Univerzita Pardubice

Fakulta ekonomicko-správní

Zabezpečení uživatelských počítačů proti zneužití k útoku na služby v Internetu

Tomáš Zima

Bakalářská práce
2017

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš Zima**
Osobní číslo:	**E13116**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Zabezpečení uživatelských počítačů proti zneužití k útoku na služby v Internetu**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je identifikovat možnosti zneužití a pomocí případových studií navrhnout opatření proti zneužití počítačů koncových uživatelů k distribuovaným útokům v síti Internet.

Osnova:

1. Identifikace možností zneužití počítačů koncových uživatelů.
2. Vypracování případových studií s návrhem opatření proti možným zneužitím.
3. Porovnání výstupů a celkové shrnutí.

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 - 40 stran**

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

Seznam odborné literatury:

DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. 2. aktualiz. vyd. Praha: Computer Press, 2003. ISBN 80-7226-849-X.

PUŽMANOVÁ, Rita. TCP/IP v kostce. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

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

TANENBAUM, Andrew S. Computer networks. 5th ed. New Jersey: Prentice-Hall, c2010. ISBN 0-13-038488-7.

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

Datum zadání bakalářské práce: **4. září 2016**

Termín odevzdání bakalářské práce: **28. dubna 2017**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
děkanka

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 4. září 2016

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

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

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 15.8. 2017 Tomáš Zima

PODĚKOVÁNÍ:

Tímto bych rád poděkoval svému vedoucímu práce Mgr. Ing. Oldřichovi Horákovi, Ph.D., za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Tato bakalářská práce se zabývá problematikou zneužívání uživatelských počítačů a útoky na služby v síti Internet. Pomocí případových studií navrhuje řešení na ochranu pro jednotlivé uživatele. V závěru řeší konkrétní e-mailový spam a způsoby detekování možného zneužívání ze strany útočníka.

KLÍČOVÁ SLOVA

Bezpečnost, škodlivý program, botnet, případové studie

TITLE

Security of user's computers against misusing and attacks services on the Internet

ANNOTATION

This bachelor thesis deals with the problem of abuse of user computers and attacks on Internet services. Using case studies, he proposes solutions for individual users. In the end, he addresses specific e-mail spam and ways of detecting potential abuse by the attacker.

KEYWORDS

Security, malware, botnet, case studies

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

DoS – Denial of Services

DDoS – Distributed Denial of Services

DRDoS – Distributed Reflected Denial of Service

IP – Internet Protocol

ICMP – Internet Control Message Protocol

SYN – Synchronizovat

TCP – Transmission Control Protocol

UDP – Use Datagram Protocol

USB – Universal Serial Bus

Úvod

Tato práce je zaměřena na hrozby, které přestavují distribuované útoky na služby v síti Internet pro uživatele. Jedná se o nebezpečí, o kterém mnoho uživatelů nemá povědomý. Většinou je to proto, že zde uživatelé nejsou cílem útočníků, ale pouze prostředkem, kterým je prováděn útok na cílovou oběť. Útočník se navíc snaží, aby si uživatel nevšiml, že je prostředkem k distribuovaným útokům, proto může být často počítač uživatele dlouhodobě zneužíván útočníkem, aniž by si toho on sám všiml.

I když zde uživateli nevzniká většinou žádná škoda, je určitě pro uživatele nepřípustné, aby jeho počítač byl zneužíván, proto je nutné, aby byl uživatel před případnými zneužíváním dobře zabezpečen.

Ve své práci uvedu tři případové studie, které se budou týkat různých druhů fiktivních uživatelů. Nejdříve zjistím, jakými riziky jsou jednotlivý uživatelé ohroženi, a potom navrhnu možná řešení zabezpečení.

V závěru své práci uvedu příklad spamu, u kterého navrhnu možnosti, jak ho uživatel může odlišit od žádoucího e-mailu. Také uvedu možnosti, jak sám uživatel může detekovat, že je jeho počítač zneužíván.

Cílem práce je identifikovat možnosti zneužití a pomocí případových studií navrhnout opatření proti zneužití počítačů koncových uživatelů k distribuovaným útokům v síti Internet.

