Možnosti útoků na současné informační a komunikační prostředky (ICT)

Lucie Benedíková

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lucie Benedíková**
Osobní číslo:	**L15030**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**prezenční**

Téma práce: **Možnosti útoků na současné informační a komunikační prostředky (ICT)**

Zásady pro vypracování:

1. **Seznamte se se základními pojmy v oblasti bezpečnosti informačních a komunikačních technologií.**
2. **Analyzujte současné možnosti útoků na informační a komunikační technologie ve vybrané oblasti.**
3. **Seznamte se s možnostmi tvorby malwaru pro vybranou oblast.**
4. **Diskutujte získané výsledky s cílem identifikace klíčových částí.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] SINGER, P.W. a FRIEDMAN, Allan. Cybersecurity and cyberwar: What everyone needs to know. New York, NY: Oxford University Press, 2014. viii, 306 s. ISBN 978-0-19-991811-9.

[2] KOLOUCH, Jan. CyberCrime. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016. 522 s. CZ.NIC; 14. publikace. ISBN 978-80-88168-15-7.

[3] JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti = Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. 240 s. ISBN 978-80-7251-436-6.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

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

Datum zadání bakalářské práce: **3. listopadu 2017**

Termín odevzdání bakalářské práce: **15. května 2018**

V Uherském Hradišti dne 10. listopadu 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

L.S.

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ / DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1)];
- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou/diplomovou 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[2)];
- podle § 60[3)] 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[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou/diplomovou 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/diplomové 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/diplomové práce využít ke komerčním účelům;
- pokud je výstupem bakalářské/diplomové 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/diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti 7. 5. 2018

.....
podpis studenta

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich části, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.

2) 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, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) 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, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Tato bakalářská práce je zaměřena na možnosti útoků na informační a komunikační technologie, kdy v teoretické části popisuje základní názvosloví informačních a komunikačních technologií, bezpečnost a bezpečnostní informační systém, počítač a počítačový systém. Dále se v práci nachází samotné možné útoky na tyto informační a komunikační technologie, kde jsou zmíněny nejzákladnější a nejznámější útoky. Následně se dostáváme k praktické části bakalářské práce, která je zaměřena na instalaci a vytvoření virtuálního počítače, nainstalování operačních souborů Windows a poté stažení vybraného ransomwaru, a jeho aplikování, tedy útok na vybraný nainstalovaný operační systém a postupné sledování, jak virtuální počítač na tento ransomware reaguje. V závěru práce najdeme možnosti obrany proti těmto útokům.

Klíčová slova: Informační a komunikační technologie, malware, operační systém, Petya, ransomware, virtuální počítač, WannaCry

ABSTRACT

This bachelor thesis aims to possibilities of an attack on information and communication technologies. The theoretical part describes basic expressions, safety and safety systems, processes in information and communication technologies. There are also mentioned the most basic and known attacks on these technologies. The second practical part deals with installation and creation of virtual computer, installation of operating system Windows and downloading a chosen ransomware followed by applying the ransomware to the operating system. The ransomware attack is monitored and the reaction of the virtual computer is recorded. At the end of this thesis protection measurements and possibilities can be found.

Keywords: Information and communication technologies, malware, operating system, Petya, ransomware, virtual computer, WannaCry

Ráda bych poděkovala svému vedoucímu Ing. Petru Svobodovi za cenné rady, jeho ochotu a věnovaný čas. Děkuji Janu Zýbalovi za pomoc při anglickém překladu a Mgr. Jitce Rosochové za pomoc při gramatické kontrole. Velké díky patří také mé rodině za možnost studovat a jejich podporu po celou dobu studia, ale také přátelům, kteří mi byli velkou oporou.

„Naší největší chloubou není to, že nikdy nepadneme, ale že se pokaždé znovu zvedneme."

Hal Urban

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

V Uherském Hradišti, 8. 5. 2018

Lucie Benedíková

OBSAH

ÚVOD

Informační a komunikační technologie jsou v dnešní době více a více populárnější, než bývaly dříve. Jsou součástí všech podniků, firem, ale i domácností, jak již českých, tak zahraničních a mnohé z nich si bez nich vůbec nedovedou představit běžný chod firmy či života. Dříve lidé používali papyrus, tuš, klacík, technické pero, či obyčejnou tužku a papír. Veškeré knihy, data a informace byly psané ručně, postupem času na psacím stroji a až ve 20. století se začaly používat osobní počítače. Ty se samozřejmě s časem posunovaly a neustále vyvíjely. Dnes by si už člověk řekl, že jsou veškeré technologie tak dokonalé, že už nejdou ani zdokonalit. Ale opak je pravdou a neustále se vyvíjejí. Ne každý vývoj je však vždycky šťastným řešením a může být i propadákem. S vývojem informačních a komunikačních technologií ale také úzce souvisí možnosti jejich napadení a lidí, které by je chtěli napadnout. Myslím si, že s emailovým spamem se už potkal alespoň jednou za život každý z nás. Naštěstí jsou dnes emailové schránky dost chytré na to, aby takové spamy házely rovnou do koše a neohrožovaly nás. Alespoň většinou. Bohužel například o phisingu, crackingu či ransomwaru se to říct nedá. A jelikož je v dnešní době ve světě informačních technologií ransomware stále populárnějším, rozhodla jsem se zaměřit právě na něj.

Je také důležité zmínit nové obecné nařízení o ochraně osobních údajů GDPR, neboť má za cíl hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů, tudíž představuje nový právní rámec ochrany osobních údajů v evropském prostoru. Toto nařízení bylo přijato v dubnu 2016, ale vstoupí v platnost od 25. května 2018. GDPR se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data uživatelů. Zavádí také astronomické pokuty za porušování nových pravidel a nařizuje některým správcům nebo zpracovatelům osobních údajů zřídit nezávislou kontrolní funkci DPO (Data Protection Officer), což je pověřenec pro ochranu osobních údajů.

V teoretické části jsou popsána základní názvosloví informačních a komunikačních technologií, zabývá se její bezpečností, informační bezpečností, bezpečnostním systémem, procesem. Jsou zde popsána aktiva, která jsou v rámci informačních a komunikačních technologií důležitá, její možné hrozby, rizika, zranitelnost a prevence. Ve druhé kapitole se práce zabývá počítačem a počítačovým systémem, který je důležitou součástí, neboť je při útocích ohrožen nejvíce. Je zde popsán software a hardware počítače, peopleware, dále data a informace, počítačová síť. Třetí kapitolou jsou samotné možné útoky na tyto informační

a komunikační technologie, kde je zmíněno sociální inženýrství, malware, pod který spadá ransomware, adware, spyware, viry, červi, trojský kůň či backdoors. Dále je zde zmíněný spam, phishing, pharming, podvodné webové stránky, hacking, cracking, sniffing a DOS/DDOS útok. Praktická část bakalářské práce je zaměřena na vytvoření virtuálního počítače, naistalování operačních souborů Windows XP, 7 a 10 na vytvořený virtuální počítač a poté stažení vybraného ransomwaru, v mém případě se jedná o ransomware WannaCry a ransomware Petya a jeho aplikování, tedy infiltrace na vybraný nechráněný nainstalovaný operační systém a postupné sledování, jak virtuální počítač na tento ransomware reaguje. V závěru práce najdeme možnosti obrany proti těmto útokům.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE A BEZPEČNOST

V úvodu mé bakalářské práce je popsáno základní názvosloví informačních a komunikačních technologií a bezpečnosti.

1.1 Základní názvosloví

V této podkapitole jsou podrobně vysvětleny pojmy informační a komunikační technologie a bezpečnost, bezpečnostní informační systém a jeho možnosti aplikování, dále také informační proces a komunikační bezpečnost.

1.1.1 Informační a komunikační technologie

Veškerou technikou zabývající se zpracováním a přenosem informací, hlavně výpočetní a komunikační techniky a jejího programového vybavení se rozumí informační a komunikační technologie. [1] Jsou to veškeré informační technologie, které se používají pro komunikaci a práci s informacemi. Původně byla využívána pouze zkratka IT, jako informační technologie, ale později byla doplněna o „C“, neboť mezi sebou začaly jednotlivé počítače či uzavřené sítě komunikovat, z čehož plyne ICT. Nejedná se však jen o prvky hardwarové (počítače, servery), ale také o softwarové vybavení (operační systémy, síťové protokoly, internetové vyhledávače). V dnešním světě se ICT staly důležitou a nepostradatelnou součástí státní, podnikatelské i soukromé sféry, tudíž jejich ovládání patří mezi klíčové odbornosti. [2]

1.1.2 Bezpečnost

Řekne-li se pojem bezpečnost a zeptáme se deseti lidí, co si pod tímto slovem představují, dostaneme pravděpodobně deset nejrůznějších odpovědí. Protože každý si pod tímto pojmem může představit něco jiného. Záleží totiž na tom, o jakou bezpečnost se jedná. Bezpečnost však znamená určitou míru jistoty, snižující pocit ohrožení. Hlavním předmětem zabezpečení a ochrany byly vždy tři hlavní skupiny, a to i když se důvody a metody zabezpečení postupem času měnily. Do těchto skupin patří v první řadě zdraví a život, což je vše, co souvisí s fyzickou existencí jedinců, dále pak majetek, jak už hmotný tak nehmotný a v neposlední řadě také informace a znalosti na těchto informacích založené. Tyto skupiny však nefungují jenom samostatně, ale mohou spolu úzce souviset

a prolínat se. Například porušení a ztráta bezpečností informace může vést ke ztrátám na majetku. [3]

Znalosti a poznatky, které nejsou běžně dostupné, jsou náročné na zpracování a méně dostupné většímu okruhu subjektů, a jsou získané na základě informací, patří do zvláštní skupiny bezpečnosti. Nepatří sem tedy veškeré informace, nýbrž pouze ty, které mají určitou důležitost pro jejich nositele a subjekty, kteří by tuhle informaci mohli získat. Jsou to tedy informace, jejichž dostupnost je omezená a které můžou jejich nositeli získat určitou výhodu před ostatními subjekty a pokud by ji nositel ztratil, mohla by mu způsobit škodu. Subjekty ochrany, v jejichž zájmu se provádí zabezpečení a ochrana jsou všichni uživatelé informačních systémů. Patří mezi ně především fyzické osoby, právnické osoby, stát a jeho orgány, asociace více států, asociace fyzických nebo právnických osob apod. [3]

Chceme-li řešit bezpečnostní problematiku u subjektů vyžadující posouzení individuálních podmínek, musíme si položit a odpovědět na základní otázky. Těmi jsou „zda a co“, „před čím“ a „jakým způsobem“ mají být předměty chráněny. Okolnosti, na nichž jsou závislé odpovědi na tyto otázky, můžeme rozlišit na vnitřní a vnější. Existence hrozeb a míra rizika s jakou se mohou hrozby uskutečnit, patří mezi vnější okolnosti, ale například ekonomické možnosti subjektu realizovat potřebná protiopatření patří mezi vnitřní okolnosti. [3]

1.1.3 Informační bezpečnost

Je důležité si uvědomit, že neexistuje bezcenná informace a kdykoliv smíme říct, jaký potenciální zisk či ztrátu pro nás může znamenat. Informaci můžeme chápat jako skutečnost s určitou hodnotou, se kterou lze nakládat v podstatě jako s penězi. Lze s ní obchodovat, lze ji ničit, poškozovat nebo transformovat. Informace jsou tedy jako peníze a proto bychom měli k informacím, které vlastníme, přistupovat a chránit je stejně, jako naše finance. I přes to, že se v průběhu historie a vývoje života informace měnila z klasického chápání psaní na papíře, které vydrželo až do dvacátého století, a postupně se díky globalizaci počítačů, komunikační sítě a celosvětovému internetu měnila do takové podoby, jak již ji známe dnes, tedy do podoby elektronické, kdy se stává něčím uchopitelným, stává se nehmotným statkem, i přes to, že je tato informace uložena v jiném tvaru, se jedna významná skutečnost nezměnila a to ta, že hodnota informace stále zůstává cennou hodnotou, kterou musíme chránit. [3]

Informační bezpečností rozumíme tedy veškerou ochranu informace tak, aby nedošlo k nechtěnému narušení či změně, zneužití, úniku, odcizení nebo ztrátě informací. Snažíme se tedy zabránit všem negativním událostem, které by mohly nastat. Cílem je tedy zejména ochrana informací a dat tak, aby nedošlo k negativním důsledkům. Riziko úniku informace však může nastat jak z okolního prostředí, tak i zejména zevnitř organizace, proto je třeba ji chránit ze všech různých pohledů. Součástí informační bezpečnosti jsou všechny oblasti ukládání či přenosu dat, a to jak v psané, digitální či mluvené podobě. [4] S tímto úzce souvisí také přístup do systému, manipulace s hodnotami, vytváření záloh či antivirová ochrana, což je chápáno jako komplexnější zajištění systému, tedy bezpečnost systému. [3]

„Definici informační bezpečnosti chápeme jako zodpovědnost za ochranu informace během jejího vzniku, zpracování a ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.“ [3]

1.1.4 Bezpečnostní informační systém

Bezpečnostní informační systém využíváme k ochraně informací během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti při jejich likvidaci proti ztrátě důvěrnosti a také uchovává záznamy o úpravách zpracovaných informací. Je důležité si ale uvědomit, že absolutní bezpečnostní systém neexistuje a vždy existuje míra akceptovatelného rizika. Musíme rozlišovat bezpečnostní systém ve státních sektorech (armáda, policie) a komerčních sektorech, dále v kritické infrastruktuře státu, kde se ale už nerozlišuje, zda se jedná o státní nebo soukromý sektor. Liší se také funkce počítačového zabezpečení a to v závislosti na typu organizace a její velikosti. Sektor, který pracuje s informacemi a má za úkol je ze zákona chránit, například osobní údaje zaměstnanců nebo i třetích osob, je specifickým odvětvím. [4,5]

Možnosti aplikování bezpečnostní politiky informačního systému

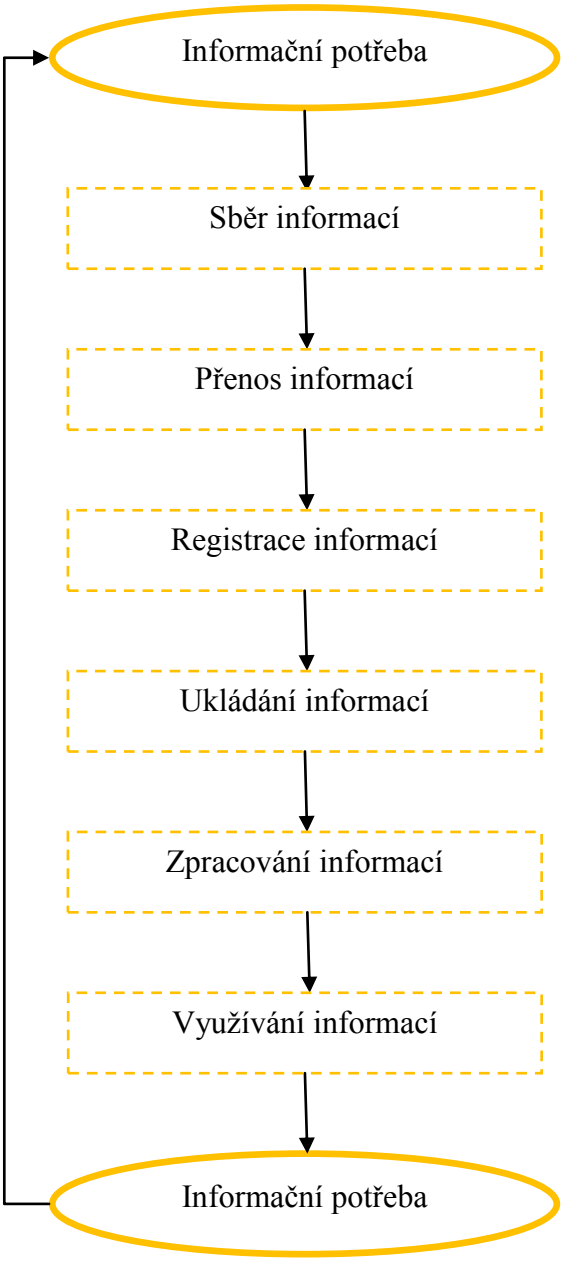
Mezi možnosti aplikování bezpečnostní politiky informačního systému patří politika paranoidní, přísná, povolná a promiskuitní.

- Paranoidní politika je taková, kdy je zabezpečeno absolutně všechno, uživatelům je téměř vše zakázáno a z důvodu bezpečnosti neexistuje žádné spojení s okolním světem.
- Přísná je definovaná tak, že je zakázáno všechno, co není výslovně dovoleno.

- Povolná udává, že co je povoleno, to není zakázáno.
- Promiskuitní politika říká, že to, co by mělo být z důvodů základní ochrany zakázáno, je dovoleno. [3]

1.1.5 Informační proces

Na uvedeném schématu (sch. 1) můžeme jednoduše pochopit, že informační proces je provádění jistých pracovních činností s informacemi, podle kterých se poté mění procesy, činnosti a chování organizace. Informační proces je tedy uzavřený cyklus, ve kterém je vždy na jeho začátku i na jeho konci určitá informační potřeba, a informace v něm prochází od svého vzniku až ke svému užití, přes přenos informací od zdroje k místu zpracování a jejich soustřeďování, registrování informací na místě zpracování, ukládání informací pro jejich budoucí využití, a zpracování informací, které zahrnuje nejen třídění a posuzování kvality vlastností, ale také vyhledávání doplňkových informací a jejich výběr, analýzu a syntézu. Tato získaná data a informace pro informační proces jsou zabezpečovány vhodným informačním systémem. [6]



Obrázek 1 – Informační proces [Zdroj: 5]

1.1.6 Komunikační bezpečnost

Komunikační cesty informačních systémů a tedy i jejich bezpečnost je dnes jedno z nejdůležitějších a zároveň nejvíce zranitelných míst, neboť je v komunikačních systémech velmi obtížné sledovat toky informací, jejich ukládání na elektronická média a jejich distribuci, zvláště, jedná-li se o rozsáhlé komunikační systémy. Základním pojmem je zde počítačová síť, díky které mohou jednotliví uživatelé mezi sebou komunikovat

(viz. kapitola 2). Přináší to však jisté hrozby, kdy můžou být napadena data a to za různým účelem, neboť je velmi obtížné neustále sledovat toky dat a jejich distribuci.

Komunikační systém je složen z několika podsystémů mající zcela zvláštní poslání a úkoly. Bezpečnostní podsystém komunikace musí zajišťovat ochranu všech prvků sítě a zároveň by jej chyba jiného podsystému neměla vyřadit z provozu tak, aby přestal plnit své funkce. Platí zde tedy také zásada všech podsystémů, že bezpečnost komunikačního podsystému odpovídá bezpečnosti jeho nejslabšího článku, kdy každý jeden takový článek musí splňovat minimální úrovně bezpečnosti. Možnosti ochrany bychom však mohli rozdělit do tří základních skupin a to na prevenci, kde je důležité si uvědomit bezpečnostní nedostatky sítě a vytvořit krizový plán pro případ útoku; detekci, kde je vhodné vytvořit či implementovat prostředky a stanovit kritéria pro detekci distribuovaného útoku, vytvořit algoritmy pro případ velkého objemu datové komunikace a vyvinout prostředky pro automatizované reportování podrobností o útocích; a v neposlední řadě reakci, kde je důležité zajistit schopnost odhalení rozsahu útoku, identifikování zdroje útoku, zablokovat provoz těchto zdrojů a předat dostatečné informace o útoku k dalším právním krokům. Hlavním předmětem ochrany komunikačních systémů jsou však zejména zdroje sítě, vzájemná relace mezi komunikujícími stranami, informace a data tak, aby nebylo možné narušení jejich integrity a důvěrnosti a také komunikační protokoly. [6]

1.1.7 Bitcoin

Bitcoin je první decentralizovaná digitální měna. Bitcoiny jsou digitální peníze, které můžete posílat skrz internet a v porovnání s ostatními alternativami má bitcoin mnoho výhod. Bitcoiny jsou převedeny přímo od osoby k osobě přes internet, bez přechodu bankou nebo zdaněním. To znamená, že poplatky jsou mnohem nižší, můžete je použít v jakékoli krajině, vaše konto nemůže být zmrazené, a že zde neexistují žádné podmínky nebo iracionální limity. A jak to funguje? Existuje několik výměnných kurzů, podle kterých můžete nakupovat a podávat bitcoiny za dolary, eura a jiné měny. Bitcoiny máte ve vaší digitální peněžence v počítači nebo mobilu a jejich posílání je stejně jednoduché, jako posílání emailů a můžete si s nimi koupit cokoli. Platby probíhají tak, že odesílatel zadá požadovaný počet bitcoinů, vyplní bitcoinovou adresu a transakcí potvrdí svým klíčem. Platba postupně prochází sítí, je ověřována a nakonec je zařazena do blockchainu, čímž je potvrzena. Síť bitcoinů je také zabezpečená lidmi nazývanými hornici. Ti zjišťují bezpečnost a fungování sítě, za což jsou odměňováni nově generovanými bitcoiny

za potvrzování transakcí. V síti probíhá každou minutu velké množství transakcí. Ty se sdružují do bloků (každých deset minut vzniká jeden blok) a bloky dávají dohromady Blockchain- řetězec bloků. Blockchain můžeme chápat jako databázi nebo veřejný záznam všech transakcí, který se pravidelně aktualizuje. Software je kompletně otevřený a kdokoli si může zkontrolovat kód. [7]

1.2 Základní pojmy informační bezpečnosti

V této podkapitole jsou uvedena základní aktiva informační bezpečnosti, její hrozby, rizika, zranitelnost a opatření proti nim.

