívat doplňkové antimalwarové programy, které se zaměřují na pokročilé typy hrozeb (například Malwarebytes, Emsisoft Emergency Kit nebo HitmanPro).
4. **Pravidelné aktualizace systému a softwaru:** Uživatel by měl vždy instalovat dostupné aktualizace systému i aplikací, protože obsahují opravy bezpečnostních chyb, které mohou být zneužity malwarem.
5. **Zálohování důležitých dat:** Pravidelné zálohování dat, ať už na externí disk nebo do cloudového úložiště, může minimalizovat dopad v případě infekce malwarem nebo selhání systému.
6. **Vzdělávání uživatelů:** Zvyšování povědomí o kybernetických hrozbách a bezpečném chování na internetu je klíčem k vyšší bezpečnosti. Doporučuji jednoduché online kurzy, školení, nebo pravidelné čtení článků o kybernetické bezpečnosti.

5.5 Celkové shrnutí

Testování ukázalo, že Windows Defender představuje základní, ale omezenou ochranu pro běžného uživatele. Sice spolehlivě zachytí tradiční hrozby, ale u méně zjevných nebo sofistikovanějších útoků zůstává riziko nedetekování vysoké. Běžný uživatel by proto neměl spoléhat pouze na výchozí ochranu systému, ale měl by kombinovat více vrstev obrany a být aktivně zapojen do správy vlastní kybernetické bezpečnosti.

Bez vhodné prevence a zvýšené obezřetnosti může být osobní počítač i při základní ochraně zranitelný vůči nejrůznějším typům útoků. Důrazně proto doporučuji implementaci výše uvedených opatření.

5.6 Testování antivirové ochrany u hráče PC her

Počítačoví hráči představují specifickou skupinu uživatelů, která se v mnoha ohledech odlišuje od běžných uživatelů osobních počítačů. Hráči tráví u počítače často mnoho hodin, a jejich primární činností je hraní moderních her, stahování aktualizací, herních klientů, módů a doplňkového obsahu. V honbě za novými zážitky mohou hráči stahovat obsah i z méně známých nebo neoficiálních zdrojů, což podstatně zvyšuje riziko stažení škodlivého softwaru.

Pro tuto skupinu je klíčové, aby antivirová ochrana nejenom účinně bránila hrozbám, ale zároveň nerušila výkon počítače a nepřekážela při hraní. Cílem této části praktického testování bylo simulovat reálné situace, se kterými se hráči často setkávají, a ověřit, jak efektivně a zároveň nenápadně funguje antivirová ochrana v takovém prostředí.

5.7 Průběh testování

1. Stažení neověřené hry

Prvním testem bylo stažení hry **Zombie Derby 2** z alternativního zdroje, který nebyl oficiální platformou jako Steam či Microsoft Store. Hra byla stáhnuta v instalačním souboru, bez nutnosti registrace nebo kontroly pravosti.

Proces stažení a následné instalace hry proběhl hladce a bez jakéhokoliv zásahu ze strany Windows Defenderu. Ani při samotném spuštění hry nebyla detekována žádná podezřelá aktivita. Hra fungovala normálně a nevykazovala známky škodlivého chování.

Tento test ukázal, že základní antivirová ochrana neprovádí hlubší analýzu nově instalovaných aplikací, pokud neobsahují známé signatury škodlivého softwaru. Přestože se konkrétně v tomto případě jednalo o bezpečnou hru, v praxi by podobný scénář mohl vést k instalaci škodlivého softwaru bez jakéhokoliv varování.

2. Pokus o stažení potenciálně rizikového cheatovacího nástroje

Ve druhém testu jsem simuloval situaci, kdy hráč hledá cheatovací nástroje pro herní výhodu. Pokusil jsem se stáhnout program, který sliboval neomezené zdroje ve hrách. Po kliknutí na odkaz vedoucí na stažení se stránka zobrazila jako nedostupná s hlášením 404 error. Tento test ukázal, že mnoho těchto zdrojů není spolehlivých, a že už samotný pokus o stažení z pochybných zdrojů je velkým rizikem.

I když ke stažení nakonec nedošlo, pokud by hráč na podobné stránce skutečně stáhnul soubor, riziko infikace systému trojským koněm, spywarem nebo jiným druhem malwaru by bylo značné.

