Srovnání bezpečnosti vybraných operačních systémů osobních počítačů

Radek Kuna

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radek Kuna**
Osobní číslo:	**L16490**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**prezenční**
Téma práce:	**Srovnání bezpečnosti vybraných operačních systémů osobních počítačů**

Zásady pro vypracování:

1. **Zpracujte rešerši vztahující se k problematice bezpečnosti operačních systémů osobních počítačů.**
2. **Vymezte problematiku bezpečnosti operačních systémů osobních počítačů.**
3. **Proveďte analýzu a komparaci bezpečnosti vybraných operačních systémů osobních počítačů.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[2] KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[3] WHITE, Alan a Ben CLARK. BTFM /: Blue team field manual :. USA: CreateSpace Independent Publishing Platform, 2017. Version 1.2. ISBN 978-1541016361.

[4] BROOKSHEAR, J. Glenn, David T SMITH a Dennis BRYLOW. Informatika. Brno: Computer Press, 2013. ISBN 978-80-2513-805-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.
③

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Radek Kuna

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zabývá srovnáním bezpečnosti operačních systému Windows Vista, Windows 8 a Ubuntu. První část práce je věnována popisu počítače, operačního systému, jeho struktuře a historii. Dále jsou rozepsány hrozby a rizika, která mohou ohrozit operační systém a data v něm. V části praktické jsou vytvořeny virtuální počítače, do nichž jsou posléze nainstalovány výše uvedené operační systémy a na kterých je proveden útok pomocí trojského koně MEMZ. V závěru práce jsou vybrané operační systémy srovnány a je doporučen nejbezpečnější z těchto operačních systémů.

Klíčová slova: bezpečnost, operační systém, virtuální počítač, trojský kůň, MEMZ, srovnání, Windows Vista, Windows 8, Ubuntu

ABSTRACT

The bachelor thesis deals with comparison of security of operating systems Windows Vista, Windows 8 and Ubuntu. The first part is devoted to the description of computer, operating system, its structure and history. Furthermore are write down threats and risks that may jeopardize the operating system and data in it are discussed. In the practical part, there are created virtual computers,into which the above mentioned operating systems are installed and on which the Trojan horse MEMZ is executed. In the conclusion, the selected operating systems are compared and the safest of these operating systems is recommended.

Keywords: safety, operating system, virtual computer, trojan horse, MEMZ, comparsion, Windows Vista, Windows 8, Ubuntu

Rád bych poděkoval panu Ing. Petru Svobodovi za poskytnutí cenných rad a připomínek a za věnovaný čas při vedení mé bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti, 15.5 2019.

Radek Kuna

OBSAH

ÚVOD

V dřívější době byly osobní počítače v domácnosti spíše výjimkou. Jelikož jeho prostřednictvím komunikujeme s přáteli, sdílíme s ostatními uživateli myšlenky, informace, zkušenosti a názory, bavíme se a hrajeme hry, tvoříme videa, prezentace či jiné textové soubory, stávají se osobní počítače nedílnou součástí běžného života každého člověka. Už nemusíme sedět u klasických stolních počítačů, ale můžeme si vzít přenosný počítač v podobě notebooku například do postele. Stejně jako se vyvíjí osobní počítače, vyvíjí se také operační systémy, které jsou jejich důležitou součástí. Vytváří totiž kooperaci mezi strojem a uživatelem a zjednodušuje tomuto uživateli celkovou práci na počítači.

Osobní počítač nevyužíváme pouze k zábavě či sdílení informací, ale jehož pomocí dnes můžeme například provádět různé platby a zadávat tak citlivé informace. S tímto přichází i různé útoky a taktiky od hackerů, kteří se tyto citlivé osobní informace snaží získat z našeho počítače. S tímto souvisí kybernetické hrozby, kterým se snaží věnovat kybernetická bezpečnost, avšak útočníci jsou dnes tak sofistikovaní, že tyto neustálé boje o bezpečnost jsou nekonečné.

Teoretická část je zaměřena na získání základních poznatků o osobním počítači, vymezit jeho definice a jak se může dělit. Charakterizovat operační systém, co je jeho úlohou, popis jeho struktury a historie. Dále bylo cílem vymezit kyberprostor a s tím související kybernetickou bezpečnost, hrozby v kyberprostoru, které jsem rozdělil na základní skupiny a to sociální inženýrství, malware, spam a DDoS útok. Na závěr teoretické části je vymezeno, jaké prostředky je možno použít k ochraně proti těmto hrozbám.

Praktická část bakalářské práce je zaměřena na vytvoření virtuálního počítače, naistalování operačních souborů Windows Vista, Windows 8 a Ubuntu, což je operační systém Linuxu, následně proběhlo aplikování malwaru na tyto operační systémy, v mém případě se jedná o malware typu trojského koně a postupné sledování, jak vybrané operační systémy na tento malware reagují. Dále v praktické části najdeme možnosti obrany proti tomuto útoku. Na závěr je použita metoda SWOT analýzy.

I. TEORETICKÁ ČÁST

1 REŠERŠE LITERATURY

V bakalářské práci bylo čerpáno z odborné literatury, která přinesla nové poznatky, užitečné informace a nové nápady pro řešení mé praktické části. Byly vybrány čtyři nejpodstatnější knihy, které řeší problematiku zabývající se bezpečností operačních systémů osobních počítačů.

První vybranou literaturou je kniha, která nese název Bezpečný internet. Tato kniha má jednoho autora, který se jmenuje Šulc Vladimír. Autor se zde zabývá problematikou zabezpečení citlivých dat, vymezením kybernetických útoků a obranou před nimi. Dále vysvětluje, jaké chování uživatelů vede ke ztrátě či zneužití informací a jak tomu předcházet.

Druhá hlavní kniha se nazývá CyberCrime a autorem této knihy je Jan Kolouch. Obsahuje vysvětlení počítačové sítě a kybernetických pojmů, dále jsou zde popsány projevy kyberkriminality a působnost práva v kyberprostoru a na závěr vymezuje trestněprocesní a kriminalistické aspekty prověřování, odhalování a vyšetřování kyberkriminality.

Třetí kniha s názvem Bezpečně n@ internetu má dva autory. První se jmenuje Martin Kožíšek a tím druhým je Václav Písecký. V knize autoři popisují a vymezují problematiku internetových rizik a největších nebezpečí, které se na internetu vyskytují. Dále zde pojednávají o zásadách bezpečného chování v kyberprostoru a řeší formy kriminality, jako jsou výhružky, podvody, porušování lidských práv a radí jak se jim bránit.

Cybersecurity – attack and defend strategies je poslední vybranou literaturou. Tato kniha je napsána v angličtině a má dva autory se jmény Yuri Diogenes a Erdal Ozkaya, kteří se zde zabývají kybernetickou bezpečností a popisují techniky a programy používané ke kybernetickým útokům v současné době, dále řeší obrannou strategii a vylepšení zabezpečení. Popisují i hrozby a rizika spojené s kyberprostorem a snaží se ukázat, které části systému při napadení jsou zranitelné.

2 OSOBNÍ POČÍTAČ

Osobní počítač můžeme vymezit jako soubor technického vybavení, tedy hardware, který je schopný vyplňovat posloupnost předem stanovených příkazů. Tyto příkazy jsou ve formě programu nebo sady programů, kterému říkáme software. Přívlastek osobní pak už jen znamená, že přístroj je určený pro použití jednotlivcem. [35]

„V nejobecnějším smyslu lze za počítač považovat přístroj, který může být naprogramován za účelem samostatné realizace aritmetických a logických operací.“ [23]

„Elektronické zařízení, které je schopné přijímat informace (data) v určité formě a provádět sekvenci operací v souladu s předem nastavenou, ale variabilní sadou procesních instrukcí (program) za účelem vytvoření výsledku ve formě informací nebo signálů.“ [21]

Počítač můžeme podle typu chápat buď jako klasický stolní PC nebo přenosný, např. laptop či notebook. [30]

2.1 Stolní počítač

Klasický stolní počítač se skládá ze tří komponent. První je samostatná skříň, která obsahuje napájecí zdroj, chladicí ventilátor, základní desku s procesorem, vyrovnávací paměti, harddisk, grafickou a zvukovou kartu a může obsahovat i další komponenty – např. DVD mechaniku, wi-fi nebo bluetooth moduly, plus konektory pro připojení externích periferií (reproduktory, USB, atd). Ke skříni je poté připojen monitor, který přenáší výsledný obraz. Dále je potřeba připojit myš a klávesnici pro ovladatelnost. Myš a klávesnice mohou být připojeny kabelem nebo bezdrátově. Základním znakem stolního počítače je tedy horší přenositelnost (Navarrů, 2017, s. 19).

2.2 Přenosný počítač

Přenosný počítač neboli notebook netvoří jednotlivé komponenty, ale jsou uspořádány jako jeden celek. Při přenášení je monitor přiklopený k počítači, aby se zabránilo poškození monitoru, klávesnice a touchpadu. Touchpad je destička, která je umístěna před klávesnicí. Po této destičce se posouvá prstem a počítač reaguje na pohyb stejně jako myš u stolního počítače. Práce s touchpadem je náročnější a proto se často k notebooku připojuje myš pomocí USB kabelu nebo bezdrátově. [19]

2.2.1 Ultrabook

V souvislosti s notebooky je potřeba uvést i ultrabooky. Ultrabook je chráněná známka společnosti Intel. V podstatě jde o samé zařízení jako notebook, avšak abychom mohli označit nějaké zařízení jako ultrabook musí splňovat určité parametry, jako jsou například nízká hmotnost, vysoká výdrž baterie, atd. [19]

2.2.2 Netbook

Vedle notebooků a ultrabooků se můžeme také setkat s pojmem netbook. Jde o přenosný počítač menší než je právě notebook. Je také levnější a méně výkonnější. Je také zapotřebí uvést, že netbooky nemají CD/DVD mechaniku, proto je potřeba ji pořídit jako externí zařízení. [19]

3 OPERAČNÍ SYSTÉM

Operační systém je základní programové vybavení počítače. Funkce operačního systému tvoří podstatnou složku činností počítače. Je to rozhraní, jehož prostřednictvím uživatel komunikuje s hardwarem. Jinak řečeno je to soubor systémových programů, které nám umožňují spouštět aplikační programy. OS je zaveden do počítače při jeho startu a zůstává v činnosti až do jeho vypnutí. Je tvořen sadou samostatných dílů. Nutnou součástí je jeho jádro, které by však bez příslušných knihoven a hardwarových ovladačů nebylo k ničemu. Nesmí samozřejmě chybět ani uživatelsky přívětivé grafické rozhraní. Operační systém si lze představit jako prostředek komunikace mezi uživatelem a zařízením. Jinými slovy, poskytuje vrstvu abstrakce mezi uživatelem a holým strojem. [20]

V každém počítači musí být OS nainstalován, jinak se stává počítač nefunkčním. Pokud si koupíme nebo sestavíme nový počítač bez OS, nebude umět nic, nezobrazí se žádné ikony a s počítačem nebude možno komunikovat. Operační systém patří mezi tzv. systémový software, který umožňuje efektivně využívat hardware počítače. Dalo by se říci, že OS je taková duše celého počítače a uvede ho k provozu do námi přijatelné podoby. Teprve do operačního systému se pak instalují konkrétní programy. Tyto konkrétní programy neboli tzv. aplikace již pak využívají služeb OS. [29]

3.1 Hardware

Hardware je technické vybavení počítače. Tento pojem vyjadřuje hmotné technické prostředky, které nám umožňují nebo rozšiřují provozování počítače. Je to fyzické zařízení v počítači, tedy zařízení, na které si můžeme sáhnout a je potřeba pro funkci systému a zpracovávání informací. Dalo by se říci, že hardware je vše, co není programovým vybavením počítače. [14]

3.2 Software

Software je pojem, který označuje veškeré programové a netechnické vybavení nutné k provozu počítače. Zahrnuje všechny programy od základních vstupních nebo výstupních systémů, přes operační systémy, grafická rozhraní a veškeré aplikace od jednoduchých až po komplexní programové systémy. [14]

„Software jsou instrukce, které způsobí, že počítač může být využit. Označuje tedy „logickou“ část počítače, kterou nelze vnímat přímo lidskými smysly, tj. „vidět ji nebo si na ni

sáhnout“. V širším slova smyslu to jsou veškeré informace, které jsou v počítači nějakým způsobem uloženy a dále se dělí podle způsobu použití do dvou základních skupin. Jsou to PROGRAMY a DATA.“ [24]

3.3 Úloha operačního systému

Operační systém se stará především o to, aby ostatní programy mohly v počítači správně pracovat, těmto programům přiděluje místo v operační paměti, stará se o organizaci dat na disku, umožňuje pomocí klávesnice nebo myši zadávat počítači různé příkazy. [9]

Tyto systémy vznikly proto, aby mohly zabezpečit programové sdílení prostředků, plánování úloh, plánování a přidělování paměti, aby ochraňovaly data a programy a odhalovaly chyby při běhu programů. [12]

OS vykonává celou řadu operací, které by jinak musel vykonávat každý program zvlášť, což by bylo velmi náročné. Jestliže by každý program obstarával zápis na disk, nastavení klávesnice, myši, tiskárny a podobně, vedlo by to k nejednotnosti vzhledu, nastavení a chování programů, ale také k přemazávání dat na disku, protože by jeden program zapsal na disk podle určitého algoritmu jednu informaci, kterou by pak podle jiného algoritmu přepsal jiný program. [29]

3.4 Struktura operačního systému

Strukturu operačního systému můžeme rozložit na čtyři části a to na jádro, též nazývaného jako kernel, ovladače, ty jsou označovány jako drivery, příkazový procesor (shell) a podpůrné systémové programy. [6]

3.4.1 Jádro

Poskytuje základní úroveň pro řízení všech zařízení počítačového hardwaru. Mezi hlavní role patří čtení dat z paměti a zápis dat do paměti, zpracování prováděcích příkazů, určení způsobu přijímání a odesílání dat pro zařízení, jako je monitor, klávesnice a myš, a určování způsobu interpretace dat přijatých ze sítí. [32]

Jádro OS můžeme rozdělit na tři druhy a to na monolitické, mikrojádro a hybridní.

Monolitické

V monolitickém jádru běží všechny služby OS spolu s hlavním vláknem jádra ve stejné oblasti paměti, to pak umožňuje neomezený přístup k hardwaru. Nevýhodou je, že jakákoliv chyba v libovolném ovladači zařízení pak může shodit celý operační systém. [11]

Mikrojádro

Mikrojádro poskytuje jen základní funkčnost pro vykonávání operací. Ostatní služby, které běžně poskytuje jádro, jsou vykonávány v uživatelském prostředí. Mikrojádra jsou jednodušší než monolitické jádra, ale může v nich docházet k řetězovým změnám kontextu, které způsobí, že OS bude pomalejší. [11]

Hybridní

Hybridní jádro je kombinace dvou předešlých jader, která se snaží vzít od obou to nejlepší a to rychlost od monolitických jader a stabilitu od mikrojader. [11]

3.4.2 Ovladač

Ovladače jsou zvláštní podprogramy pro ovládání konkrétního zařízení. Instalaci těchto ovladačů nabízejí samotné operační systémy při své instalaci, ale je možno je nainstalovat i později. [13]

3.4.3 Příkazový procesor

Je to program, který se spustí po přihlášení uživatele do systému a umožňuje lidem zadávat příkazy do příkazového řádku, pomocí kterého pak uživatel může komunikovat s počítačem a to ve speciálním, ale obvykle jednoduchém jazyce. [2]

3.4.4 Podpůrné systémové programy

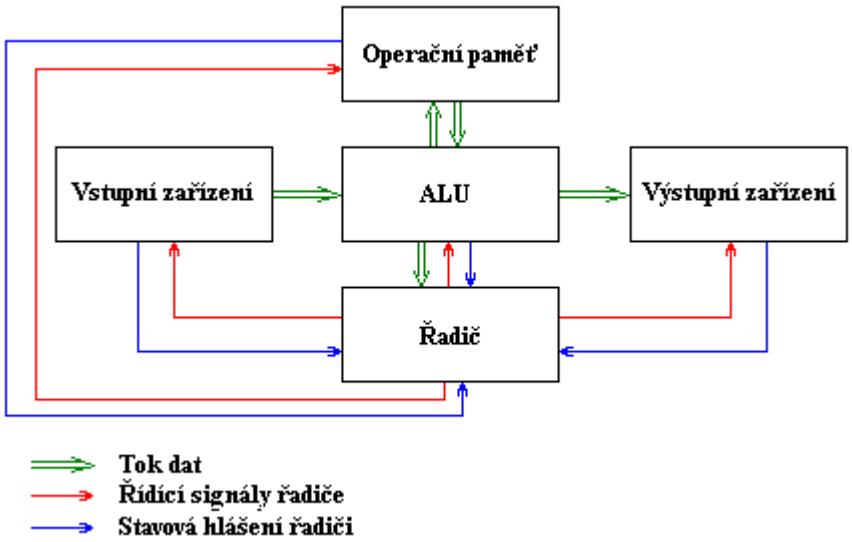
Zde můžeme zařadit překládací programy pro operační systém a sestavující programy. Bez těchto podpůrných systémových programů by některý hardware nefungoval správně nebo vůbec. [29]

4 HISTORIE OPERAČNÍCH SYSTÉMŮ

První počítače neměly žádný operační systém. Každý počítač byl unikátní a bylo nutno napsat program přímo pro něj a často jej dokonce zadávat přímo v binárním kódu, programátor tak musel zadávat přesně jedničky a nuly. Programy byly implementovány napevno v hardwaru a změna programu znamenala i výměnu samotných hardwarových komponent. Tento princip změnil až maďarský matematik John von Neumann, jenž tehdy přišel se zásadním návrhem počítacího stroje s uloženým programem označovaným jako Von Neumanovo schéma. [18]

Ve Von Neumannově schématu se počítač skládá z těchto částí:

- Operační paměť – ukládá programy a data, které jsou pak přemisťovány ke zpracování do procesoru počítače.
- Aritmeticko-logická jednotka (ALU) – procesor, který slouží k vlastnímu zpracování informací.
- Řadič – je to řídící část, která řídí celý počítač podle instrukcí programů.
- Vstupní nebo výstupní zařízení – je to zařízení sloužící ke komunikaci počítače s uživatelem a vnějším okolím počítače. [18]



Obrázek 1 - Von Neumannovo schéma [Zdroj: 18]