1.2.1 Aktiva

Aktiva jsou všechny hmotné i nehmotné statky, vše, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu. Za nejcennější aktiva považujeme hlavně data a informace. Aktiva dělíme na hmotná a nehmotná. Mezi **hmotná aktiva** řadíme především výpočetní techniku, což jsou počítače, servery a disková pole a komunikační technologie (strukturovaná kabeláž, aktivní síťové prvky). Za **nehmotná aktiva** považujeme především programové vybavení a data. Jedná se o operační systémy, aplikační programy a programové nástroje pro správu a řízení informačního systému. Každé aktivum má svoji **hodnotu aktiva,** kdy každý chráněný objekt má svoji cenu, která je jak pro majitele, tak pro útočníka rozdílná. Hodnota aktiva je ocenění důležitosti a významu pro vlastníka. [3]

Mezi aktiva patří také **bezpečnost**, což je určení míry ochrany proti možným škodám či ztrátám, zneužití nebo zničení stavu nebo vlastnosti prvku, v našem případě informačního systému. **Citlivá data** jsou takové informace, které je potřeba chránit, protože mají pro organizaci určitou úroveň důležitosti a jejich existence může způsobit určitou škodu a to například jejím zneužitím nebo změněním. **Citlivé informace** jsou informace, jež se musí chránit, protože jejich možná ztráta, změna nebo zničení by mohla způsobit škodu. Tyto informace určuje odpovědná osoba. V neposlední řadě sem patří také **objekt,** jímž v informačním systému rozumíme především soubor na nepaměťovém nosiči, záznam, blok dat, apod. a **subjekt,** což je aktivní osoba, která má přístup k objektům. [3]

1.2.2 Hrozby

Hrozba nastává v případě, že dojde k ohrožení informačního systému, nebo dat v něm obsažených. Jedná o příčinu nechtěného incidentu, například k poškození, zničení, ke ztrátě důvěry nebo hodnoty aktiva. Je to reálné, známé nebo potenciální nebezpečí.

Mezi další hrozby řadíme **bezpečnostní incident,** který využívá zranitelných míst informačního systému a snaží se o průnik nebo jinou nepovolenou škodlivou činnost. **Expozici,** jež je místem, které je vystavené riziku, kde může dojít k potenciálnímu poškození nebo ztrátě informací či snížení funkčnosti systému. **Narušení bezpečnosti -** naruší-li se bezpečnostní politika získáním přístupu k informacím nebo některé části informačního systému, a poruší-li se bezpečnostní kontroly informačního systému, jedná se o narušení bezpečnosti. **Průnik**, což je zneužití informačního systému. [3]

1.2.3 Rizika

Riziko je účinek nejistoty na dosažení cílů, možnost škody nebo ztráty dat a informací. Jde o míru ohrožení aktiva. Hodnota informačního rizika je dána pravděpodobností, že se uplatní některá z hrozeb nebo zranitelných míst informačních systémů. Je-li systém dodán, instalován nebo používán způsobem, který není bezpečný, pramení z toho nejpravděpodobnější riziko. Omyly a nedbalost personálu spolu s nesprávnou manipulací bývají nejčastější příčinou rizika. [3]

1.2.4 Zranitelnost

Zranitelnost existuje v každém informačním systému a můžou to být právě takové prvky, které využívá útočník k útoku na data nebo celý systém. Zranitelnost je tedy nedostatek nebo slabé místo aktiva. Software, aplikace, ale i lidské chyby, neznalost nebo podcenění bezpečnosti mohou být slabinou zranitelnosti. **Útočník je** někdo, kdo se snaží o krádež, zneužití nebo poškození dat či celého systému či o nepovolený zásah do informačního systému. [3]

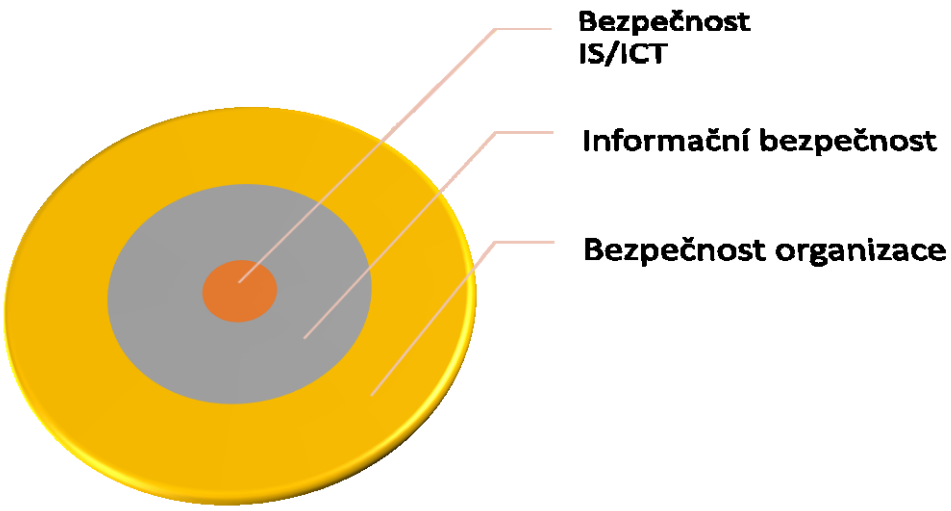
1.2.5 Prevence

Mezi hlavní prvky prevence patří **autentizace,** kterou charakterizujeme jako *„proces ověření identity uživatele“*a **autorizace,** což je udělení práv, které zahrnuje udělení přístupu na základě přístupových práv pracovat například s daty, provádět různé úkony,

funkce, apod. **Elektronický podpis** je podpis uživatele v digitální podobě, namísto písemné, **certifikát** se používá pro identifikaci uživatele. Propojuje digitální potvrzení totožnosti s digitálním podpisem. **Integrita,** což je vlastnost ochrany přesnosti a úplnosti informace v průběhu jejich přenosu od zdroje k cíli a také **detekce průniku,** jež je technický systém, díky kterému můžeme zjistit, zda byl učiněn pokus o průnik do informačních systémů a sítí, nebo zda takový čin nastal. [3]

Dalšími prvky prevence jsou **bezpečnostní analýza IS,** jejímž cílem je odborná analýza zjištění rizik, hrozeb a navržení protiopatření pro maximální zabezpečení zkoumaného informačního systému. **Bezpečnostní audit,** který je prováděn externím nebo interním ověřovatelem. Jedná se o nezávislé testování činnosti informačního systému a těchto záznamů s cílem určit, zda jsou kontroly odpovídající a zda existuje shoda s bezpečnostní politikou nebo zda jsou doporučené případné změny v systému protiopatření. **Bezpečnostní funkce** je způsob, jakým můžeme dosáhnout požadovaného zabezpečení jednotlivých informací v informačním systému. Základní dokument vymezující strukturu bezpečnostního rizika, souhrn požadavků, potřeb a pravidel, směrnic, předpisů a zásad, které zabezpečují veškeré prvky informačního systému a chrání citlivé nebo kritické zdroje systému se nazývá **bezpečnostní politika**. Cílevědomé a systematické shromažďování, zpracování, uchovávání a zpřístupňování informací a dat zabezpečuje **informační systém** jako funkční celek. Je souborem technického (hardware) a programového (software) vybavení. **Ocenění rizik** zajišťuje, aby byla pravděpodobnost škody snížena na přijatelnou úroveň, k čemuž je třeba definovat úroveň rizika a hrozeb, které mohou působit na informační systém a také zjistit, zda jsou bezpečnostní opatření dostatečně účinná. [3]

Důležitá je také **ochrana aktiv,** která chrání data a informace před působením hrozeb, tedy rizik. V neposlední řadě sem patří také **protiopatření,** které provádí jakoukoliv činnost, proces nebo techniku, která je určena k minimalizaci zranitelnosti. Chrání aktiva před působením hrozby úplně, nebo zmírňuje její působení a vzniklé škody a proces **zvládání rizik**, díky kterému můžeme určit, kontrolovat a omezovat vliv nepředvídatelných a nepříznivých událostí – hrozeb. [3]



Obrázek 2 – Vztah úrovní bezpečnosti [Zdroj: 6]

Obrázek č. 2 nám ukazuje základní vztah úrovní bezpečnosti, kde nejvyšší kategorií je bezpečnost organizace nebo firmy. Její součástí je zajištění bezpečnosti objektů, majetku organizace. Její součástí kromě jiných je i informační bezpečnost, jejímž cílem a úkolem je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů. Samotná bezpečnost IS/ICT má za úkol chránit pouze ta aktiva, která jsou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi. Proto je relativně nejužší oblastí řízení bezpečnosti. [6]

2 POČÍTAČOVÝ SYSTÉM

V této kapitole je uvedeno co je to počítačový systém a počítač, neboť se může zdát, že jde o jednu a tutéž věc, ale opak je pravdou, protože jejich vymezení nemusí být vždy jednoznačné. Pro pojem počítač existuje mnoho různých definic.

1) Počítač je zařízení, které obsahuje centrální procesorovou jednotku, která je schopná řídit se programovým kódem a je schopná ovládat přidružené periferie, ale také další části počítače; následně pak zařízení obsahuje médium pro ukládání dat, např. paměť či disk; zařízení pro zobrazování, čímž obvykle bývá monitor a dále jiné periferie. [8]
2) Počítač je zařízení pro zpracování dat, které provádí samočinně či podle zadaného programu posloupnosti různých logických a aritmetických operací. [9]
3) Počítačem se rozumí elektronické zařízení, umožňující zpracovávání dat, které se skládá z hardwaru (pevné části počítače) a softwaru (programové vybavení).
4) Počítač můžeme podle typu chápat buď jako klasický stolní PC nebo přenosný, např. laptop či notebook. [10]

Jestliže chceme využívat počítač, musí být každá činnost předem naprogramována. Počítač je schopen uchovávat informace, které do něj vložíme, zpracováváme nebo transformujeme a to pomocí paměťových médií, nebo tyto informace také může počítač zpětně poskytovat ve vnímatelné podobě (na zobrazovacím zařízení nebo jako zvukové signály).

Pod pojmem počítačový systém rozumíme funkční jednotku, která se skládá z jednoho nebo více počítačů a přidruženého softwaru, který využívá paměťové médium pro všechny, nebo alespoň část programů a dat, které jsou nezbytné pro vykonání programů, což vychází z definice Úmluvy o kyberkriminalitě. Počítačový systém však také může pracovat samostatně, např. osobní počítač či notebook jako samostatná funkční jednotka, nebo jako soubor několika vzájemně propojených počítačových systémů (např. počítačová síť). [8]

2.1 Hardware

Hardware (z ang. Významu „Technické vybavení“) můžeme laicky pojmenovat jako všechno, co se nachází v počítači a na co si můžeme sáhnout. Jedná se tedy o všechny části počítače, které napomáhají k jeho fungování. V podstatě můžeme říct, že se jedná o počítač samotný. Základní deska, paměť RAM, grafická karta, pevný disk, ale i například

klávesnice nebo myš, což řadíme mezi specifický druh hardwaru - periferii, jsou součástí hardwaru. [11]

2.2 Software

V této podkapitole je nutné vymezit pojmy programové vybavení a počítačový program, protože mezi těmito dvěma pojmy a softwarem je značný rozdíl a často jsou tyto pojmy chybně považovány za synonyma.

Programové vybavení je součást výpočetní techniky. Jedná se o programy a dokumentace, kterými je doplněno technické vybavení počítače pro umožnění jeho využití. Zahrnuje v sobě programy počítačů, počítačové programy včetně software.

Systém na zpracování údajů, který je dokáže zpracovat v takovém tvaru, jako zápis algoritmu, je charakterizován jako **počítačový program**. Můžeme říci, že se jedná o ucelený souhrn instrukcí, díky kterým dokáže počítač provádět určitou činnost. Dostatečně schopné provádění předepsané činnosti je možné za pomoci souboru nebo více souborů, které tvoří počítačový program.

Veškeré programové či netechnické vybavení, které je nutné k provozu počítačů označuje anglický výraz **software**. *„Zahrnuje všechny programy od základních vstupně/výstupních systémů (BIOS) a jednoduchých utilit přes operační systémy (MS Windows a OS Linux), grafická rozhraní a veškeré aplikace, od jednoduchých až po komplexní programové systémy.“ [8]*

2.3 Peopleware

Peopleware se týká lidské role v IT systému. V mnoha případech lidé vytvářejí jakýsi "koncepční trojúhelník" s hardware a software. Termín označuje lidský talent jako druh přeměňovaného kusu IT procesu a klíčovou část poskytování různých technických obchodních modelů a dalších plánovacích prostředků. Jedná se o lidi, jež provádějí různé úlohy, které jsou běžně chápány jako součásti procesu IT. To zahrnuje počítačové inženýry, návrháře webových stránek, techniky a další IT specialisty, jako jsou například správci databází nebo specialisté na vytváření sítí. Pracovníci, kteří jsou zařazeni do širokého zastřešení osobních počítačů, mívají obvykle klíčovou certifikaci v těchto a dalších oblastech IT specializace. [12]

2.4 Data a informace

„Data jsou fakta, čísla, události, mapy, grafy, transakce, atd., které byly zaznamenány. Jsou základním materiálem, surovinou pro informace.“[8] Jedná se tedy o prvky s informační hodnotou zpracované počítačem, uchovávána v ucelených souborech různého typu, tvořící následně informaci.

Informace je něco, co má pro nás určitý přínos. Je to určité sdělení, které má smysl buď pro toho, kdo informaci zpracovává, nebo přijímá. Každá informace je tedy údajem, datem, ale ne všechna uložená data se musejí nutně stát informací. Informace je tedy něco víc než data, neboť data jsou pouze fakta a informací se stávají až tehdy, jsou-li vnímány v kontextu a mají určitý význam pochopitelný pro lidi. [8]

2.5 Počítačová síť

„Počítačová síť je soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.“ [1] Tuto definici uvádí Výkladový slovník kybernetické bezpečnosti, existuje však celá řada různých definic.

Můžeme také říct, že počítačová síť pracuje tak, že spojuje dva a více počítačů pro vzájemné sdílení svých prostředků, jak hardwarových, tak softwarových. [13] Nejjednodušším vysvětlením počítačové sítě je asi takové, že se jedná o soubor počítačových systémů, které jsou navzájem propojeny a dochází mezi nimi k výměně dat či informací. [8]

Počítačovou síť můžeme rozdělit z celé řady různých hledisek, nejzákladnější však jsou:

1. Dělení dle rozlehlosti sítí
    - PAN (Personal Area Network – Osobní síť) – Tuto síť nejčastěji využívají jednotlivci či domácnosti, neboť se jedná o malou privátní síť a propojují se v ní jednotlivé počítačové systémy, například mobilní telefon nebo notebook za pomocí WiFi nebo Bluetooth.
    - LAN (Local Area Network – Lokální počítačová síť) – Jedná se o místní síť, což je síť, ve které dochází k propojení uzlů v rámci jedné či více budov. Způsob propojení jednotlivých uzlů není důležitý a tato síť má

typicky menší vzdálenost mezi jednotlivými uzly a vyšší přenosovou rychlost.

- MAN (Metropolitan Area Network – Metropolitní síť) – Síť, která propojuje LAN sítě v městské zástavbě a jednotlivé uzly spojuje v řádech jednotek až desítek kilometrů.
- WAN (Wide Area Network – Vzdálená počítačová síť) – Označuje počítačové sítě propojující geograficky vzdálené oblasti.

2. Dělení dle postavení síťových uzlů
    - Peer-to-peer („rovný s rovným“, či klient-klient) - decentralizovaný komunikační model, ve kterém má každá strana stejné možnosti a každá strana může zahájit komunikační relaci. Tato síť umožňuje každému uzlu, aby fungoval jak pro klienta, tak i pro server.
    - Klient-server - popisuje vztah mezi dvěma počítačovými programy, v nichž první program, klient, žádá o služby jiný program zvaný server. Na tomto modelu je založen například přístup na E-mail, Web, přístup k databázi.
3. Dělení dle vlastnictví sítí
    - Privátní síť - Privátní adresy jsou běžně používány pro domácí, kancelářské a podnikové lokální sítě (LAN), kde veřejné adresy (tj. globálně směrovatelné v Internetu) nejsou žádoucí nebo nejsou dostupné a jsou označovány jako soukromé.
    - Veřejná síť – jedná se o síť, která se vytváří za účelem komunikace s jinými subjekty (také připojenými k veřejné datové síti), aby prostřednictvím veřejné datové sítě propojovaly mezi sebou své dílčí lokální sítě. Vlastník sítě tedy pronajímá svou přenosovou kapacitu jiným subjektům, téměř vždy však na komerčním základě.
    - Virtuální privátní síť - jde o bezpečné spojení vytvořené mezi koncovým zařízením (osobní počítač, smartphone, tablet) a serverem který je uvnitř počítačové sítě organizace. [8]

Tyto sítě jsou důležitou součástí počítačového systému, neboť právě díky nim je možné využívat možnosti aplikování počítačových virů a útoků na informační a komunikační technologie.

3 DRUHY ÚTOKŮ NA INFORMAČNÍ A KOMUNIKAČNÍ PROSTŘEDKY

Třetí kapitola se zabývá jednotlivými útoky na informační a komunikační technologie, které jsou v dnešní době mnohem častější a známější.

3.1 Sociální inženýrství

Jak říká Albert Einstein: *„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.“ [8]* A právě lidská hloupost je předpokladem pro fungování sociálního inženýrství, neboť nejslabším článkem bezpečnostního systému byl, je a vždycky bude lidská bytost – uživatel. Sociální inženýrství můžeme definovat tak, že jde o ovlivňování, přesvědčování či manipulování s lidmi tak, aby byli donuceni provést určitou akci či získat informace, které jsou běžně nedostupné. Jelikož hlavní myšlenkou není využívat ryze technické přístupy či nástroje například k prolomení hesla, ale využít lidské hlouposti a uvést oběť v omyl, ve kterém oběť sama heslo prozradí, je pro útočníka vhodné využít tohoto typu útoku, neboť na světě neexistuje počítačový systém, který by alespoň v nějaké fázi nebyl závislý na člověku a tím je pro něj nejjednodušší cestou získat potřebné informace právě od člověka. Získat co nejvíce informací o cíli útoku je jedním z klíčových faktorů sociálního inženýrství. Útočník často využívá lidské neopatrnosti, důvěřivosti, ochoty pomoci jiným, slabosti či hlouposti k tomu, aby si vybudoval důvěru s obětí před tím, než provede útok. Tvoření této důvěry však může být dlouhodobým procesem, ale napomáhá mu tak k realizaci útoku. Ty jsou většinou vedeny třemi způsoby, které se navzájem kombinují a to;

- Sběr volně dostupných dat o cíli útoku,
- fyzický útok pro získání co nejvíce informací,
- psychologický útok.

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit;

- Telefonický hovor,
- útok „tváří v tvář“,
- prohledávání webu, sociálních sítí aj.,
- doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči,
- nabídku vyzkoušení služby online,

- falešného servisního technika. [8]

3.2 Malware

Výraz malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“ a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Jako malware lze označit jakýkoli software, který je využíván k narušení normální činnosti počítačového systému, získávání informací nebo k získání přístupu k počítačovému systému. Jsou pojmenovány podle toho, jakou činnost provádějí, proto může mít malware mnoho podob. Malware se může šířit sám prostřednictvím e-mailů, například v rámci přílohy a zároveň může získávat e-mailové adresy z napadeného počítačového systémy, z čehož vyplývá, že jeden malware je schopný plnit několik funkcí najednou. Pod souhrnné označení malware se zahrnuje adware, spyware, viry, červi, trojské koně, backdoors, aj. [14]

3.2.1 Možnost tvorby malware

Pro vytvoření malwaru je nutné znát alespoň základy programování a programovací jazyky. Mluvíme-li v informatice o programování, mluvíme o vytváření procesu od návrhu řešení problému za pomoci výpočetní techniky ke spustitelnému počítačovému programu. Jsou zde zahrnuty činnosti od analýzy problému, přes jeho pochopí, nalezení algoritmu až po zápis zdrojového kódu v cílovém programovacím jazyce, jehož cílem je nalezení takové sekvence příkazů, které bude počítač schopný provést a realizovat zadaný úkol. [15]

Programovací jazyk je prostředek pro zápis algoritmů, které mohou být provedeny na počítači a je komunikačním nástrojem mezi programátorem formulující postup řešení daného problému v programovacím jazyce a počítačem interpretující technické prostředky problému. Jedná se tedy o soubor pravidel pro zápis algoritmu. Programovacích jazyků existuje hned několik, nejlépe hodnocenými v roce 2018 však jsou JavaScript, SQL, Python, Kotlin, PHP a C/C++. [15]

JavaScript

JavaScript je nejvíce požadovaný programovací jazyk. Byl primárně používán na webu pro zvýšení dynamiky stránek, dnešní JavaScript se však vyvinul tak, aby se stal něčím mnohem víc. Celé přední koncové rámce jsou postaveny na tomto jazyce a hybridní aplikace napsané ve formátu HTML + JS jsou postaveny tak, aby fungovaly na libovolné mobilní platformě. [16]

SQL

SQL je dotazovací jazyk sloužící k načítání dat z databází. Existuje mnoho implementací SQL, ale více méně jsou všechny podobné a jsou používány všude. [16]

Python

Python lze použít v různých oblastech jako je vývoj aplikací, her, skriptování, vědecké výzkumy a téměř ve všem, co si představíte. Má velmi jednoduchou syntaxi a vzhledem k tomu, že pro seskupování bloků kódu používá odsazení místo složených závorek, je kód velmi čistý. [16]

Kotlin

Kotlin je novější jazyk, který byl oficiálně podporován aplikací Google pro Android. Jedná se o pokles náhrady pro Javu a bezproblémově pracuje s jeho kódem. [16]

PHP

PHP je jeden z nejlepších skriptovacích jazyků serveru s velmi jednoduchou strukturou syntaxe. Více než polovina internetu běží na PHP a internet se nejspíše zblázní, až PHP zemře. [16]

C/C++

Jedná se pravděpodobně o první jazyk, který je vyučovaný na středních a vysokých školách. C je jeden z nejstarších jazyků, který je stále funkční díky své rychlosti provedení a jednoduchosti kódu. Jazyk C je využíván pro vestavěná zařízení, C++ je využíván pro tvorbu systémového software, her a webových aplikací. [16]

Swift

Programovací jazyk Swift je prvním programovacím jazykem od společnosti Apple, který byl zneužit pro vytvoření falešného patche. Po rozbalení se malware rozšíří po celém počítači Mac a požaduje po uživateli zaplacení výkupného v hodnotě 0,25 Bitcoinů na určenou adresu a dešifrování má být po zaplacení do 24 hodin opět přístupné, ale ani po zaplacení nedostane uživatel svůj disk zpět. [17]

3.2.2 Dělení dle způsobu útoku

Malware byl pro potřeby této bakalářské práce rozdělen dle způsobu útoku, kam spadá adware, spyware a ransomware.