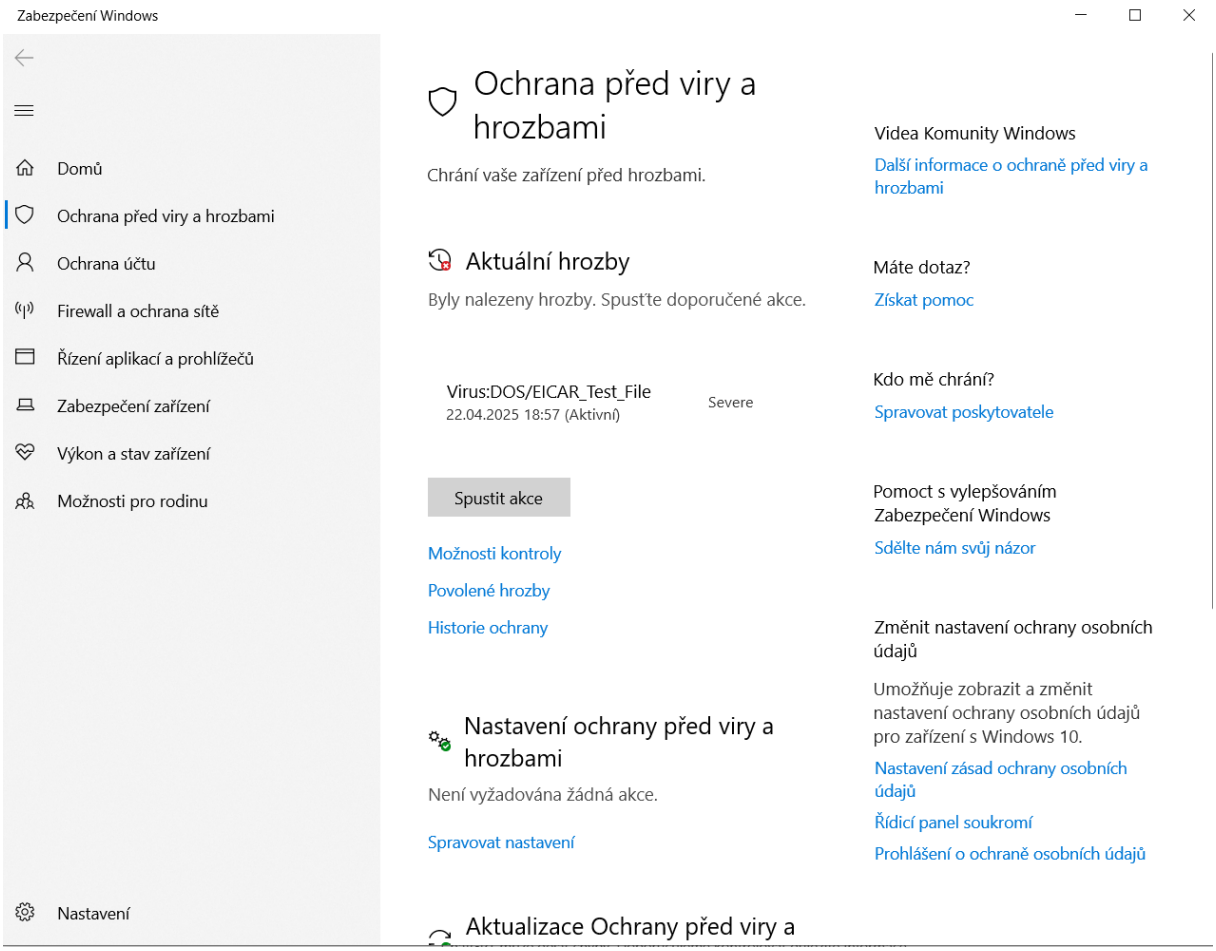
Obrázek 4: Nedostupná stránka.

Zdroj: vlastní zpracování

3. Pokus o spuštění testovacího EICAR souboru v herním režimu

Pro třetí test jsem se rozhodl ověřit, jak se Defender chová při současném spuštění hry a simulovaného malwaru (EICAR souboru). Testovací soubor jsem stáhnul a pokusil se jej spustit během hraní hry, kdy byl zapnutý režim optimalizace výkonu.

Windows Defender reagoval okamžitě i v herním režimu – soubor byl detekován, zablokován a byla zobrazena notifikace bez výrazného ovlivnění chodu hry. To ukazuje, že Defender je schopný zachytit hrozby i při zvýšené zátěži systému a při běžném hraní, což je pozitivní signál pro hráče, kteří se obávají možného zpomalení ochrany při vyšším vytížení.