1 ZPŮSOBY ZNEUŽITÍ UŽIVATELSKÝCH POČÍTAČŮ

Uživatelské počítače jsou často v hledáčku různých útočníků, je to především kvůli jejich zranitelnosti, která vyplívá z nízkého zabezpečení. Hlavním úkolem útočníka před tím, než se pokusí zaútočit, je často zamaskování své identity. Existuje mnoho způsobů, jak je toto možné provést, ale v poslední době je velmi časté, že útočník využívá počítače různých uživatelů, kteří sami ani neví, že můžou být nástrojem často protiprávního jednání. V této kapitole se tedy budu věnovat jen způsobům, jakým se mohou útočníci zmocnit uživatelských počítačů a využít je k útoku na služby v síti Internet.

V závěru této kapitoly uvedu možnosti, jakými se lze chránit před případnými útoky ze strany útočníka.

1.1 Malware

Pojem malware vychází z anglických slov malicious (škodlivý) a software. Malware je tedy jakýkoli typ škodlivého softwaru, který se snaží způsobit škodu jednotlivému počítači, serveru nebo počítačové síti. Některé typy škodlivé softwaru jsou popsaný níže.[15]

1.1.1 Počítačový virus

Jedná se o počítačový program nebo skript, který se snaží šířit z jednoho souboru do druhého souboru na jednom počítači. Většinou je však jejich snahou rozšířit se z jednoho počítače na druhý počítač, pokud možno, tak aby si toho uživatel počítače ani nevšiml. Uživatel právě svým normálním chováním přispívá k šíření.[15]

1.1.2 Počítačový červ

Stejně jako počítačový virus se také počítačový červ snaží především šířit z jednoho počítače na druhý, ale na rozdíl od viru, červ automaticky provádí neustálého ukládání své kopie do pamětí počítačů, proto se šíří samovolně bez jakéhokoliv přičinění uživatele.[15]

1.1.3 Trojský kůň

Trojský kůň využívá programy, které jsou nastrčeny místo běžně užívaných programů. Vykonávají sice stejné funkce, ale zároveň můžou například odchytávat citlivé informace a ty potom posílat útočníkovi. Velmi často mají v sobě ukryt mimo jiné také funkci, která umožňuje, aby útočník přes síť Internet dával příkazy uživatelskému počítači.[11]

1.1.4 Backdoors

Backdoors neboli zadní vrátka jsou velmi výstižným názvem pro kódy, které umožňují útočníkovi vzdáleně řídit počítač oběti. Jedná se vlastně o typ trojského koně, který je popsán výše. Pokud je Backdoors nainstalován na nějaký počítač, tak je vždy spouštěn jako normální služba při startu sytému. Uživatel si většinou ničeho nevšimne, protože to vypadá, že daná služba neprovádí žádnou neobvyklou činnost.[11]

1.1.5 Rootkit

Rootkit je podle definice soubor technik pro skrývání činnosti na operačním systému. Jedná se o podmnožinu výše zmíněných nástrojů backdoors. Rootkity jsou, ale mnohem více sofistikovanější, a tak je mnohem těžší je odhalit, protože jsou více skryty. [11]

1.1.6 BOOT viry

Toto jsou viry, které se šíří přes přenosná paměťová média. Dříve se šířila především přes diskety. Dnes jsou diskety nahrazeny USB Flash disky, a tak se šíří většinou právě přes toto médium. Pro své šíření využívají vlastnost automatického otevření média díky souboru autorun.inf, který řídí automatické spuštění po vložení USB Flash disku do počítače.[13]

1.2 Spamming

Spamming je zasílání nevyžádaného sdělení, nejčastěji v elektronické podobě pomocí Internetu, přičemž útočník nemusí posílat jen v podstatě neškodnou reklamu, ale třeba také nějaký velmi nebezpečný škodlivý program. V současné době existuje mnoho antispam filtrů, které většinou rozeznávají spamy podle IP adresy odesílatele, ale velmi často se spamy odesílají z IP adresy uživatele, který o tom ani neví. Útočníci ve spamech používají velmi často metodu zvanou Phishing.[11][22]

1.3 Phishing

Jedná se o způsob útoku, který využívá sociální inženýrství. Většinou je phishing využíván pro získávaní přihlašovacích údajů. Útočník používá podvodný e-mail, který vypadá jako normální e-mail například od banky, ale v něm se nachází odkaz na podvodné stránky, které mohou napodobovat přihlašovací formulář, který když oběť vyplní, tak útočník získá její údaje, které potom může zneužít. Útočník může donutit touto metodu uživatele ke stáhnutí škodlivého programu.[18]