ADWARE

Adware, neboli „advertising supported software“ můžeme volně přeložit jako software podporující reklamu. Zobrazování reklam (např. pop-up okna v počítačovém systému nebo na webových stránkách), na počítačovém systému uživatele je jednou z hlavních úloh adwaru, které sice mnohdy uživatele obtěžují, ale neubližují. Adware totiž není tolik nebezpečný, jako spíš výnosný pro malware. Může však dojít k nebezpečnému spojení adware se spyware, který má za účel sledovat činnost uživatele a odcizit důležité informace. [8]

SPYWARE

Spyware je v podstatě špion, který špehuje uživatele a získává důležité informace a data, jak o počítačovém systému, tak i informace osobního charakteru či o osobě uživatele, bez jeho vědomí, a dále jsou odesílána do datové schránky útočníka, který s těmito údaji může dále pracovat, ale také může obsahovat další nástroje ovlivňující vlastní činnost uživatele. Může být nainstalován buď jako samostatný malware, nebo může být součástí jiných, volně šířených programů. Jedním z typu spyware může být např. keylloger, což je software využívaný k získávání údajů jako jsou uživatelská jména a hesla k účtům, pomocí zaznamenávání konkrétních stisků kláves na napadeném počítači, které jsou následně zaslány útočníkovi.[8]

RANSOMWARE

Ransomware (z anglického „ransom“ – výkupné) je označení pro tzv. vyděračský malware, který brání či omezuje uživateli v užívání počítačového systému do doby, dokud nedostane útočník zaplaceno „výkupné“. Většinou se šíří do počítačového systému pomocí malware (trojský kůň nebo červ) umístěného na webových stránkách nebo může být přílohou v emailu. Ihned po jeho bezpečném „usídlení“ v počítačovém systému se stáhne vlastní ransomware. Rozlišujeme dva typy ransomware a to ransomware, který omezí funkčnost celého počítačového systému a uživatel jej následně nemůže vůbec využívat a ransomware, který nechá počítačový systém funkční, ale uzamkne a znepřístupní data uživatele, což bývá v současnosti využívanějším typem, kdy je účelem zašifrovat pevný disk či vybrané soubory, přičemž zašifruje soukromé soubory, jako jsou fotky, textové dokumenty, aj. Následně se uživateli zobrazí zpráva, že byly tyto soubory zašifrované a pokud je chce získat zpět, musí za ně zaplatit ve stanovené lhůtě určitý obnos na účet

útočníka. Po uplynutí dojde ke smazání klíče, který může zašifrované soubory otevřít. Takovým typem může být například ransomware WannaCry nebo Petya. [18]

3.2.3 Dělení dle způsobu šíření

Dále následují zástupci dělení dle způsobu šíření s následnou specifikací jednotlivých druhů, konkrétně tedy virů, červů, trojských koní a backdoors.

VIRY

Viry ke svému spuštění nepotřebují činnosti uživatele, neboť se nejčastěji šíří sdílením softwaru mezi jednotlivými počítačovými systémy, kdy se reprodukuje ve chvíli spuštění napadeného software či otevřením infikovaného dokumentu. Jedná se o program natolik chytrý, že dokáže sám sebe připojit k jinému, již existujícímu spustitelnému souboru či dokumentu. Ničení nebo usazení se v co největším počtu počítačových systémů k využití k následnému cílenému útoku je hlavním cílem virů. Projevy virů však mohou být různé. Příkladem je například virus Melissa, u kterého se původně myslelo, že byl vytvořen jako žert, neboť si mladí programátoři pouze zkoušeli, zda daný vir dokážou vytvořit a přitom se stal prvním virem, který se dokázal samostatně šířit. Dalším je např. virus Chernobyl, LoveLetter nebo Happy99.[8]

ČERVI

Červi (worms) si jsou dosti podobné s viry, neboť se svému spuštění nepotřebují žádného hostitele, ale na rozdíl od virů se šíří zcela samostatně. Je-li systém napaden, je následně červem využit k dalšímu odeslání kopií sebe sama dalším uživatelům pomocí síťové komunikace, čímž se velmi rychle rozšiřuje, a může to vést až k zahlcení celé sítě a tím i celé infrastruktury. Červi bývají velmi často využíváni ke hledání bezpečnostních mezer v systému. Příkladem je například ExploreZip, Code Red worm nebo Ramen worm.[8]

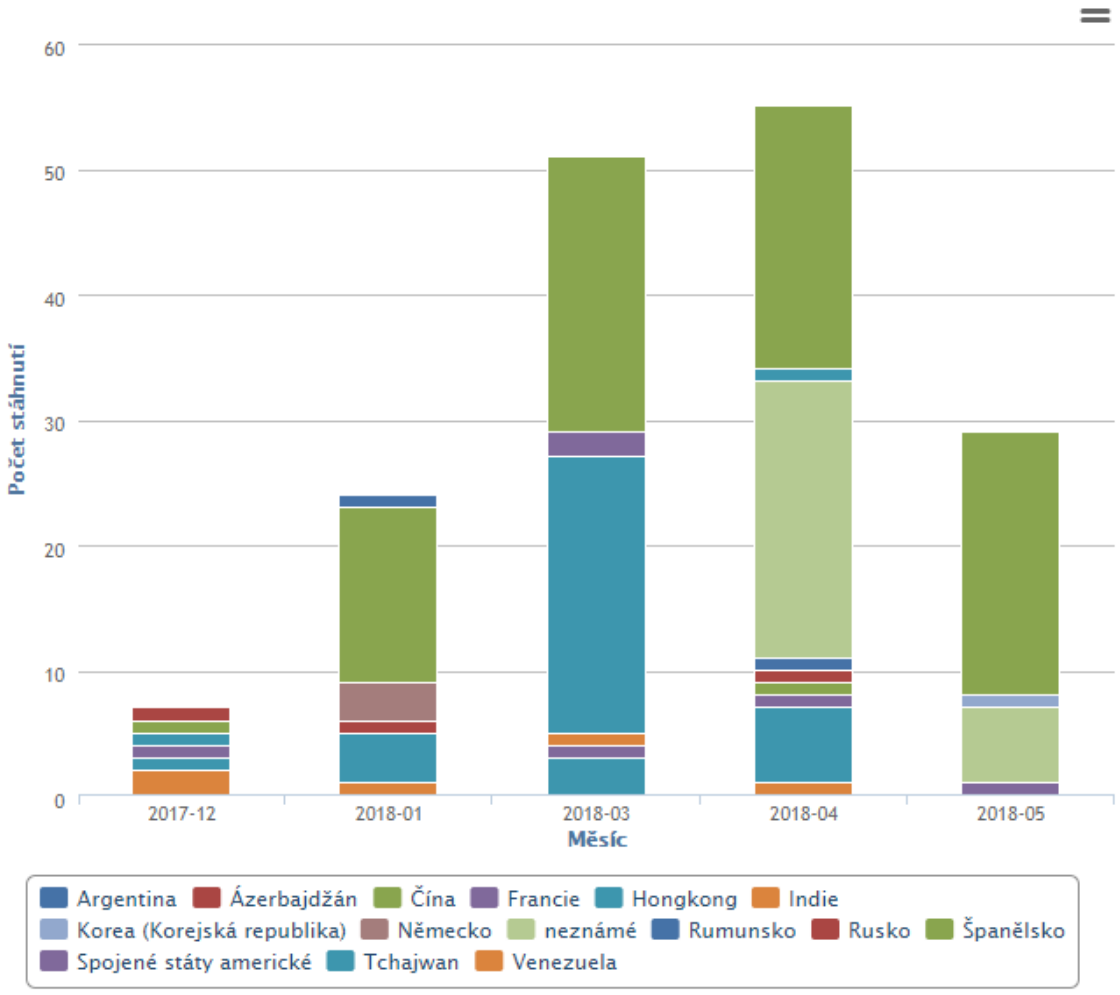
TROJSKÝ KŮŇ A BACKDOORS

Skryté funkce, se kterými uživatel nesouhlasí nebo o nich neví a jsou nebezpečné pro další fungování systému, jsou počítačové programy zvané trojský kůň. Mohou být připojeny k dalšímu nebezpečnému programu nebo vypadat samy jako neškodný počítačový program. Ke svému šíření však potřebují uživatele a v případě jeho aktivaci může dojít např. k mazání či kopírování dat. Příkladem trojského koně jsou například trojský kůň FakePlayer nebo Duqu. Za backdoors jsou označovány takové trojské koně, které po aktivaci

bez vědomí uživatele otevřou „zadní vrátka“ jiným škodlivým programům, které se tak snadno dostanou do počítačového systému, nebo jej mohou ovládat tzv. na dálku. [8]

3.2.4 Statistika

Následující obrázek (obr. 3) zobrazuje státy podle počtu stažení malware za posledních šest měsíců, od prosince 2017 do května 2018. Vidíme zde, že největší počet stažení nastal v březnu a dubnu roku 2018 a nejvíce stahovanými zeměmi byla Čína, Hongkong a Tchajwan. Naopak měsícem s nejmenším počtem stažení byl prosinec 2017 a státem Spojené státy Americké.

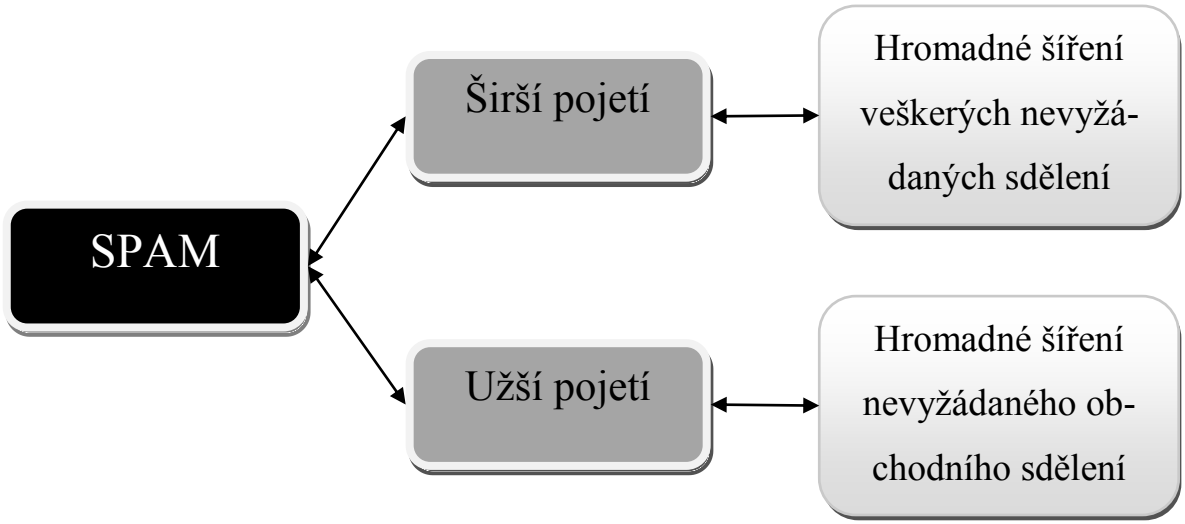


Obrázek 3 – Statistika [Zdroj: 19]

3.3 Spam

Mluvíme-li o spamu, mluvíme o něčem, co nechceme. Jedná se o určité sdělení zasílané elektronicky, hromadně a bez vyžádání. Spam můžeme rozdělit na širší a užší pojetí,

kdy do širšího pojetí spadá hromadné šíření veškerých nevyžádaných sdělení, tedy např. zprávy, které obsahují viry či trojské koně, a do užšího pojetí hromadné šíření nevyžádaného obchodního sdělení, nejčastěji reklamního charakteru pomocí internetu. (obr. 4) K tomu, aby mohl spam rozesílat tyto nevyžádané zprávy, využívá různé komunikační kanály, jimiž jsou například email, messenger (ICQ, Skype, Facebook), SMS, MMS, blogy, sociální sítě, aj. Obsahem spamu můžou být informace obchodní, reklamní, lékařské, finanční, náboženské, kriminální nebo třeba pornografické. [20]



Obrázek 4 – Rozdělení spamu [Zdroj: 8]

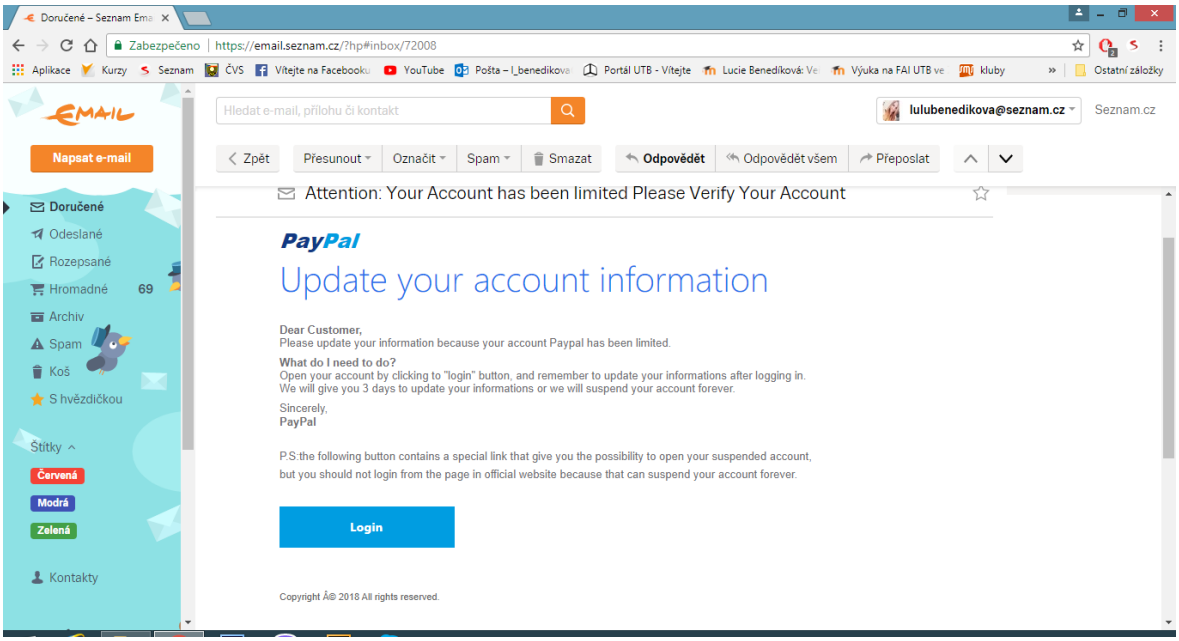
3.4 Phishing

Phishing si díky jedné teorii můžeme vysvětlit jako spojení dvou slov; fishing, což je rybaření, které v kontextu naznačuje rozesílání „návnady“ v naději, že se oběť „chytí“ a phreaking, což byl první hackerský útok na telefonní síť v USA. [21].

Hlavní úlohou phishingu je získávání přihlašovacích údajů a hesel nejčastěji k bankovním účtům za účelem využití dostupných prostředků jednotlivých klientů, jež funguje na principu rozesílání emailových zpráv, která nabádá ke kontaktování klientského centra prostřednictvím interaktivního odkazu, který je součástí emailu. Záminkou často bývá žádost o aktualizaci údajů či varování o chybě v bezpečnostním systému, které mají vyvolat pocit

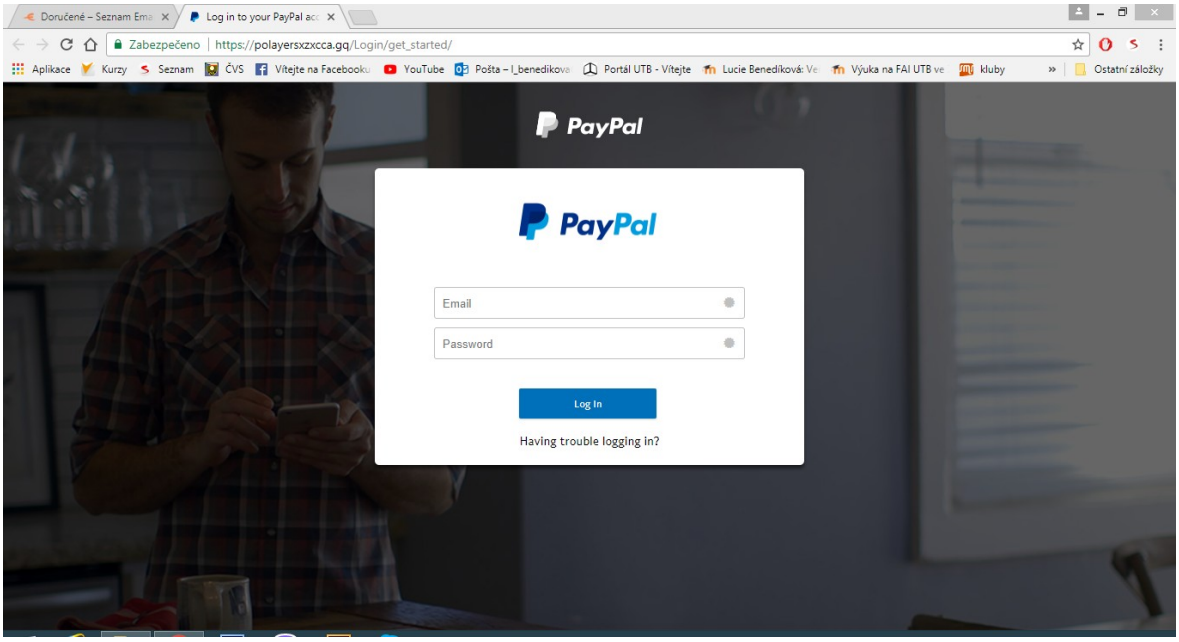
autentičnosti u klienta, po jehož aktivaci je klient přesměrován na podvodnou stránku vypadající téměř stejně jako originální stránka, která již typicky obsahuje malware. Následně je klient požádán o vyplnění přihlašovacích údajů, ty jsou poté odeslány na adresu phishera, který se může přihlásit ke skutečnému účtu a čerpat z něj finanční prostředky a způsobittím klientovi škodu. [8] Nejčastěji využívané pro phishingové útoky bývají stránky jako PayPal, PayPay, BidPay, E-gold. V České republice se pak nejvíce jedná o útoky na účty klientů České spořitelny, a.s. [22] Je možné jej využívat i v reálném světě, avšak svět virtuální je mnohem jednodušší a pohodlnější a umožňuje rozesílat obrovské množství podvodných zpráv. Není však zaměřen pouze na emaily, ale je možné jej najít i v rámci Instant messages (Skype, ICQ, Jabeer aj.), sociálních sítí, SMS a MMS zpráv apod. [23]

Obrázek č. 5 ukazuje doručený podvodný email nabádající ke kliknutí na odkaz, který je přílohou emailu, a aktualizování přihlašovacích údajů k účtu PayPal.



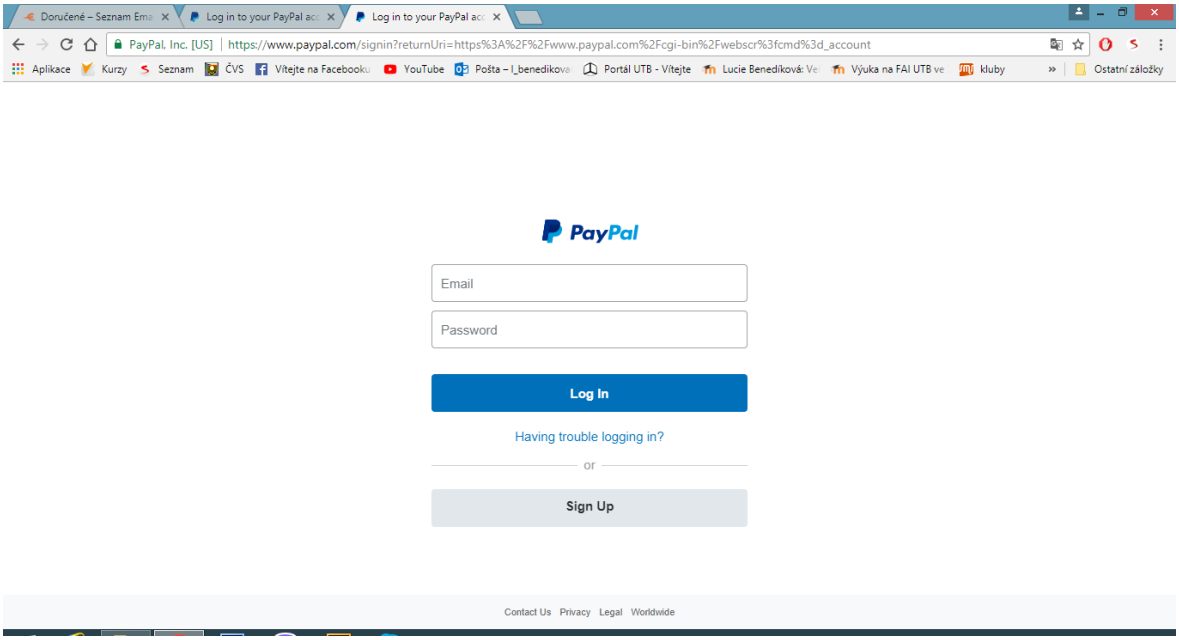
Obrázek 5 – Podvodný email formou phisingu [Zdroj: Vlastní]

Na obrázku č. 6 je vidět, jak vypadá podvodná webová stránka po otevření přílohy v podvodném emailu. Na první pohled se zdá, že vypadá jako originální, což je taky účelem podvodníka, ale podíváme-li se pořádně, vidíme, že http adresa v adresním řádku je podvodná.



Obrázek 6 – Podvodná stránka PayPal [Zdroj: Vlastní]

Obrázek č. 7 ukazuje originální webovou stránku PayPal, kde jsou vidět rozdíly s podvodnou webovou stránkou. Tyto rozdíly jsou však pro běžného uživatele nepatrné, a na první pohled si jich nemusí každý všimnout.