4.1 60. léta

Vývoj operačních systémů započal v 60. letech minulého století. Vznikla potřeba vytvořit program, jenž by základní funkce systému obstarával sám a ulehčil tak práci programátorovi. Ten totiž stále musel znát hardware počítače a musel strojovým kódem zadávat, na jaké místo se můžou nahrát data. V případě chyby a zadání již obsazeného úseku nevyskočila žádná chybová hláška a programátor nijak nezjistil, že původní data přepsal. To vedlo k impulsu pro vznik nových operačních systémů. Nejdříve přišla na scénu se svým OS firma IBM, která byla monopolem pro sálové počítače. V roce 1960 vyrobila firma Digital Equipment Corporation první počítač pro širokou veřejnost s názvem PDP-1, který byl vybaven obrazovkou a klávesnicí. Se vznikem těchto minipočítačů vybavených obrazovkovým terminálem vznikla v polovině 60. let potřeba takových operačních systémů, jak je známe dnes. [4]

4.2 70. léta

V 70. letech vznikl snad jeden z nejvýznamnějších operačních systémů vůbec a to OS UNIX od firmy AT&T, protože dal předlohu pro vznik nových a jiných verzí UNIXu. Jeho výjimečnost a síla byla v jednoduchosti, nezávislosti na jakémkoliv hardware a především ve velké standardizaci, která umožňovala správcům systému přecházet mezi jednotlivými verzemi Unixu bez časově náročného zaškolování pro jeho obsluhu na úplně jiné prostředí. Každá verze měla své speciální vlastnosti, ale základ byl všude stejný. Další významné operační systémy, které vznikly v 70. letech, byly například Multics a VMS. Multics byl velkým konkurentem operačního systému Unix, protože byl honosně prosazován firmou Honeywell ve spolupráci s univerzitou MIT. Multics byl hlavně rozšířen v sálových počítačích počátkem 80. let, ale už v roce 1985 byl oznámen konec jeho vývoje, ale i přesto byl poslední systém, který vlastnilo ministerstvo obrany Kanady, vypnut až v říjnu 2000. Další zmíněný operační systém VMS byl od firmy DEC. Jeho první verze byla vydána roku 1978 a na svoji dobu měl velmi moderní sestavení. Vývoj tohoto OS skončil roku 2000. Za zmínku také stojí, že v 70. letech se značně rozvinulo grafické uživatelské rozhraní. Napomohla tomu společnost Xerox, která položila základy pro grafické uživatelské rozhraní dnes známé firmy Apple. [34]

4.3 80. léta

Roku 1981, již známá firma IBM, uvedla na trh svůj osobní počítač s operačním systémem MS-DOS (Microsoft Disk Operating System), kterým ho vybavila právě firma Microsoft. Paradoxem zůstává to, že Microsoft vůbec neměl tento počítač vybavit tímto systémem, ale firma IBM nestíhala svůj operační systém Top - View dokončit v termínu, tak sáhla po variantě od Microsoftu. Kdo ví, co by se stalo, kdyby svůj OS stihli dokončit, možná by Microsoft zanikl a dnešní svět operačních systémů by vypadal úplně jinak. Zajímavé také je, že operační systém MS-DOS nebyl vůbec produktem firmy Microsoft, ve skutečnosti se jednalo o mírně upravený operační systém CP/M (Control Program for Microcomputers), který vznikl již dříve pro zjednodušení UNIXu a jeho přínosem bylo například to, že označoval disketové jednotky písmeny. Oba tyto systémy byly na svou dobu zastaralé, nedostatečné a nepohodlné, protože podporovali jen jednoho připojeného uživatele, který mohl pracovat pouze s jedním jediným programem v daném okamžiku, navíc zde byla hardwarová omezení, která nedovolila uživateli pracovat s pamětí větší než 640 kB nebo s disky, které byly větší než 30 MB. Toho se snažila využít firma Apple a drala se do popředí trhu roku 1983 se svým počítačem Lisa, který obsahoval operační systém s grafickým uživatelským rozhraním, což přinášelo to, že uživatel mohl myší ovládat okénka, namísto příkazového řádku. Tento počítač byl ale propadák, a tak firma Apple rok na to vydala počítač s názvem Macintosh, který byl jednodušší, levnější, bylo možné přímé editování dokumentů, označení disků a pro své ovládání myší se s ním mohl naučit zacházet prakticky kdokoliv a právě tyto prvky mu pomohly se na trhu prosadit. [4]

Obrázek 2 – Apple Macintosh [Zdroj: 4]

Další operační systémy, které se objevily v 80. letech a stojí za zmínku, jsou například operační systémy Solaris od firmy Sun Microsystems a NeXT Step, který byl vydán jedním ze zakladatelů firmy Apple a to Stevem Jobsem, který skrz neshody firmu opustil a snažil se na trhu prosadit sám právě tímto systémem, to se mu ale nepovedlo, i když systém měl

plně grafické rozhraní, byl vázán na předem daný hardware, a proto u široké veřejnosti neuspěl. Steve Jobs se po neúspěchu vrátil do firmy Apple. [27]

4.4 90. léta

V roce 1991 vytvořil finský student Linus Torvalds operační systém s názvem Linux, což byl jakýsi klon UNIXu pro PC a dostal se do popředí, protože byl jednoduchý a nebyl tak pomalý. Jedná se o systém, který poskytuje zdarma své produkty a zdrojové kódy a umožňuje tak každému upravit si systém podle svého. [4]

Obrázek 3 – Logo operačního systému Linux [Zdroj: 4]

V devadesátých letech na trhu naprosto kralovala firma Microsoft a stala se tak obávaným monopolem ve světě operačních systémů. Tato firma se poučila ze svých minulých chyb, zapracovala a snažila se změnit své nedostatky, jako byly např.: změna virtuální paměti, výkonné grafické prostředí a uživatelské rozhraní a skvělá spolupráce s hardwarovou technikou. Roku 1995 vydala firma Microsoft svůj povedený OS s názvem Windows 95, který této firmě zajistil nesmrtelnost na trhu a možnost se dále rozvíjet. Avšak o 3 roky později přišel lehký pád se systémem Windows 98, který sice přinášel pozitivní změny jako nový Internet Explorer 4, nová úhlednější okna a podporu USB portů, ale širokou veřejností byl odsouzen, protože obsahoval spoustu chyb v jádře a špatné ovladače, které způsobovaly, že systém byl nestabilizovaný a často padal. [27]

Dle mého názoru to do budoucna vypadá tak, že trh si rozdělí operační systémy Windows, protože ho používá většina lidí, a Linux protože se neustále vyvíjí, dostává se do povědomí lidí a je zdarma. Za to Mac OS od firmy Apple je pomalu vytlačován, ale zachová si na trhu své místo, protože je určen pro lidi s větším obnosem peněz a lidi, kteří očekávají od svého systému jistotu.

5 KYBERPROSTOR

Tímto termínem se označuje virtuální prostor uměle vytvořený člověkem, ve kterém dochází ke zpracování, uchování a výměně informací. Kyberprostor je neomezený a nemá svůj konec ani začátek. Předmětem tohoto prostoru jsou kybernetické aktivity a tvoří jej informační systémy, služby a sítě elektronických komunikací. Jednoduše by se za kyberprostor dal označit celý internet, který vede signál či data vzduchem, kabely nebo jinými přenosovými médii a je to soustava vzájemně propojených počítačů, které dovolují sdílet, komunikovat a přistupovat k obsahovaným informacím v rámci celé sítě. Mezi znaky kyberprostoru lze zařadit jeho decentralizovanost, globálnost, otevřenost, bohatost na informace, interaktivnost a možnost ovlivňování domněnek a myšlení skrze uživatele. Do podvědomí lidí se pojem kyberprostor začal dostávat po vydání deklarace Johna Barlowa ve švýcarském Davosu roku 1996, která upozorňuje a varuje před riziky a hrozbami spojené s kyberprostorem. V poslední době se ukazuje, že projev světa virtuálního může a má dopady ve světě reálném. [14]

5.1 Kybernetická bezpečnost

Je ochrana dat před zcizením, zničením či poškození v souvislosti s počítači a počítačovými sítěmi. Jsou to určité postupy a mechanismy, jejichž úkolem je chránit cenné informace a služby před zveřejněním, poškozením nebo kolapsem neoprávněnou činností nebo činností nedůvěryhodné osoby a neplánované události. Kybernetická bezpečnost je modelový stav, který je narušován různými kybernetickými hrozbami. Cílem kybernetické bezpečnosti je zajištění dostupnosti počítačů a jejich sítí, zajištění důvěrnosti a integrity uchovávaných, zpracovávaných a přenášených dat. Předmětem kybernetické bezpečnosti je problém narušení fungování kyberprostoru a reálného světa. [26]

5.2 Kybernetické hrozby

Kybernetické hrozby mají velký potenciál způsobit značnou škodu a jsou čím dál častější, proto se právem řadí mezi nejzávažnější rizika. Jejich nebezpečnost spočívá právě v tom, že náklady na jejich realizaci jsou zanedbatelné vzhledem ke škodě, kterou mohou napáchat. Uvádí se, že dopad kybernetických útoků může být dokonce větší, než škody způsobené přírodními katastrofami a klasickými teroristickými útoky, protože mohou narušit či dokonce způsobit selhání kritické infrastruktury. [39]

Je jisté, že hrozba a potencionál kybernetických útoků nadále poroste, protože roste počet zařízení připojených k Internetu, počet potencionálních obětí, počet útočníků a tím i logicky roste počet kybernetických útoků. Dnešní trend je mít přístup na internet kdykoliv, odkudkoliv a z čehokoliv. Lidé si neuvědomují rizika spojené používáním svých soukromých zařízení na veřejných sítích, kde je ochrana dat slabá a zadávají své osobní informace. Další skutečnost, která může nahrávat potencionálním útočníkům je otevřenost na Internetu, kde může kdokoliv vytvářet a sdílet obsah, své know-how, včetně informací, jak na někoho provést kybernetický útok. [31]

Tabulka 1 – Základní typy hrozeb [Zdroj: 5]

HROZBY	**NÁHODNÉ**	**ÚMYSLNÉ**
EXTERNÍ	Přírodního původu	Hacking
INTERNÍ	Technické selhání (lidská chyba)	Sabotáž

Postupem času hackeři dokázali odborníkům na kybernetickou bezpečnost, že mohou být vytrvalí, kreativní, a stále sofistikovanější s jejich útoky na operační systém. Naučili se, jak se přizpůsobit změnám v kybernetickém prostředí, a tím upravit své kybernetické útoky. [8]

5.2.1 Sociální inženýrství

Sociální inženýrství můžeme definovat tak, že je to způsob ovlivňování, přesvědčování či manipulování s lidmi tak, aby lidé byli donuceni provést určitou akci či útočníkům se podařilo získat informace, které jsou běžně nedostupné. Ve většině případů útočník nepřichází do osobního kontaktu s obětí a své oběti si vybírá nahodile nebo svůj útok vede cíleně na konkrétní osoby. Sociální inženýři se dokážou ze svých chyb poučit, a proto neustále své útoky vylepšují a přizpůsobují prostředí. [15]

Jestliže neopatrný uživatel uvěří věrohodnosti podvodného emailu a klikne na falešný odkaz, dostane se na podvodné stránky, kde jsou po něm požadovány přístupové údaje k účtům, platebním kartám nebo jiné osobní a důvěrné informace. Pokud je uživatel naivně vyplní, získají tato data podvodníci, kteří je následně využijí ve svůj prospěch. [14]

5.2.2 Malware

Malware je obecné označení běžně používané pro jakýkoliv škodlivý software. Malware je zkratka z anglického malicious software, což znamená, jak už bylo v úvodu napsáno, škodlivý software. Projevy napadnutí můžou být různé, protože malware může napadnout v podstatě cokoliv. Výsledek je ale vždy téměř stejný. Útočník získá přístup do počítače, a tím pádem i k souborům a programům a může ovlivnit chod vašeho počítače. Většina tohoto škodlivého softwaru se vyznačuje tím, že se v zařízení skrývá a snaží se v počítači zůstat i po restartu. Obvykle platí, že k útoku je potřeba součinnost ze strany napadeného uživatele. [31]

Základní malware můžeme rozdělit na viry, trojské koně, červy, ransomware a spyware.

Vir

Vir je program nebo obecně nějaký škodlivý kód, který sám sebe připojí k existujícímu spustitelnému programu či dokumentu a začne se reprodukovat v momentě, kdy dojde ke spuštění softwaru nebo infikovaného dokumentu. Existuje nespočet druhů virů a jejich chování se může různě lišit, třeba od neškodného vyhrávání melodie, přes zahlcení systému, změnu či, zničení dat, až po celkovou destrukci napadeného systému. [14]

Viry můžeme rozdělit podle, toho jaký software napadají:

- Systémová oblast – boot viry
- Soubory – souborové viry
- Soubory i systémové oblasti – multiparitní viry
- Aplikace – makroviry [14]

Trojský kůň

Trojský kůň je škodlivý malware, jak už z názvu napovídá, který je ukryt v údajně užitečných programech a souborech, které se stáhnou z internetu. V podstatě si stáhnete dva programy v jednom, kdy ten první dělá to, co od něj očekáváte, a druhý provádí v počítači nekalou činnost. Trojský kůň může zašifrovat soubory, smazat je, způsobit blikání obrazovky či dokonce vyvést z provozu celý operační systém. [22]

Červ

Program, který se šíří pomocí počítačové sítě, za využívání sdílených disků či jiných komunikačních kanálů, nejčastěji pomocí elektronické pošty. Adresa odesílatele bývá většinou podvržena. [16]

Červ pomocí svého programového kódu infikuje všechny soubory, které mu mohou posloužit jako nosič. Šíří se pomocí nevinného programu a může infikovat i soubor vytvořený pomocí aplikace Microsoft Office a právě proto jsou v posledních verzích přidána upozornění, varující před nežádoucím přenosem programových kódů do souboru s excelem, wordem apod. [22]

Ransomware

Je typ malwaru, jehož prostřednictvím vyžaduje útočník na náš operační systém peníze, ať už pod různými výhružkami, zašifrováním dat nebo pod falešnou výzvou k zaplacení pokuty za porušení autorských práv nebo používání nelegálního softwaru. Když dojde k napadení tímto malwarem, vetšinou jsme vyzvání k provedení platby na nějakou adresu či bankovní konto. [16]

Spyware

Další internetová hrozba, jak už z názvu napovídá, provádí na počítači nežádoucí špionáž. Může se jednat o program, který za vás vyřizuje určité záležitosti, avšak mezi tím prohledává počítač a získává z počítače data, které dává nenápadně dohromady a ve vhodnou chvíli je pošle druhé osobě. [31]

Spyware se nejvíce zaměřuje na následující data:

- Přístupové údaje a hesla k e-mailovým službám, internetovému bankovnictví apod.
- Údaje o kreditních kartách.
- Sériová a registrační čísla softwaru.
- Osobní informace. [22]

5.2.3 SPAM

Zjednodušeně se dá spam popsat jako nevyžádaná pošta, která se rovněž nazývá jako junk mail nebo unsolicited mail. Jedná se o určité sdělení zasílané elektronicky, hromadně a bez vyžádání. K tomu, aby mohl spam rozesílat tyto nevyžádané zprávy, využívá různé komunikační kanály, jimiž jsou například e-mail, messenger (ICQ, Skype, Facebook), SMS,

MMS, blogy a jiné sociální sítě. Obsahem spamu můžou být informace obchodní, reklamní, lékařské, edukační, finanční, náboženské, kriminální nebo třeba pornografické. [3]

Z hlediska informačních a komunikačních technologií lze spam chápat ve dvou směrech. V užším slova smyslu můžeme říct, že se jedná o hromadné šíření nevyžádaného sdělení nejčastěji reklamního charakteru pomocí Internetu, nejčastěji prostřednictvím elektronické komunikace. V širším slova smyslu se pak jedná o všechny doručené nevyžádané zprávy, tedy i např. o zprávy obsahující viry, trojské koně apod. [14]

Obrázek 4 – Rozdělení spamu [Zdroj: 14]

Spam s sebou může nést závažnější riziko, kdy bude například antispam filtr příliš omezující nebo bude příjemcem smazán e-mail, který měl být přečten či jinak zpracován. V množství doručených e-mailů se může snadno stát, že příjemce důležitou zprávu přehlédne, smaže ji nebo přesune do složky se spamem a stane se tak, že zde skončí důležitá zpráva, kdy příjemce pak nepotvrdí účast na důležitém setkání či jinak neodpoví a může se tak snadno díky spamu dostat do problémů. [25]

HOAX

Hoax je jedna z forem spamu. Z anglického jazyka to lze přeložit jako podvod, kanadský žertík či smyšlenka. Je to označení pro lživé, zkreslené zavádějící či jinak falešné informace. Obsahuje varování před útoky, popisy nebezpečí, prosby o pomoc, výzvy, petice, prohlášení slavných, řetězové dopisy štěstí, žertovné zprávy, obrázky a videa. [14]

K jeho šíření napomáhají především samotní příjemci tohoto e-mailu, kteří falešné zprávě uvěří a začnou ji šířit dál. V případě dopisů štěstí, kdy je příjemce varován, že pokud nepřepošle zprávu dál, tak se jeho přání nesplní, případně bude mít smůlu, tak nejde o to, že by byly nebezpečné z pohledu toho, že zatěžují síťovou infrastrukturu nebo že dochází

k šíření lživých informací, ale jde především o to, že jak dochází k přeposílání dalším příjemcům, internetem se přenáší seznam aktivních e-mailových adres a tyto adresy pak mohou být zneužity k dalšímu šíření spamu. [31]

SCAM

Scam je komunikování s obětí nejčastěji přes e-mail, kdy je cílem podvodníka vytáhnout z oběti peníze, za využití technik sociálního inženýrství. Může vás oslovit neznámý člověk, že zdědil, získal nebo dokonce spravuje něčí majetek ve výši několika desítek milónů dolarů a potřebuje pomoc při jeho převodu ze země. Za to je slíbená odměna ve výši několika desítek procent z celkové částky. Princip podvodu spočívá v tom, že oběť musí neustále platit nečekané administrativní poplatky a převod majetku se stále oddaluje. Patří sem i podvodné loterie, výhry, žádosti o finanční pomoc nebo příspěvek na charitativní akci, která ve skutečnosti neexistuje, popřípadě na ni parazituje. Některé podvody bývají provedeny jednoduše, ale velmi často bývají propracovány i do drobných detailů, jako jsou profesionálně vytvořeny webové stránky neexistujících společností a bankovních institucí nebo si pachatel nechá posílat peníze přes další oběť, kdy ji využívá jako prostředek pro převod peněz, oběť tak o tom nemá ani ponětí a může se tak snadno dostat do problému. Obětem bývají zasílány i podvržené falešné dokumenty a certifikáty. [10]