1.4 Hoax

Stejně jako phishing také hoax využívá především sociální inženýrství, ale tady útočník šíří poplašné, nebezpečné a zbytečné řetězové zprávy. Také zde, může být součástí těchto zpráv nebezpečný škodlivý program. Nejčastěji hoax znamená poplašnou zprávu, která varuje před neexistujícím virem.[4]

1.5 Botnet

Pojem botnet označuje síť botů. Tito boti jsou počítače, které byli infikování pomocí nějakého druhu škodlivého programu. Bot pochází z českého slova robot. Jinými slovy útočník si z počítače uživatele dělá svého robota, který plní jeho příkazy, ale také může zachytávat jeho data jako jsou například přihlašovací údaje. Uživatel může být nakažen přímo od útočníka, nebo pomocí jiného bota. Botům se také při velkém množství může říkat „Zombies“ nebo „Slaves“.[22]

1.6 Možnosti obrany uživatele

V této části jsou možnosti obrany, jakými se může uživatel chránit před různými hrozbami.

1.6.1 Firewall

Firewall je něco jako zeď mezi počítačem a sítí. Tato zeď zablokuje jakoukoliv podezřelou aktivitu a možnou hrozbu. Upozorní také například před spuštěním programu bez vědomý uživatele. Pro většinou operačních systému je běžnou součástí.[20]

1.6.2 Antivirový program

Podle názvu by se dalo říci, že uživatele antivir chrání jen před viry, ale to už dnes není vůbec pravda, protože antivirový program se snaží chránit uživatele před jakýmikoliv škodlivými programy. Antivirový program sleduje všechny nejpodstatnější vstupní a výstupní místa, kterými by škodlivé programy mohly do systému proniknout.[2]

1.6.3 Antispamový filtr

Jedná se o inteligentní systém, který se snaží identifikovat spam, a ten buď smaže, nebo ho převede do speciální složky. Téměř každý poskytovatel e-mailových schránek, poskytuje tuto službu.[1]

Antispamové filtry se dále dělí podle způsobů, jakým rozhodují, o tom, který e-mail je spam. Jednotlivý poskytovatelé e-mailových schránek můžou volit různý typ filtru.

Blacklisting

Blacklisting patří k velmi častým způsobům, jakým lze určit spam. Tento způsob, který využívá takzvaných „blacklistů“, což jsou seznamy, na které se přidávají IP adresy, ze kterých již byl v minulosti odeslán spam. Jednotlivý poskytovatelé e-mailových schránek, který používají tento způsob si tyto seznamy posílají, a tím zvyšují efektivitu. Zároveň se vytvářejí také takzvané „whitelisty“, což je opak. Tedy jsou to seznamy důvěryhodných IP adres a z těchto adres se nepředpokládá, že budou posílány spamy.[17]

Nevýhoda tohoto systému je patrná, nelze předem říci, že z dané IP adresy přijde spam, nebo se může stát, že dojde ke zneužití důvěryhodné IP adresy útočníkem.

Greylisting

Dalším velmi častým způsobem filtrace je **greylisting**. Tento koncept je založen na tom, že odesílatel, který posílá adresátovi poprvé e-mail, tak jeho e-mail se nepřijme. Očekává se, že útočník nebude spam posílat znovu, ale odesílatel, který posílá skutečný e-mail, tak pošle svůj e-mail znovu.[17]

Také zde je nevýhoda zřejmá. Útočník může zkusit svůj spam poslat znovu, a naopak odesílatel nemusí poslat znovu svůj e-mail v domnění, že je adresa špatná.

Bayesovské filtry

Bayesovské filtry zkoumají obsah e-mailu, a na základě toho určují, jestli se jedná o spam či nikoliv. Tyto filtry využívají umělé inteligence, takže se postupem času učí, ale k tomu je nutné, aby uživatel sám nejdříve určoval, co je spam.[17]

Nevýhoda u tohoto filtru je, že se musí zapojit také uživatel, který musí nejdříve sám určit, co je spam.

1.6.4 Znalosti a zkušenosti uživatele

Velmi důležitou obranou proti možným útokům jsou znalosti a zkušenosti, které má uživatel o bezpečnosti svého počítače a možném nebezpečí, které mu může hrozit na Internetu.