Obrázek 7 – Originální stránka PayPal [Zdroj: Vlastní]

3.5 Pharming

Pharming je rozšířenější a nebezpečnější verzí phishingu, kdy se útočník snaží získat citlivé údaje uživatelů na principu napadení DNS na kterém dochází k přepsání IP adresy, což při zadání údajů přesměruje klienta na podvodné stránky internetbankingu a po zadání adresy na internetovém prohlížeči finančního ústavu klientem dochází k útoku, kdy útočník získá citlivé údaje. Druhým způsobem pharmingu je napadení počítače koncového uživatele, kde se dá předpokládat menší míra zabezpečení. Pokud se podaří počítač úspěšně napadnout, stačí v něm upravit soubor Hosts obsahující URL adresu a jim přiřazené IP adresy. [24]

Pod pojem phishing a pharming také často spadá podvodná webová stránka, která funguje za stejným účelem, na stejném principu. Útočníci ke svému napadení využívají sociálního inženýrství a spoléhají na důvěřivost a neopatrnost lidí. Jedná se o vytvoření totožné stránky již existující jedním kliknutím. Podvodné webové stránky slouží útočníkovi pro získání citlivých informací, jako jsou přihlašovací údaje, hesla, PIN kódy, doručovací adresy, e-maily, většinou za účelem registrace, doručení zboží, výhry apod., jež může útočník ná-

sledně, stejně jako u phishingu, použít ve svůj prospěch k různým aktivitám, např. pokušení získání přístupu k dalším službám, které uživatel využívá. Dalším důvodem podvodných webových stránek je vylákání finančních prostředků z uživatele, např. nabízením levnějších produktů, jako jsou automobily, motocykly či elektronika. [8]

3.6 Hacking

„Hackerem se člověk nestane, narodí se jím.“ [Mentor]

V dnešní době si pod pojmem „hacker“ valná většina veřejnosti představuje někoho, kdo se snaží dostat k citlivým údajům za účelem jejich následného zneužití, za zloděje či vetřelce. Ve skutečnosti se však jedná o člověka, který se zajímá a bádá po detailech programových systémů a překračování jejich schopností, neboť ho to baví a má z toho potěšení. Považují se poté za experty na určité programy či obory, které jsou mnohdy vyhledávané. [25] Hacking je tedy proniknutí do počítačového systému jiným než obvyklým způsobem, většinou prolomením nebo obejítím bezpečnostního systému za účelem pouhého dokázání si své schopnosti a intelektuální převahy bez zájmu získání citlivých informací k dalšímu použití [26], neboť hackery jsou většinou lidé, jež byli v dětství považováni za outsidery bez budoucnosti. Není však pochyb o tom, že ne každá aktivita hackera je legální. Hackery můžeme rozdělit do třech hlavních skupin a to White Hats, což jsou hackeři, kteří k průniku využívají bezpečnostních slabin za účelem odhalení těchto slabin a vytvoření mechanismů, které by tyto útoky měli znemožnit a nezpůsobují žádnou škodu uživateli. Black Hats jsou jejich opak, kdy se snaží způsobit uživateli napadeného systému škodu či újmu. Gray Hats jsou hackeři šedé zóny, kteří můžou porušit práva, ale jejich činnost není primárně hnána snahou o způsobení škody. Dalšími skupinami mohou být také Script Kiddies, Hactivists, státem sponzorované hackery, Spy hackers, kyber teroristy, začátečníky, či Blue Hat hackers. [27]

3.7 Cracking

Cílem crackingu je neoprávněné užití prolomených nebo obejítých ochranných prvků programů, aplikací nebo počítačových systémů. Za hackery, kteří se snaží o prolomení do systému s cílem způsobit uživateli škodu, získat informace, jsou považování hackeři řazeni do kategorie Black Hats. Cracking je také spojován s porušováním autorských práv. Formou crackingu je i „password cracking“, který slouží ke zjišťování přístupových hesel

do počítačových systémů, kdy hacker většinou vytvoří keygen, což je program generující sériová čísla, nebo crack – program sloužící k odstranění či omezení funkčnosti ochranných prvků jiného programu, který umožní následné užití programu. [8]

3.8 Sniffing

Sniffing je v podstatě odposlech datové komunikace. Jedná se o nelegální metodu odposlechu dat, které prochází počítačovou sítí při komunikace mezi poskytovanou službou a počítačovým systémem pomocí tzv. snifferu, což je v podstatě čichač, neboť sniffing je z anglického slova volně přeloženo jako čmuchat. [28] Jedná se tedy o techniku, při které dochází k ukládání a následnému čtení TCP paketů. Normálně se používá při diagnostice sítě, dá se ale i zneužít k nelegálnímu odposlouchávání jak útočníkem, tak i zaměstnavatelem. V praxi může sloužit k získávání hesel, uživatelských jmen či jiných citlivých informací, které mohou být použity při špionáži nebo pro odhalení tajemství a následného útoku na celou organizaci. Sniffing může také využívat škodlivý software, např. trojské koně nebo keyloggery. Ochranou proti sniffingu může být zabezpečení všech aktivních i pasivních prvků počítačové sítě (router) a využívání kvalitních síťových prvků se zabudovanými ochrannými prvky, které znemožní zachytávání packetů a také ochrana datové komunikace např. pomocí šifrování. [29]

3.9 DoS/DDoS

Denial of Service (DoS) znamenající v překladu odmítnutí služby nebo taky útok zablokováním služeb, je útok cílený, jež způsobí nedostupnost poskytované služby. Útok proti softwarové severové službě mající za následek přetížení serverového procesu či celého serveru, kdy dojde k přerušení v poskytování služeb je nejčastějším útokem Dos. Druhem takového útoku může být zahlcení serveru velkým množstvím požadavků během krátké časové doby nebo využívání chyb v serverovém software, které způsobují zastavení serverového procesu či jeho nadměrné zatížení například pomocí příliš velkého nebo nekorektně formulovaného požadavku. **Distributed Denial of Serivce (DDoS)**, neboli distribuované odmítnutí služby, je v podstatě stejným typem útoku jako Dos, jen s rozdílem, že je k němu použito velké množství různých počítačů (klientů). Prvním krokem útočníka je získání co největšího počtu klientů, tzn. Proniknout do velkého počtu počítačů a v nich aktivovat proces, který čeká na vydání povelu a následně začne vysílat požadavky na cílový server. Proti takové formě útoku je pro oběť velmi těžké, někdy

i nemožné, se bránit, a pro útočníka naopak velmi výhodné, neboť je v takovémto případě velmi obtížné vystopovat zdroj útoku. [8] Rozdíl mezi Dos a DDoS je tedy v tom, že útok typu Dos je prováděný z jednoho počítače, zatímco k útoku DDoS je zapojeno více počítačů. [30]

Obrana proti těmto útokům není nemožná, avšak poměrně obtížná a závislá na formě útoku. Jedná-li se o útok, při kterém je využíváno známých chyb nebo vlastností určité verze aplikačního software či přenosového protokolu, mohlo by stačit update nebo oprava software. Platí zde však pravidlo o nutnosti neustálé kontroly bezpečnostních nedostatků operačních systémů a aplikačního serverového software. Je možné použít filtrů či směrovacích služeb a zakázat připojení z dané adresy v případě, že je útok vede běžnými prostředky, které směřují k přetížení serveru velkým množstvím požadavků a pochází pouze z omezeného počtu zdrojů. V takovémto případě však majitel velmi často netuší, že k útoku vůbec dochází. [30]

Botnet

Jednou z možností DDoS útoku je botnet. Jednoduše můžeme říci, že se jedná o síť softwarově propojených botů, nebo třeba internetové roboty, kteří pracují automaticky na základně příkazu „vlastníka“ této sítě. Může se jednat o síť, která je využívána k legální činnosti, ale i nelegální. Získání uznání a finančního zisku je hlavní hnací silou k vytváření botnetu. Podaří-li se botnetu infikovat cílový počítačový systém, následně se tento systém nazývaný „zombie“ či „bot“ připojí k centrálnímu řídícímu serveru. Útočník, zvaný botmaster či botherder má pak kontrolu nad celým tímto systémem, který řídí boty prostřednictvím centrálního řídícího serveru. Botnety jsou většinou pojmenovány podle malwaru, pod kterým se šíří. [8]

4 CÍL A ZVOLENÉ METODY ZPRACOVÁNÍ

Cílem teoretické části bylo seznámení se se základními pojmy v oblasti bezpečnosti informačních a komunikačních technologií, rozebrání počítačového systému, analyzovat současné možnosti útoků na informační a komunikační technologie ve vybrané oblasti a seznámit se s možnostmi tvorby malware pro vybranou oblast.

Cílem praktické části je vytvoření testovacího prostředí, v mém případě virtuálního počítače, jenž není chráněný antivirovým programem, následné nainstalování tří operačních systémů a nejdůležitější částí pak aplikování dvou zvolených ransomware na jeden vybraný operační systém. Těmito zvolenými ransomwary jsou WannaCry a Petya a zvoleným operačním systémem je nejnovější verze operačního systému Windows 10. Tato část je zvolena hlavně z důvodu narůstající nebezpečnosti a závažnosti těchto útoků, neboť žijeme ve světě informačních technologií a každé napadení je pro nás nežádoucí a ukazuje nám, jak je takové napadení snadné a je důležité se před každou možnou hrozbou bránit.

4.1 Metody použité při zpracování práce

V teoretické části jsem studovala literární odborné prameny, použila jsem dostupné zdroje ve formě internetových publikací. Pro studium odborných tištěných zdrojů jsem navštěvovala knihovnu UTB ve Zlíně a Uherském Hradišti, kde jsem čerpala z publikací pro zjištění obecné problematiky informačních a komunikačních technologií souvisejících s tématem.

V praktické části jsem využívala učebny IT na Fakultě logistiky a krizového řízení v Uherském Hradišti, díky které jsem měla přístup k počítači s nainstalovaným programem pro virtuální počítač, za jehož pomoci jsem mohla aplikovat škodlivý ransomware na operační systém a následně analyzovat průběh nákazy.

II. PRAKTICKÁ ČÁST

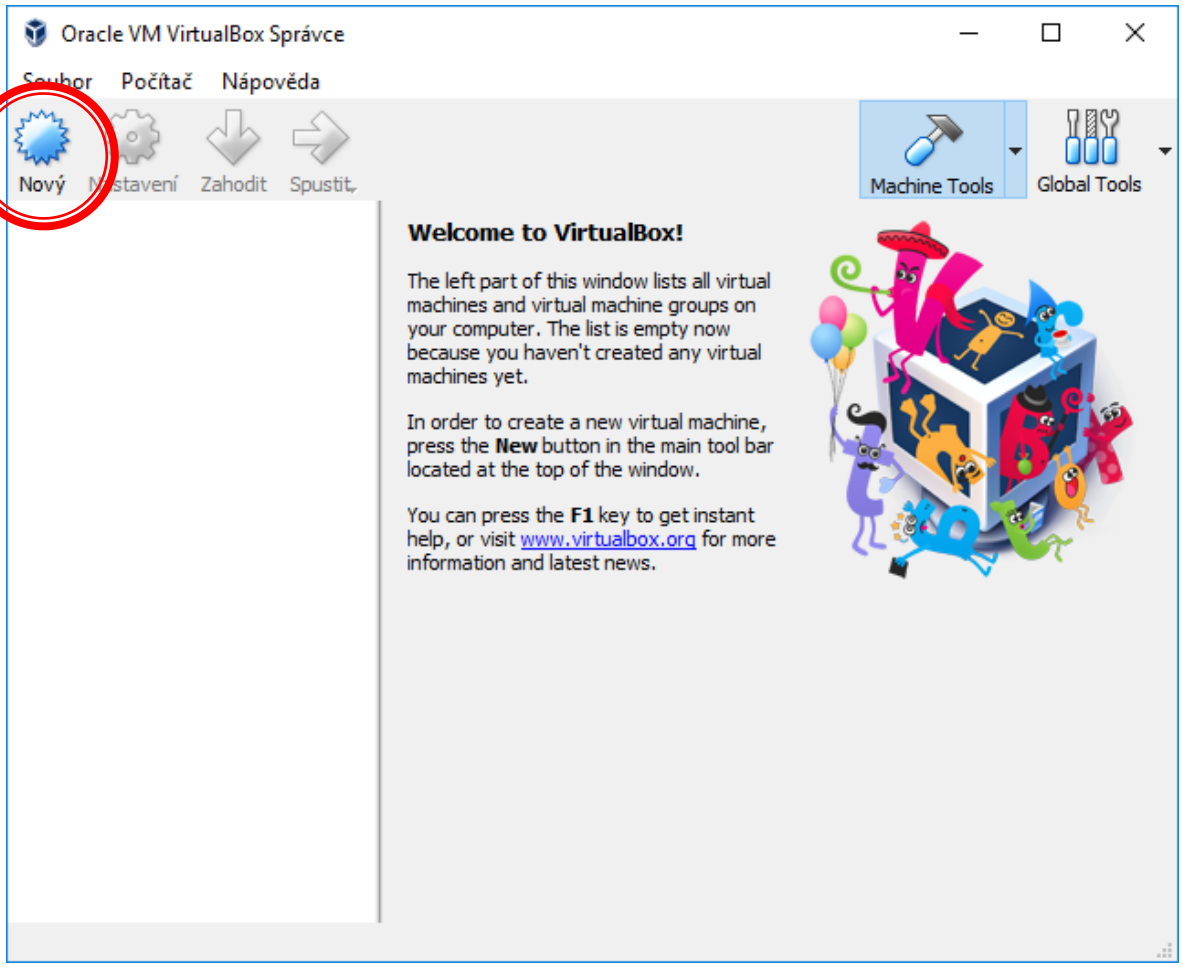
5 PŘÍPRAVA TESTOVACÍHO PROSTŘEDÍ

Vytvoření testovacího prostředí bylo prvním krokem praktické části bakalářské práce. Za přípravné prostředí byl zvolen virtuální počítač, jehož vytvoření a instalace je poměrně snadná a rychlá.

Virtuální počítač je počítač v počítači. Tak by se dal jednoduše nazvat. Jedná se totiž o počítačový program, často označovaný jako image, chovající se jako skutečný počítač, který můžeme jednoduše spustit v okně podobně jako ostatní programy a který umožňuje koncovému uživateli ve virtuálním prostředí stejné prostředí, jaké by měl v samotném hostitelském operačním systému. Velkou výhodou virtuálního počítače je to, že je oddělený od zbytku systému, což znamená, že software ve virtuálním počítači jej nemůže opustit, a hlavně nemůže být nijak úmyslně napadený a poškozený samotný počítač. Testování dalších operačních systémů, přístup k datům napadenými viry, vytváření záloh operačního systému a spouštění softwaru nebo aplikací v operačních systémech, pro které nebyly původně určeny, jsou úkony, pro které nám virtuální počítač vytváří ideální prostředí. [31]

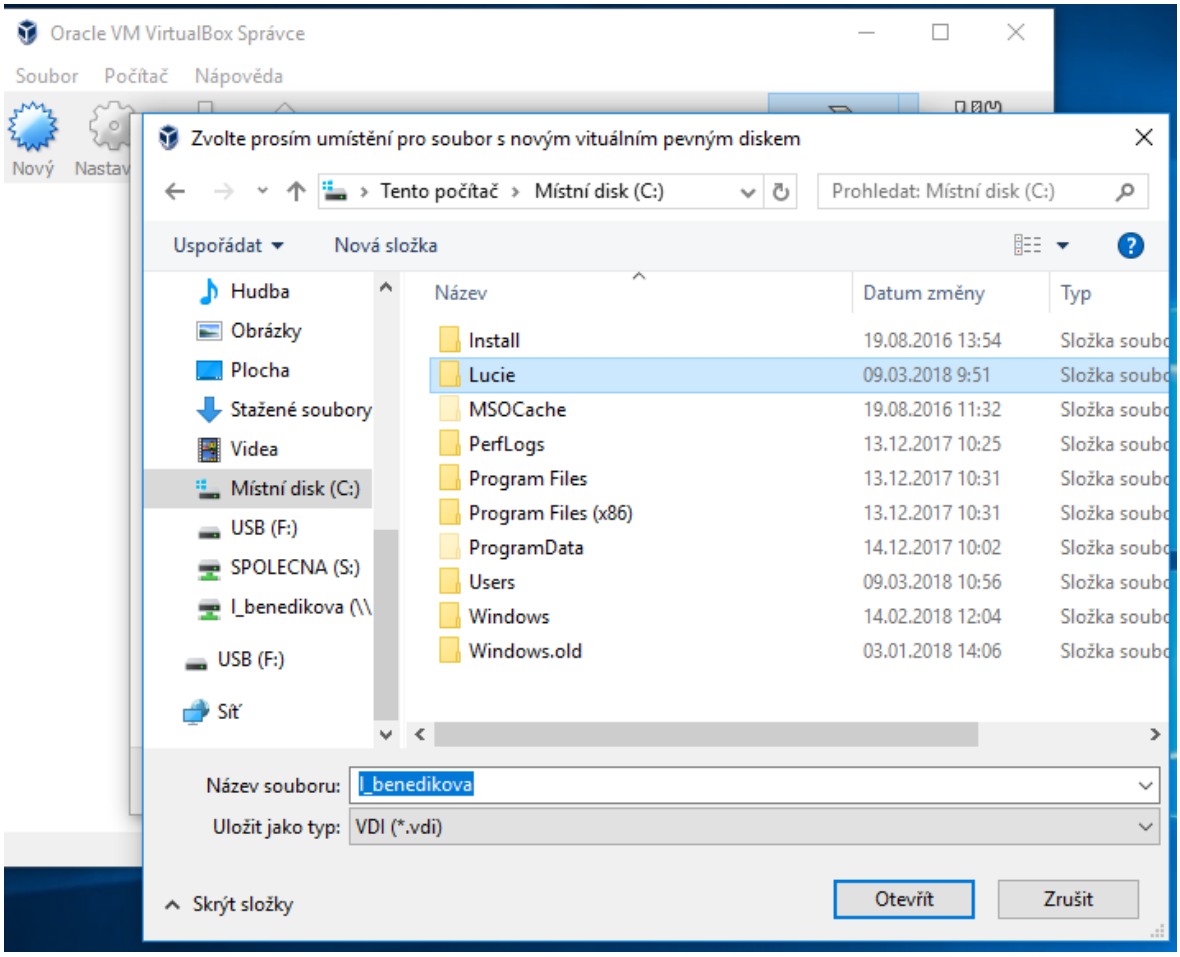
Další výhodou je také to, že v jednom fyzickém počítači může být spuštěných několik virtuálních počítačů současně. Softwaru zvaný hypervisor spravuje několik operačních systémů v případě serverů spuštěných vedle sebe. Jedná-li se o stolní počítač, používá se ke spouštění ostatních operačních systémů v oknech programu obvykle jeden operační systém. Vlastní virtuální hardware, včetně procesorů, paměti, pevných disků, síťových rozhraní a dalších zařízení poskytuje každý virtuální počítač. Následně se virtuální počítač mapuje na skutečný hardware ve fyzickém počítači, díky čemuž šetří náklady, neboť omezuje potřebu fyzického hardwaru pro systémy, také s tím snižuje související náklady na držbu a ještě i snižuje nároky na energii a chlazení. [32]

Nyní si popíšeme samotnou instalaci. Pomocí programu Oracle VM VirtualBox byl vytvořen vlastní virtuální počítač s názvem „l_benedikova“. Obrázek č. 8 zobrazuje zvolení nového virtuálního počítače, ve kterém byly prováděny další úkoly. Nejprve byla nastavena velikost paměti na 25 GB, vytvořil se nový virtuální pevný disk, poté byl zvolen typ souboru s pevným diskem a to VDI (VirtualBox Disk Image), následně bylo vybráno úložiště na fyzickém pevném disku, které se bude zvětšovat podle potřeby - dynamicky alokované, což znamená, že virtuální disk bude zabírat na fyzickém disku místo tak, jak bude zaplněn (do definované maximální velikosti, ale nebude automaticky zmenšen, pokud se v něm místo uvolní).



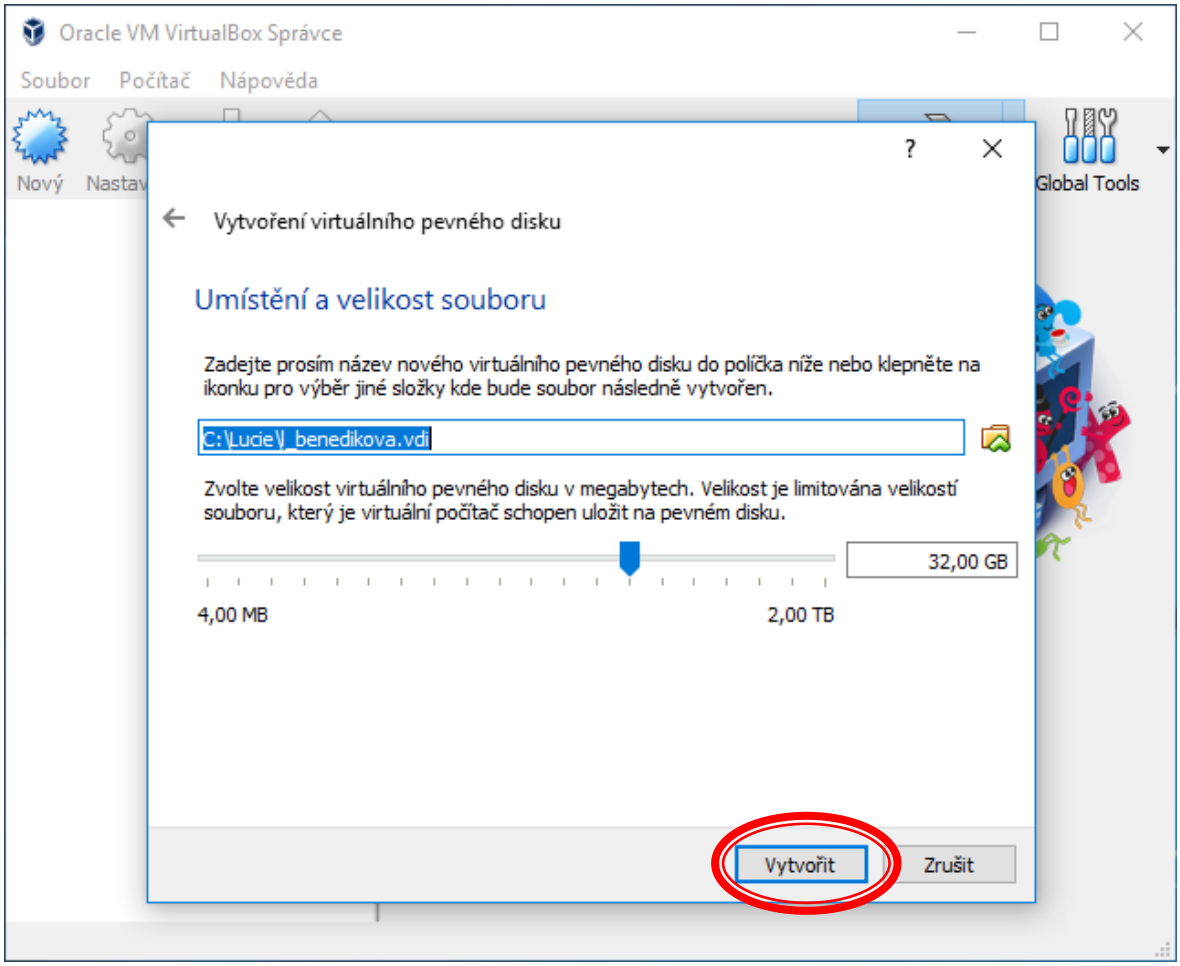
Obrázek 8 – Nový virtuální počítač [Zdroj: Vlastní]

V dalším kroku bylo zvoleno umístění pro soubor s novým virtuálním pevným diskem a to ve složce „Tento počítač – místní disk“, ve kterém byla pro tento virtuální počítač vytvořena složka „Lucie“ (obr. 9) a virtuální počítač pod názvem „l_benedikova“ byl uložen.