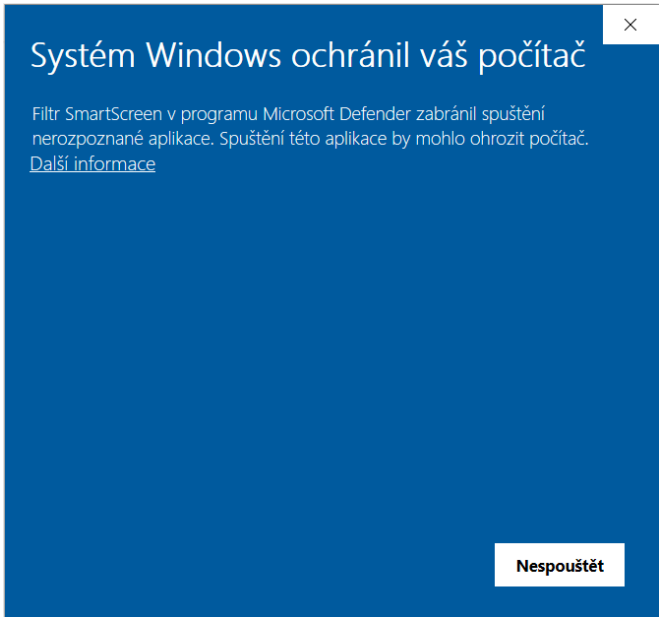


Obrázek 5: Detekce EICAR souboru v herním režimu.

Zdroj: vlastní zpracování

4. Stažení a pokus o spuštění simulovaného "cracku"

Čtvrtý test simuloval pokus o spuštění cracku ke hře, což představuje časté riziko u hráčské komunity. Při pokusu o spuštění souboru zasáhl bezpečnostní mechanismus SmartScreen, který zobrazil modré varovné okno s hláškou "Systém Windows ochránil váš počítač." Tato ochrana zabránila spuštění neověřeného softwaru a ukázala, že kromě antiviru fungují i další vrstvy zabezpečení systému.



Obrázek 6: Bezpečnostní mechanismus SmartScreen.

Zdroj: vlastní zpracování

5.8 Vyhodnocení testování

Testování ukázalo několik důležitých skutečností. Windows Defender poskytuje hráčům základní úroveň ochrany, která je schopná efektivně detekovat známé a standardizované hrozby, aniž by negativně ovlivnila herní zážitek nebo výkon systému.

Nicméně v případě stahování a instalace neověřených her a nástrojů z pochybných zdrojů je ochrana nedostatečná. Antivir neprovedl hloubkovou kontrolu souborů a neupozornil na možné riziko, což by v reálném scénáři mohlo vést ke kompromitaci systému, a to i bez vědomí hráče.

Výkon počítače zůstal během celého testování stabilní, Defender nijak nenarušil plynulost herního prostředí, což je bezesporu velké pozitivum. Přesto je třeba si uvědomit, že samotné spolehnutí na integrovanou ochranu nemusí být pro aktivního hráče, který často pracuje s neoficiálními soubory, dostatečné.

5.9 Návrh vlastních doporučení

Na základě výsledků praktického testování doporučuji hráčům následující opatření pro zvýšení bezpečnosti při zachování vysokého výkonu systému:

1. **Vždy používat oficiální zdroje pro stahování her:** Stahování her a souvisejícího obsahu by mělo probíhat pouze prostřednictvím oficiálních obchodů a platforem jako je Steam, Epic Games Store nebo Microsoft Store.
2. **Vyhnout se cheatovacím nástrojům:** Používání cheatovacích nástrojů nejenže porušuje pravidla většiny her, ale představuje obrovské bezpečnostní riziko. Většina těchto nástrojů je infikována malwarem.
3. **Využití herního režimu v antivirovém programu:** Windows Defender i některé jiné antiviry umožňují aktivovat herní režim, který minimalizuje rušivé notifikace a zároveň zachovává ochranu v reálném čase.
4. **Pravidelná kontrola systému antimalwarovým nástrojem:** Kromě Defenderu doporučuji pravidelně používat nástroje typu Malwarebytes pro hloubkovou kontrolu systému.
5. **Důsledné aktualizace systému a herních klientů:** Aktualizace nejen zvyšují výkon a stabilitu, ale často obsahují i bezpečnostní opravy.
6. **Zálohování herních dat:** V případě infekce nebo útoku ransomwarem mohou být herní profily, uložené pozice a nastavení nenávratně ztraceny. Pravidelné zálohování na externí disky nebo cloud může minimalizovat škody.
7. **Opatrnost při instalaci módů a rozšíření:** Módy a rozšíření by měly být instalovány pouze z ověřených komunit a platforem, kde je nižší riziko podvrženého obsahu.