Například ve firmě, která využívá ke své činnosti počítače, je nutné, aby byla prováděna pravidelná školení na téma bezpečnost počítačů. Zároveň je nutné kontrolovat, zda uživatelé nevystavují firemní počítače zbytečnému riziku.

Možnost, jak zvýšit svoje znalosti problematice zabezpečení svého počítače pro normálního uživatele, který nevyužívá počítač ve své práci, je například dobré sledovat různé weby, které informují o možných nebezpečí.

Například bezpečnostní tým CSIRT.CZ poskytuje na svých webových stránkách aktuální informace v oblasti bezpečnosti. Jedná se o tým, který naplňuje zákon o kybernetické bezpečnosti v České republice. Dále vydává zprávy o nových bezpečnostních rizicích v kyberprostoru.[5]

2 ÚTOKY NA SLUŽBY V SÍTI INTERNET

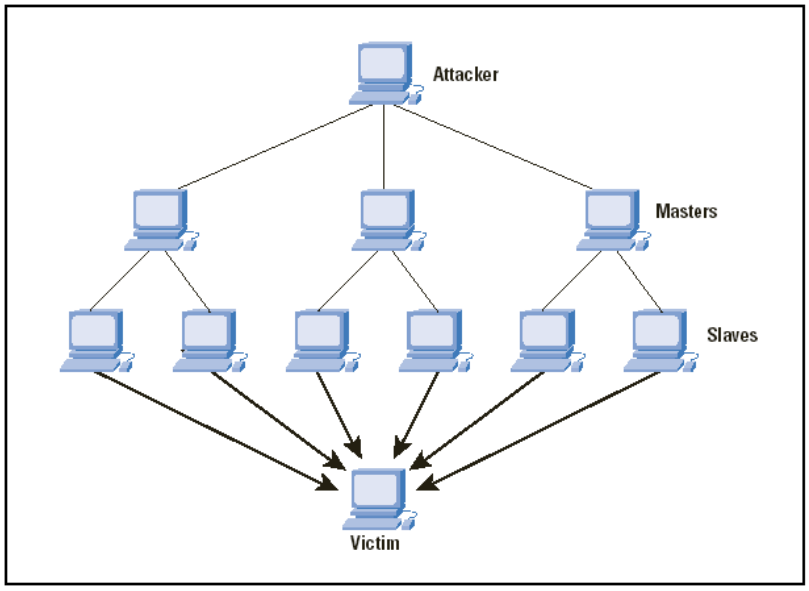
Síť Internet se stává pro čím dál více lidí téměř nutností. To samozřejmě vede mimo jiné k poskytování různých služeb pro uživatele, ale také to vede k provádění různých útoků na uživatele a služby v síti Internet. Útočníci nejsou motivováni jenom penězi, ale také potřebou na sebe upoutat pozornost. V této kapitole se zaměřím na útoky, při kterých je uživatel pouze nástroj nikoliv cílovou obětí.

2.1 Útoky typu DoS a DDoS

Zkratka DoS znamená Denial of Service, což se do češtiny může přeložit jako odepření služby. Cílem tohoto útoku je znemožnit uživatelům přístup na webovou službu, tím že využívají chyb, nebo vyčerpávají systémové prostředky. Díky své nenáročnosti jsou typy těchto útoků velmi oblíbené.[19]

Občas je potřeba k útoku použít více prostředků, než má útočník k dispozici, proto využije jiné uživatele. V takovém případě se mluví o útoku typu DDoS (Distributed Denial of Service), což je o distribuovaný DoS útok. Využitým uživatelům a jejich počítačům se říká v tomto případě „Slaves“ nebo „Zombies“, protože jsou infikování a útočí na základě rozkazu útočníka. V případě velmi rozsáhlých útoků se ještě vyčlení skupina s názvem „Masters“, která ovládá jednotlivé skupiny „Slaves“ a sama je ovládána přímo útočníkem.[16][23]