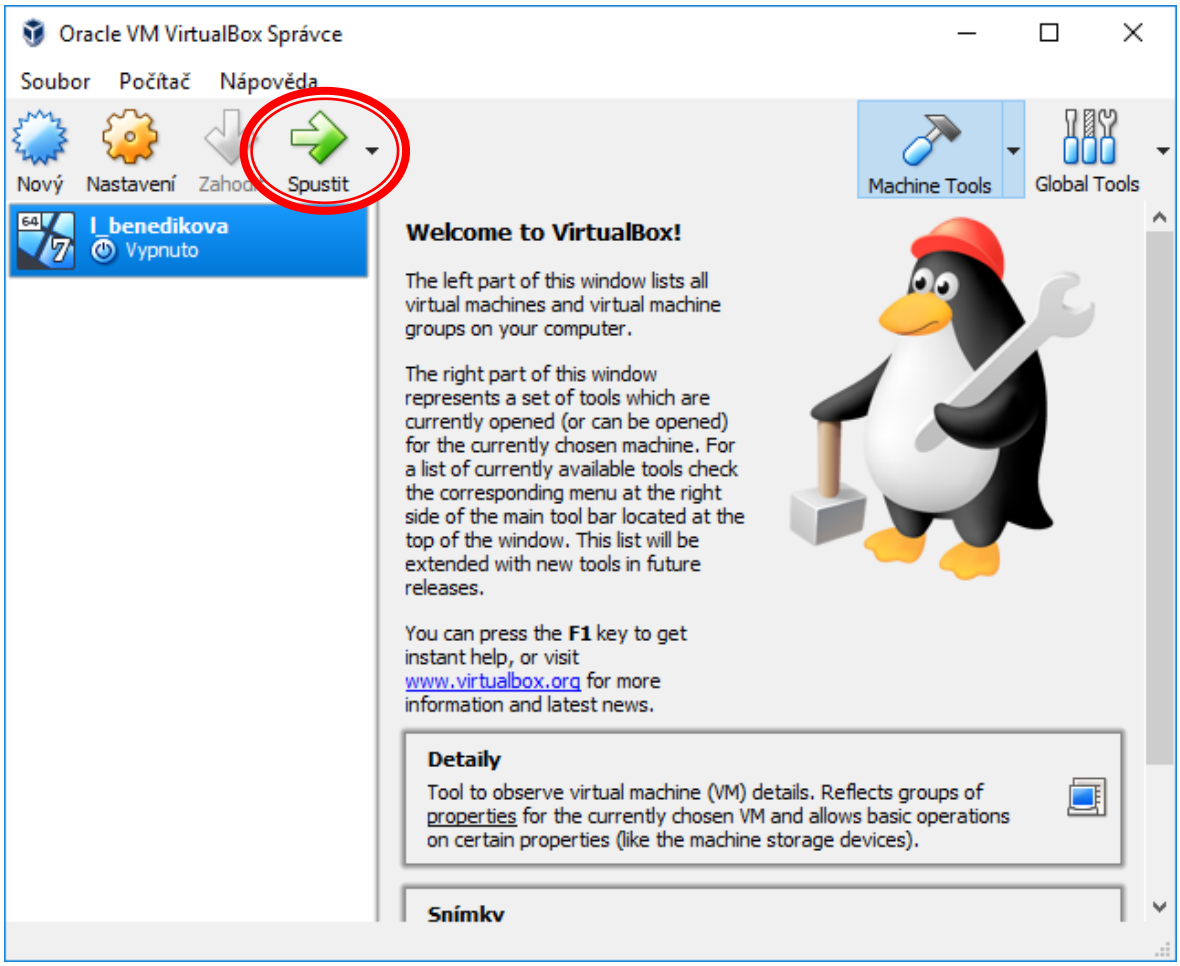
Obrázek 9 – Umístění virtuálního disku [Zdroj: Vlastní]

Po zvolení umístění virtuálního pevného disku a jeho uložení do vytvořené složky následovala finalizace procesu vytvoření, což zobrazuje obr. č. 10, a virtuální pevný disk byl vytvořen.



Obrázek 10 – Vytvoření virtuálního pevného disku [Zdroj: Vlastní]

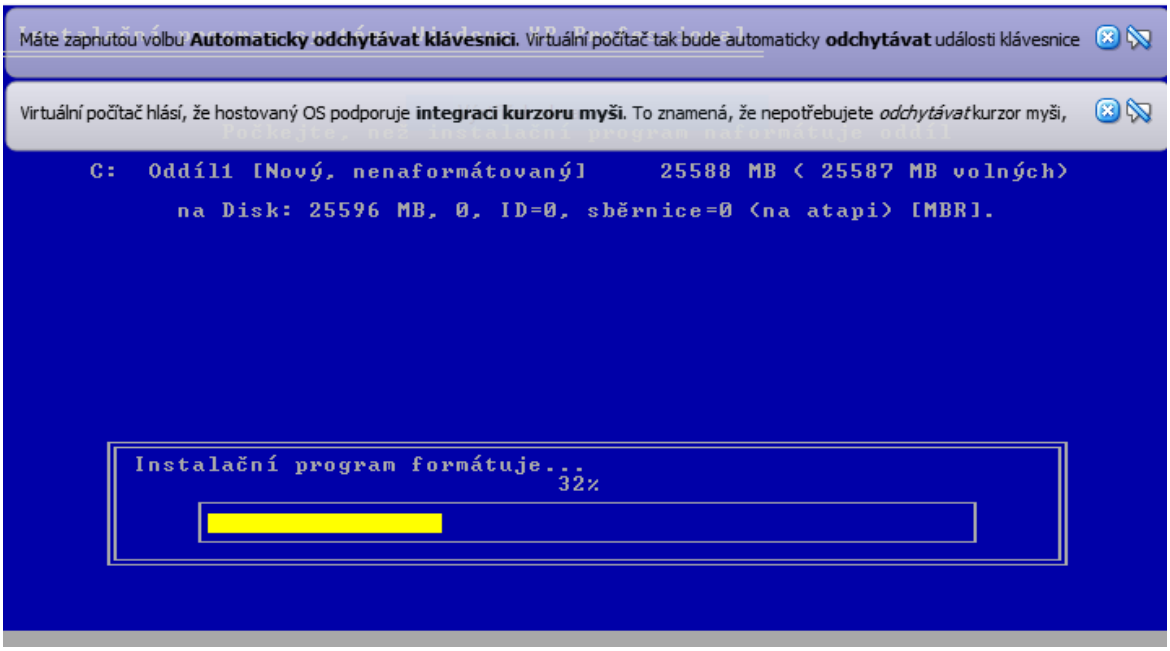
Po vytvoření tohoto virtuálního počítače byl virtuální počítač spuštěn (obr. 11) a začaly se instalovat operační systémy.



Obrázek 11 – Spustit virtuální počítač [Zdroj: Vlastní]

5.1 Windows XP

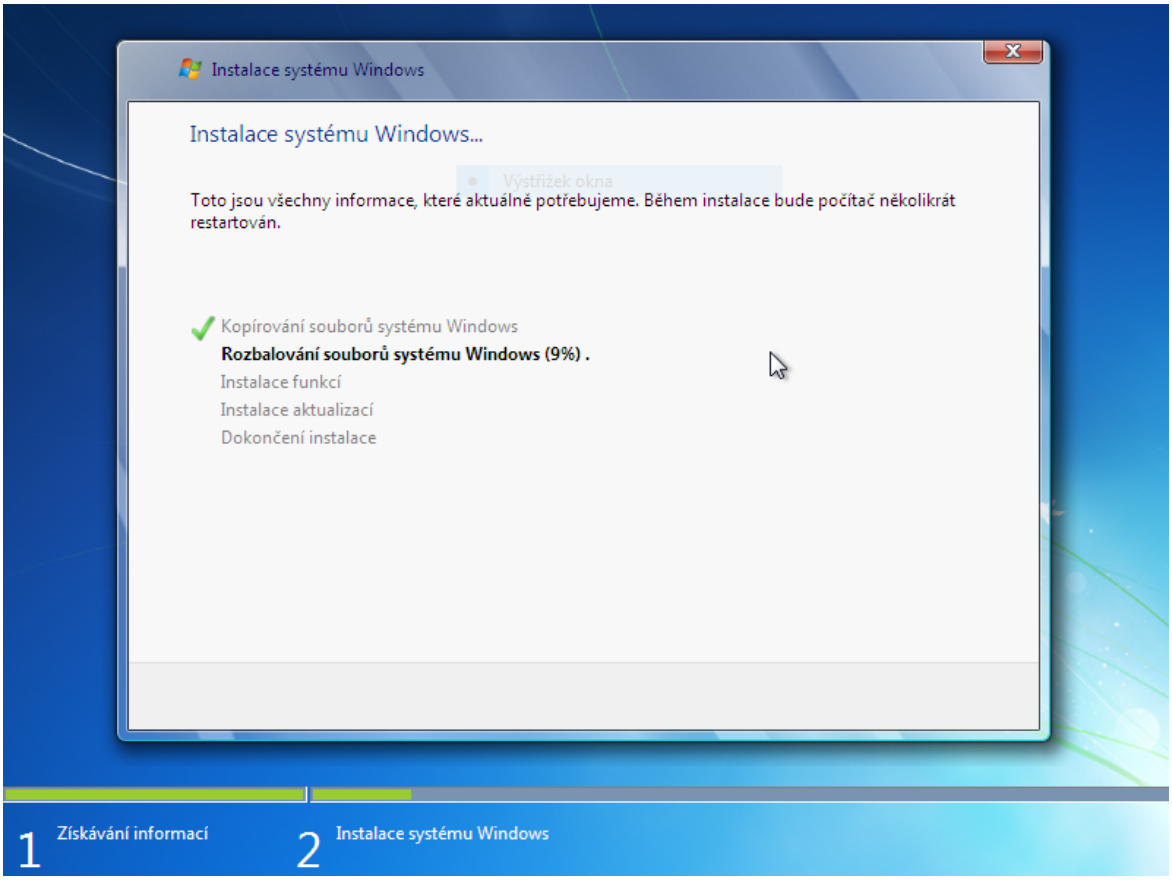
Druhým krokem byla instalace operačního systému. Zvolila jsem tři operační systémy, na kterých byly provedeny pokusy napadení virem, a bylo zkoumáno, jak na ně dané operační systémy reagují. Prvním z nich je operační systém **Windows XP** (obr. 12), který pochází od firmy Microsoft vydaný v roce 2001. Zkratka XP označuje zkušenost, z anglického slova eXPerience. Je určen pro obecné použití na domácích či firemních počítačích, ale jelikož se jedná o starší verzi operačních systémů od Windows a jeho prodej byl ukončen v roce 2008, není v dnešní době nejspíše už vůbec využíván, a to také díky své „neschopnosti“, aktualizacím a neustále novým vývojům. V roce 2010 byly ještě převedeny do tzv. rozšířené podpory, ta však skončila v roce 2014 a proto již nejsou poskytovány ani bezpečnostní aktualizace. [33]



Obrázek 12 – Instalace Windows XP [Zdroj: Vlastní]

5.2 Windows 7

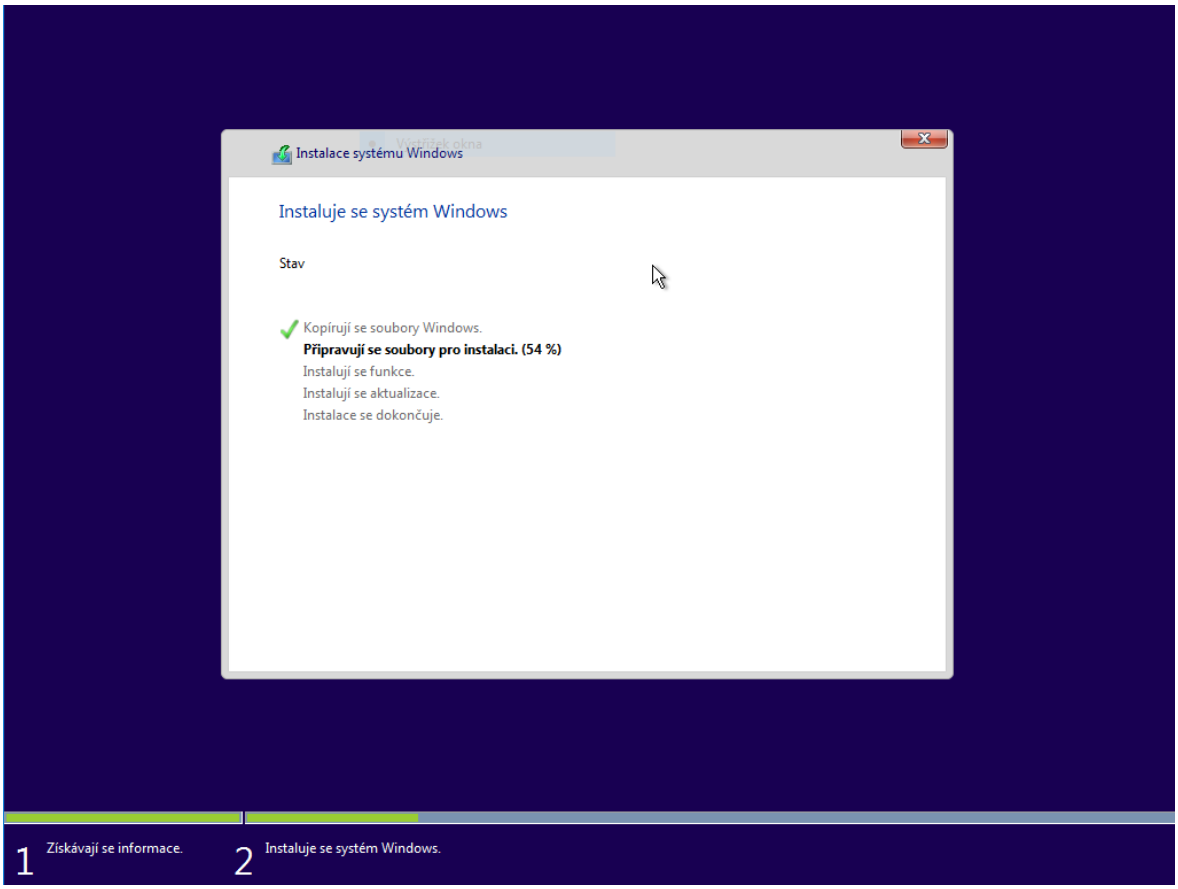
Druhým je operační systém **Windows 7** (obr. 13), který je již novější a v dnešní době hodně využívanou verzi operačního systému. Jedná se také o verzi operačního systému od firmy Microsoft vydanou roku 2009. Rozšířila se velmi rychle a napravila tak špatnou reputaci předchozích Windows Vista a teprve začátkem roku 2018 klesl jejich podíl na trhu pod Windows 10. Windows 7 byl zaměřen převážně na multidotykové ovládání, přestavěné Windows s novým hlavním panelem, domácí síť nazvanou HomeGroup a na zvýšení výkonu.[33]



Obrázek 13 – Instalace Windows 7 [Zdroj: Vlastní]

5.3 Windows 10

V neposlední řadě došlo k instalaci OS Windows 10 (obr. 14), který byl vydán v roce 2015 a je úplně nejnovější verzí instalovaných na nejnovějších zařízeních. Zavádí jednotné uživatelské prostředí různé platformy, např. stolní počítače, notebooky, tablety, chytré telefony, herní konzole Xbox a propojuje moderní aplikace, přidává podporu pro virtuální plochy a sjednocuje obchod s aplikacemi Windows Store. Jeho předchůdcem je systém Window 8.1. [33]



Obrázek 14 – Instalace Windows 10 [Zdroj: Vlastní]

Jednotlivé útoky pomocí malwaru WannaCry a Petya byly aplikovány na všech těchto operačních systémem, ale největší pozornost byla nakonec věnována pouze operačnímu systému Windows 10, neboť je-li možné napadnout nejnovější operační systém, který je instalován do většiny verzí počítačů a notebooků, jak již pro obyčejného uživatele či velkou firmu, je jasné, že jsou napadnutelné i starší verze těchto operačních systémů.

6 INFILTRACE RANSOMWARE

Praktická část byla tedy zaměřena na operační systém Windows 10, na který bylo zaútočeno jak pomocí ransomware WannaCry, tak následně také pomocí ransomware Petya. Jednáse o dva druhy ransomware, které zablokují a znemožní jakékoliv používání počítače a dat umístěných v něm.

6.1.1 Doporučené kroky při nákaze ransomwarem

V případě, že se staneme obětí ransomware WannaCry a je po nás vyžadováno výkupné, ptáme se na otázku, zda toto výkupné zaplatit či nikoli. Odpověď však není jednoznačná. Každý z nás se nad tím musí zamyslet a zvážit si své důvody v rozhodování. Nejprve bychom si měli uvědomit, zda nemohu své informace obnovit ze zálohy, jestli neexistuje již známé řešení pro dešifrování infikovaných souborů, zda hrozí, že ukradené informace budou zveřejněny a jak důležité jsou informace, které jsem ztratil? [34]

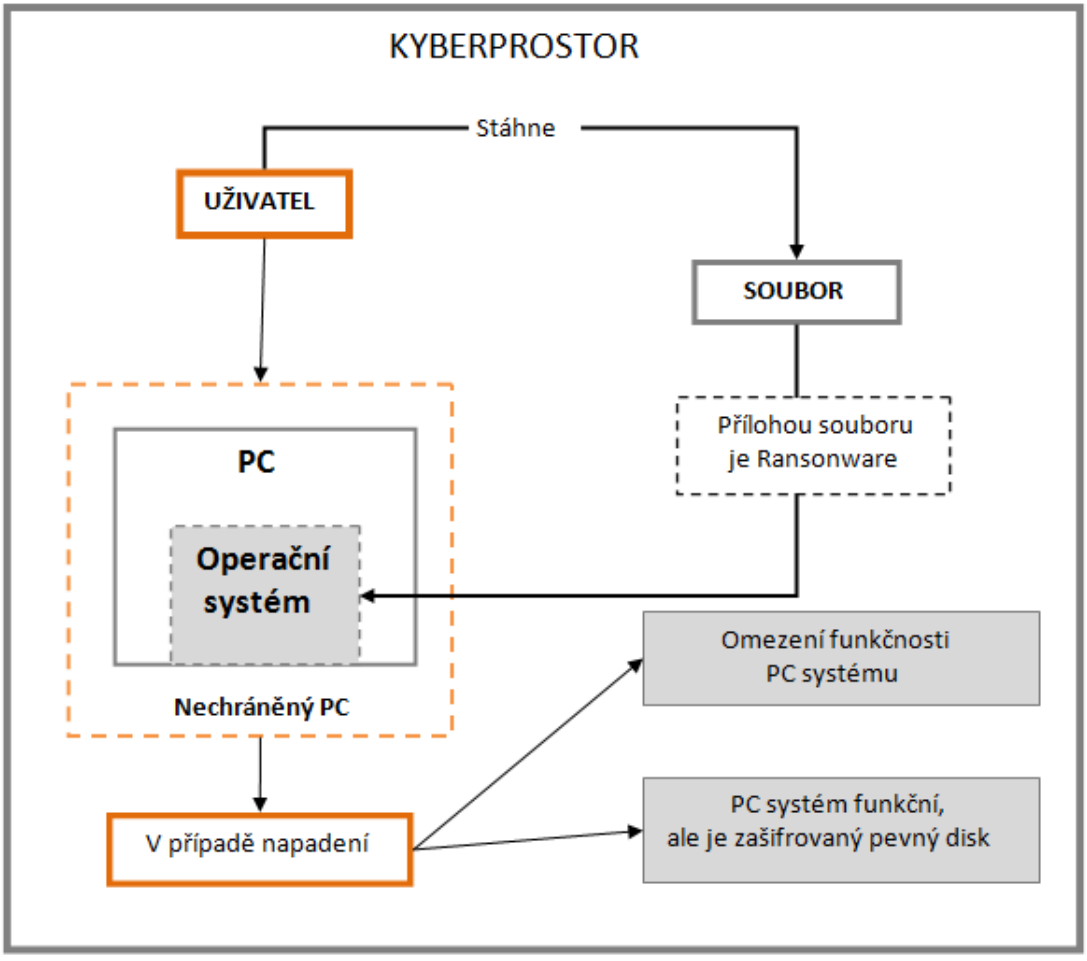
Pokud jsem byl napaden jako jednotlivec a obyčejný uživatel, a má data nejsou natolik důležitá, že by ohrozila můj život či chod firmy, je dobré se nejprve ujistit, zda není požadovaný klíč již dostupný online nebo zda nemůžu nějakou dobu, například měsíc až šest měsíců počkat, zda tento klíč nebude veřejně dostupný, a do té doby používat jiný hardware, neboť tyto typy virů se neustále obnovují a nezůstávají dlouho používanými. Pokud je však napadena firma a hrozí jí, že by musela zastavit chod firmy například na 14 dní a tím přijít až o miliony, je lepší toto výkupné zaplatit okamžitě. V takovém případě je však dobré mít nakoupené již zmiňované bitcoiny dopředu, což v dnešní době některé společnosti nakupují v předstihu, aby v případě útoku mohly zaplatit obratem, neboť získání bitcoinů může někdy trvat až několik dní a ve většině případů po několika dnech uplyne možnost kontaktovat vlastníka klíče k obnovení souborů. [34]

Před posláním požadovaného výkupného je však dobré se ujistit, že daný útočník může skutečně dešifrovat vaše soubory. To lze udělat například tak, že mu zašlete soubor a požádáte jej o jeho zpětné zaslání v dešifrované formě, abyste se ujistili, že to může skutečně provést. Pokud však ne, jedná se pravděpodobně pouze o pachatele, který tento ransomware koupil na černém trhu a nemá klíč k dešifrování vašich souborů. Zaplatím-li tedy výkupné, vyvstává zde další otázka, zda dostanu opravdu svá data zpět. Je nutné vzít v úvahu, že podle neoficiálních údajů, v 90 % případech, zločinci vrátí data po provedení platby, neboť se snaží udržet obchodní model. Kdyby tak neučinili, lidé by automaticky

přestali platit a jejich příjem by klesal, což nechtějí. Musíte si však být vědomi toho, že pokud zaplatíte výkupné, pomáháte tak vytvořit nový trh pro kybernetické oběti, což může vést k většímu počtu ransomware útoků a dalším druhům útoků. Nejlepším rozhodnutím však není volba, zda zaplatit či ne, nejlepší možnou cestou je důkladná prevence, abychom tomuto rozhodnutí vůbec nemuseli čelit. [34]

6.1.2 Proces šíření ransomwaru

Následující obrázek (obr. 14) popisuje proces šíření ransomwaru. Jedná se o proces odehrávající se v kyberprostoru, kde uživatel pracující na svém počítači stáhne soubor, jehož přílohou je škodlivý ransomware, který je připravený napadnout operační systém v počítači, jenž není chráněný žádným antivirovým programem. V případě napadení tímto ransomwarem následně dojde k poškození počítače, které může nastat dvěma způsoby. Prvním z nich je omezení funkčnosti celého počítačového systému, nebo může dojít k situaci, kdy je počítačový systém funkční, ale je zašifrovaný pevný disk a veškeré jeho soubory.