5.10 Celkové shrnutí

Výsledky testování naznačují, že Windows Defender nabízí hráčům dostatečnou ochranu proti základním hrozbám, aniž by narušil herní výkon. Nicméně v situacích, kdy hráči stahují software nebo obsah z neoficiálních zdrojů, ochrana selhává a riziko zavlečení malwaru se výrazně zvyšuje.

Hráči by proto neměli ochranu podceňovat a měli by kombinovat více vrstev zabezpečení, využívat ověřené zdroje a pravidelně kontrolovat své zařízení pokročilými nástroji. Kombinace kvalitní ochrany, bezpečných návyků a pravidelné kontroly systému tvoří nejlepší obranu proti potenciálním hrozbám v herním světě.

5.11 Testování antivirové ochrany u programátora

Programátoři tvoří skupinu uživatelů, kteří běžně pracují s velkým množstvím zdrojového kódu, skriptů a různých vývojových nástrojů. Jejich pracovní prostředí je specifické tím, že často stahují nové knihovny, experimentují s neověřenými skripty, vytvářejí vlastní aplikace nebo testují cizí kód. Programátoři se tak mohou nechtěně stát oběťmi útoků nejen kvůli stažení infikovaných souborů, ale také prostřednictvím podvržených závislostí, neověřených repozitářů nebo chybných skriptů.

Cílem této části praktického testování bylo simulovat reálné prostředí programátora, který pracuje s různými skripty a nástroji, a vyhodnotit, jak Windows Defender reaguje na činnosti, které by mohly být potenciálně rizikové. Zajímalo mě, jak efektivně antivirový systém odhalí podezřelé aktivity a zda nebude zároveň zbytečně zasahovat do běžného pracovního procesu.

5.12 Průběh testování

1. Stažení balíku Python skriptů z neověřeného zdroje

V rámci prvního testu jsem stáhl archiv obsahující několik Python skriptů ze zdroje, který nebyl oficiálně ověřen. Soubory byly uloženy do nově vytvořené složky a jednotlivé skripty jsem otevřel v editoru. Při tomto kroku Windows Defender nijak nereagoval, soubory byly považovány za bezpečné.

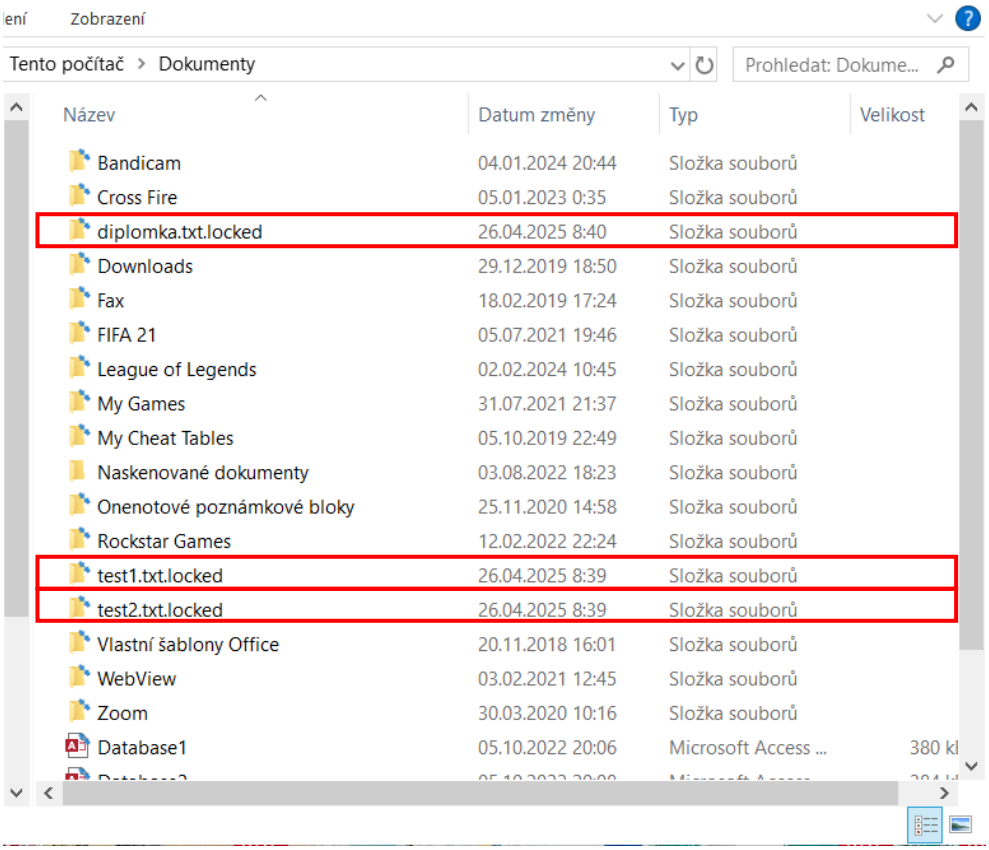
Žádná upozornění ani automatická kontrola nebyla zaznamenána, což poukazuje na to, že Defender neprovádí hlubší kontrolu zdrojového kódu, pokud neobsahuje přímo identifikovatelné signatury malwaru. V tomto případě šlo skutečně o neškodné skripty, ale v praxi může podobná situace vést ke spuštění infikovaného kódu bez jakéhokoliv varování.