Phishing

Phishing je další druh nevyžádané pošty, který stejně jako oba předešlé druhy spamu využívá technik sociálního inženýrství. Tento termín připomíná anglické slovo fishing, tedy rybaření a ve skutečnosti to není daleko od pravdy, protože útočník nahodí pomyslnou návnadu a snaží se příjemce přesvědčit, aby kliknul na nějaký odkaz či otevřel přílohu v e-mailu. Pokud je otevřen odkaz, příjemce je přesměrován na stránky podobné firmám či institucím a je následně vyzván k vyplnění citlivých osobních údajů, jako jsou hesla, údaje o platebních kartách, rodná čísla nebo čísla bankovních účtů, ty jsou poté zcizeny, zneužity nebo přeprodány. V druhém případě, kdy e-mail obsahuje přílohu a příjemce ji otevře, tak je do jeho počítače načten škodlivý kód či malware, který později může způsobit problémy. [31]

Jedna z technik, která se stává čím dál více používanější, je, že útočník pošle e-mail, který vypadá například jako od Facebooku a v něm je psáno, že máme zmeškanou nějakou událost nebo upozornění. Tímto vzniká zvědavost uživatele a ten pak klikne na odkaz, který ho

přesměruje na podobné stránky a vyplní své údaje, ve skutečnosti tak ale své citlivé osobní informace pošle útočníkovi. [8]

Tabulka 2 – Rozdíl mezi jednotlivými typy spamu [Zdroj: 28]

E-MAIL	REKLAMNÍ SPAM	HOAX	SCAM	PHISHING
ADRESA ODESÍLATELE	Je zneužit e-mail někoho jiného nebo je založen za účelem jednorázového rozesílání pošty.	Příjemce zprávy dobrovolně přepošle e-mail dalším lidem.	E-mailová adresa je platná po celou dobu, neboť podvodník s obětí cíle komunikuje.	Je zneužit e-mail někoho jiného nebo je založen za účelem jednorázového rozesílání pošty.
PŘÍLOHA E-MAILU	Zpravidla neškodná.	Zpravidla bez příloh, ale může obsahovat obrázky.	Zpravidla neškodná.	Pokud obsahuje přílohu, vždy se jedná o malware.
OBSAH A FORMA E-MAILU	HTML s obrázky, bez chyb, často v jiném jazyce.	V jazyce příjemce bez očividných chyb. Podpořený odkazy a citacemi.	Různá úroveň. Často strojový překlad.	Různá úroveň. Bez zjevných gramatických chyb.

5.2.4 DDoS útok

Nejprve než vysvětlím, co to DDoS útok je, je potřeba si vymezit, co tato zkratka vůbec znamená.

Zkratka DDoS je složeninou ze dvou částí, kdy první písmeno D znamená distributed, neboli distribuovaný a to v tomhle případě znamená rozložený na větší množství uživatelů. Druhá část složeniny DoS znamená denial of service, což můžeme přeložit jako odmítnutí služby. Tento útok je prováděn převážně proti velkým společnostem a spočívá zjednoduše-

ně v tom, že jeden nebo více útočníků zatíží server, což způsobí, že na serveru nepůjde nějaká konkrétní služba nebo stránka nepůjde vůbec zobrazit, protože to server nebude stíhat. Může se také stát, že požadovaná stránka se nebude zobrazovat ani po skončení zátěže, takže se administrátor serveru musí stránku sám znovu zprovoznit. Je zajímavé, že tento útok není trestným činem ani nelegálním jednáním a je brán jako demonstrativní vyjádření a nesouhlasu s něčím. [7]

6 OCHRANA DAT

Existuje mnoho postupů a technik, kterými může útočník poškodit operační systém a narušit tak data v něm, proto je důležité data určitým způsobem chránit. Cílem ochrany dat je zabezpečit informace a data před zcizením, zneužitím, smazáním či jiné negativní manipulace s nimi.

6.1 Firewall

Firewall je síťové, technické či programové vybavení OS, které slouží jako vstupní a výstupní brána pro komunikaci mezi počítačem a internetem, kdy data putující ven a zejména dovnitř jsou kontrolována tímto programem a na základě předdefinovaných nebo dynamických pravidel jsou pak tyto data povoleny nebo blokovány, a tím je zajištěna bezpečná komunikace mezi počítačem a sítí. Firewall za anglického překladu znamená ohnivzdorná zeď, což v internetovém světě znamená software, který filtruje příchozí i odchozí komunikaci do sítě. Firewall běží jako program na pozadí a pro zjednodušení tohoto pojmu by se dalo představit, že firewall je jakási stráž, která podle příkazů rozhodne, koho pustí dovnitř a ven. [16]

6.2 Antivirový program

Mezi základní a nejdůležitější ochranu dat před negativními jevy patří aktualizovaný antivirový program, který pomáhá identifikovat podezřelé aktivity v počítači, odstranit, přesunout do karantény a eliminovat počítačové viry a jiný škodlivý software. Například Windows Defender je do Windows 8 pevně integrován, ale většina antivirových programů jsou nainstalovány do systému jako doplňkové aplikace posléze. Antivirový program je jedním z nejprodávanějších doplňkových programů k operačním systémům, avšak některé druhy antiviru poskytují tzv. free verze, kdy je ochrana počítače základní a za plnou verzi si poté musíme připlatit. Aby byl antivirový program funkční a zcela účinný, musí být pravidelně aktualizován. [21]

6.3 Zálohování

Je určitá ochrana dat před kybernetickým útokem nebo selhání hardwaru či softwaru, kdy zálohovaná data jdou po negativní události obnovit. Zálohování dat spočívá v utvoření kopií souborů, které poté chceme obnovit. Tento proces se nazývá backup a procesu obno-

vy dat restore. Zálohování může být prováděno ručně nebo automaticky. Když jsou zálohována všechna data, tak mluvíme o plné záloze, což je v angličtině označováno jako full backup. Pokud zálohujeme nově vytvořená data od minulé zálohy, tak zde mluvíme o přírůstkové záloze, která je v angličtině označována jako incremental backup. Tato činnost k ochraně dat může probíhat nepravidelně nebo pravidelně podle rozvrhu a za použití speciálního programu v operačním systému. Zálohovat data můžeme na pevný disk, CD/DVD, flashdisk či dokonce na virtuální úložiště označované jako cloud. [31]

6.4 Šifrování

Za účelem ochrany dat před zneužitím, můžeme tyto data určitým způsobem šifrovat, a tím je zajištěno, že útočník, který nám data ukradne a získá k nim neoprávněný přístup, nebude moci tyto data použít. K šifrování dat se používá kryptografický algoritmus, který převádí námi napsaný text na zašifrovaný text. Tento proces je se označuje jako šifrování a není nic jiného než matematická operace, kdy dochází k převodu jedné množiny znaků na druhou. Klíč, který je použit k šifrování by měl být dostatečně dlouhý a měl by být požit pouze jednou z důvodu bezpečnosti. [31]

7 CÍL A ZVOLENÉ METODY ZPRACOVÁNÍ

Cílem teoretické části bylo se seznámit s informacemi co to vůbec osobní počítač je, vymezit jeho definice a jak se může dělit. Charakterizovat operační systém, co je jeho úlohou, popis jeho struktury a historie. Dále bylo cílem vymezit kyberprostor a s tím související kybernetickou bezpečnost, hrozby v kyberprostoru a na závěr teoretické části jaké prostředky je možno použít k ochraně proti těmto hrozbám.

Cílem praktické části je vytvoření testovacího prostředí, kdy v mém případě je to virtuální počítač a následné nainstalování tří operačních systémů. Nejdůležitější částí je pak útok pomocí zvoleného malwaru. Tímto zvoleným malwarem je trojský kůň MEMZ, který je aplikován na všechny tři operační systémy. Cílem bylo sledovat, jak se tyto systémy zachovají a posléze doporučit nejbezpečnější z nich.

7.1 Metody použité při zpracování práce

V teoretické části jsem prostudoval odbornou literaturu a použil jsem dostupné zdroje ve formě internetových publikací. Pro studium odborných tištěných zdrojů jsem navštěvoval knihovnu UTB ve Zlíně, kde jsem čerpal z publikací, které souvisely s problematikou operačních systémů a možných útoků na ně.

V praktické části jsem využíval virtuálního počítače, díky jehož pomocí jsem mohl aplikovat škodlivý malware na vybrané operační systémy a následně analyzovat průběh nákazy. V závěru praktické části je použita metoda SWOT analýzy na vybrané operační systémy.

II. PRAKTICKÁ ČÁST

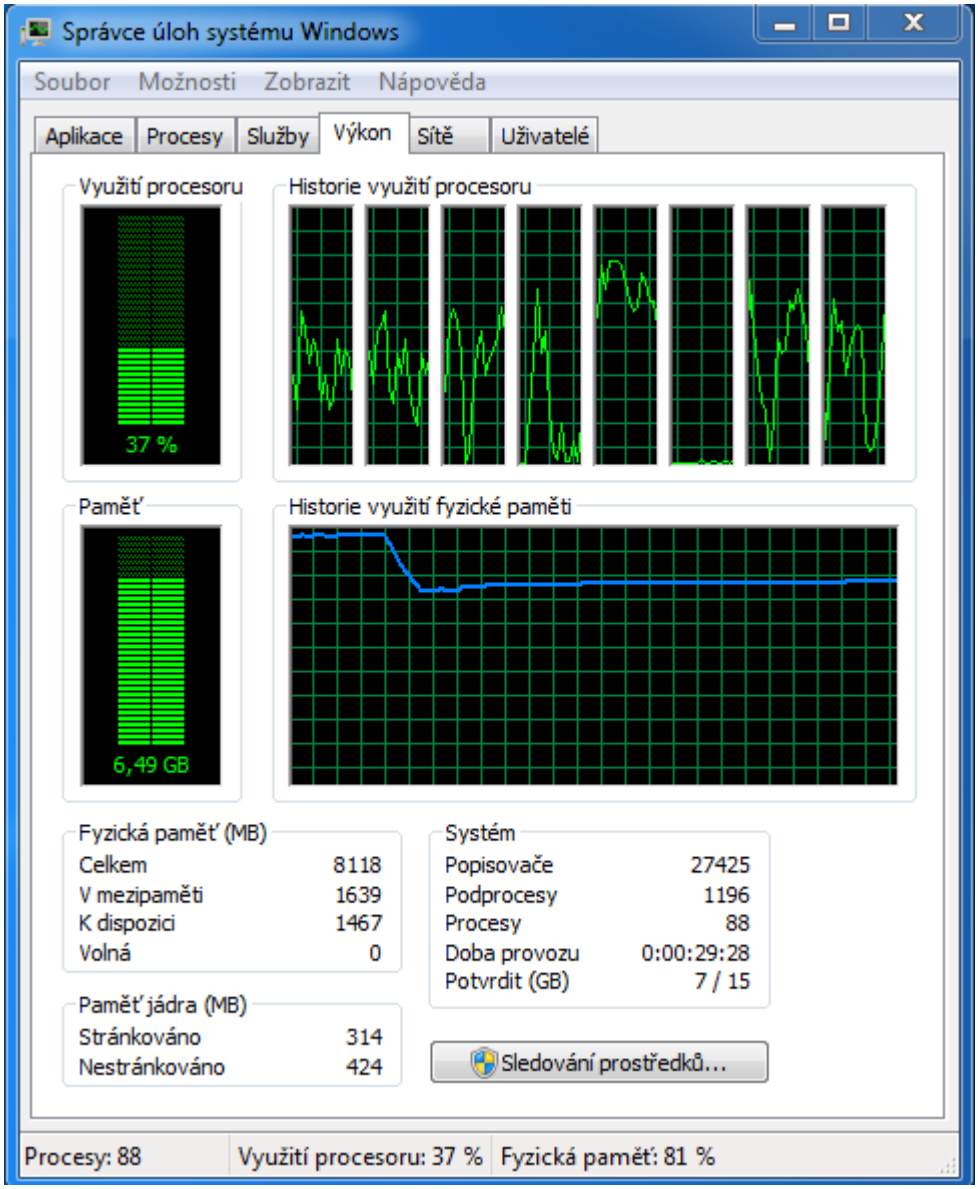
8 TESTOVACÍ PROSTŘEDÍ

Připravit testovací prostředí byl první krok v praktické části mé bakalářské práce. Za testovací prostředí byl zvolen virtuální počítač s následně nainstalovanými operačními systémy, který byl vytvořen konkrétně v programu VMware Workstation Pro. Tato aplikace je placená, avšak její vyzkoušení je na 30 dní zdarma. Tento program je složitější, než podobné aplikace na vytvoření virtuálního počítače, ale mnou byla zvolen pro jeho rozsáhlejší funkce a možnosti využití neplacené verze po dobu třiceti dní.

8.1 Virtuální počítač

Pod pojmem virtuální počítač si můžeme představit jednoduše počítač v počítači. Jedná se tedy o jakýsi druh počítače, který není hmatatelný, ale je vytvořený v počítači již hmatatelném, tedy v aktuálním stroji co používáme, např.: stolní počítač, notebook, atd. a to za použití hardwarových prostředků hostitelského stroje. Pro vytvoření virtuálního počítače je potřeba použít virtualizační aplikaci. Virtualizační aplikace pak umožňuje na počítači spustit současně několik operačních systémů najednou. Můžete např.: pracovat v Linuxu a v dalším okně mít spuštěné Windows, nebo jiný podporovaný operační systém. [1]

Virtuální počítač je počítačový soubor, obvykle označovaný jako image. Jeho velkou výhodou je to, že je oddělený od zbytku systému, což znamená, že software ve virtuálním počítači nemůže nijak napadnout a poškodit samotný počítač. Testování dalších operačních systémů, simulování útoku napadení virem, vytváření záloh operačního systému a spouštění softwaru nebo aplikací v operačních systémech, pro které nebyly původně určeny, jsou úkoly, pro které nám virtuální počítač vytváří ideální prostředí. Každý virtuální počítač poskytuje vlastní virtuální hardware, včetně procesorů, paměti, pevných disků, síťových rozhraní a dalších zařízení. Virtuální počítač se následně mapuje na skutečný hardware v námi používaném fyzickém počítači. Díky tomu šetří následné náklady, protože omezuje potřebu fyzického hardwaru pro systémy, tím snižuje související náklady na údržbu a navíc snižuje nároky na energii a chlazení. V případě serverů, kdy je vedle sebe spuštěných několik operačních systémů, které spravuje jeden kus softwaru, tak bývá označován jako hypervisor. Pokud chceme mít spuštěno několik operačních systémů, musíme tomu přizpůsobit hardware skutečného počítače. [17]

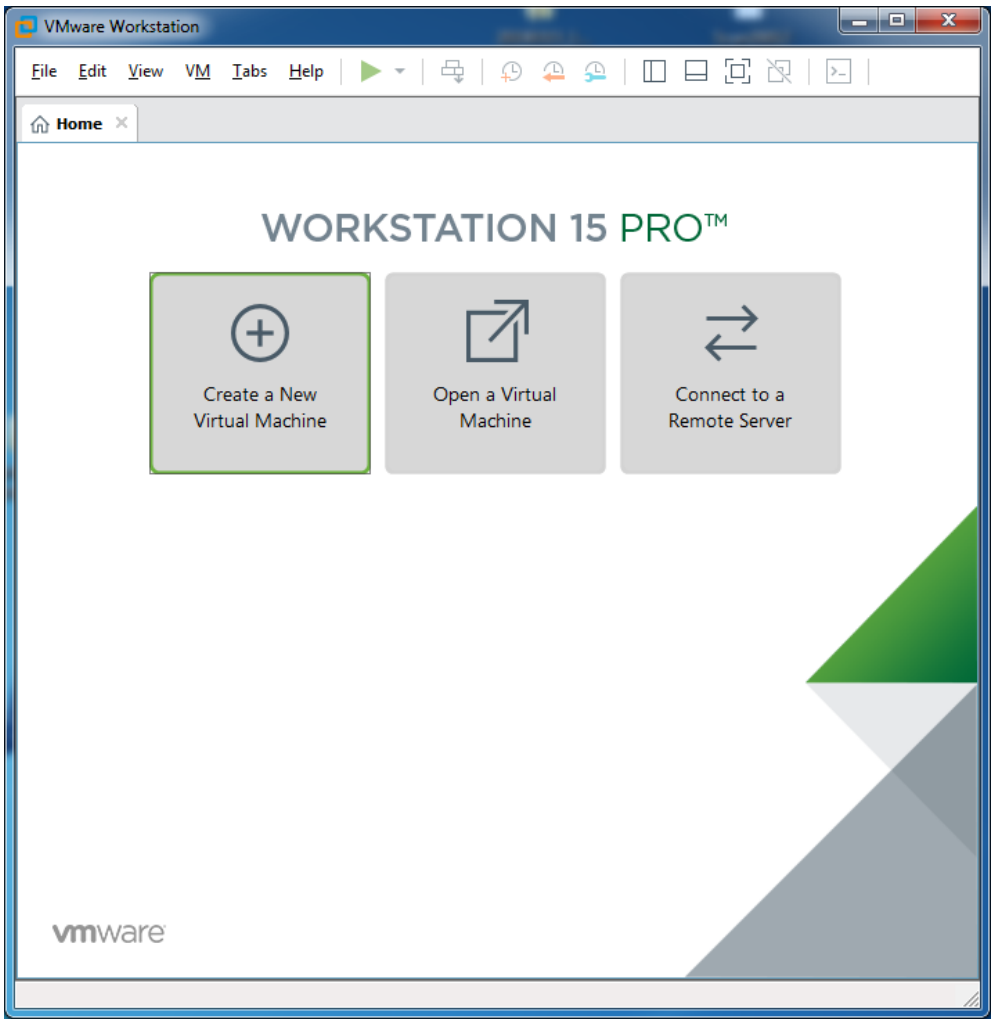


Obrázek 5 – Zatížení hardwaru při spuštění více virtualních počítačů zároveň

[Zdroj: Vlastní]

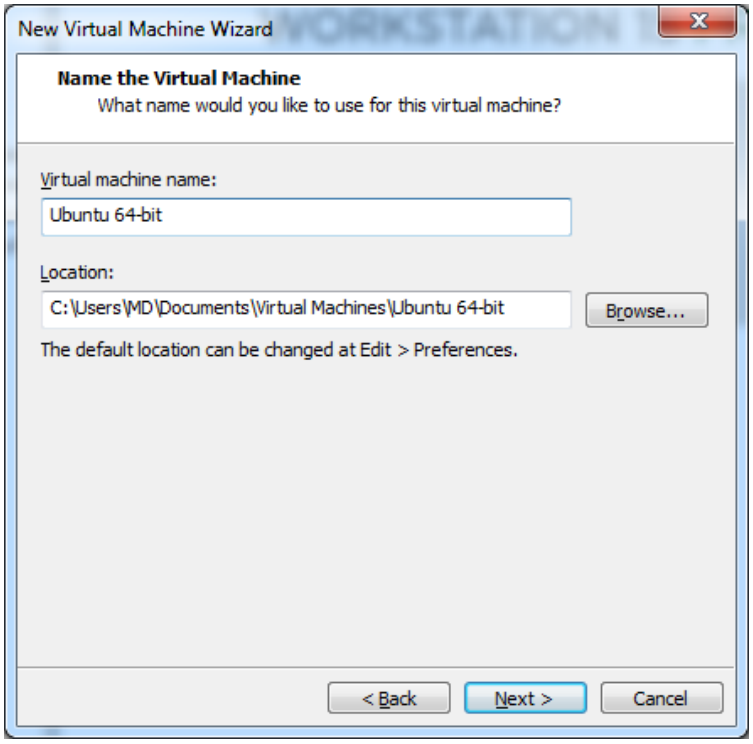
8.2 Vytvoření virtuálního počítače

Nyní popíšu samotnou instalaci virtuálního počítače. První krok k vytvoření virtualitzačního prostředí pomocí aplikace VMware Workstation Pro bylo kliknutí na ikonku „Vytvořit nový virtuální počítač“, což zobrazuje obrázek s číslem 6.