Obrázek 15 – Proces šíření ransomwaru [Zdroj: Vlastní]

6.2 WannaCry

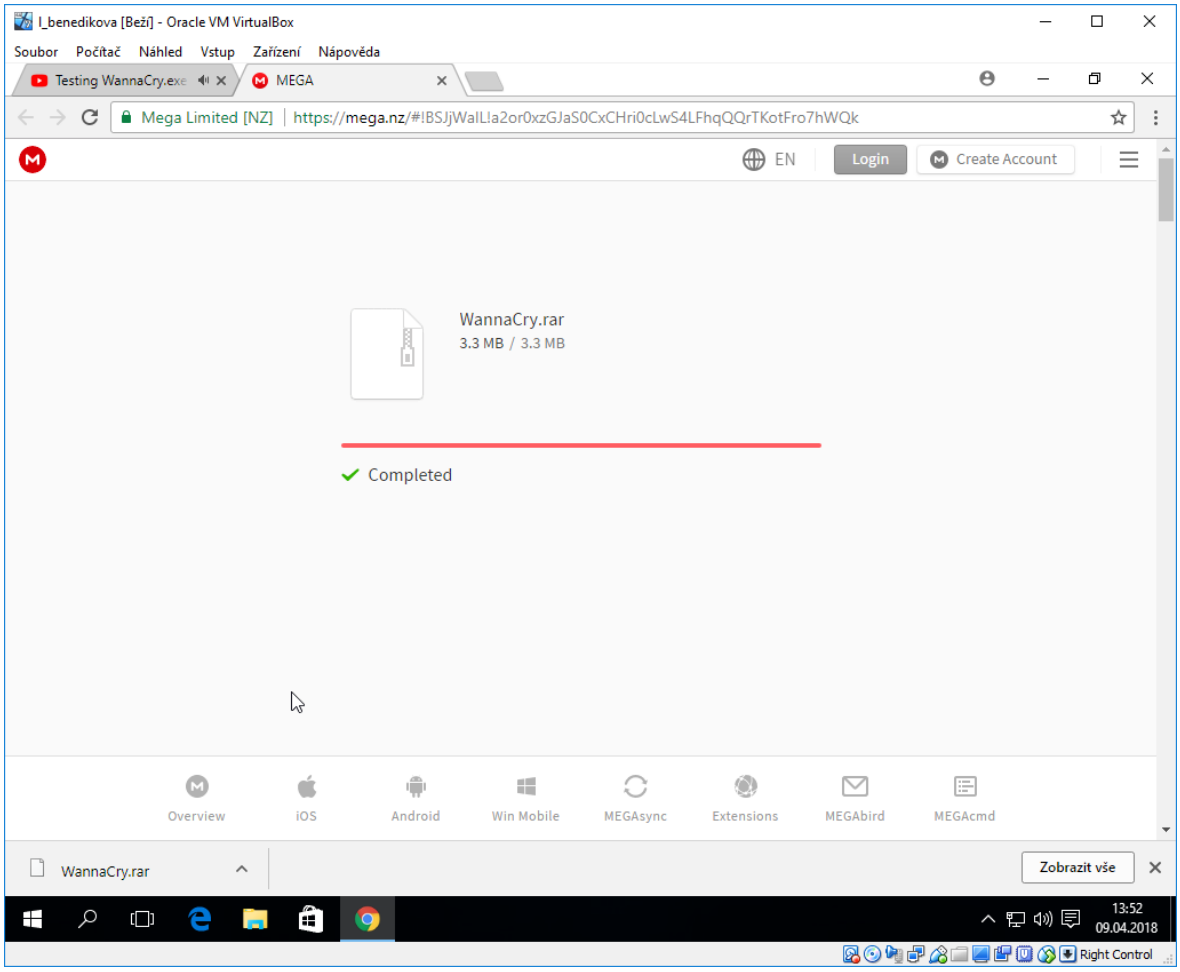
WannaCry je ransomware, který útočí na sítě pomocí protokolu SMB verze 1, jenž napomáhá počítačům komunikovat s tiskárnami a jinými síťovými zařízeními a projevuje se tak, že v počítačích s Windows šifruje soubory a následně k nim znemožní přístup a požaduje po uživatelích zaplacení výkupného do 3 dnů v bitcoinech v hodnotě přibližně 300 USD, což je cca. 6200 Kč. [1]Nezaplatíte-li však do tří dnů, požadovaná cena se zdvojnásobí. WannaCry podle statistik z roku 2017 nejvíce útočí na státní organizace, nemocnice, univerzity, železniční společnosti, technologické firmy nebo telekomunikační společnosti ve více než 150 zemích, nejvíce však v Rusku, Číně, na Ukrajině, na Tchaj-wanu, v Indii a Brazílii. WannaCry však může zaútočit i na obyčejného jednotlivce. Bohužel však tento ransomware před jeho napadením nejspíše nepoznáte, neboť k tomu, aby vás napadl, nepotřebuje žádnou aktivitu. Šíří se jako červ přes sítě a v infikovaných počítačích šifruje uživatelské soubory. Po infikování počítače zobrazí varování a znemožní mu přístup k jeho datům, případně mu znemožní se vůbec do počítače přihlásit. WannaCry můžete odstranit antivirovým softwarem, avšak zašifrované soubory se tím nezachrání. Pokud vás jednou napadne, nemáte moc na výběr. Vyčištění a aktualizování počítače může být jednou z cest, jak obnovit soubory ze zálohy, máte-li je zálohované. [35]

6.2.1 Aplikace na OS Windows 10

Dalším krokem po nainstalování operačních systémů byla aplikace a instalace ransomwaru WannaCry na operační systém Windows 10. Nejprve byla stažena novější verze internetového prohlížeče Google Chrome a následně stažen WinRAR, aby mohl být spuštěn samotný ransomware, neboť jeho instalační soubor byl k dispozici ke stažení ve formátu WannaCry.rar. Před stažením ransomwaru byla provedena kontrola, zda počítač funguje tak, jak má, pomocí poznámkového bloku a následně zkontrolování vlastností počítače.

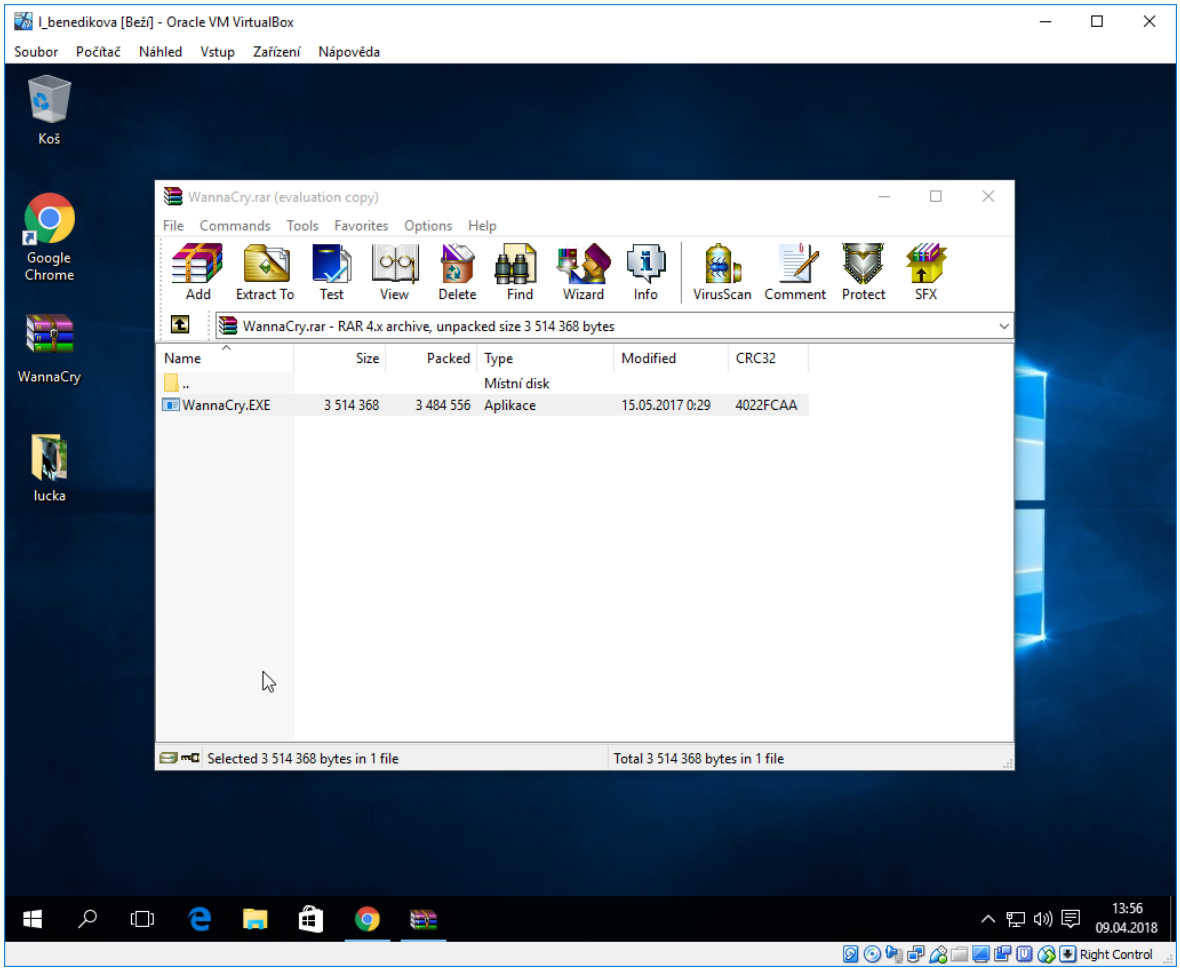
[1] Údaj k bitcoinu je čerpán z 2. 4. 2018 a je třeba se na něj dívat s nadhledem, neboť kurz bitocinu je rapidně proměnlivý.

Následně proběhlo stažení ransomware WannaCry a jeho naistalování do nechráněného virtuálního počítače, což zobrazuje obr. č. 16.



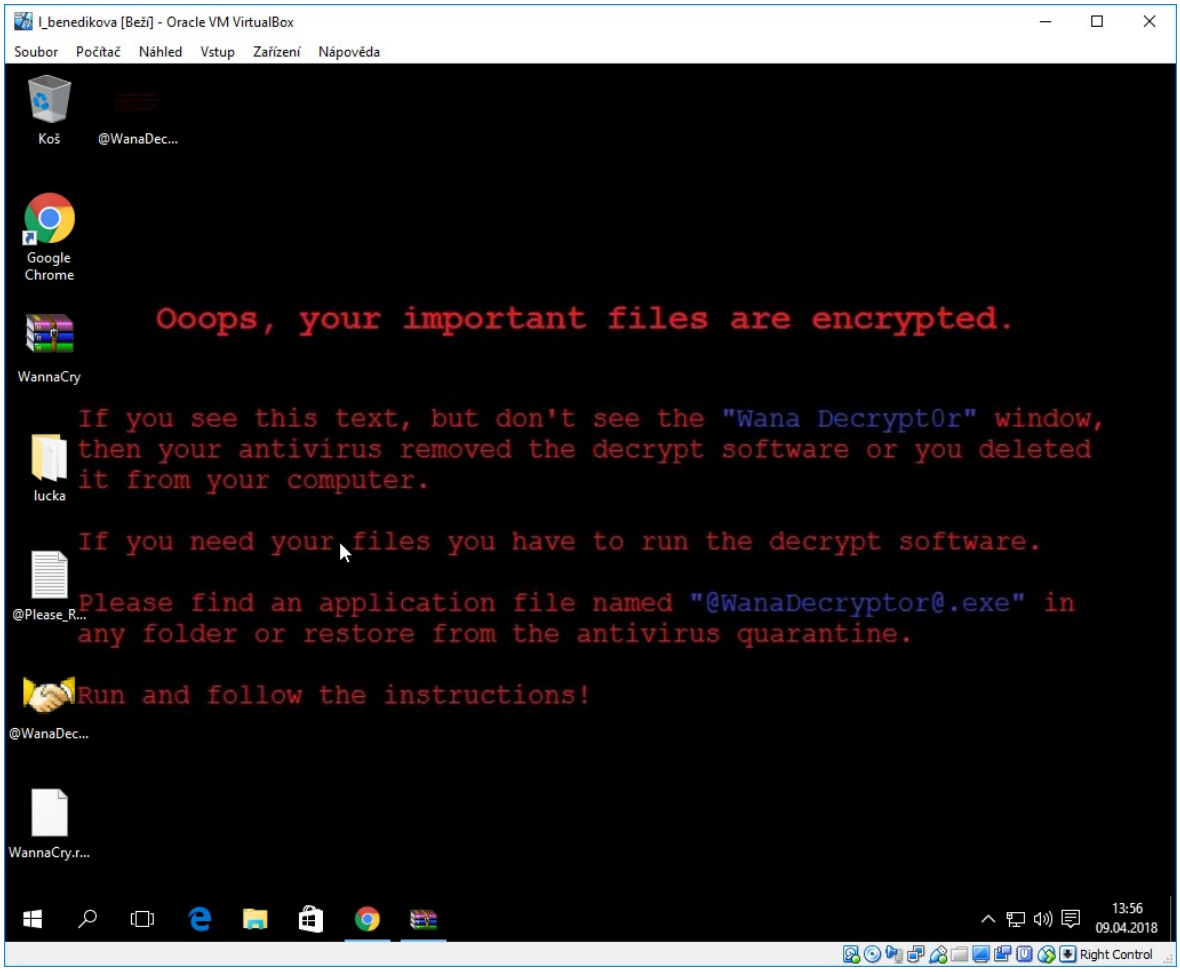
Obrázek 16 – Stažení WannaCry [Zdroj: Vlastní]

Po stažení ransomwaru WannaCry došlo k jeho samotnému spuštění pomocí programu WinRAR, jež zobrazuje obr. č. 17, v jehož formátu byl daný ransomware stažený.



Obrázek 17 – Spuštění WannaCry [Zdroj: Vlastní]

Po spuštění ransomwaru WannaCry se objevilo na ploše varování (obr. 18), že důležitá data byla zakódována.



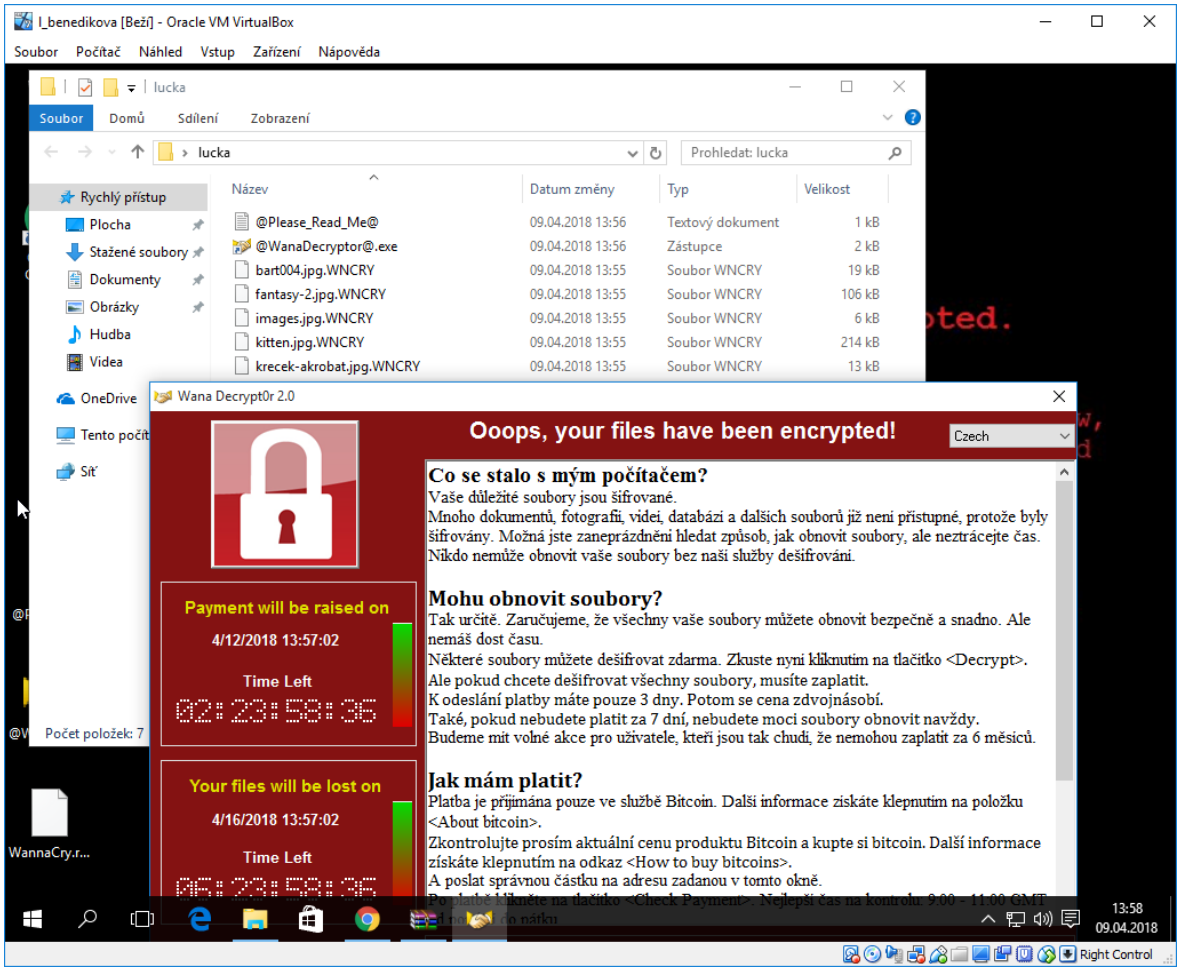
Obrázek 18 – Varování [Zdroj: Vlastní]

Po otevření jakéhokoli souboru vyskočilo oznamovací okno sdělující, co se stalo s daty a co je nutné udělat pro jejich obnovení (obr. 19). V tomto případě se jedná o požadování výkupného, které je potřebné zaplatit do 3 dnů, jinak se výkupné zdvojnásobí a pokud nebude zaplaceno do 7 dnů, budou soubory ztraceny navždy.

Obrázek 19 – WannaCry [Zdroj: Vlastní]

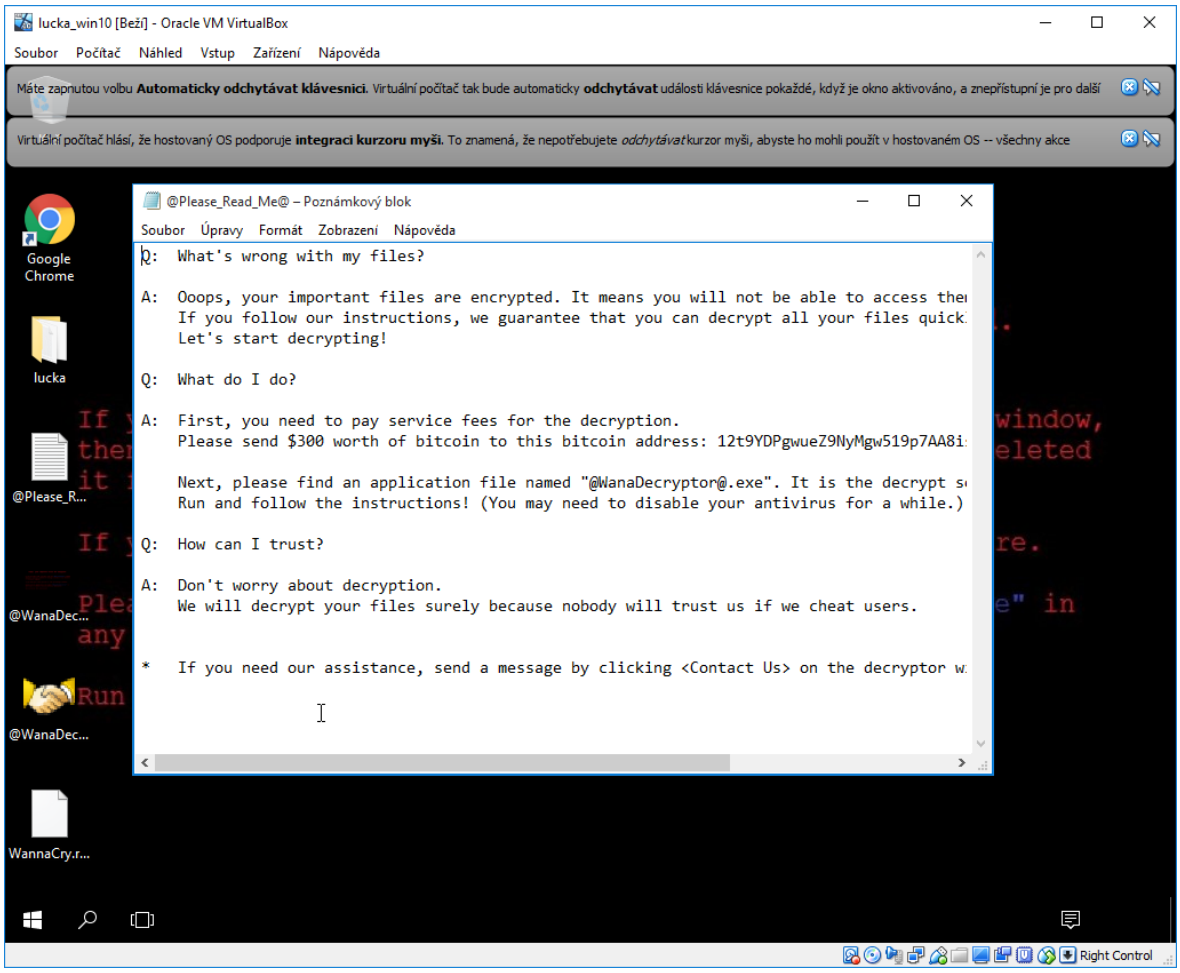
WannaCry dává také možnost kontaktovat pomocí zprávy majitele ransomware. Můžeme se také pokusit spuštěný ransomware jednoduše odstranit, což však nic nevyřeší, neboť i po jeho ukončení, je jím počítač stále napaden a při otevření jakéhokoliv dalšího souboru po nás vyžaduje výkupné.