2. Simulace falešného ransomwaru v PowerShellu

Ve druhém kroku jsem vytvořil vlastní skript ve formátu PowerShell (.ps1), který měl za úkol přejmenovat všechny soubory s příponou .txt v uživatelské složce „Documents“ přidáním přípony „. locked“. Tento jednoduchý skript měl simulovat základní chování ransomwaru – tedy manipulaci se soubory bez souhlasu uživatele.

Po spuštění skriptu pomocí PowerShellu došlo k přejmenování všech cílových souborů podle očekávání. Windows Defender ovšem nijak nezasáhl, žádné varování nebylo zobrazeno a ani po dokončení akce nebyly zaznamenány žádné upozornění.

Tento test potvrdil, že jednoduché skripty vykonávající neobvyklé operace s uživatelskými daty mohou proběhnout bez jakékoliv detekce, pokud nejsou předem známy v databázích malwarových vzorců. To je velmi významné zjištění, protože v reálném scénáři by podobný útok mohl mít vážné důsledky.



Obrázek 7: Selhání zabezpečovacího mechanismu.

Zdroj: vlastní zpracování

3. Simulace reverse shellu přes PowerShell

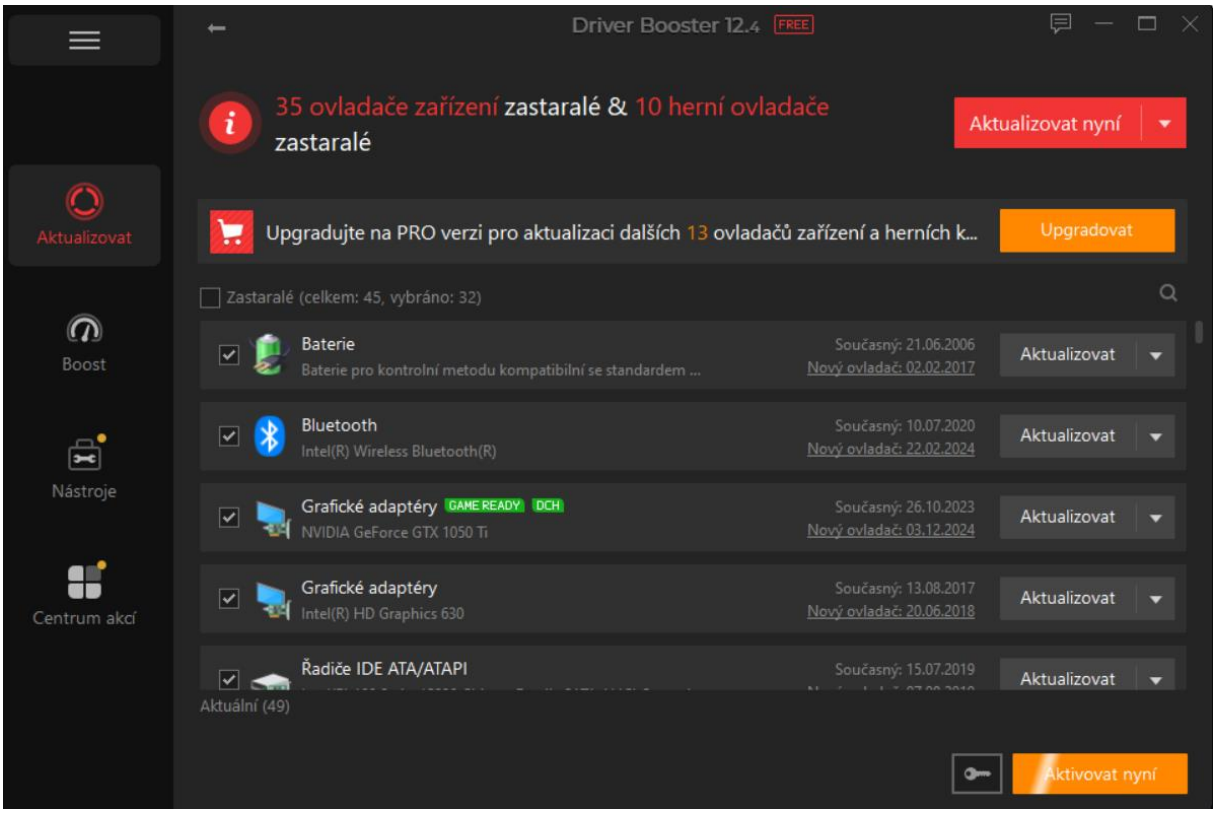
Pro třetí test jsem se pokusil stáhnout a vytvořit jednoduchý reverse shell skript, který by navázal zpětné spojení mezi počítačem oběti a útočníkem. I přes několik pokusů o stažení funkčního skriptu jsem narazil na omezení — většina odkazů na internetu byla buď nefunkční, nebo vyžadovala přihlášení.