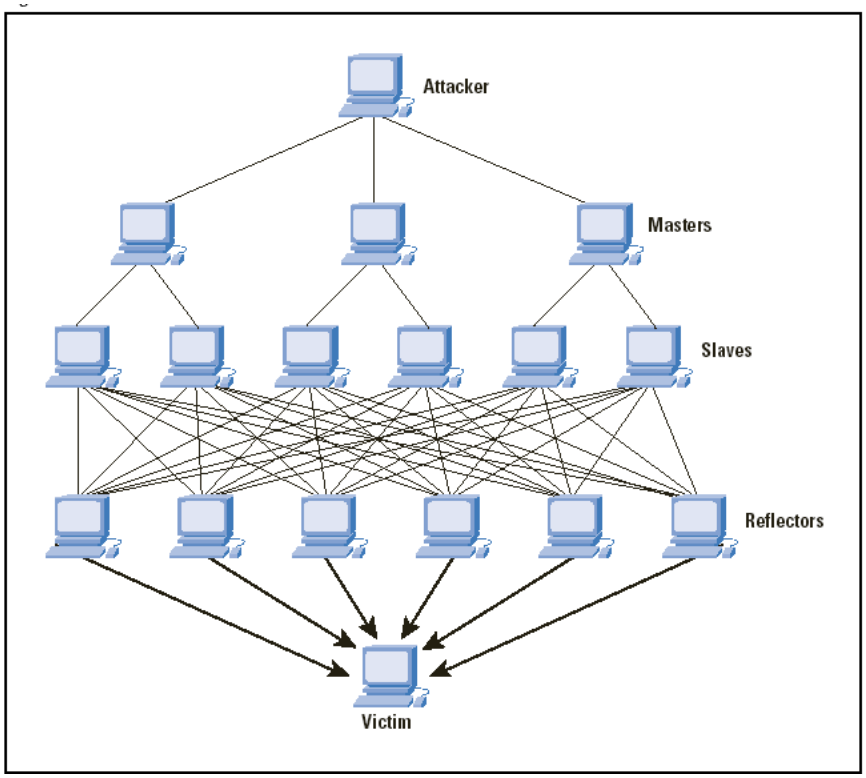
Na obrázku 1 je vidět vizuálně, jak takový útok typu DDoS vypadá.



Obrázek 1: Útok typu DDoS

Zdroj: [16]

Speciálním případ je útok typu DRDoS (Distributed Reflected Denial of Service), který je zobrazený na obrázku 2. Postupuje se stejně jako při útoku DDoS, nicméně se objevuje ještě jedna skupina nazvaná „Reflektors“ ti jsou vybízeni k útoku na cílovou oběť skupinou Slaves.[16]



Obrázek 2: Útok typu DRDoS

Zdroj:[16]

Existuje nepřeberné množství metod, jak provést DoS nebo DDoS útok. Pro svou práci jsem se rozhodl v následujících bodech uvést jen některé způsoby, které považuji za nejlepší příklady jednoduchosti a zároveň také nebezpečnosti těchto typů útoků.

DoS útoky se dělí na dvě velké skupiny podle způsobu provedení na techniku zaplavení a techniku zneužití chyb.[10]

2.1.1 Smurf

Svého času zřejmě nejnebezpečnější a zároveň nejběžnější útok. Útočník nechá rozeslat všem připojeným na broadcast[1] adresu podvržený ICPM ECHO pakety. Tyto pakety neboli bloky dat mohou představovat různá upozornění, o kterých si myslí jiné systémy připojené ve

[1] Zpráva, kterou přijmou všechna připojená síťová rozhraní.

stejné síti, že je posílá cíl útoku, a proto svou odpověď vysílají právě jemu. Podobný útok se nazývá Fraggle DoS útok, ten využívá generování UDP paketů na místo ICMP paketů. Je nutno říci, že tyto typy útoků již nejsou příliš vysokou hrozbou, protože při správné konfiguraci sítě je toto nebezpečí z cela odstraněno.[19][21]

2.1.2 Ping of death

Tento útok byl v minulosti velmi nebezpečný. Využíval chyby ve specifikaci paketů. Délka IP paketu má danou maximální možnou délku 65.535 bytů. Útočníci, ale přišli na to, jak tuto délku lze překročit. Rozdělili paket na několik fragmentů, které dohromady dali větší velikost, než byla ta maximální možná, a když se je oběť pokusila složit dohromady, tak systém oběti zkolaboval. Tato chyba byla již opravena, proto je tento útok spíše minulostí.[7]