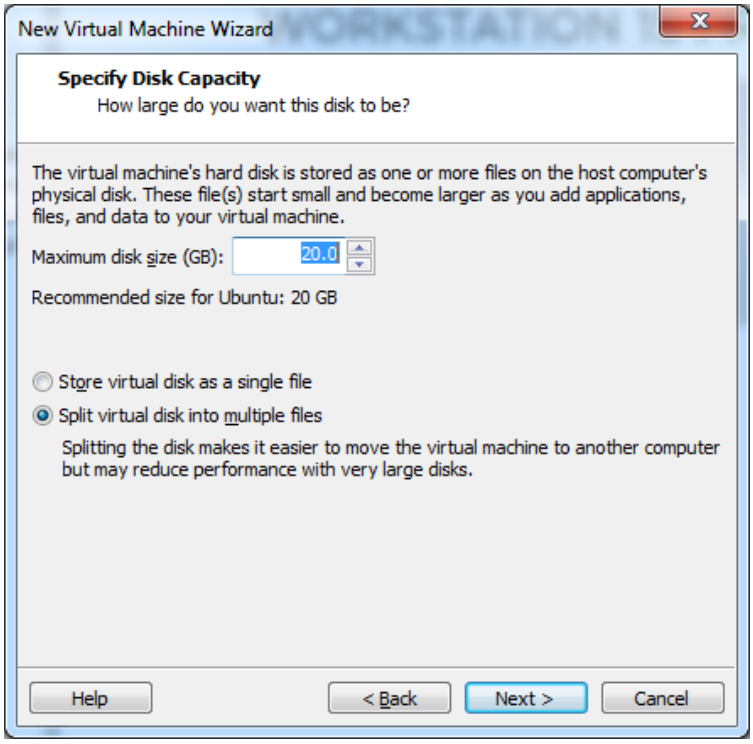
Obrázek 6 – Aplikace VMware workstation 15 Pro [Zdroj: Vlastní]

Dalším krokem bylo pojmenování virtuálního počítače a nadefinování jeho umístění ve fyzickém počítači (obr. č. 7). Protože jsem se rozhodl mít ve virtualizační aplikaci vytvořených více virtuálních počítačů, tak pro lepší přehlednost jsem zvolil pojmenování virtuálních počítačů podle jejich operačních systémů.



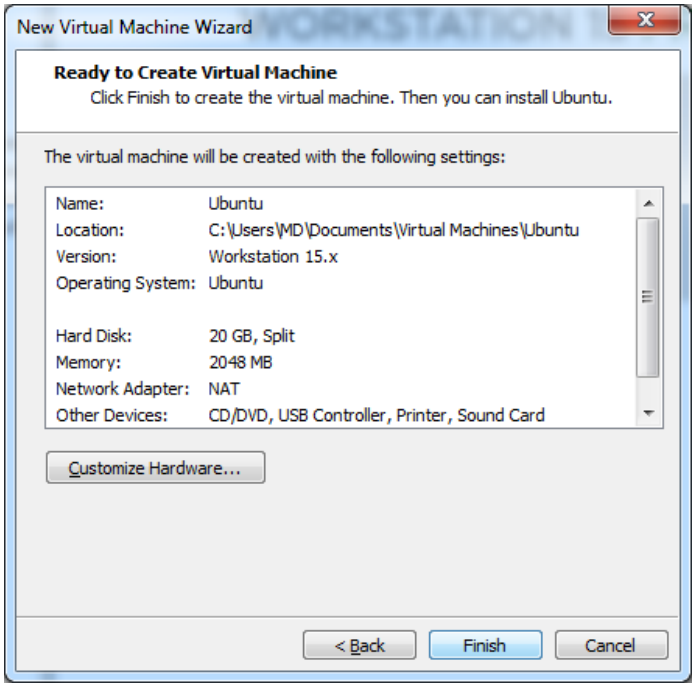
Obrázek 7 – Pojmenování a umístění virtuálního počítače [Zdroj: Vlastní]

Poté byla zvolena velikost hard disku virtuálního počítače, která byla nastavena na 20 GB. (Obr. č. 8)



Obrázek 8 – Nadefinování velikosti hard disku virtuálního počítače [Zdroj: Vlastní]

Na následujícím obrázku č. 9 vidíme shrnutí nastavení virtuálního počítače, kdy při kliknutí na tlačítko dokončit vytvoříme virtuální počítač, do kterého můžeme následně nainstalovat operační systém, a ve kterém byly prováděny další úkony.



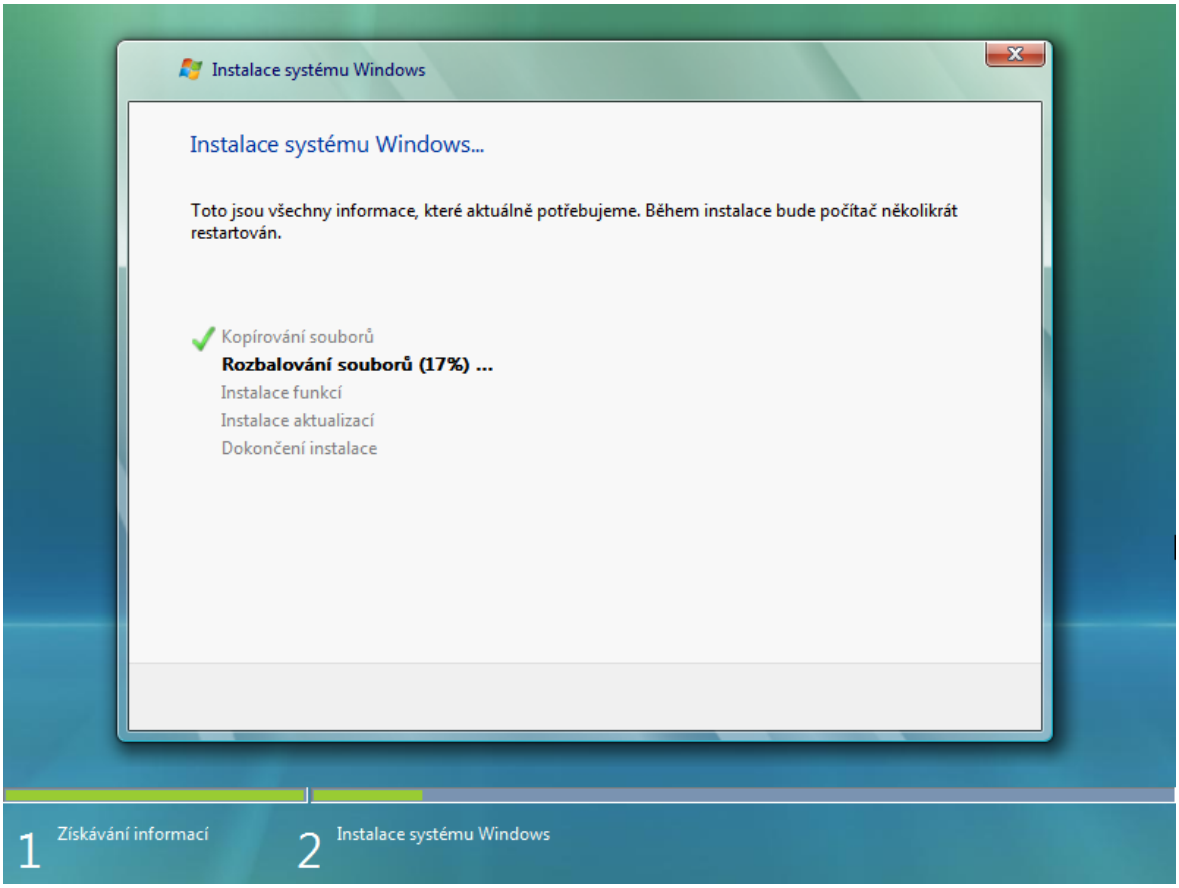
Obrázek 9 – Shrnutí nastavení virtuálního počítače [Zdroj: Vlastní]

8.3 Instalace operačních systémů

Pro srovnání bezpečnosti byly vybrány a nainstalovány tyto operační systémy: Windows Vista, Windows 8 Pro a Linux (Ubuntu).

8.3.1 Windows Vista

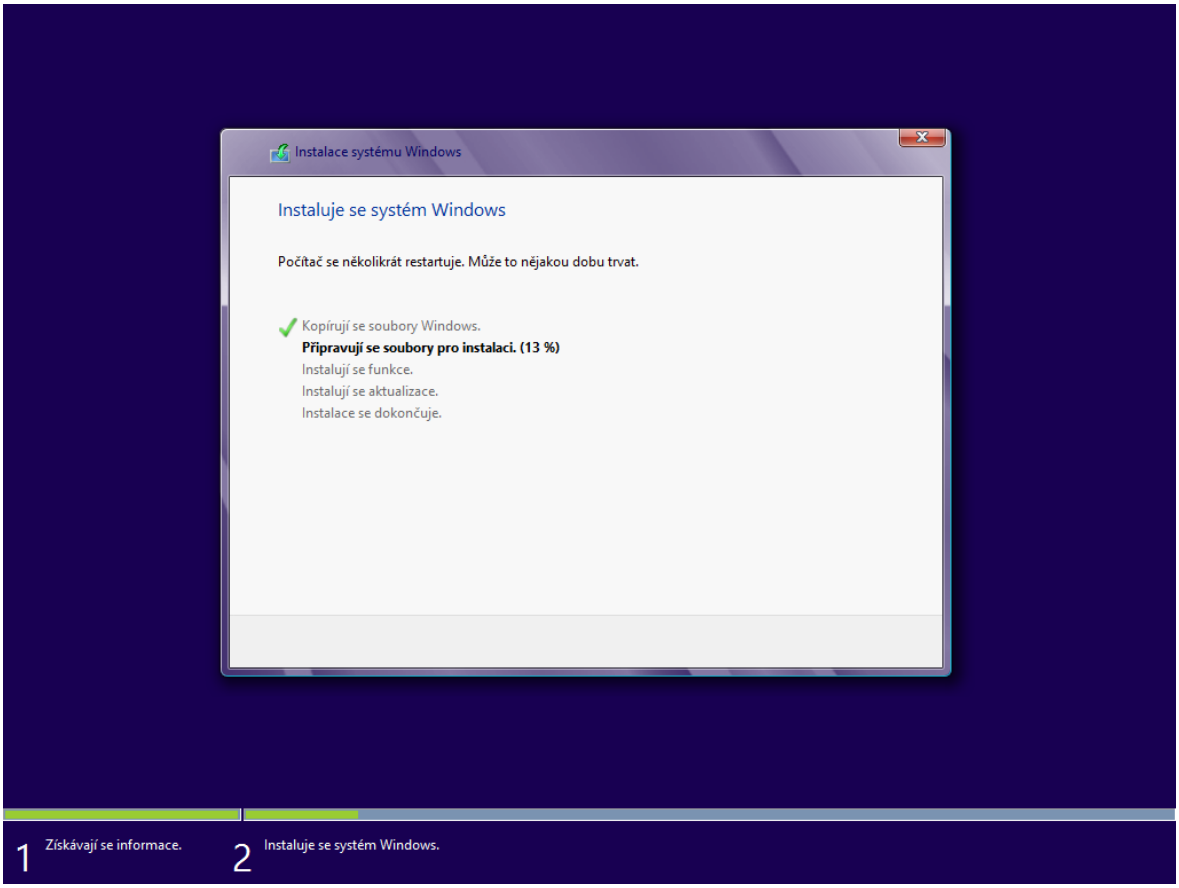
Windows Vista je operační systém od firmy Microsoft a byl vydán 30. ledna roku 2007. Přívlastek Vista znamená výhled či rozhled a tento přívlastek byl přidán, protože bylo aktualizované uživatelské grafické rozhraní a vizuální styl s názvem Aero. Dále byly přepracovány síťové, zvukové, tiskové a zobrazovací podsystémy a nové multimediální nástroje. Na tomto OS je zajímavé, že byl vydán až pět let po svém předchůdci Windows XP, což bylo nejdelší časové rozpětí mezi vydání operačních systémů od firmy Microsoft, ale ani tato velká časová prodleva nezajistila tomuto OS první příčky na trhu. Systém Windows Vista se stal kritizován pro své vysoké systémové požadavky, špatnou komptabilitu s některým hardwarem a softwarem, dlouhou dobu spouštění, přísnější licenční podmínky, atd. Jeho nástupcem se stal legendární a dodnes hojně používaný Windows 7. [38]



Obrázek 10 – Instalace operačního systému Windows Vista [Zdroj: Vlastní]

8.3.2 Windows 8

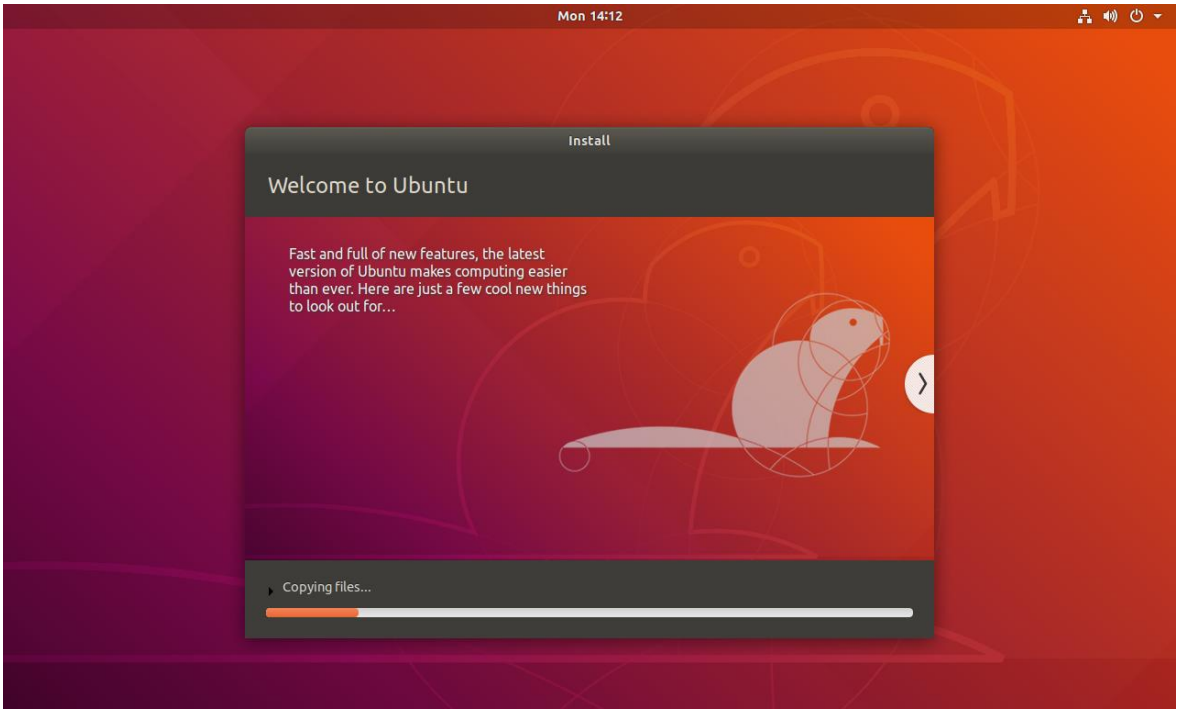
Windows 8 je taktéž operační systém od firmy Microsoft, který byl vydán 26. října roku 2012. Tento OS byl nově určen také pro tablety, proto byla z tohoto OS odstraněna nabídka start a byla nahrazena přehledem nainstalovaných aplikací v podobě obdélníkových tvarů, což systému umožnilo rychlejší spouštění. Byl přidán nový správce úloh a byla přidána také podpora aplikací ve virtuálním obchodě Windows Store, kdy za účelem bylo zvýšit bezpečnost a usnadnit instalaci těchto aplikací. Windows 8 je nástupce OS Windows 7, ale nedočkal se takového úspěchu, jako jeho předchůdce a dokonce nepřekonal v podílu na trhu ani zastaralou a již nepodporovanou verzi Windows XP. Jeho nástupcem je Windows 10. [36]



Obrázek 11 – Instalace operačního systému Windows 8 [Zdroj: Vlastní]