Vytvořil jsem tedy vlastní jednoduchou simulaci reverse shellu v PowerShellu. Při pokusu o spuštění Defender opět nijak nereagoval, a skript se okamžitě uzavřel bez jakýchkoli bezpečnostních hlášení. To ukazuje na to, že Defender není schopný efektivně detekovat vlastní vytvořené hrozby, které nejsou známé v jeho signaturách.

Tento fakt podtrhuje význam behaviorální analýzy, kterou by měl moderní antivirový systém mít, protože pouze hledání podle signatur není pro ochranu programátorů dostatečné.

4. Instalace Driver Booster Free

Poslední test spočíval v instalaci programu Driver Booster Free, který je známý svou agresivní reklamní politikou a potenciálním šířením nežádoucích programů. Instalace proběhla bez zásahu antivirového systému, což ukazuje na slabší místa v detekci potenciálně rizikového softwaru, zejména pokud se software prezentuje jako legitimní nástroj. Tento poznatek podtrhuje nutnost zvýšené obezřetnosti při práci s méně známými aplikacemi i v prostředí programátorů.



Obrázek 8: Driver Booster Free.

Zdroj: vlastní zpracování

5.13 Vyhodnocení testování

Testování ukázalo, že Windows Defender je schopen chránit systém před známými hrozbami, avšak vůči nově vytvořeným a jednoduchým škodlivým skriptům je v současné podobě poměrně bezmocný. Programátoři, kteří běžně pracují se skripty a neověřenými knihovnami, se tak stávají rizikovou skupinou.

Během všech prováděných testů nebyl zpozorován žádný negativní dopad na výkon systému, což je pozitivní. Nicméně skutečnost, že nebyly detekovány ani jednoduché škodlivé operace jako hromadné přejmenování souborů či pokus o vytvoření síťového spojení, je velmi alarmující.

Výsledky ukazují, že základní antivirová ochrana, jakou je Windows Defender, nestačí pro uživatele, kteří se věnují vývoji a experimentování s kódem.

5.14 Návrh vlastních doporučení

Na základě provedených testů a zjištěných nedostatků doporučuji programátorům následující bezpečnostní opatření:

1. **Používat sandbox prostředí:** Testování neověřených skriptů by mělo probíhat ve virtuálním prostředí nebo sandboxu, aby se minimalizovalo riziko poškození systému.
2. **Využívat pokročilé bezpečnostní nástroje:** Programátoři by měli používat antiviry s behaviorální analýzou (např. ESET, Bitdefender, Sophos) a antimalwarové nástroje, které detekují podezřelé chování, nikoliv jen známé hrozby.
3. **Ruční audit kódu:** Před spuštěním cizího skriptu je důležité ručně prověřit jeho obsah a ověřit, co přesně kód provádí.
4. **Pravidelné zálohování důležitých dat:** I když programátor pracuje opatrně, hrozí mu riziko nákazy. Pravidelné zálohování na oddělené disky nebo cloudová úložiště je nezbytné.
5. **Důsledné aktualizace nástrojů a knihoven:** Aktualizace minimalizují riziko zneužití známých zranitelností.
6. **Používání bezpečných repozitářů:** Instalace knihoven a nástrojů by měla být prováděna pouze z důvěryhodných zdrojů, jako jsou oficiální repozitáře GitHubu nebo PyPI.
7. **Nastavení restrikcí pro spouštění skriptů:** V prostředí Windows lze pomocí zásad zabezpečení omezit spouštění neověřených PowerShell skriptů, což výrazně snižuje riziko nákazy.