2.1.3 ICMP Flood

ICMP flood je tzv. záplavový útok, který se snaží zaplavit cíl útoku pakety nejčastěji typu ICMP Echo, což jsou pakety, které využívají ping a slouží k zjišťování, zda je vzdálené zařízení dostupné.[8][6]

2.1.4 SYN flood

Jedná se o typ záplavového DDoS útoku, který útočníci velmi často používají. Tento útok využívá principu zahajování spojení po TCP. Útočník vysílá zprávy SYN se zfalšovanou (neexistující) zpáteční adresou, oběť vysílá na tuto adresu zprávy typu SYN-ACK, ale protože na ně žádné potvrzení neobdrží, hromadí se tyto zprávy ve vyrovnací paměti, kde musí čekat na (nepřicházející) potvrzení nebo na chybové hlášení, až začne odmítat žádosti o navázaní spojení, které je oprávněné.[19]

2.2 Kybernetické výpalné

Jedná se o nový typ trestné činnosti. Zdá se, že z reálného světa vstoupil také do virtuálního světa druh kriminality, který se označuje jako vymáhání výpalného. Také na internetu se objevují útočnici, kteří chtějí dostat peníze za to, že nepoškodí například běžný chod služby v Internetu. Velmi často podepřou svá tvrzení také tím, že provedou demonstraci své síly a zaútočí. Používají k tomu velmi často útoky DDoS popsané výše. Je nutno říci, že také sama výhružka může být považována za trestný čin, ale útočníci to přesto zkoušejí. Využívají přitom především strach, provozovatelů internetových služeb.[11]

V roce 2015 byla na švýcarskou firmu provozující službu ProtonMail, proveden DDoS útok. Útočníci vydírali tohoto poskytovatele bezpečného e-mailu, že dokud nezaplatí, bude útok pokračovat. Útok byl zcela ochromující, a i když se firma nakonec rozhodla zaplatit, tak útok pokračoval dál.[12]

2.3 Spamming

Tento způsob útoku byl již uveden v kapitole 1.2., ale tam se jednalo o spamming v kontextu útoků na uživatele. Tady je posílána nevyžádaná pošta nikoliv uživateli, ale například administrátorovi webové služby. Nemusí se jednat, ale jen o nevyžádané e-maily. Můžou to být například příspěvky na různých fórech.[22]

3 PŘÍPADOVÉ STUDIE

V této části uvedu tři případové studie s fiktivními uživateli, pro které navrhnu bezpečnostní opatření proti možnému zneužití ze strany útočníka. Fiktivní uživatelé jsou využity především proto, aby nemohlo dojít například ke zneužití osobních údajů.

Nejdříve budou jednotlivý uživatelé popsány pomocí různých informací. Dále se pokusím charakterizovat uživatele podle jejich chování, znalostí a zkušeností. Poté provedu analýzu rizik, a na základě toho potom navrhnu pro jednotlivé uživatele řešení na jejich zabezpečení. V poslední časti porovnám výstupy a provedu celkové shrnutí.

3.1 Jednotlivý uživatelé

U jednotlivých uživatelů je evidován jejich **věk**. Podle věku se můžou určit jejich zkušenosti s prací na počítači. Například většinou mají více zkušeností s počítači nezletilé děti než lidé v důchodovém věku. Na druhou stranu lidé v důchodovém věku, ale velmi často dokáží identifikovat podvod.

Dále je evidováno **zaměstnání**, což je především proto, že lidé, kteří například v zaměstnání používají počítač, musí často řešit různorodé problémy, které mohou být spojeny také se zabezpečením počítače.

Jiní uživatelé vyjadřuje, jestli počítač využívají také další uživatelé nebo jestli uživatel používá svůj počítač pouze sám. To může mít určitý vliv na zabezpečení, protože další uživatel může představovat například možné bezpečnostní riziko.

Poslední údaj je jaké **činnosti** provádí daný uživatel na počítači. Seznámení se s těmito činnostmi může být využito pro určení možných rizik.

3.1.1 Uživatel Jan

Uživatel Jan je důchodce. Je mu 75 let a na počítači netráví příliš mnoho času. Svůj počítač využívá především pro e-mailovou komunikaci a získávání novinek ze zpravodajských serverů. Jeho počítač také používá jeho manželka. Uživatel má na počítači nainstalovaný operační systém Microsoft Windows 10 Home.