Ransomware po napadení operačního systému také přepíše veškeré soubory na soubor s koncovkou „WNCRY“ (obr. 20), díky čemuž máme další důvod se obávat a víme, že něco není v pořádku.



Obrázek 20 – Přepsání souboru [Zdroj: Vlastní]

Útočník spolu s napadeným ransomware odešle také zprávu pomocí poznámkového bloku s požadovanými informacemi (obr. 21).



Obrázek 21 – Textová zpráva [Zdroj: Vlastní]

6.3 PETYA

Petya je dalším typem ransomwaru, který se chová stejně jako ostatní jemu podobný malware a to tak, že požaduje výkupné za obnovení přístupu k osobním datům. Petya pracuje tak, že nešifruje jednotlivé soubory, ale šifruje hlavní tabulku souborů (MFT), a tím zablokuje přístup k celému pevnému disku, kvůli čemu není možné číst souborový systém a Windows nelze spustit. Existují však i verze, které šifrují nejen tabulku MFT, ale také samotné soubory. Dopad to má však stejný, a to ten, že uživatel nemůže přistoupit ke svým souborům. Petya nejčastěji útočí pomocí falešných e-mailových žádostí o pracovní pozici obsahující odkaz ke stažení souborů z Dropboxu v oddělení lidských zdrojů ve státních úřadech a soukromých společnostech. Jakmile uživatel na tento odkaz klikne, stáhne se mu soubor .exe, který zašifruje počítač a následně se objeví zpráva, která

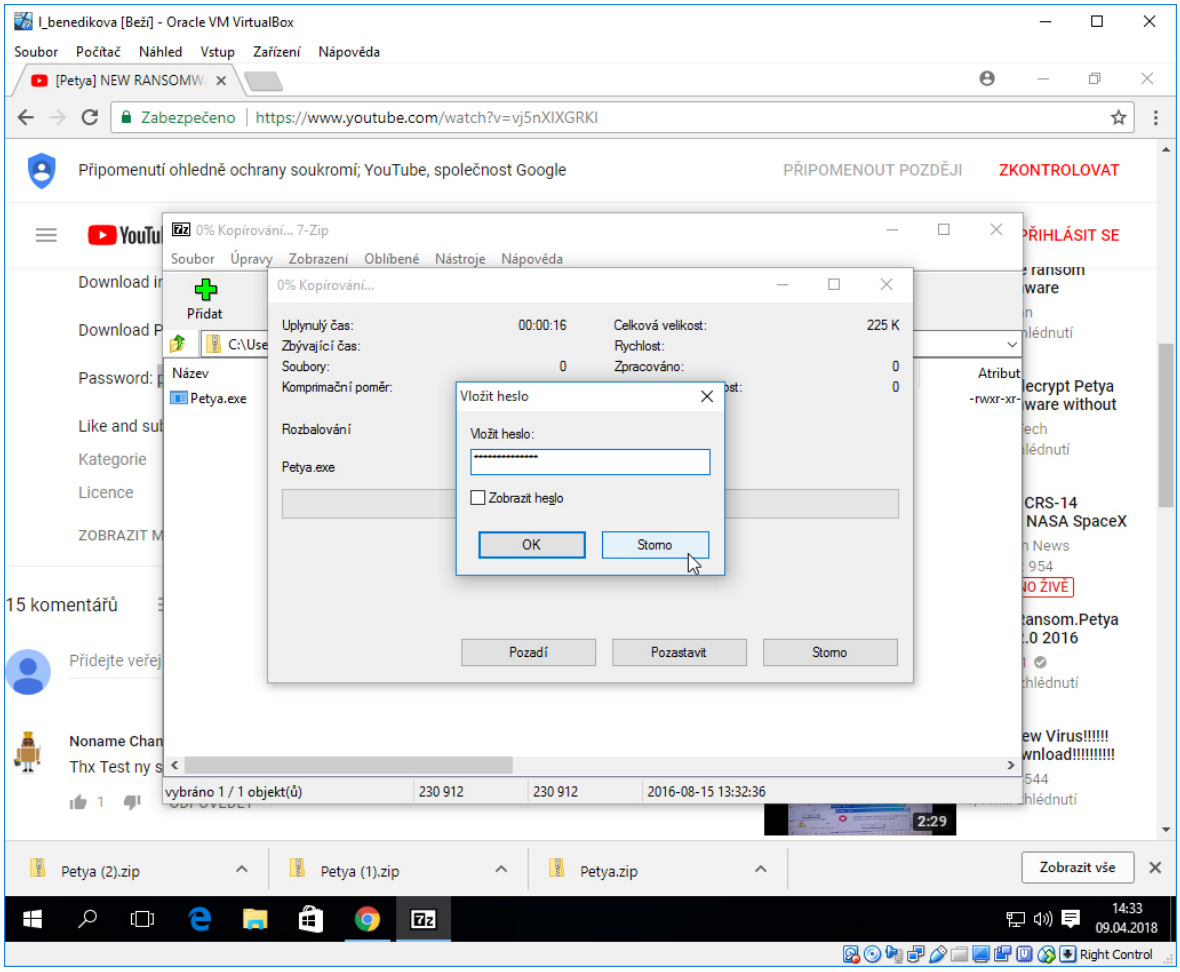
vzkazuje, že pokud nezaplatí určitou částku v bitcoinech, přijde o svá data. Nejprve se však zobrazí takzvaná modrá obrazovka smrti, kdy uživatel začne mít podezření, že něco není v pořádku. Mezitím začne Petya šifrovat hlavní tabulku souborů a zobrazí varovnou obrazovku – obvykle blikající lebku na červenošedém pozadí a následně zprávu požadující výkupné. V tento moment už nemá uživatel nejmenší šanci se bránit. Při otázce, zda zaplatit požadované výkupné, platí stejná odpověď, jako v případě ransomwaru WannaCry. [36]

Největší škody napáchal tento ransomware na Ukrajině, kde napadl několik míst, jako je kyjevské metro, Ukrajinská národní banka či několik letišť. Odkud Petya pochází, dodnes nikdo přesně neví. Mimo Ukrajiny napadl také Rusko, Velkou Británii a Indii. [36]

6.3.1 Aplikace na OS Windows 10

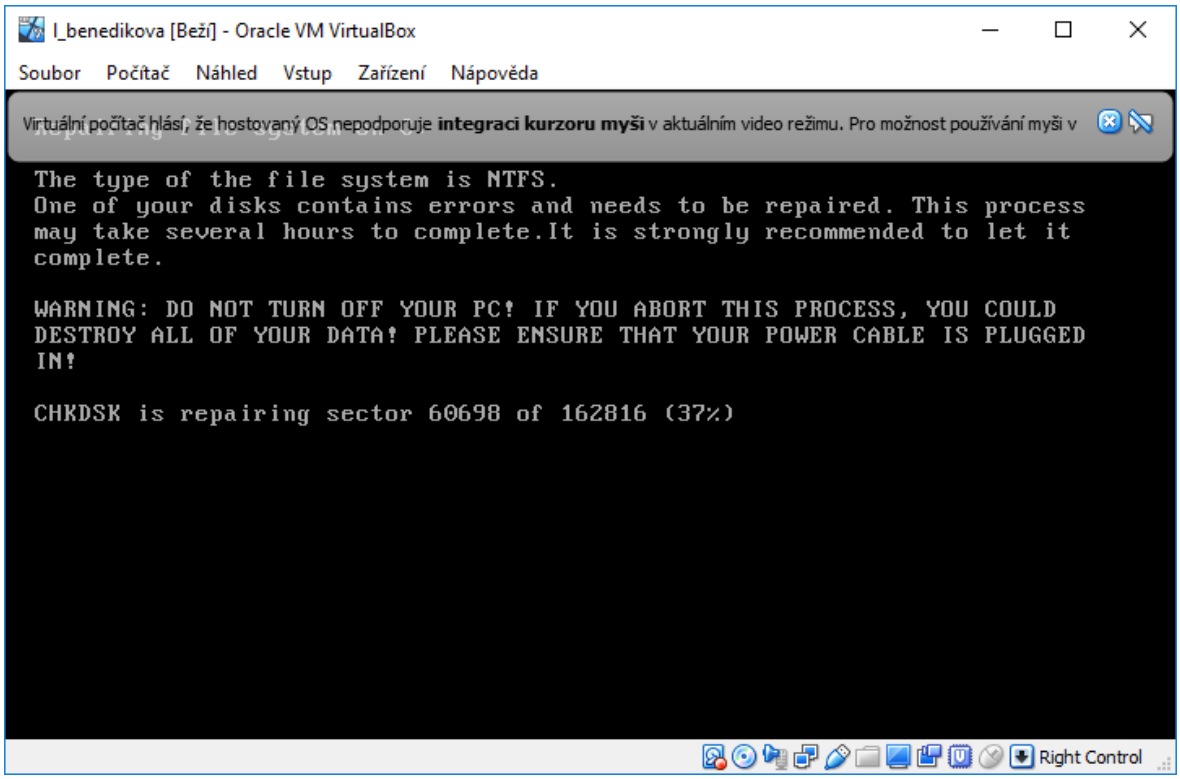
Prvním krokem při aplikaci ransomware Petya na operační systém Windows 10 bylo opět stažení novější verze internetového prohlížeče Google Chrome a následně stažení programu 7-zip, ve kterém jsem daný ransomware otevřela. Nejprve jsem zkontrolovala správné fungování počítače pomocí zobrazení obrázku a následně vlastností počítače.

V dalším kroku byly zkontrolovány funkce počítače, zda fungují tak, jak mají, a následně byl spuštěn ransomware Petya. V podstatě je napadení tímto malwarem velmi rychlé, jednoduché a účinné. Nejprve však k tomuto spuštění muselo být zadáno požadované heslo (obr. 22). Heslo v tomto případě bylo „petyabyitzluk3“ a je volně dostupné na internetu.



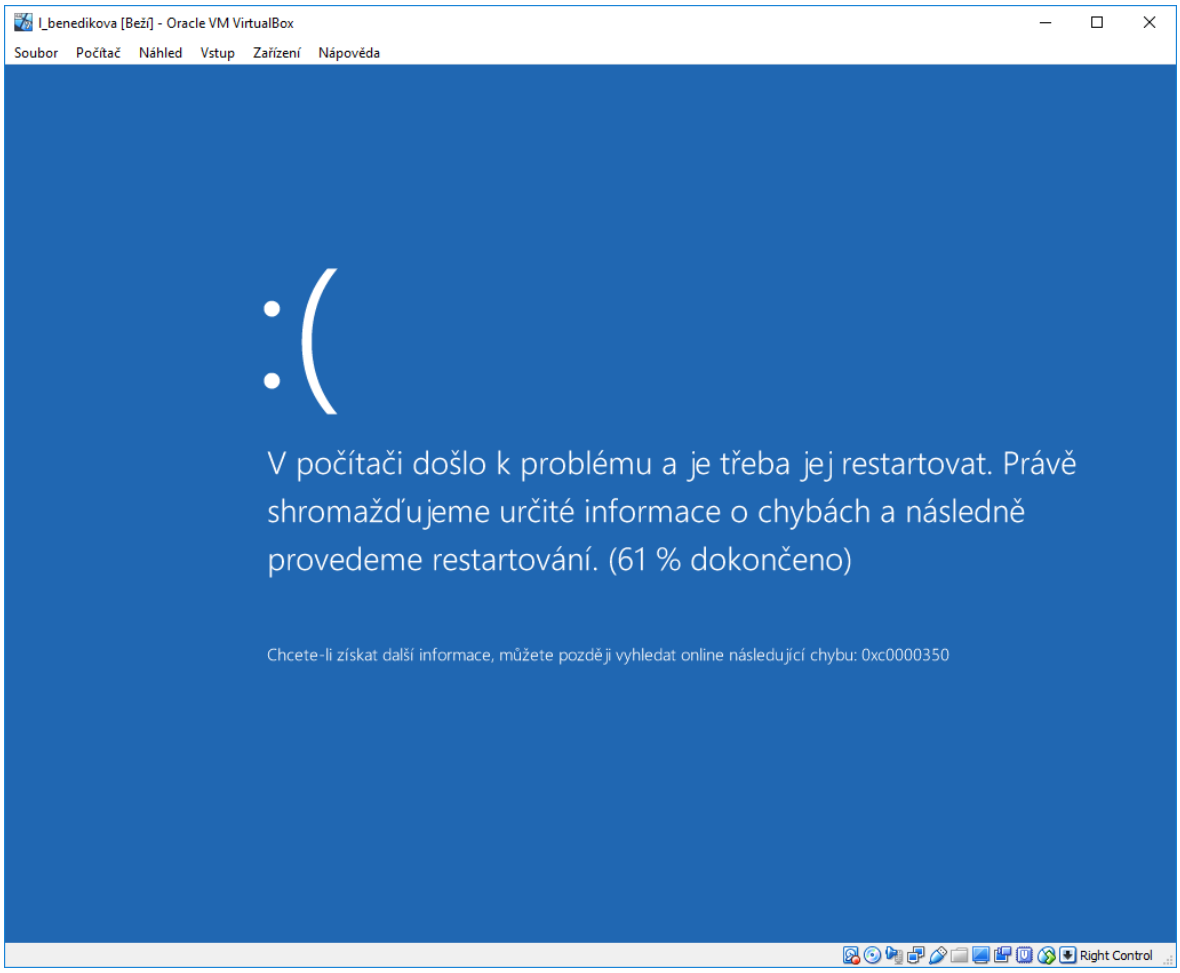
Obrázek 22 – Vložit heslo [Zdroj: Vlastní]

Po zadání hesla a povolení ke spuštění začal ransomware Petya pracovat. Na obrazovce se nejprve objevilo černé okno s upozorněním, že něco není v pořádku (obr. 23).



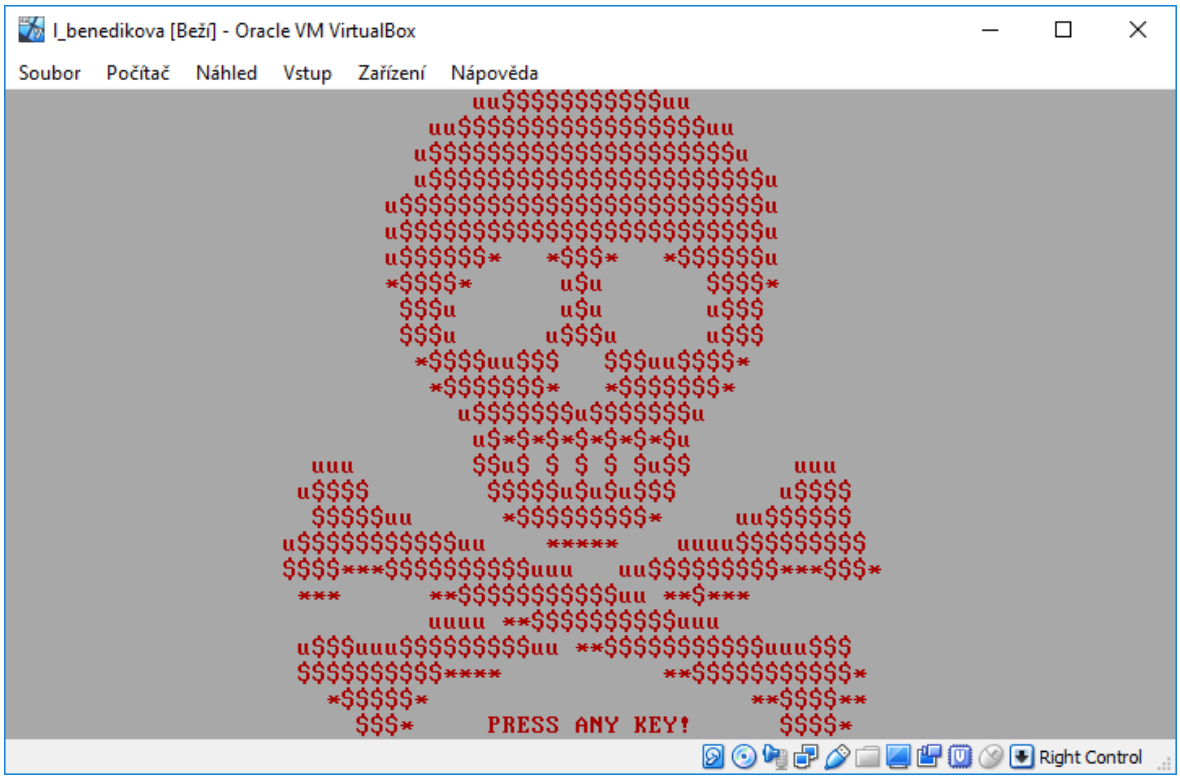
Obrázek 23 – Varování [Zdroj: Vlastní]

Po pár sekundách jakéhokoliv zareagování na probíhající situaci, se zobrazila tzv. modrá obrazovka smrti, kdy se začal počítač restartovat, a v tom šifrovat veškerá data (obr. 24).



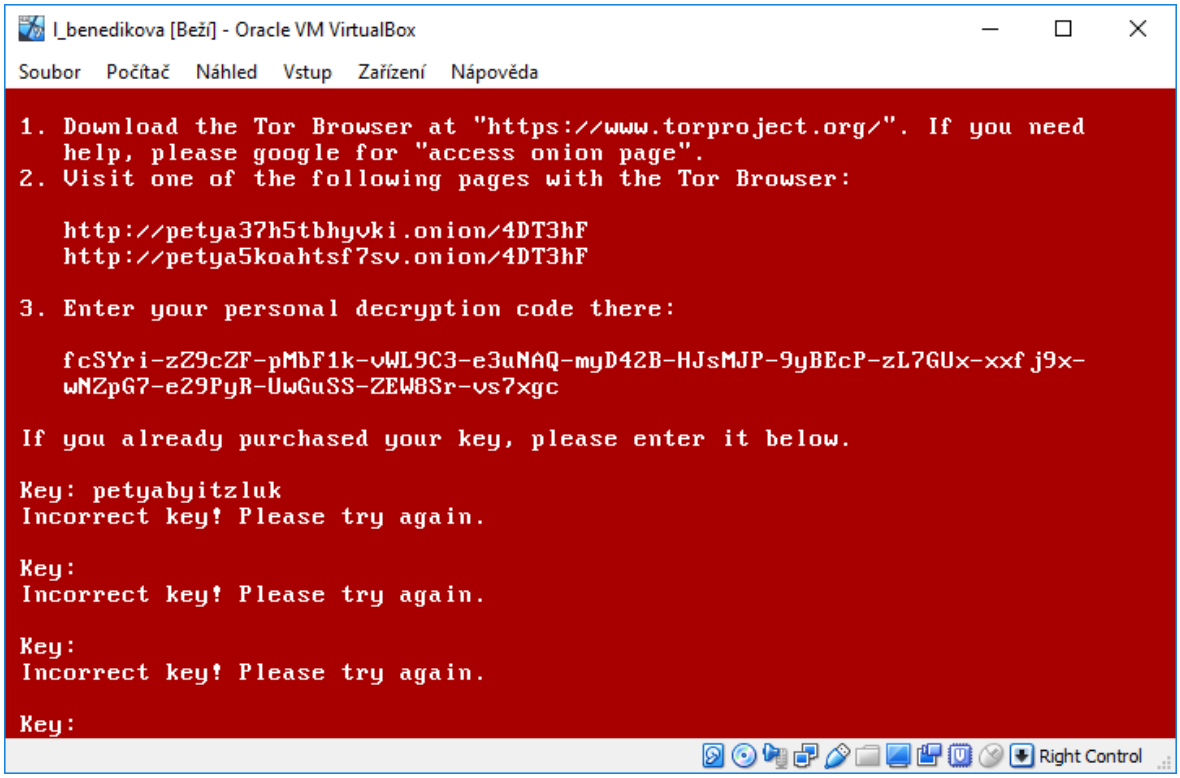
Obrázek 24 – Modrá obrazovka smrti [Zdroj: Vlastní]

Následně již vyskočila blikající červeno-šedá obrazovka s lebkou, která vyžadovala výkupné a blikala tak dlouho, dokud na ni nebylo kliknuto (obr. 25).



Obrázek 25 – Napadení [Zdroj: Vlastní]

Po kliknutí vyskočila tabulka se zprávou a požadováním klíče (obr. 26). Klíč, jenž byl dostupný, však v tomto případě nebyl nic platný, neboť i po jeho zadání chtěl další a další, a nebylo umožněno přístupu zpět k souborům.