5.15 Celkové shrnutí

Výsledky testování jasně ukazují, že Windows Defender poskytuje pouze základní úroveň ochrany vhodnou pro běžné uživatele, ale pro programátory je nedostatečný. Schopnost detekovat nové, vlastní nebo upravené skripty je velmi omezená a hrozby založené na PowerShell skriptech nebo neověřeném Python kódu mohou snadno projít bez povšimnutí.

Programátoři by měli klást mimořádný důraz na bezpečnostní opatření, a to nejen při práci s cizím kódem, ale také při vlastním vývoji. Pouze kombinací bezpečných návyků, pokročilé antivirové ochrany a používáním oddělených testovacích prostředí lze výrazně snížit riziko infekce a zachovat bezpečnost pracovního prostředí.

Závěr

Tato bakalářská práce se zaměřila na antivirovou ochranu různých typů uživatelů a ověřila teoretické poznatky pomocí praktického testování. Cílem bylo ukázat, jak se liší potřeby a reálné hrozby u běžného uživatele počítače, hráče počítačových her a programátora, a zároveň posoudit účinnost standardních bezpečnostních opatření, zejména antivirového programu Windows Defender.

V praktické části byly simulovány reálné situace, se kterými se uživatelé mohou běžně setkat. U každého typu uživatele byly provedeny čtyři testy, které reflektovaly nejčastější způsoby, jakými mohou být zařízení infikována – od stažení testovacího EICAR souboru, přes instalaci potenciálně nežádoucí aplikace, až po pokusy o spuštění neověřených nebo rizikových programů. Testy probíhaly přímo na fyzickém zařízení, aby byly podmínky co nejvíce autentické a odpovídaly skutečnému použití.

Výsledky testování ukázaly, že Windows Defender je schopen velmi efektivně zachytit některé typy hrozeb, zejména standardizované testovací soubory a zjevně škodlivé aplikace. Například při stažení EICAR testovacího souboru byl soubor okamžitě detekován a zablokován bez potřeby jakékoli akce ze strany uživatele, což potvrdilo správnou funkčnost základní detekční vrstvy antiviru. Podobně při pokusu o spuštění potenciálně nebezpečných souborů, jako byl simulovaný crack, reagoval systém varováním a zabránil spuštění bez souhlasu uživatele.

Na druhé straně se testování ukázalo, že v některých případech ochrana selhává nebo není dostatečně proaktivní. Například při instalaci programu YouPlay (potenciálně nežádoucí aplikace) nebyla zobrazena žádná varovná notifikace a instalace proběhla hladce. Stejně tak při instalaci programu Driver Booster Free, který byl stažen v rámci scénáře programátora, nebyl Windows Defender schopen adekvátně upozornit na možné riziko. Tato situace ukazuje, že některé hrozby, které se nacházejí na hranici mezi škodlivým a legitimním softwarem, mohou unikat základní ochraně.

Z hlediska doporučení lze říct, že samotné spoléhání na výchozí nastavení antivirového programu není dostatečné. Uživatelé by měli pravidelně kontrolovat stav zabezpečení, dbát na aktualizace systému i antivirové databáze, a měli by být obezřetní při stahování a instalaci softwaru z méně známých zdrojů. Pro zkušenější uživatele nebo ty, kteří vykonávají rizikovější aktivity (například programátoři pracující se spustitelnými soubory nebo hráči využívající

alternativní herní platformy), lze doporučit použití pokročilejších antivirových řešení nebo doplnění ochrany o specializované nástroje (např. antimalware skenery, sandboxy, behaviorální analýzu).

Praktická část dále ukázala, že ochrana na úrovni systému Windows je nastavena tak, aby minimalizovala zátěž běžného uživatele a omezila nutnost rozhodování o bezpečnostních incidentech. Toto je sice výhodné pro méně zkušené uživatele, na druhou stranu to může vést ke snížené kontrole nad tím, co je do systému instalováno. Míra důvěry v automatizovaná řešení může vést k přílišnému spoléhání se na ně a k opomíjení základních pravidel bezpečného chování.