Tabulka 1: Základní informace o uživateli Janovi

Jméno	Jan
Věk	75
Zaměstnání	Důchodce
Jiní uživatelé	Ano
Nejčastější činnosti prováděné uživatelem	E-mailová komunikace, sledování zprávy, vyhledávání informací

Zdroj: vlastní zpracování

3.1.2 Uživatel Jaroslav

Uživatel Jaroslav je manažerem ve společnosti zabývající výrobou automobilových součástek. K práci neustále potřebuje svůj počítač. Jeho práce na počítači se skládá většinou z komunikace pomocí e-mailů. Sledování novinek a vyhledávání informací. Instaluje většinou licencované aplikace. Svůj počítač využívá jen on sám. Uživatel Jaroslav má na svém počítači nainstalovaný operační systém Microsoft Windows 10 Home stejně jako uživatel Jan.

Tabulka 2: Základní informace o uživateli Jaroslavovi

Jméno	Jaroslav
Věk	35
Zaměstnání	Manažer
Jiní uživatelé	Ne
Nejčastější činnosti prováděné uživatelem	E-mailová komunikace, sledování zpráv, instalovaní aplikací, internetové bankovnictví

Zdroj: vlastní zpracování

3.1.3 Uživatelka Lucie

Uživatelka Lucie je studentka a její 22 let. Svůj počítač využívá především k zábavě a studiu. Komunikuje přes e-mail a sociální sítě. Stahuje a instaluje různé aplikace, které jsou většinou volně ke stažení na různých serverech. Svůj počítač používá jen ona sama. Uživatelka Lucie má na svém počítači nainstalovaný operační systém Microsoft Windows 8.1 Professional.

Tabulka 3: Základní informace o uživatelce Lucii

Jméno	Lucie
Věk	22
Zaměstnání	Studentka
Jiní uživatelé	Ne
Nejčastější činnosti prováděné uživatelem	E-mailová komunikace, instalace aplikací, používání sociálních sítí, internetové bankovnictví, zábava

Zdroj: vlastní zpracování

3.2 Analýza rizik

V této části bude popsáno, jaké jsou možnosti infikování počítačů jednotlivých uživatelů útočníkem, který chce uživatele zneužít k útoku na služby v síti Internet. Dále jaká je pravděpodobnost, že tento způsob může být u daného uživatele úspěšný. Tato pravděpodobnost bude odhadována na základě chování, zkušeností a znalostí jednotlivého uživatele. Budu jí hodnotit slovy **vysoká, střední a nízká**.

3.2.1 Uživatel Jan

Pan Jan je velmi nezkušený uživatel a nemá téměř žádné znalosti o rizicích spojených s používáním počítačů a Internetu. Svůj počítač používá především kvůli e-mailové komunikaci. Nemá žádné zkušenosti se spamy, proto je vysoce pravděpodobné, že by nerozpoznal spam od útočníka. Uživatel Jan například neví, že by příloha mohla obsahovat škodlivý program, nebo v textu by mohl být uložen odkaz, který by ho zavedl na stránky útočníka.

Sleduje zprávy z několika zpravodajských serverů a vyhledává různé informace. Uživatel při vyhledávání může vstoupit na nebezpečné stránky, které by vytvořil útočník s úmyslem donutit uživatele stáhnout a nainstalovat například trojského koně. Je pravděpodobné, že by si uživatel Jan nevšiml, že se nachází na podstrčené stránce, ale uživatel příliš často nehledá informace, které by ho mohli zavést na útočníkovi stránky, proto je pravděpodobnost střední.

Uživatel Jan občas dostává obrázky nebo dokumenty na USB Flash disku, což je přenosné paměťové zařízení. Na tomto zařízení může být uložen škodlivý program od útočníka, aniž by o tom věděl majitel tohoto zařízení. Uživatel Jan nemá znalosti ani zkušenosti s touto

problematikou, proto je u něj střední pravděpodobnost, že by mohl být tímto způsobem infikován.

Jak již bylo zmíněno na začátku, s uživatelem Janem sdílí počítač také jeho manželka, která má prakticky stejné znalosti a zkušenosti. Většinou jen vyhledává různé informace a čte si zprávy z různých zpravodajských serverů stejně jako uživatel Jan.