8.3.3 Linux (Ubuntu)

Ubuntu je jedna ze softwarových distribucí od Linuxu, běžící nejen na osobních počítačích a serverech, ale také na mnoha malých zařízeních, jako jsou mobilní telefony, tablety a popřípadě drony. Je navržena tak, aby byla využitelná ve všech oblastech a spolehlivě fungovala na nespočtu různých zařízení v různých aplikacích. Ubuntu je tzv. OpenSource, což znamená, že je oproštěn od licenčních poplatků a je zcela zdarma. Dále obsahuje kancelářský balík, který je plně kompatibilní s formáty Microsoft Office. Je přeložen do více než 100 jazyků. Je také důležité podotknout, že není moc náročný, a proto jej můžeme používat i na starších počítačích. S dlouhým seznamem vzdělávacího softwaru a certifikovaného hardwaru poskytuje Ubuntu bezpečný, cenově výhodný a dostupný systém pro studenty, učitele i školní správce, takže je vhodný i do škol. V Ubuntu můžeme instalovat pomocí příkazů v terminálu nebo stahovat licencovaný software z Ubuntu Software Center. [33]



Obrázek 12 – Instalace operačního systému Ubuntu [Zdroj: Vlastní]

9 TROJSKÝ KŮŇ MEMZ

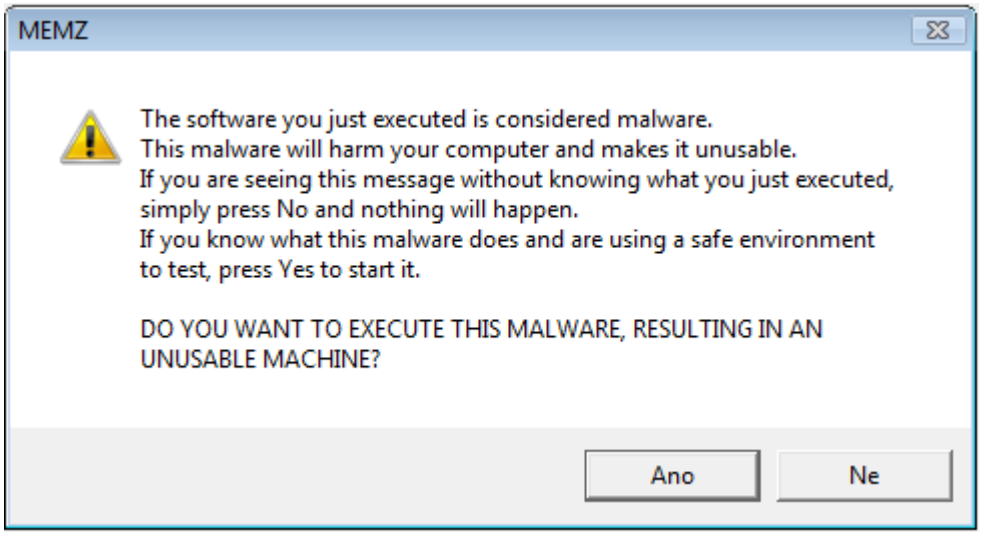
MEMZ je název pro malware typu trojského koně, který byl vytvořen youtuberem s přezdívkou Leurak. Tento trojský kůň využívá jedinečného zatížení systému, které je aktivováno v řadě po sobě. Prvních pár zatížení je neškodných, ale po několikati zatíženích může počítač zcela zkolabovat. Pokud je operační systém virem infikován, zobrazí se poznámkový blok se zprávou, ve kterém je napsáno, že byl počítač napaden trojským koněm MEMZ a uživatel nebude schopen po restartu počítač používat a poté se začnou odehrávat divné věci jako např.: pohybování kurzoru myši, vyhledávání pochybných stránek v našem webovém prohlížeči, otevření náhodných programů jako jsou kalkulačka, příkazový řádek, správce úloh, poznámkový blok, malování, dále nastane problikávání obrazovky, převrácení textu, vyskakování oken s upozorněním apod. Když už se na počítači nedá dělat nic a vy se rozhodnete počítač restartovat, místo zavedení do operačního systému se na obrazovce zobrazí zpráva, že náš počítač byl zničen trojským koněm MEMZ a poté následuje animace s běžící kočkou, která vypouští duhu a je k tomu puštěna melodie, která je přehrávána z reproduktorů stále dokola. [37]

10 NAPADENÍ VYBRANÝCH OPERAČNÍCH SYSTÉMŮ

Ke srovnání bezpečnosti a k napadení operačních systémů jsem si vybral malware typu trojského koně s názvem MEMZ, jehož charakteristika je uvedena výše.

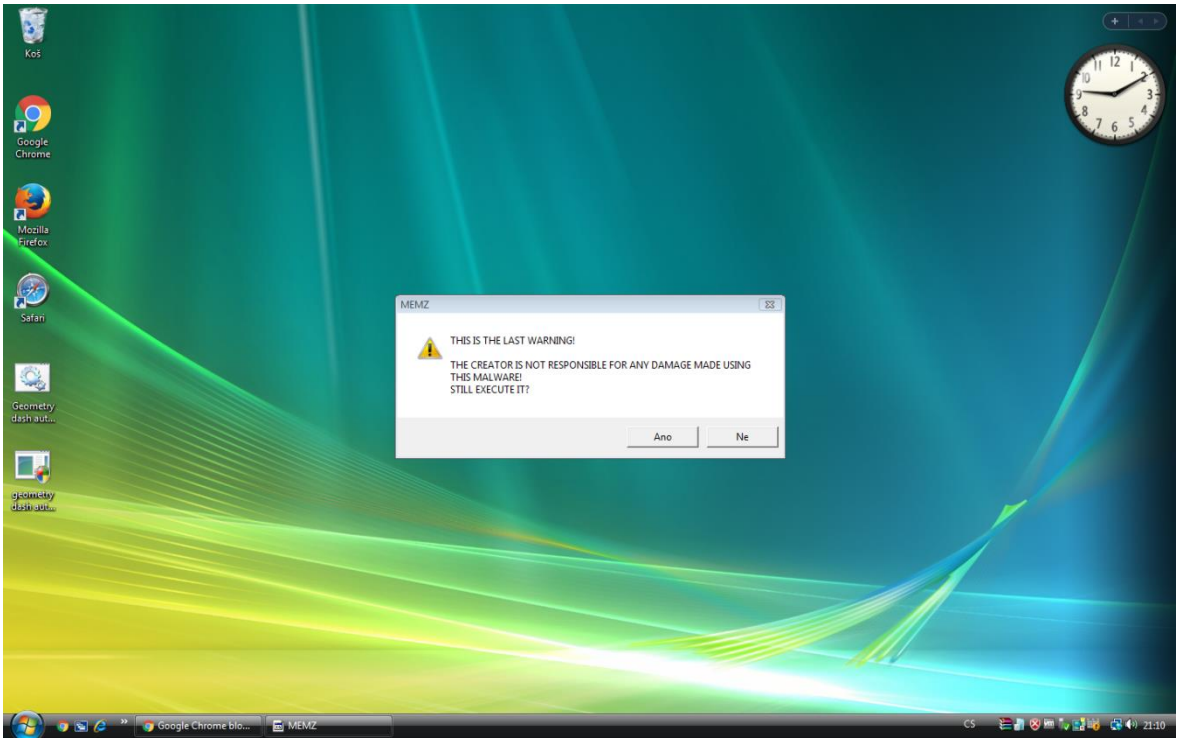
10.1 Windows Vista

Jako první systém určený k napadení byl zvolen trochu starší operační systém Windows Vista, kdy při otevření viru, jak můžeme vidět na obrázku číslo 13, vyskočilo na monitoru okno s následujícím textem: „Software, který jste právě otevřel, je považován za malware. Tento malware ublíží vašemu počítači a udělá jej nepoužitelným, jednoduše stiskněte Ne a nic se nestane. Pokud víte, co tento malware dělá a používate ho v bezpečném prostředí na testování, stiskněte Ano k začnutí. CHCETE TENTO MALWARE SPUSTIT, I KDYŽ BUDE ZA NÁSLEDEK NEPOUŽITELNÝ STROJ?“



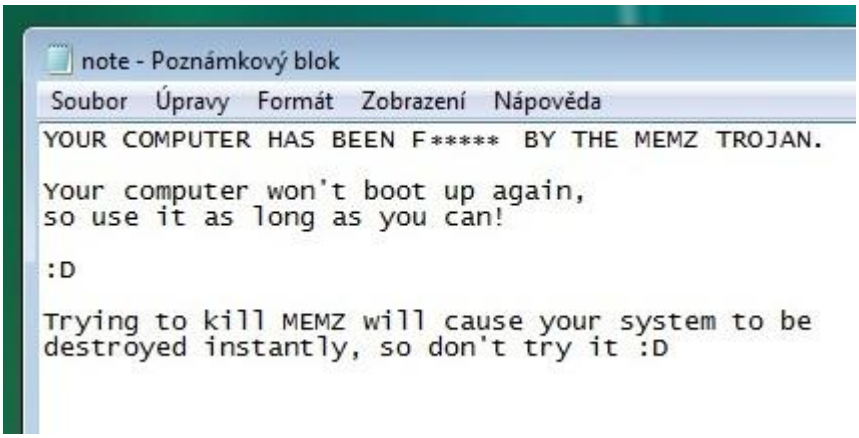
Obrázek 13 - Varovné okno při otevření trojského koně MEMZ [Zdroj: Vlastní]

Po potvrzení vyskočí další varovné okno s textem: „ TOTO JE POSLEDNÍ VAROVÁNÍ! TVŮRCE NENÍ ODPOVĚDNÝ ZA ŽÁDNOU ŠKODU PŘI POŽÍVÁNÍ TOHOTO MALWARU! STÁLE PROVÉST?“ (Obr. č. 14).



Obrázek 14 – Druhé varovné okno [Zdroj: Vlastní]

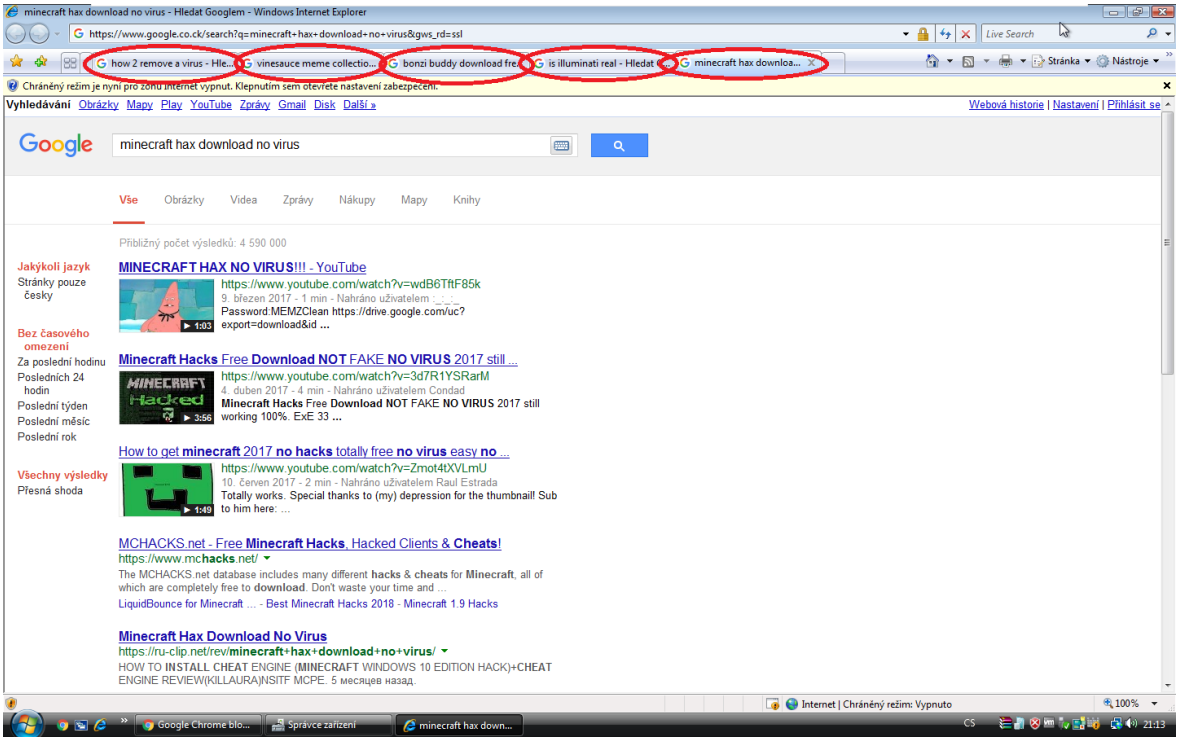
Po potvrzení druhého varovného okna vyskočí na obrazovce poznámkový blok, kde je napsáno, že byl počítač napaden trojským koněm MEMZ a uživatel nebude schopen po restartu počítač používat a že zkoušení zrušení tohoto viru způsobí zničení systému okamžitě. V této zprávě jsou použity vulgarismy, a proto je obrázek č. 15 upraven a použity k zakrytí tohoto vulgarismu byly hvězdičky.



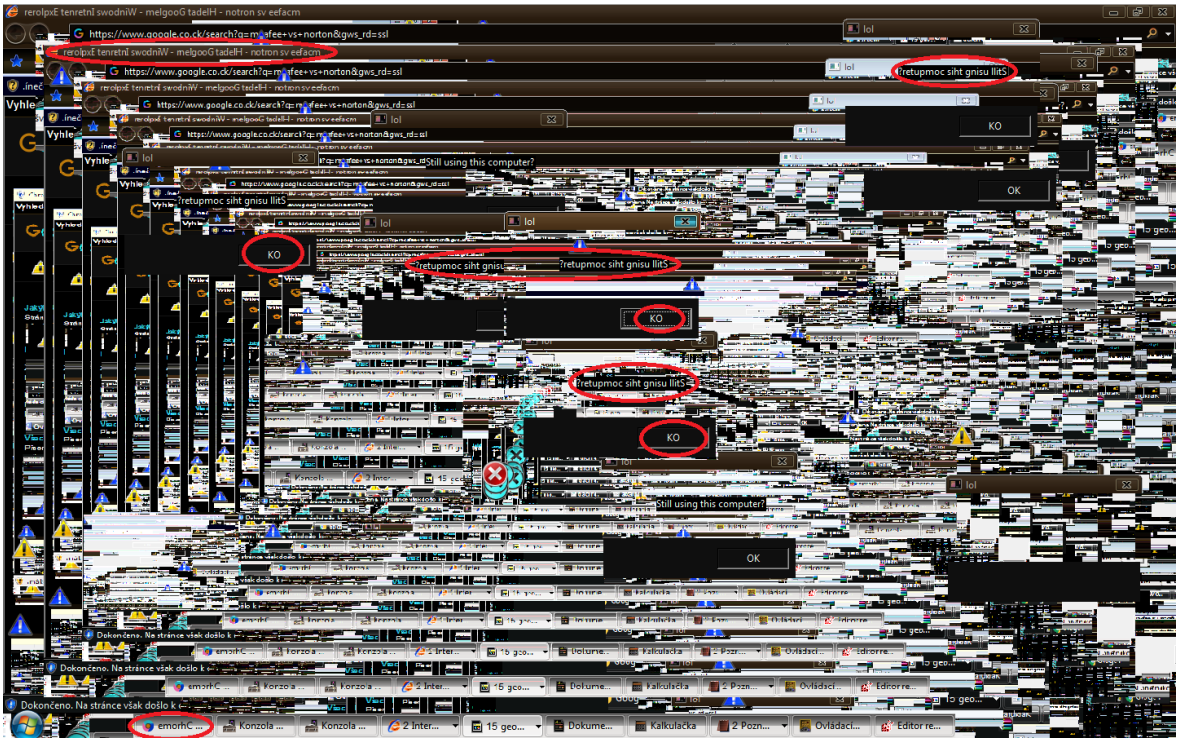
Obrázek 15 - Poznámkový blok s vulgární zprávou [Zdroj: Vlastní]

Po chvíli se otevře webový prohlížeč a začne vyhledávat pochybné stránky, jak je vidět na obrázku číslo 16. Poté se změní kurzor myši na červený křížek a střídá se se žlutým trojúhelníkem s vykřičníkem, dále dochází k otevření náhodných programů, jako jsou kalkulač-

ka, příkazový řádek, správce úloh, poznámkový blok, malování a nastane problikávání obrazovky s převráceným textem, vyskakování oken se stručným vzkazem. Poté jak jsou okna nakopírována přes sebe a jsou stále menší, nastane tzv. tunel efekt (Obrázek č. 17).

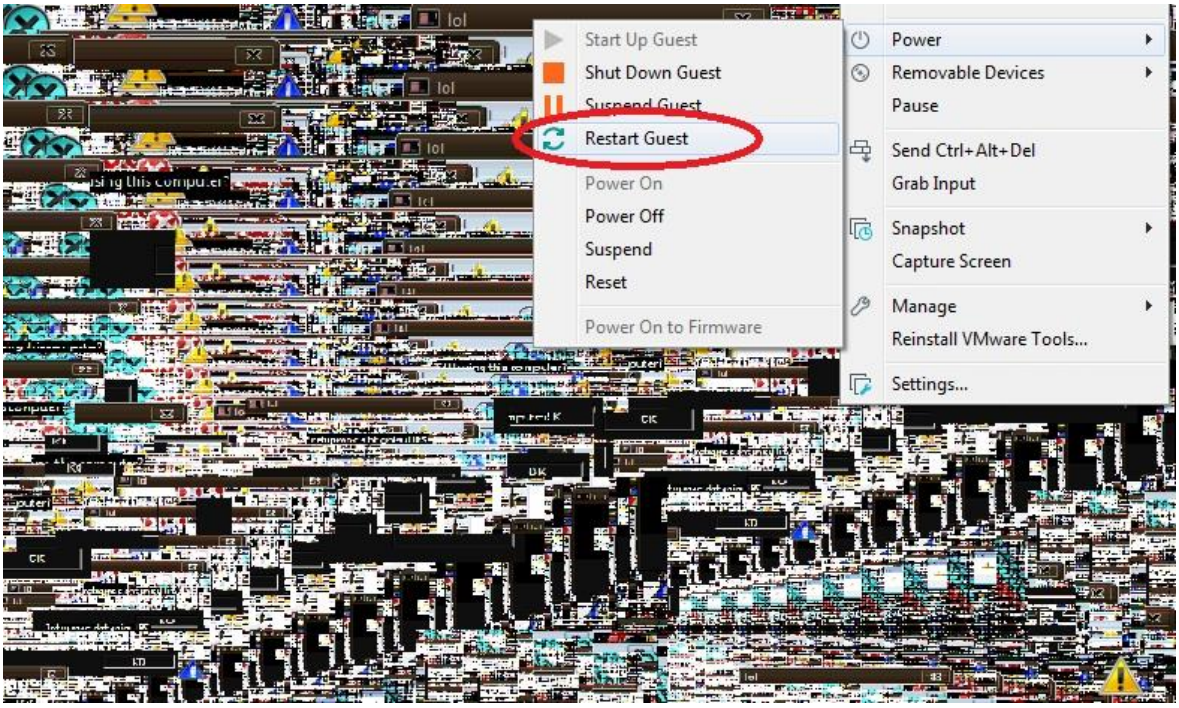


Obrázek 16 – Vyhledávání pochybných webových stránek [Zdroj: Vlastní]



Obrázek 17 – Převrácení textu a tunel efekt [Zdroj: Vlastní]

Poté se s počítačem nedá dělat nic, tak jej zkusíme restartovat (Obr. č. 18).