Z celkového pohledu lze konstatovat, že antivirová ochrana v moderních systémech dosahuje velmi solidní úrovně základní bezpečnosti, avšak není neomylná. Uživatelé by měli být vedeni k větší odpovědnosti a měli by být vzděláváni v oblasti digitální bezpečnosti. Velmi důležitou roli zde hraje prevence – tedy důkladné ověřování zdrojů stahovaných souborů, využívání oficiálních obchodů s aplikacemi a pečlivé sledování všech bezpečnostních upozornění systému.

Z dlouhodobého hlediska se domnívám, že antivirová ochrana bude čím dál více založena na umělé inteligenci a strojovém učení. Technologie, které se dnes nacházejí především v rukou specializovaných firem, se postupně stanou běžnou součástí operačních systémů. Detekce škodlivého chování nebude spočívat pouze v porovnávání známých vzorců, ale v komplexním sledování chování programů v reálném čase. Tím však také vzniká nové riziko – uživatelé mohou mít ještě menší přehled o tom, co jejich systém dělá, protože většina rozhodnutí bude činěna automaticky a bez zpětné vazby. Důvěra v technologii tak bude hrát stále větší roli.

V budoucnu bude klíčové najít rovnováhu mezi efektivní ochranou a transparentností. Je nutné, aby uživatelé nejen spoléhali na nástroje, ale zároveň chápali jejich limity a byli schopni včas rozpoznat potenciální hrozbu. Věřím, že s postupem času se bude stále více prosazovat koncept „zero trust“, tedy nulové důvěry, kde se žádná aplikace nebo připojení nepovažuje za bezpečné, dokud není výslovně ověřeno. Tato filozofie by mohla výrazně snížit úspěšnost útoků, ale vyžaduje vyšší technické znalosti, a tedy i větší osvětu mezi uživateli.

Závěrem mohu říct, že osobní zkušenost s infekcí počítače, která byla impulsem k výběru tématu této bakalářské práce, mi pomohla hlouběji pochopit problematiku kybernetické

bezpečnosti. Při práci jsem si ověřil, že žádný bezpečnostní nástroj není stoprocentní, a že hlavním faktorem ochrany je vždy člověk – jeho přístup, obezřetnost a informovanost. Téma antivirové ochrany považuji za čím dál důležitější a jsem přesvědčen, že i do budoucna bude nutné ho neustále rozvíjet a aktualizovat, jak na úrovni technologií, tak i vzdělávání uživatelů.

POUŽITÁ LITERATURA

AVAST. *Antivirová ochrana a internetová bezpečnost* [online]. [cit. 2025-04-15]. Dostupné z: https://www.avast.com/cs-cz/index#pc

AVG TECHNOLOGIES. *Antivirová ochrana pro domácnosti a firmy* [online]. [cit. 2025-04-27]. Dostupné z: https://www.avg.com/cs-cz/homepage#pc

EC-COUNCIL. *Threats and Defense Mechanisms: EC-Council – Press – Book 2 of 4: CEH – Ethical Hacking and Countermeasures*, 2017.

ESET. *Kybernetická bezpečnost a antivirová ochrana* [online]. [cit. 2025-03-18]. Dostupné z: https://www.eset.com/cz/

JALŮVKA, Josef. *Moderní počítačové viry*. 2. aktualizované vydání. Praha: Computer Press, 2000.

KASPERSKY. *What is antivirus software?* Kaspersky [online]. 2023 [cit. 2025-02-21]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-antivirus-software

KASPERSKY. *Antivirová ochrana a kybernetická bezpečnost* [online]. [cit. 2025-03-20]. Dostupné z: https://www.kaspersky.cz/

KIM, Peter. *Hacking: praktický průvodce penetračním testováním*. Praha: Grada, 2015.

KRÁL, Mojmír. *Bezpečnost domácího počítače*. Praha: Grada, 2010.

MICROSOFT. *Security documentation*. Microsoft Learn [online]. [cit. 2025-04-10]. Dostupné z: https://learn.microsoft.com/en-us/security/

MICROSOFT. *Zabezpečení Windows* [online]. 2025 [cit. 2025-04-10]. Dostupné z: https://www.microsoft.com/cs-cz/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Computer Security Resource Center (CSRC)*. NIST [online]. [cit. 2025-03-15]. Dostupné z: **https://csrc.nist.gov/**

SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. Praha: Computer Press, 2005.