Obrázek 26 – Zadání klíče [Zdroj: Vlastní]

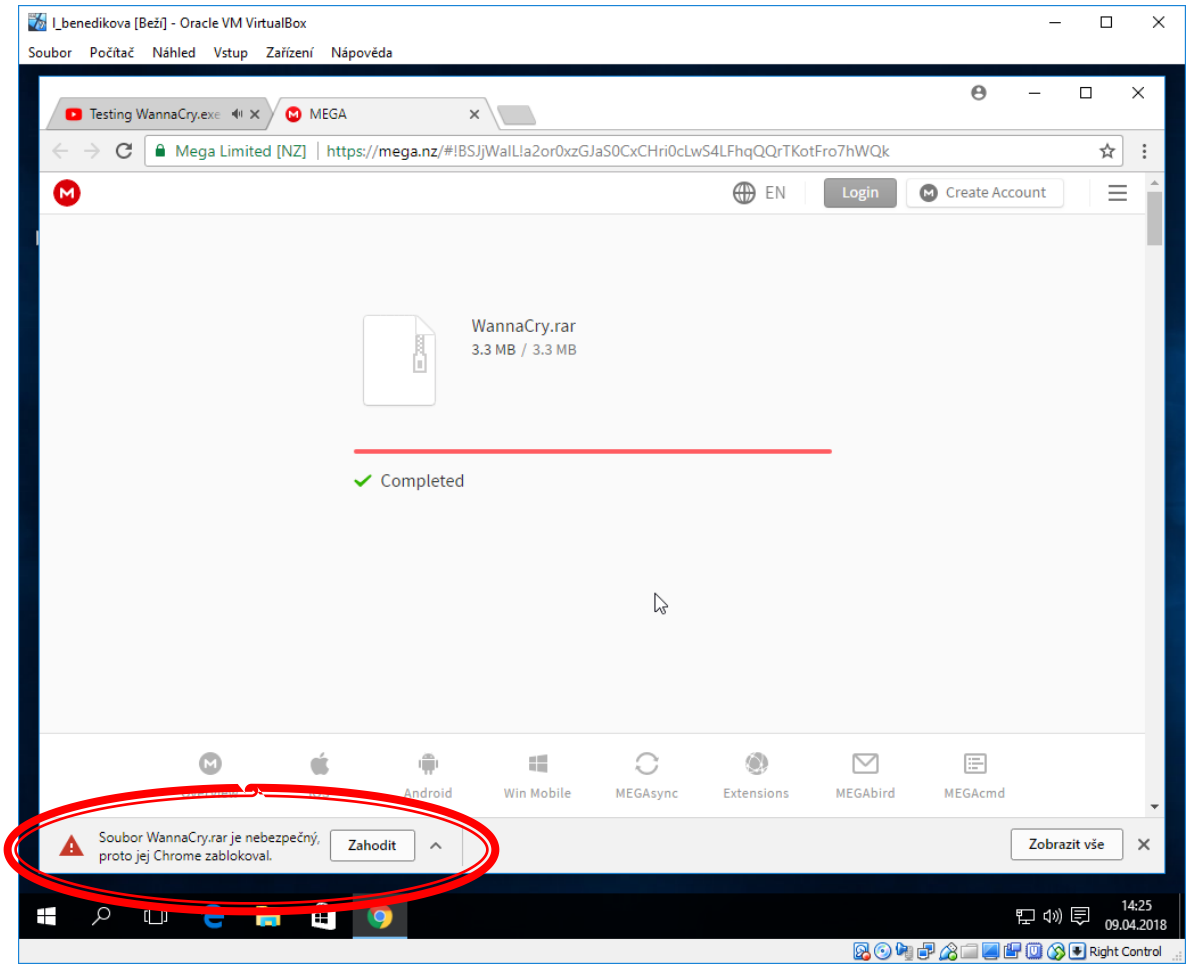
7 OBRANA PROTI MALWARU

Před útoky ransomwaru ať už WannaCry, Petya či úplně jiného, je důležité;

- Pravidelně aktualizovat operační systém,
- aktualizovat webový prohlížeč,
- nainstalovat antivirový program. [36]

7.1 Ochrana webovým prohlížečem

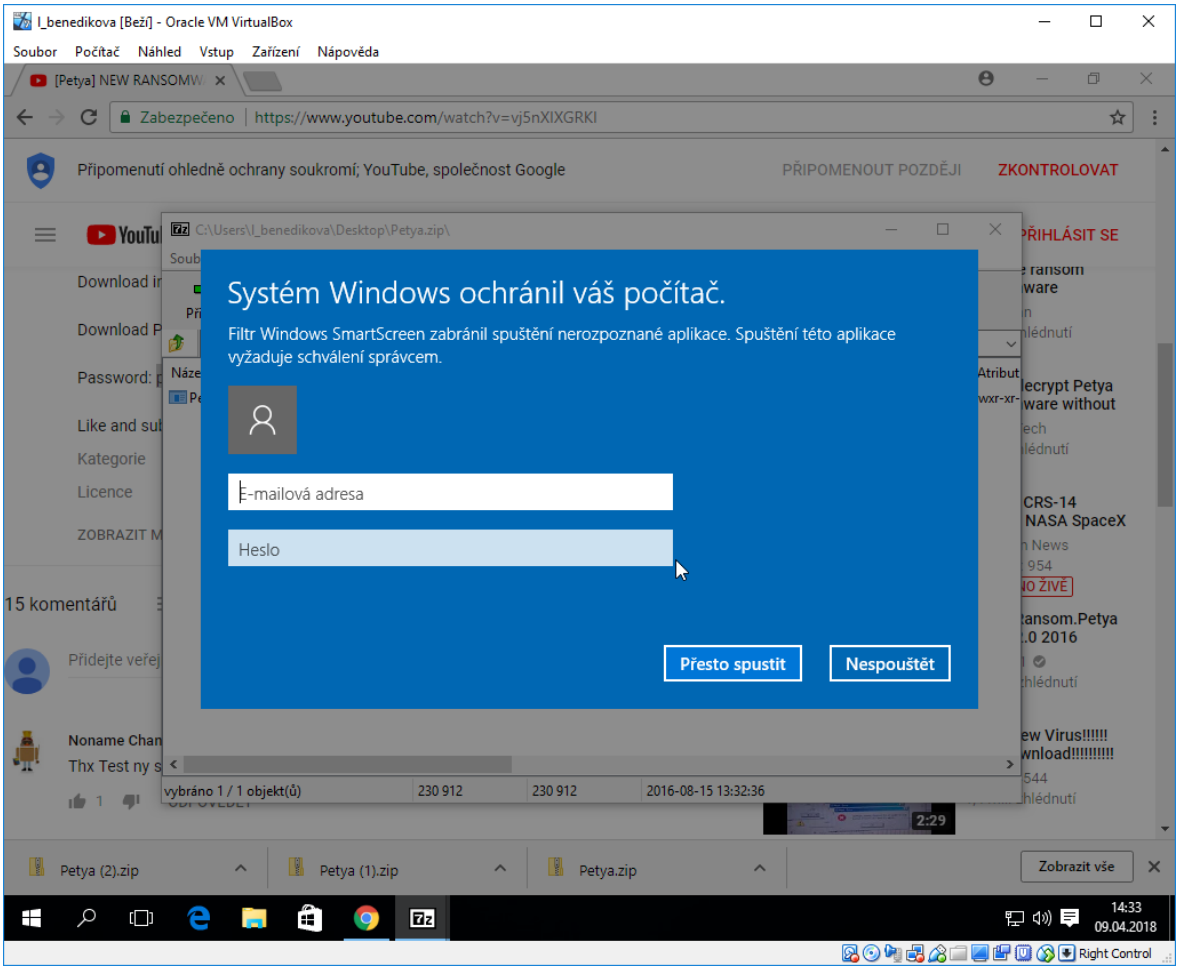
Ochrana webovým prohlížečem znamená, že je v nastavení prohlížeče, který pravidelně používáme, zapnutá funkce „Chránit mě i mé zařízení před nebezpečnými weby“, která nám automaticky hlásí přítomnost nebezpečné stránky či staženého souboru a nedovolí nám jej otevřít, což zobrazuje obr. č. 27.



Obrázek 27 – Ochrana webovým prohlížečem [Zdroj: Vlastní]

7.2 Ochrana aktualizací OS

Pokud se nám však podaří stáhnout nebezpečný soubor i přes zabezpečení webového prohlížeče, zobrazí se po otevření nebezpečného souboru zpráva, že Systém Windows ochránil náš počítač a ke spuštění nebezpečného souboru je vyžadováno schválení správcem pomocí uživatelského jména a hesla. Tuto ochranu zobrazuje obr. č. 28.

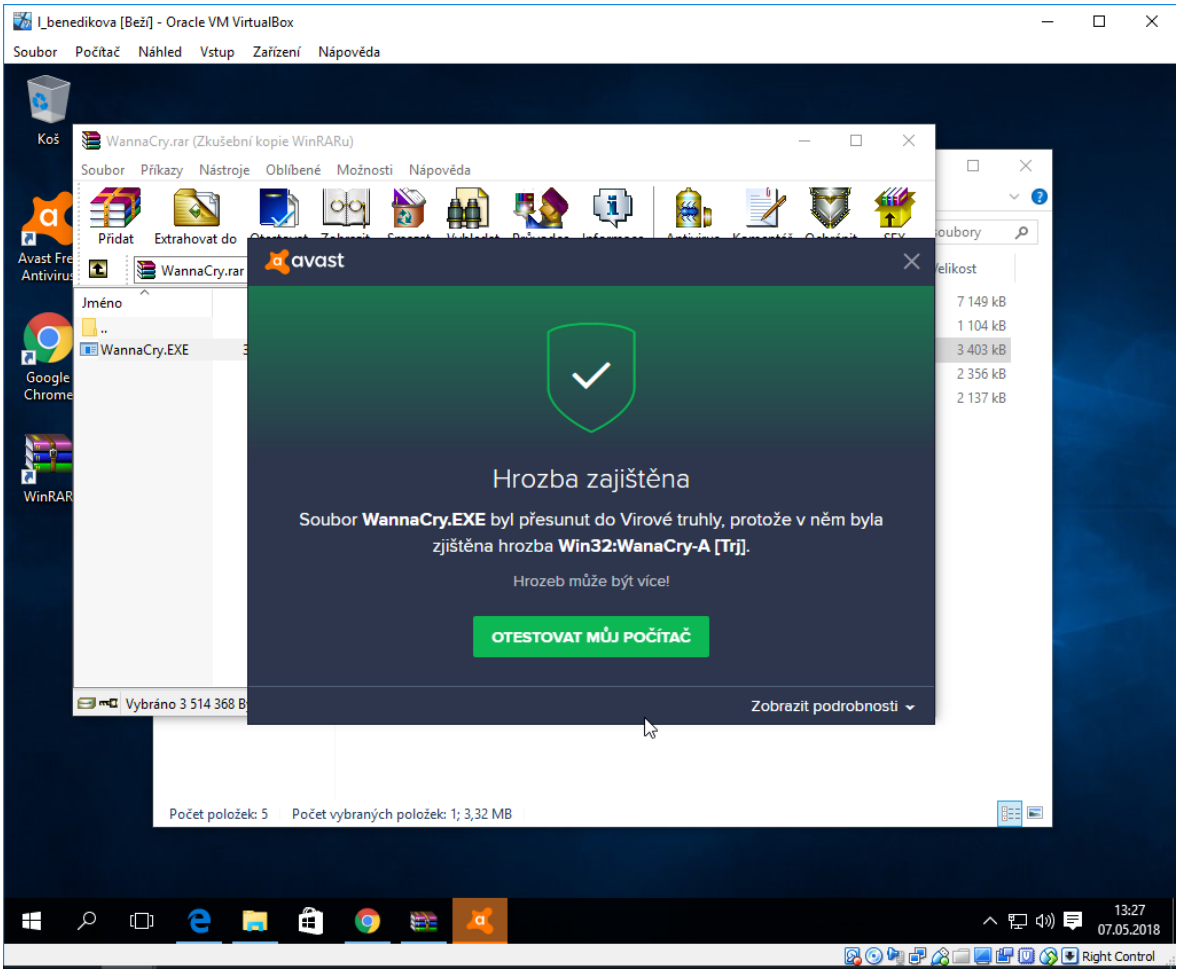


Obrázek 28 – Ochrana aktualizací OS [Zdroj: Vlastní]

7.3 Ochrana antivirovým programem

Základem ochrany počítače je aktualizovaný antivirus, protože pomáhá v počítači zjistit podezřelou aktivitu. Jedním z takových antivirových programů může být například Avast, který počítač chrání, ať už máte bezpečnostní aktivitu nainstalovanou, či nikoli. Důkladným a komplexním nástrojem, který dokáže odstraňovat malware a chránit před ním, neboť nejen Petya či WannaCry, které jsou dvěma z existujících variant ransomwaru, dokážou uškodit našemu počítači, datům a naší online bezpečnosti, může být pro nás chytrým

řešením zvolit například Avast Free Antivirus, který poskytuje základní ochranu, nebo Avast Premier s pokročilými funkcemi pro zabezpečení a ladění výkonu. [36]



Obrázek 29 – Ochrana antivirovým programem [Zdroj: Vlastní]

Na obrázku č. 29 je zobrazena ochrana počítače pomocí nainstalovaného antivirového systému Avast Free Antivirus, který zajistil hrozbu a nebezpečný soubor přesunul do Virové truhly.

ZÁVĚR

Cílem mé bakalářské práce v teoretické části bylo seznámit se se základním názvoslovím a pojmy informační a komunikační bezpečnosti, jejich aktivy, hrozbami, rizikem, zranitelností a prevencí. Dalším cílem bylo popsání počítačového systému, do kterého spadá hardware, software, peopleware, data a informace a také počítačová síť. Následně šlo o seznámení se s možností tvorby malware, základy programování a programovacího jazyka a uvedení nejvíce používané programovací jazyky dnes. Dále se jednalo o představení nejzákladnějších útoků na informační a komunikační prostředky, kterými jsou například sociální inženýrství, malware, phishing, pharming či hacking a cracking.

Hlavním cílem v praktické části mé bakalářské práce bylo jeden z těchto útoků vyzkoušet v praxi. Největší pozornost byla zaměřená na ransomware, jenž je jedním typem malware. Tento cíl jsem díky virtuálnímu počítači mohla uskutečnit. První myšlenkou bylo vytvořit vlastní typ malware, no naštěstí však nejsem žádný profesionální hacker a ani IT specialista, tudíž jsem zvolila jednodušší verzi a to tu, že jsem již vytvořený malware stáhla a následně jej aplikovala na nechráněný operační systém nainstalovaný na vytvořeném virtuálním počítači, což bylo také součástí praktické části. Myslím si, že cíl práce se mi podařil splnit na 100%, neboť po aplikování daného ransomwaru, ať už se jednalo o ransomware WannaCry nebo ransomware Petya, byl operační systém celkově zničen a počítač nebyl schopný se ubránit. Mám-li porovnat jednotlivé ransomwary tak musím říct, že ransomware WannaCry byl složitější na aplikaci, ale ransomware Petya byl rychlejší a škodlivější při svém napadání. Ve výsledku jsou však oba dva stejně škodlivé, těžko předvídatelné a ubránitelné. Myslím si, že i přes volný přístup k těmto ransomwarům na internetu jsou velice dobře zpracované a dostatečně plní potřeby jejich uživatelů, ať už pro soukromé a výzkumné využití, nebo pro skutečné napadení. Jediným nedostatkem, který jsem postřehla, pro mě bylo v případě ransomwaru Petya to, že se nezobrazila žádná zpráva o požadovaném výkupném, kolik peněz mám zaplatit a na jaký účet je poslat, přestože by měla, což považuji za důležitý nedostatek.

SEZNAM POUŽITÉ LITERATURY

[1] JIRÁSEK, Petr., NOVÁK, Luděk. a POŽÁR, Josef. Výkladový slovník Kybernetické bezpečnosti: Třetí doplněné a upravené vydání. 3. Praha: Policejní akademie České republiky v Praze, 2015. ISBN 978-80-7251-436-6

[2] BEZPALEC, Pavel. Management ICT systémů. *Publi.cz: Co je ICT - systém* [online]. [cit. 2018-01-31]. Dostupné z: https://publi.cz/books/242/01.html

[3] KRAYEM, Said a JAŠEK, Roman. *Security of information systems*. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2015. ISBN 978-80-7454-565-8.

[4] MANAGEMENTMANIA: *Informační bezpečnost a ochrana dat* [online]. ©2011-2016 [cit. 2018-01-31]. Dostupné z: https://managementmania.com/cs/informacni-bezpecnost

[5] SINGER, P.W a FRIEDMAN, Allan. Cybersecurity and cyberwar: What everyone needs to know. New York, NY: Oxford University Press, 2014, viii, 306 s. ISBN 978-0-19-991811-9.

[6] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[7] INVESTPLUS: *Bitcoin* [online]. InvestPlus.cz, 2018 [cit. 2018-04-10]. Dostupné z: https://investplus.cz/kurzy/aktualni-kurz-bitcoin-online-graf-kde-koupit-tezba-kryptomeny-cena-hodnota/

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

[9] VÝZNAMSLOVA.COM: *Význam Počítač* [online]. [cit. 2018-01-31]. Dostupné z: http://www.vyznam-slova.com/Počítač

[10] SUPERIA. *Co je to?: Co to je Počítač? Význam slova* [online]. 2017 [cit. 2018-01-31]. Dostupné z: http://cojeto.superia.cz/hardware/pocitac.php

[11] IT-SLOVNÍK. *Hardware* [online]. IT-Slovnik.cz team, 2018 [cit. 2018-01-31]. Dostupné z: https://it-slovnik.cz/pojem/hardware

[12] SITE.THE.CZ. *Počítačové sítě: Co je to počítačová síť* [online]. [cit. 2018-01-31]. Dostupné z: http://site.the.cz/index.php?id=1

[13] TECHNOPEDIA: What is peopleware?. *: Peopleware* [online]. Techopedia Inc. - Terms of Use - Privacy Policy, ©2018 [cit. 2018-04-08]. Dostupné z: https://www.techopedia.com/definition/5545/peopleware

[14] KOHOUT, Roman a KARCHŇÁK Radek. Bezpečnost v online prostředí. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

[15] *IVT.MZF: Programovací jazyky* [online]. WordPress Theme by MH Themes, ©2018 [cit. 2018-05-08]. Dostupné z: http://www.ivt.mzf.cz/seminar/14-programovaci-jazyky/

[16] LINUXANDUBUNTU: *Best Programming Languages To Learn In 2018* [online]. 2017 [cit. 2018-05-08]. Dostupné z: http://www.linuxandubuntu.com/home/best-programming-languages-to-learn-in-2018

[17] COOPER, Izzy. *AppleNovinky: První malware na macOS přes programovací jazyk Swift* [online]. AppleNovinky.cz, 2017 [cit. 2018-05-08]. Dostupné z: https://applenovinky.cz/2017/02/prvni-malware-macos-pres-programovaci-jazyk-swift/

[18] TRENDMICRO: *Ransomware* [online]. Hacker Consulting, 2014 [cit. 2018-01-30]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

[19] CZ.NIC: správce domény cz. *: Státy podle počtu stáhnutí malware* [online]. CZ.NIC, z. s. p. o., ©2018 [cit. 2018-05-08]. Dostupné z: https://stats.nic.cz/stats/countries_by_number_of_downloads

[20] ADAPTIC: *Spam* [online]. Adaptic, 2018 [cit. 2018-01-11]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/spam/

[21] David WATSON, Thorsten HOLZ a Sven MUELLER. *The Honeynet Project: Know your Enemy: Phishing*[online]. Canada, 2005 [cit. 2018-01-30]. Dostupné z: http://www.honeynet.org/papers/phishing/

[22] REPORT ON PHISHING [online]. Canada, 2006 [cit. 2018-01-30]. Dostupné z: https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf

[23] JAMES, Lance. *Phishing bez záhad*. Přeložil Lubomír MOUDRÝ. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

[24] KOLOUCH, Jan a VOLEVECKÝ, Petr. Trestněprávní aspekty phishingového útoku. *Trestní právo,* 2008, 13(9), s. 5-12. ISSN 1211-2860.

[25] SCHNEIER, Bruce. *Schneier on Security: The Seven Types of Hackers* [online]. 2011 [cit. 2018-01-30]. Dostupné z: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

[26] HACKER ACADEMY [online]. Hacker Consulting, 2014 [cit. 2018-01-30]. Dostupné z: https://www.hacker-academy.cz

[27] SCAMBRAY, Joel, Stuart MCCLURE a George KURTZ. *Hacking bez tajemství*. Vyd. 2. Praha: Computer Press, 2002. ISBN 80-7226-644-6

[28] MANAGEMENTMANIA: *Sniffing* [online]. 2015 [cit. 2018-01-30]. Dostupné z: https://managementmania.com/cs/sniffing

[29] OBR, Jiří ml. ITBIZ: Sniffing: Odposlech datové komunikace. *ITBIZ.: Vaše jednička mezi nulami.* [online]. Nitemedia, 6.3.2009 [cit. 2018-01-30]. Dostupné z: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace

[30] ČMELÍK, Martin. Security-Poral: we separate geeks from kiddies. *Seznamte se: DoS a DDoS útoky*[online]. Security-Portal.cz, 2013 [cit. 2018-04-08]. Dostupné z: http://www.security-portal.cz/clanky/seznamte-se---dos-ddos-útoky

[31] MICROSOFT. *Microsoft azure: Co je virtuální počítač?* [online]. Seattle: Microsoft, ©2018 [cit. 2018-03-27]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-a-virtual-machine/

[32] ŠIŠKA, Michal. *Virtuální počítač: Praktická řešení pro domácí uživatele*. 1. Computer Press, 2011, 256 s. ISBN 978-80-251-3334-7.

[33] MICROSOFT*: Windows* [online]. © Microsoft 2018 [cit. 2018-04-30]. Dostupné z: https://www.microsoft.com/cs-cz/windows

[34] SÁNCHEZE, Mauro. *VpnMentor: Ransomware: Měli byste zaplatit výkupné?* [online]. vpnMentor, 2018 [cit. 2018-04-10]. Dostupné z: https://cs.vpnmentor.com/blog/ransomware-meli-byste-zaplatit-vykupne/

[35] AVAST: *WannaCry* [online]. Avast software, 2016 [cit. 2018-04-10]. Dostupné z: https://www.avast.com/cs-cz/c-wannacry

[36] AVAST: *Petya* [online]. Avast Software, 2016 [cit. 2018-04-12]. Dostupné z: https://www.avast.com/cs-cz/c-petya

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIOS Basic Input-Output System

CD Compact Disk

DDOS Distributed Denial of Service

DNS Domain Name Server

DOS Denial of Service

DVD Digital Video Disk

EU Evropská unie

GB GigaBite

GDPR General Data Protection Regulation

HTML HyperText Markup Language

ICQ I Seek You

ICT Informační a komunikační technologie

IP Internet Protocol

IS Informační systém

IT Informační technologie

JS JavaScript

LAN Local Area Network

MAN Metropolitan Area Network

MFT Modulation Transfer Function

MMS Multimedia Messaging Service

MS MicroSoft

OS Operační systém

PAN Personal Area Network

PC Personal Computer

PHP	Hypertext Preprocessor
PIN	Personal Identification Number
RAM	Random-access Memory
SGL	Structured Query Language
SMB	Server Message Block
SMS	Short Message Service
TCP	Transmission Control Protocol
URL	Domain Name Server
USA	Spojené státy Americké
USD	United States Dollar
UTB	Univerzita Tomáše Bati
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
WAN	Wide Area Network

SEZNAM OBRÁZKŮ