Obrázek 18 – Restart počítače [Zdroj: Vlastní]

Po restartu, než se vůbec načte operační systém, je vyobrazena zpráva s pomocí efektu psacího stroje, že náš počítač byl zničen trojským koněm MEMZ a ať si užíváme Nyan Cat (obr. č. 19).

Obrázek 19 – Zpráva po restartu pořítače [Zdroj: Vlastní]

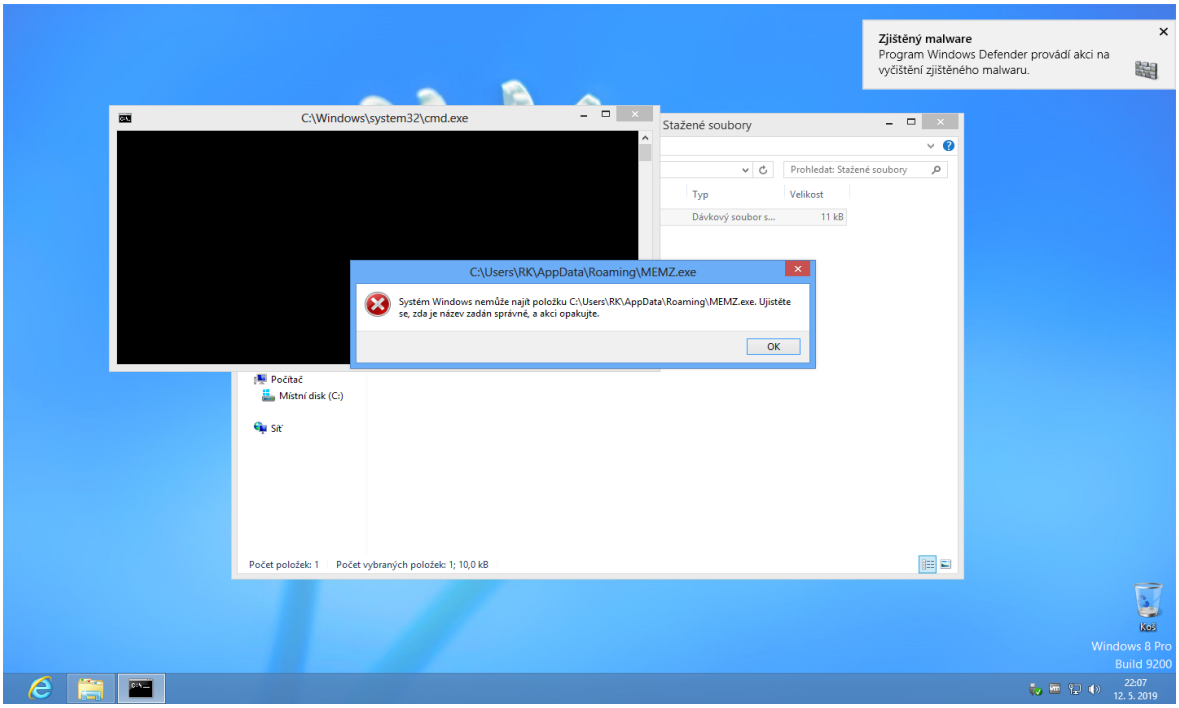
Následuje už jen animace běžící kočky, tzv. Nyan Cat, která vypouští duhu, za doprovodu melodie, která je k animaci typická a tato animace a melodie hraje pořád dokola (obr. č. 20).

Obrázek 20 – Nyan Cat [Zdroj: Vlastní]

Tato animace nezmizí ani po několikanásobném restartu či zapnutí počítače.

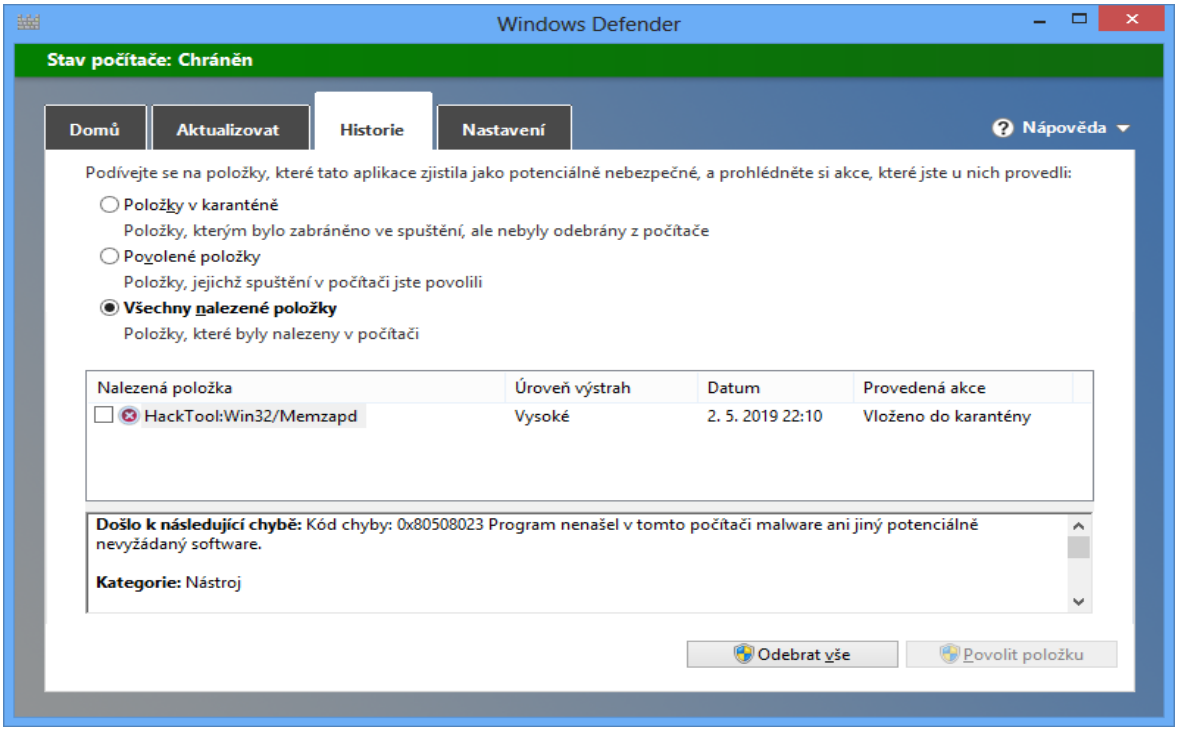
10.2 Windows 8

Jako druhý operační systém k napadení jsem si vybral Windows 8, kdy při otevření viru v tomto OS vyskočil příkazový řádek, tabulka s oznámením, že systém nemůže najít položku. Když se podíváme do pravého horního rohu, zjistíme, že program Windows Defender, který je součástí operačního systému, provádí akci a vyskočilo zde okno se zjištěním malwaru, které vidíme na obrázku č. 21.



Obrázek 21 – Vyskakovací okno po otevření trojského koně MEMZ [Zdroj: Vlastní]

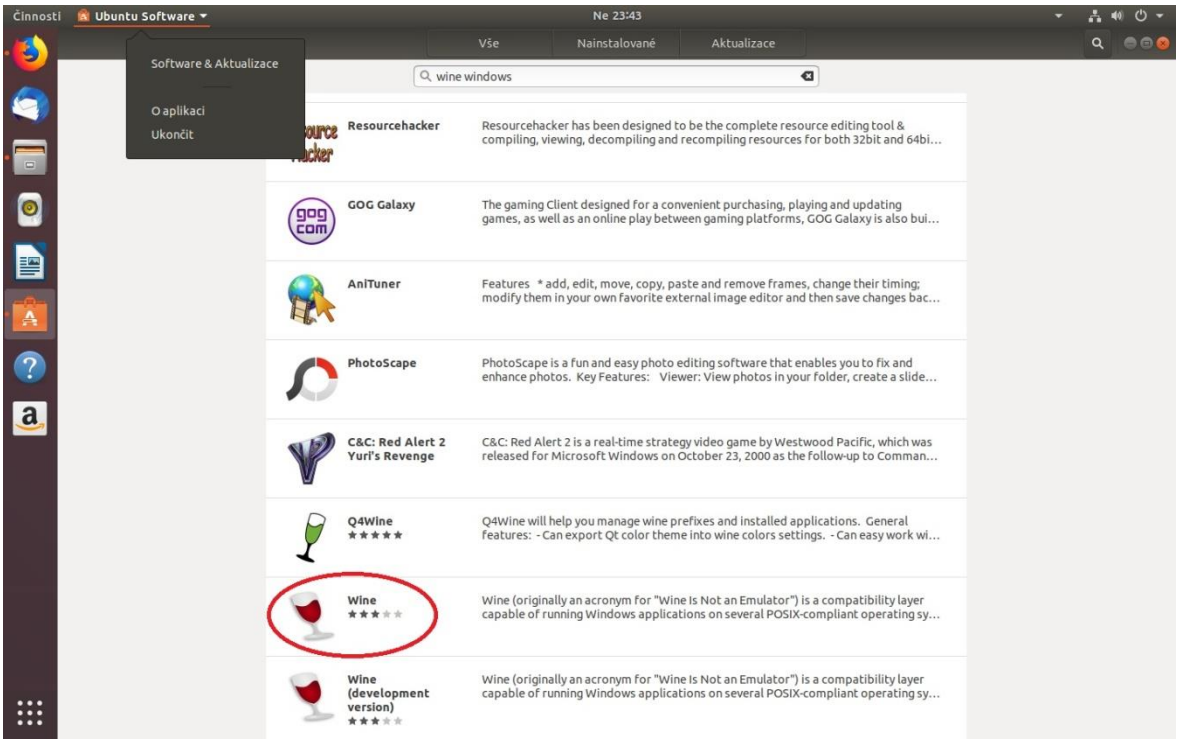
Na následujícím obrázku č. 22 můžeme vidět aplikaci Windows Defender, kde nám oznamuje, jaká nebezpečná položka byla nalezena v našem počítači, jaká je úroveň výstrahy, datum a jaká akce s touto položkou byla provedena.



Obrázek 22 – Nalezená položka programem Windows Defender [Zdroj: Vlastní]

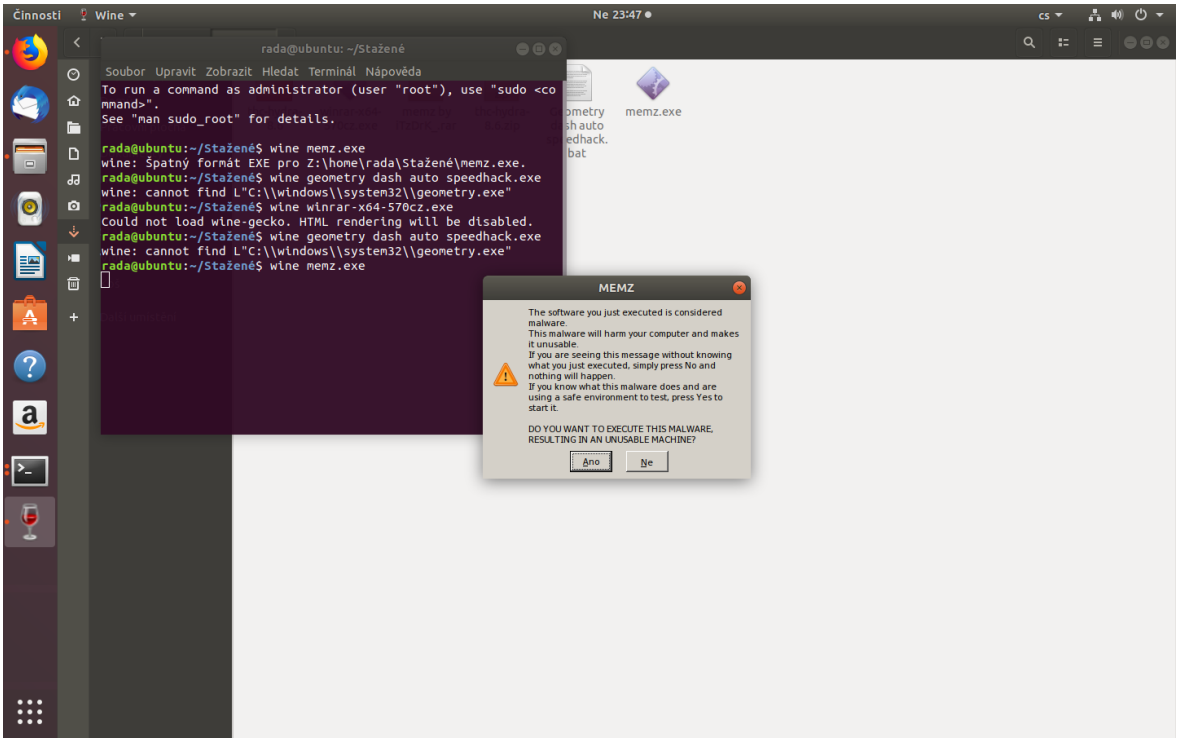
10.3 Linux (ubuntu)

Jako poslední systém k napadení jsem si vybral operační systém Ubuntu a do tohoto OS bylo zavedení trojského koně o něco komplikovanější, protože se zde instaluje pomocí příkazů v příkazovém řádku nebo stahováním licencovaného softwaru v Ubuntu Software Center. Operační systém Ubuntu není stavěný na otvírání programu s koncovkou .exe, tudíž jsem musel nainstalovat pomocí Ubuntu Software Center program Wine, který to umožňuje (obr. č. 23).



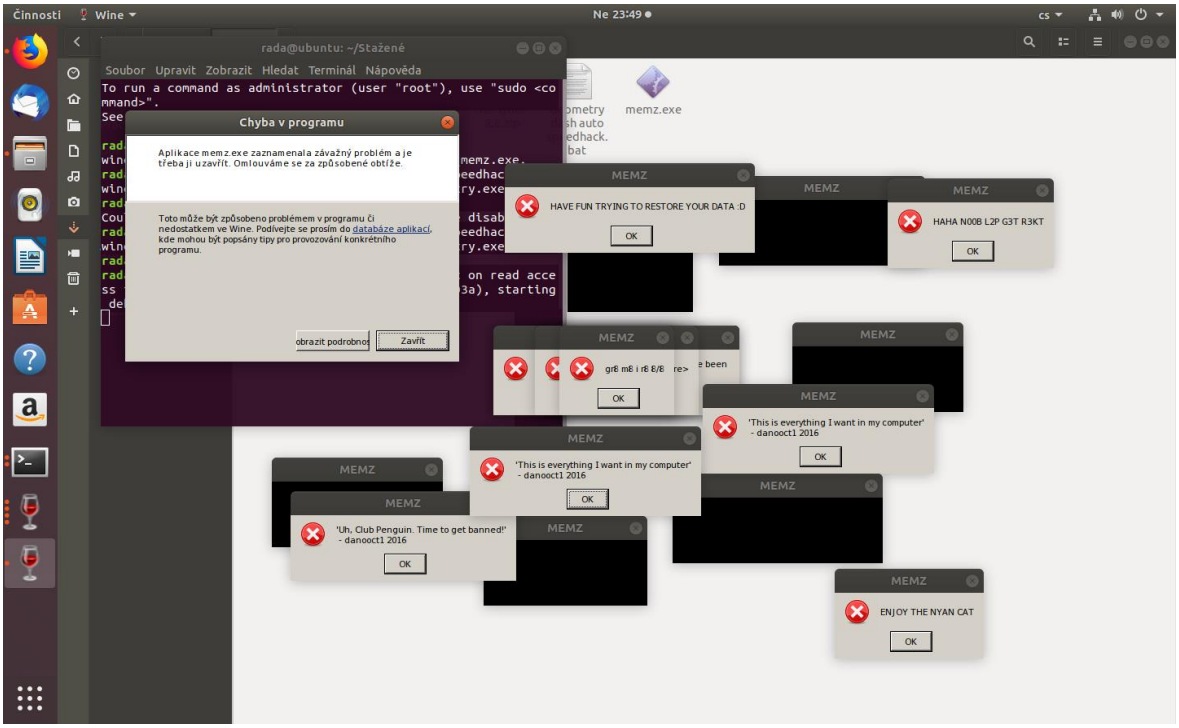
Obrázek 23 – Program Wine [Zdroj: Vlastní]

Dalším krokem po dokončení instalace programu Wine byla jeho konfigurace. V Příkazovém řádku byl zadán příkaz winecfg a tím se vytvořila složka v počítači, která sloužila jako disk C, jak je tomu známo u OS Windows a pomocí této složky se mohou spouštět programy pro Windows. Další obrázek č. 24 ukazuje, jak pomocí příkazu wine v příkazovém řádku, tzv. terminálu, je spuštěn program MEMZ.exe, tedy námi zvolený trojský kůň pro útok na tento operační systém. Po spuštění programu vyskočí podobné okno se stejným textem a varováním jako u OS Windows Vista.



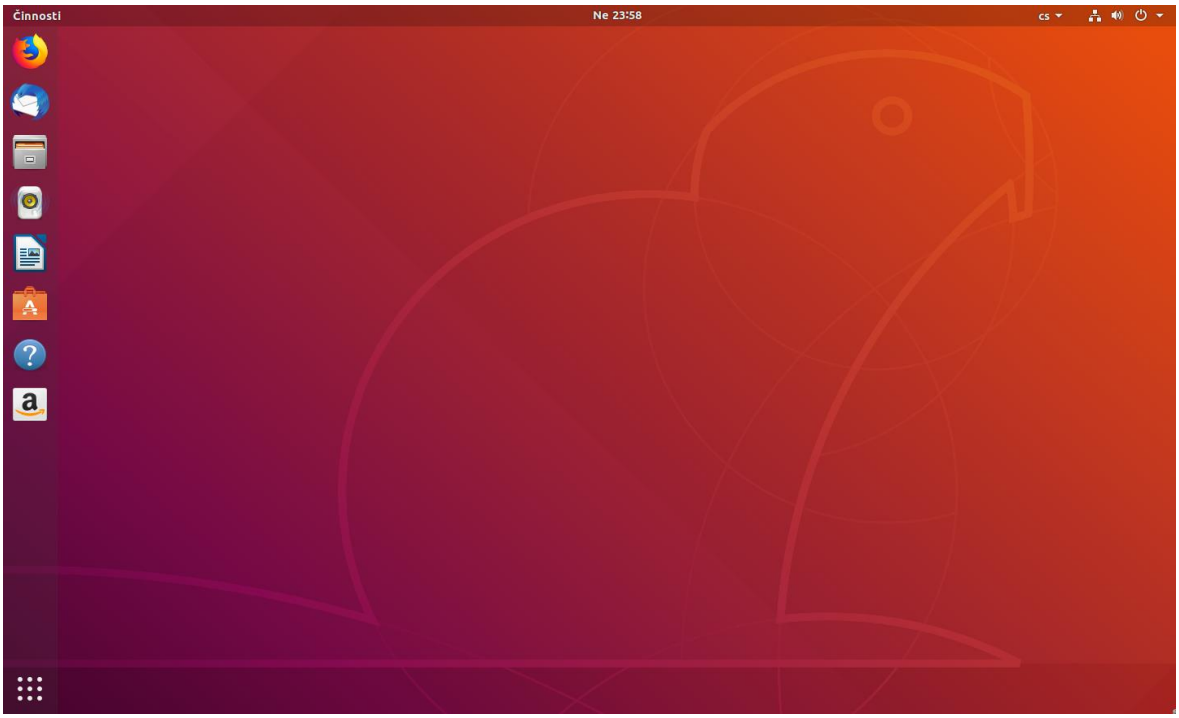
Obrázek 24 – Příkazy v terminálu a varovné okno [Zdroj: Vlastní]

Po potvrzení obou varovných oken, stejně jako v OS Windows Vista, nevyskočí žádný poznámkový blok, jako to bylo u OS Windows Vista, ale vyskočí hned varovné okna s nápisy jako např.: Hodně zábavy zkoušením obnovit vaše data; to je vše, co chci ve svém počítači; užijte si Nyan Cat atd. Vyskočí ale také varovné okno, které hlásí chybu v programu a je v něm napsáno, že aplikace memz.exe zaznamenala závažný problém a je třeba ji uzavřít, jak je vidět na obrázku s číslem 25.



Obrázek 25 – Varovná okna a chyba v programu [Zdroj: Vlastní]

Po kliknutí myší na políčko „Zavřít“ všechna okna zmizí a OS Ubuntu je uveden do normálního stavu jako před použitím trojského koně. I po restartování počítače nejsou vidět známky napadení a systém nevydal žádnou hlášku o útoku a nenásleduje žádná animace běžící kočky s melodií a všechna data jsou zachována a v pořádku.



Obrázek 26 – OS Ubuntu po restartu [Zdroj: Vlastní]

11 SROVNÁNÍ BEZPEČNOSTI NAPADENÝCH OPERAČNÍCH SYSTÉMŮ

Jak jsme mohli vidět, Windows Vista byl zcela zničen a došlo k nenávratnému poškození tohoto operačního systému, kdy nepomohlo ani několikanásobné restartování počítače. Pro jeho zastaralost, nepodporovanost a nevydávání dalších aktualizací, bych tento systém už nepovažoval za bezpečný.

Napadnout operační systém Windows 8 se mi nepovedlo, protože tomu bylo zabráněno integrovaným antivirem Windows Defender, který ihned po otevření trojského koně identifikoval přítomný malware a označil tuto položku s vysokou úrovní výstrahy a neprodleně ji přesunul do karantény.

Napadnutí operačního systému Ubuntu od Linuxu, bylo složitější, ale nakonec se to pomocí podpůrného softwaru Wine podařilo. Avšak útok se nedá považovat za úspěšný, jelikož byl trojský kůň zastaven a po zavření okna byl systém bez známek jakéhokoliv poškození či napadení a dalo se na něm dále pracovat. Ani při restartování nenaběhla animace s kočkou, jako tomu bylo u Windows Vista a systém se spustil obvyklým způsobem.

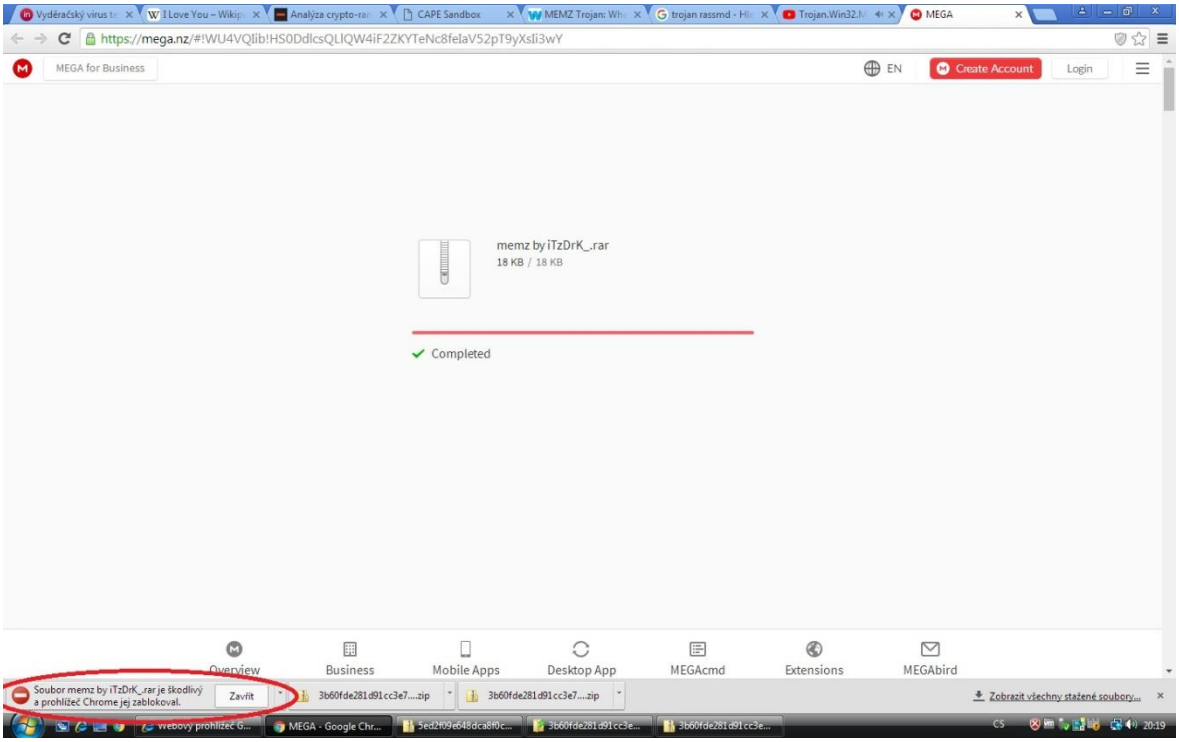
Operační systém Ubuntu, který je založen na linuxovém jádře, je od základu navržen s ohledem na bezpečnost a díky tomu se minimalizuje riziko napadení virem či jiné narušení počítače. Bezpečnost Ubuntu je nevývratná, protože pokud v tomto systému chceme provést změny, jsme vyzváni k zadání hesla pro autentizaci a to by nás podvědomě mělo donutit pečlivě si přečíst obsah sdělení a zvážit další krok. Dalším podtrhujícím faktem, že je Ubuntu bezpečný je, že existuje jen malé množství virů, které jsou hrozbou pro tento OS, protože není tak rozšířený jako například Windows. Na první pohled se může zdát že by mohl být tento systém velmi zranitelný, protože každý má přístup k otevřenému zdrojovému kódu a tak by útočníci snadno mohli najít chyby, avšak opak je pravdou protože tento otevřený zdrojový kód zase prohlíží stovky programátorů, kteří naleznou tuto chybu a opraví ji, proto bych tento systém vyhodnotil za nejbezpečnější.

12 OCHRANA PROTI TROJSKÉMU KONI

Jakékoliv stahování souborů na Internetu je potencionální hrozbou. Před napadením trojského koně se dá bránit buď to kvalitním antivirovým programem, firewalem, aktualizací webového prohlížeče a samozřejmě aktualizací samotného operačního systému. Dalšími typy jak se vyhnout na Internetu trojskému koni jsou např.: nenavštěvovat pochybné stránky, neklikat na podezřelé odkazy a pečlivě přemýšlet nad jakýmkoliv stažením souboru z Internetu.

12.1 Webový prohlížeč

Google Chrome automaticky chrání a blokuje stahování škodlivého obsahu, který by mohl instalovat viry, zavinit únik soukromých dat, změnit nastavení prohlížeče nebo počítače a přidat do prohlížeče nežádoucí rozšíření nebo lišty. Jak vidíme na obrázku č. 27, prohlížeč Google Chrome zablokoval námi stažený trojský kůň MEMZ a tento soubor nelze otevřít.

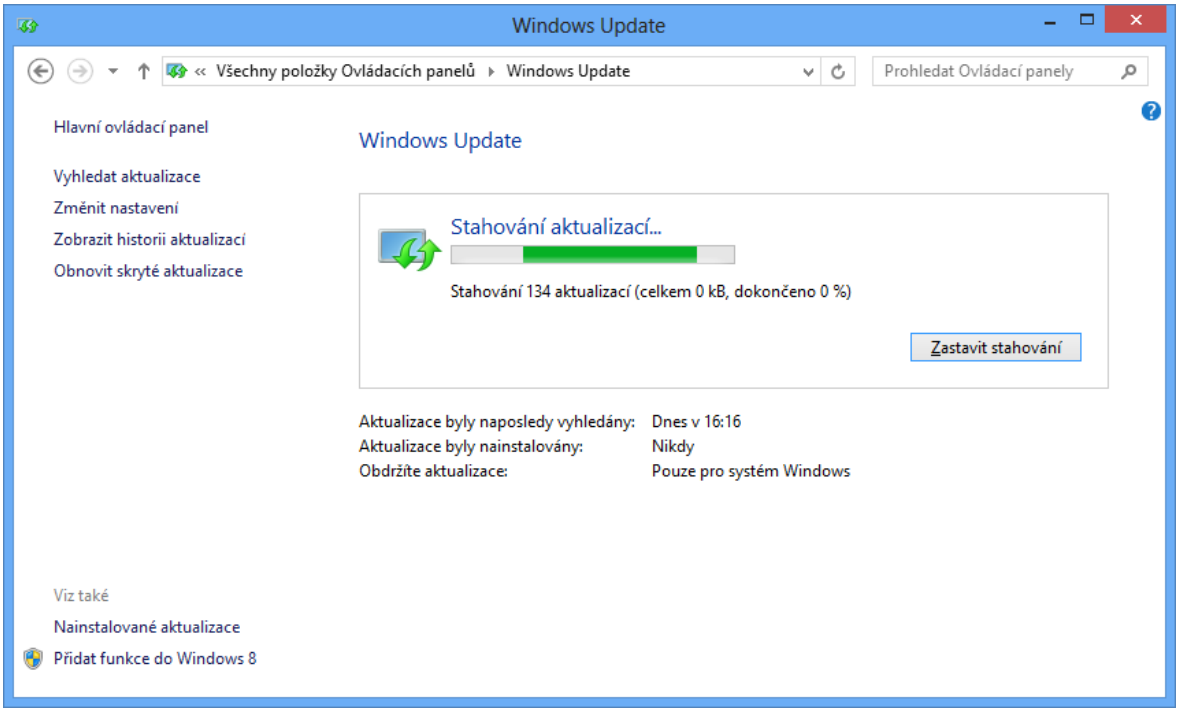


Obrázek 27 – Blokace viru prohlížečem Google Chrome [Zdroj: Vlastní]

12.2 Aktualizace operačního systému

Pro zabezpečení operačního systému je třeba mít OS aktuální. Aktualizace se provádí z důvodu vyšší bezpečnosti operačního systému, oprav programátorských chyb a různých

záplat. Tato opatření zmírní bezpečnostní ohrožení hrozící na Internetu. Na obr. č. 28 můžeme vidět okno Windows Update, kde probíhá stahování aktualizací pro operační systém Windows 8.

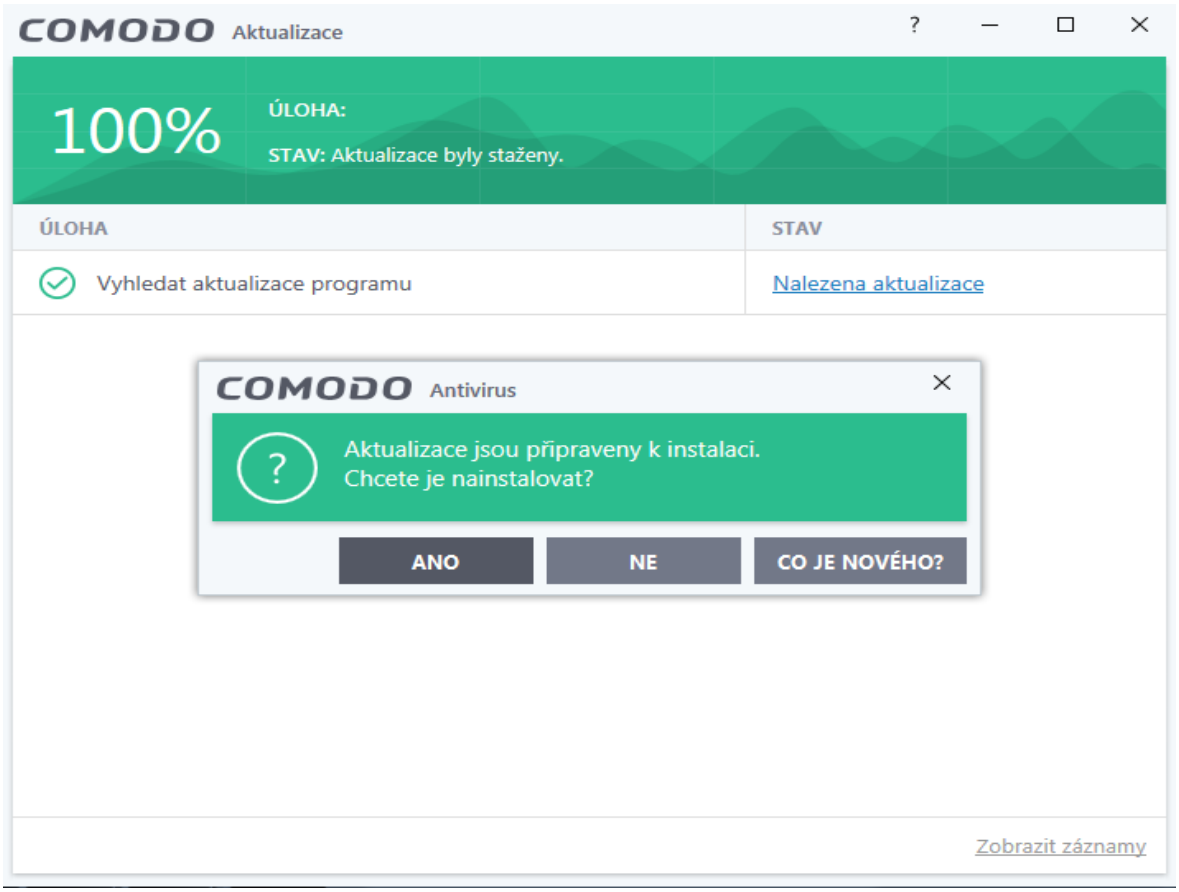


Obrázek 28 – Stahování aktualizací pro OS Windows 8 [Zdroj: Vlastní]

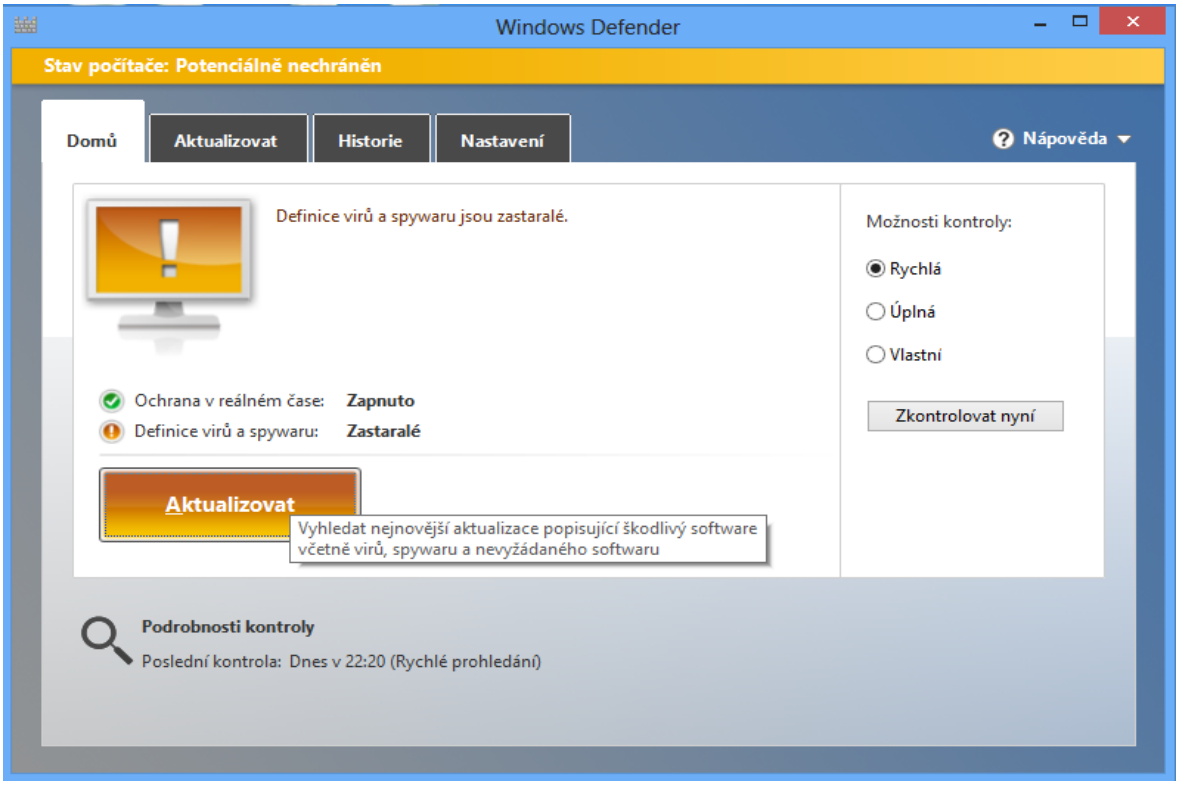
12.3 Antivirový program

Mezi základní a nejdůležitější ochranu operačního systému patří aktualizovaný antivirový program, který pomáhá identifikovat podezřelé aktivity v počítači, odstranit, přesunout do karantény a eliminovat počítačové viry a jiný škodlivý software. Mezi nejznámější antivirové programy můžeme zařadit ESET, Avast, AVG, Kaspersky, McAfee a COMODO. Některé druhy antiviru poskytují tzv. free verze, kdy je ochrana počítače základní a za plnou verzi si poté musíme připlatit. Úspěšnost antivirového programu závisí na schopnostech tohoto softwaru a na aktuálnosti databáze počítačových virů.

Na následujících obrázcích s číslem 29 a 30 je vyobrazena, jak může vypadat aktualizace antivirového programu.



Obrázek 29 – Aktualizace antivirového programu COMODO [Zdroj: Vlastní]



Obrázek 30 – Aktualizace antiviru Windows Defender [Zdroj: Vlastní]

13 SWOT ANALÝZA

V této kapitole je provedena SWOT analýza, která se týká silných a slabých stránek, příležitostí a hrozeb operačních systémů Linux (Ubuntu), Windows 8 a Windows Vista.

13.1 Linux (Ubuntu)

Následující tabulka obsahuje silné a slabé stránky, příležitosti a hrozby operačního systému Linux Ubuntu s následným komentářem.

Tabulka 3 – SWOT analýza operačního systému Linux Ubuntu [Zdroj: Vlastní]

SILNÉ STRÁNKY	SLABÉ STRÁNKY	PŘÍLEŽITOSTI	HROZBY
• Zdarma • Možnost práce na slabším počítači • Stabilita	• Obtížnost • Složitější instalace • Nelze spustit některé komerční aplikace	• Inspirace z ostatních linuxových distribucí • Rozšíření ve školách	• Zpoplatnění • Zvyk na Windows • Množství linuxových distribucí

Ubuntu je jedna z nejrozšířenějších linuxových distribucí se a může pochlubit zejména tím, že je *zdarma* a je tedy dostupná pro každého, kdo vlastní počítač. Díky unixové bázi je systém navíc velmi *stabilní* a nestává se příliš často, že by Ubuntu bezdůvodně spadlo. Na linuxové distribuce nejsou zaměřeny ani viry, takže se v současnosti jedná o bezpečný systém. Těšit se můžou i majitelé *slabších počítačů*, protože operační systém tam rozjedou poměrně bez problémů.

Při přechodu od Windows k Linuxu může nastat problém v počáteční *obtížnosti* a zmatenosti ze systému. *Složitější* jsou i *instalace* různých programů, především pomocí terminálu, Avšak v Ubuntu Software Center je instalace programů přehledná a jednoduchá. Nesednout systému může také hardware, jedná se především o některé grafické karty, které pak neběží na plný výkon. Velkým problémem je i s tím, že *nelze spustit některé komerční aplikace*, které se však linuxové distribuce snaží řešit pomocí různých emulátorů, například námi použité aplikace Wine.

Díky tomu, že Linux má *velký počet linuxových distribucí*, tak se Ubuntu může inspirovat od ostatních verzí Linuxu a vylepšit, popřípadě změnit nějaká rozhraní a nastavení, která

by byla pro uživatele příjemnější. Ubuntu je bezpečný, je zdarma a je to dostupný operační systém pro studenty, učitele i školní správce, takže *je vhodný i do škol*.

Určitě hrozí to, že díky *velkému množství linuxových distribucí* si uživatel nevybere právě Ubuntu, ale vybere si jiný OS od Linuxu, i když by Ubuntu byl pro něj ten pravý systém. Někoho může počet i odradit od linuxových distribucí úplně, proto sáhne radši po klasické variantě od Windows. Může se také stát, že uživatel vyzkouší Ubuntu, ale *vrátí se zpátky k Windows, protože je na tento OS zvyklý* a ví, co od systému čekat a tato změna mu prostě nesedí. Zůstává však otázkou, jak dlouho bude operační systém bezplatný. Tvůrci by mohli prahnout po nějakém finančním obnosu a linuxové distribuce začít *zpoplatňovat.*

13.2 Windows 8

Následující tabulka obsahuje silné a slabé stránky, příležitosti a hrozby operačního systému Windows 8 s následným komentářem.

Tabulka 4 – SWOT analýza operačního systému Windows 8 [Zdroj: Vlastní]

SILNÉ STRÁNKY	SLABÉ STRÁNKY	PŘÍLEŽITOSTI	HROZBY
• Nové grafické uživatelské rozhraní • Rozšířenost • Kompatibilní se staršími systémy Windows	• Velké množství virů • Odebrání nabídky start • Množství aktualizací	• Velká propagace • Poučení z předešlých verzí	• Touha zkusit jiný OS • Nedůvěra zákazníků

Operační systém Windows 8 se od svých předešlých verzí může pyšnit *novým grafickým uživatelským rozhraním,* kdy zmizela nabídka start a byla nahrazena dlaždicovými ikonami. Tento OS je v dnešní době aktuální, tudíž je velmi *rozšířený* a spousta uživatelů ho využívá na svém stolním počítači či notebooku. Windows 8 je *kompatibilní se staršími operačními systémy Windows,* lze v něm tedy spouštět aplikace určené pro tyto starší systémy.

Jelikož je Windows nejrozšířenějším operačním systémem, tak se útočníci a hackeři soustředí právě na něj, a proto se na tento OS vztahuje *velké množství virů*. Hodně uživatelů od

tohoto systému upustilo, jelikož byla *odebrána nabídka start*, na kterou byli dosud zvyklí. Dále také může uživatele otravovat neustále se nabízející *aktualizace* s novými záplatami.

K rozšíření tohoto systému využívá firma Microsoft *velké propagace* na Internetu, v televizi a dalších mediálních prostředcích a nabídkou na upgrade ve starších systémech Windows. Velká příležitost jak systém Windows 8 vylepšit a zabezpečit *je poučení z předešlých verzí Windows.*

Určitou hrozbou pro tento systém je, pokud by uživatel chtěl *vyzkoušet jiný operační systém*. Další hrozbou je zklamaný uživatel předchozích verzí Windows. Mohl mít špatnou zkušenost nebo byl jinak nespokojen a to může vyvolat *nedůvěru zákazníka*.

13.3 Windows Vista

Následující tabulka obsahuje silné a slabé stránky, příležitosti a hrozby operačního systému Windows Vista s následným komentářem.

Tabulka 5 – SWOT analýza operačního systému Windows Vista [Zdroj: Vlastní]

SILNÉ STRÁNKY	SLABÉ STRÁNKY	PŘÍLEŽITOSTI	HROZBY
• Jednoduchost • Možnost kompability pro starší systémy	• Zastaralý OS • Náročný na starší hardware	• Vyzkoušení staršího OS • Dostupnost pro běžného uživatele	• Přechod na novější verze Windows • Tento systém není dále podporován

Windows Vista je hned na první pohled oproti předešlým verzím systémů *jednodušší*. Jeho další silnou stránkou je, že je *kompatibilní se staršími operačními systémy Windows*, lze v něm tedy spouštět aplikace určené pro Windows XP a starší.

Jeho největší slabou stránkou je, že tento *systém je zastaralý* a již na něj nevychází žádné aktualizace. Windows Vista se vyznačoval ve své době svou *náročností na hardware*, a tak by starší počítače mohly mít problém tento systém rozchodit.

Ze zvědavosti by dnešní uživatel mohl *tento starší systém vyzkoušet* a porovnat tak změny ve vývoji oproti novým stále podporovaným systémům. Je zde také fakt, že tento systém

nemá tak přísné licenční podmínky jako stávající OS, tudíž je *dostupný pro běžného uživatele.*

Jelikož tento systém už v současnosti *není podporován* svým výrobcem, stává se pro uživatele rizikovým a nebezpečným z hlediska užívání a hrozí zde, že stávající majitelé tohoto OS budou upgradovat a *přejdou na novější verzi operačního systému Windows.*

ZÁVĚR

Bakalářská práce s názvem Srovnání bezpečnosti vybraných operačních systémů osobních počítačů se zabývá analýzou a komparací bezpečnosti zvolených operačních systémů.

Jedním z cílů této bakalářské práce v teoretické části bylo seznámit se s informacemi, co to vůbec osobní počítač je, vymezit jeho definice, charakterizovat stolní počítač a vymezit dělení přenosného počítače. V druhé kapitole je věnována pozornost operačnímu systému, jak se dělí, co je jeho úlohou, popis jeho struktury a historie, která je rozdělena na dekády. Dále bylo cílem vymezit kyberprostor a s tím související kybernetickou bezpečnost, hrozby v kyberprostoru, které jsem rozdělil na sociální inženýrství, malware, spam a DDoS útok. Na závěr teoretické části je vymezeno, jaké prostředky je možno použít k ochraně proti těmto hrozbám.

Hlavním cílem v praktické části mé bakalářské práce bylo analyzovat a porovnat bezpečnost operačních systémů Windows Vista, Windows 8 a Ubuntu. Tento cíl jsem splnil díky vykonstruovanému útoku trojským koněm MEMZ na systémy, které byly instalovány na virtuálních počítačích, načež jsem mohl sledovat, jak se tyto systémy zachovají po aplikování viru. Nejhůře obstál nejstarší z testovaných operačních systémů Windows Vista, který byl po napadení virem zcela zničen. Další dva testované systémy v testu bezpečnosti obstály a to zejména z důvodu dosavadní podpory Windows 8 a jeho aktuálnosti, kdy byl tento vir přesunut do karantény integrovaným antivirovým programem Windows Defender. Operační systém Ubuntu byl od začátku hůře napadnutelný. Po napadení systém sám tento vir ukončil a nadále byl zcela funkční bez ztráty dat. Operační systém Ubuntu není tak rozšířený jako Windows, proto se na něj útočníci velmi nesoustředí. Z tohoto důvodu bych tento operační systém vyhodnotil jako nejbezpečnější z nich.

Všem uživatelům bych doporučil používat operační systémy, které jsou stále podporovány jejich výrobci a dávat si pozor, aby sami uživatelé co nejméně ohrozili svou činností a chováním na Internetu svůj operační systém a v něm uložená data. Velmi důležité je data zálohovat a používat aktualizovaný antivirový program.

SEZNAM POUŽITÉ LITERATURY

[1] ACRONIS. *Acronis.cz: Virtuální počítač – jak jej vytvořit* [online]. ©2002 - 2019 [cit. 2019-03-26]. Dostupné z: https://www.acronis.cz/kb/virtualni-pocitac/.

[2] ADÁMEK. *Operační systémy* [online]. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií [cit. 2019-04-07]. Dostupné z: http://www.umel.feec.vutbr.cz/~adamek/komp/data/uvodos.htm.

[3] ADAPTIC. *Adaptic.cz: Spam* [online]. [cit. 2019-01-03]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/spam/.

[4] AIRBORN. *Airborn.webz.cz: Historie operačních systémů* [online]. 2003 [cit. 2019-03-05]. Dostupné z: http://airborn.webz.cz/histos.html.

[5] AMOROSO, Edward G. Cyber security. Summit, NJ: Silicon Press, c2007. ISBN 09-293-0638-4.

[6] CMSPS. *Cmps.cz: Operační systémy* [online]. [cit. 2019-02-03]. Dostupné z: https://www.cmsps.cz/~marlib/os/os.html.

[7] DIIT. *Deep in it: Co to je ddos útok a jak se dělá* [online]. CDR server, 2012 [cit. 2019-05-09]. Dostupné z: https://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela.

[8] DIOGENES, Yuri a Erdal OZKAYA. Cybersecurity – attack and defend strategies. Birmingham: Packt Publishing, 2018. ISBN 978-1-78847-529-7.

[9] DUDÁČEK, Karel, BLÁBOLIL, Roman. Poprvé u počítače: aneb začínáme pracovat s PC. 10. upr. vyd. České Budějovice: KOPP, 2007. 128 s. ISBN 80-7232-301-6.

[10] HOAX.cz: *Co je to scam* [online]. DIGITAL ACTION, 2019 [cit. 2019-05-03]. Dostupné z: http://www.hoax.cz/scam419/co-je-to-scam-419.

[11] ICT: *Operační systém microsoft windows. Informatika v kostce: Maturita snadno a rychle* [online]. Kolín, 2016 [cit. 2019-05-07]. Dostupné z: http://www.ict.mazuch.net/subdom/ict/16-operacni-system-microsoft-windows/.

[12] KLIMEŠ, Cyril. Principy výstavby počítačů a operačních systémů. 1. vyd. Ostrava: KOVOSIL, 2007. 198 s. ISBN 978-80-903694-1-2.

[13] KMOCH, Petr. Informatika a výpočetní technika pro střední školy. 1. vyd. Praha: Computer Press, 1997. 228 s. ISBN 80-7226-732-9.

[14] KOLOUCH, Jan. CyberCrime. CZ.NIC, 2016. ISBN 978-80-88168-15-7.

[15] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016, 175 s. ISBN 978-80-247-5595-3.

[16] KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. Praha: Grada Publishing, 2015, 183 s. Průvodce. ISBN 978-80-247-5453-6.

[17] MICROSOFT. *Microsoft azure: What is a virval machine?* [online]. Seattle: Microsoft, ©2019 [cit. 2019-03-26]. Dostupné z: https://azure.microsoft.com/cscz/overview/what-is-a-virtual-machine/.

[18] MIDDLEWARE. *Middleware.cz - blog nejen o informačních technologiích: Historie operačních systémů* [online]. Stanislav Jonák, 2013 [cit. 2019-04-02]. Dostupné z: https://middleware.cz/historie-pocitacu/15-historie-operacnich-systemu-1-dil.

[19] NAVARRŮ, Miroslav a Nora Izabella WALS. Nebojte se počítače - pro Windows 10 a Android. Praha: Grada, 2018, 176 s. Snadno a rychle. ISBN 978-80-247-5761-2.

[20] NAVRÁTIL, Pavel a Michal JIŘÍČEK. S počítačem nejen k maturitě. Vyd. 8. Prostějov: Computer Media, 2014. ISBN 978-80-7402-152-7.

[21] OXFORD DICTIONARIES. *Computer* [online]. [cit. 2019-03-12]. Dostupné z: https://en.oxforddictionaries.com/definition/computer.

[22] PETROWSKI, Thorsten. Bezpečí na internetu: pro všechny. Liberec: Dialog, 2014. Tajemství (Dialog). ISBN 978-80-7424-066-9.

[23] POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.

[24] PORADA, Viktor a Zdeněk KONRÁD. Metodika vyšetřování softwarového pirátství. Praha: Policejní akademie České republiky, 1999. ISBN 80-725-1024-X.

[25] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

[26] SAK, Petr. Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva. [Praha]: Petrklíč, 2018. 271 s. ISBN 978-80-7229-652-1.

[27] SEDLÁK, Jan. Živě.cz [online]. 2009-06-22 [cit. 2019-03-03]. *Historie operačních systémů: Věčná brzda hardwaru.* Dostupné z: http://www.zive.cz/clanky/historie-operacnich-systemu-vecna-brzda-hardwaru/sc-3-a-147538/default.aspx.

[28] SINGER, P. W. Cybersecurity and cyberwar: what everyone needs to know. New York: Oxford University Press, [2014]. ISBN 978-019-9918-119.

[29] *Software počítače* [online]. Brno: Pedagogická fakulta Masarykovy univerzity [cit. 2019-04-07]. Dostupné z: http://www.ped.muni.cz/wtech/03_studium/zvt/zvt_05.pdf.

[30] SUPERIA. *Co je to?: Co to je Počítač?* [online]. [cit. 2019-02-19]. Dostupné z: http://cojeto.superia.cz/hardware/pocitac.php.

[31] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, 147 s. ISBN 978-80-247-5595-3.

[32] TECHNOPEDIA. *Technopedia.com: Operating system* [online]. [cit. 2019-03-19]. Dostupné z: https://www.techopedia.com/definition/3515/operating-system-os.

[33] UBUNTU. *Ubuntu.cz: Vlastnosti* [online]. 2019 [cit. 2019-05-13]. Dostupné z: https://www.ubuntu.cz/desktop/vlastnosti/.

[34] VANĚK, Libor. *Historie operačních systémů: se zaměřením na jiné OS než Windows a UNIX* [online]. 2002 [cit. 2019-02-06]. Historie operačních systémů. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2002/xvanek.html.

[35] VÝZNAMSLOVA.COM: *Význam slova počítač* [online]. [cit. 2019-02-19]. Dostupné z: http://www.vyznam-slova.com/Počítač.

[36] Windows 8. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2019 [cit. 2019-04-13]. Dostupné z: https://en.wikipedia.org/wiki/Windows_8.

[37] WINDOWS REPORT. *MEMZ Trojan: What is it and how it affects Windows PC?* [online]. 2019 [cit. 2019-04-13]. Dostupné z: https://windowsreport.com/memz-virus-windows-pc/.

[38] Windows Vista. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2019 [cit. 2019-04-13]. Dostupné z: https://en.wikipedia.org/wiki/Windows_Vista.

[39] YANNAKOGEORGOS, Panayotis A. a Adam LOWTHER. Conflict and cooperation in cyberspace: the challenge to national security. Boca Raton, FL, [2014]. ISBN 978-146-6592-018.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Atd.	A tak dále.
Např.:	Například.
OS	Operační systém.
Tzv.	Tak zvaný.
PC	Personal computer.
CD	Compact disc.
DVD	Digital versatile disc.
Apod.	A podobně.
MB	Megabyte.
kB	Kilobyte.
USB	Universal serial bus.
IBM	International business machines
Č.	Číslo
Obr.	Obrázek

SEZNAM OBRÁZKŮ

SEZNAM TABULEK