Tabulka 4: Shrnutí rizik uživatele Jana

Způsob infikování	**Pravděpodobnost úspěšnosti infikování**
E-mailovým spamem	Vysoká
Nebezpečnými stránkami	Střední
Infikovaným přenosným paměťovým zařízením	Střední

Zdroj: vlastní zpracování

3.2.2 Uživatel Jaroslav

Uživatel Jaroslav používá svůj počítač především pro práci. Jedná se o velmi zkušeného uživatele. Přesto může být napaden přes spam, jelikož svojí firemní e-mailovou adresu má uvedenou na webových stránkách své firmy, kde jí může nalézt útočník například pomocí robota. Dále má svůj soukromý e-mail pro komunikaci například se svými přáteli. Riziko napadaní je u toho uživatel menší než u uživatele Jana, protože uživatel Jaroslav je mnohem zkušenější. Pravděpodobnost úspěšnosti infikování je zde střední.

Občas vyhledá nové programy, které by využil při své práci. Instaluje většinou prověřené programy. I přesto se může stát, že nainstaluje nedopatřením trojského koně, ale pravděpodobnost je zde nízká.

Uživatel Jaroslav hledá často nové informace, které se mohou nacházet na různých stránkách. Může se tedy stát, že vstoupí také na nebezpečné stránky. Je, ale velmi pravděpodobné, že se mu podaří rozpoznat stránky útočníka. Proto je zde pravděpodobnost také nízká.

Často se uživatel Jaroslav potýká s tím, že k přenosu dat používá různé přenosné paměťové zařízení například od kolegů. Téměř vždy se jedná o přenosné paměťové zařízení typu USB Flash disk. Uživatel Jaroslav přesto, že má mnoho zkušeností, tak stejně jako uživatel Jan nemá prakticky žádné povědomý o nebezpečí, které mu hrozí při používání přenosných paměťových zařízeních. Pravděpodobnost infikování je zde střední.

Tabulka 5: Shrnutí rizik uživatele Jaroslava

Způsob infikování	**Pravděpodobnost úspěšnosti infikování**
E-mailovým spamem	Střední
Nainstalováním trojského koně	Nízká
Nebezpečnými stránkami	Nízká
Infikovaným přenosným paměťovým zařízením	Střední

Zdroj: vlastní zpracovaní

3.2.3 Uživatelka Lucie

Uživatelka Lucie využívá svůj počítač především pro zábavu a studium. E-mailovou komunikaci nevyužívá příliš často. Většinou využívá ke komunikaci sociální sítě. Přesto také ona může být napadena pomocí spamu. Pravděpodobnost je zde střední.

Uživatelka Lucie instaluje různé programy, jak pro zábavu, tak kvůli studiu. Vybírá si především programy, které jsou dostupné zdarma. V těchto programech se objevují škodlivé kódy velmi často, proto je pravděpodobnost, že počítač uživatelky Lucie bude infikován trojským koněm vysoká.

Tato uživatelka často vyhledává různé informace na různých stránkách. Může se tedy stát, že vstoupí na nebezpečné stránky. Uživatelka Lucie i přes své zkušenosti se může stát obětí podvodníka, který tyto podvodné stránky vytvořil, protože navštěvuje různé stránky velmi často, je zde pravděpodobnost infikování také vysoká.

Uživatelka Lucie velmi ráda používá sociální sítě. Na sociálních sítích komunikuje a sdílí na nich své fotky a informace. Útočník se může pokusit zaútočit právě přes sociální síť. Může se například vydávat za přítele a sdílet program nebo odkaz. Uživatelka Lucie si pak může nainstalovat nedopatřením na počítač škodlivý program. Pravděpodobnost infikování je zde vysoká.

Tabulka 6: Shrnutí rizik uživatelky Lucie

Způsob infikování	**Pravděpodobnost úspěšnosti infikování**
E-mailovým spamem	Střední
Trojským koněm	Vysoká
Nebezpečnými stránkami	Vysoká
Infikovaným přenosným paměťovým zařízením	Střední
Přes sociální síť	Vysoká

Zdroj: vlastní zpracování

3.3 Návrh ochrany pro jednotlivé uživatele

V této části bude navrženo zabezpečení pro uživatele před jednotlivými způsoby zneužití ze strany útočníka.

3.3.1 Návrh ochrany pro uživatele Jana

Pro uživatele Jana je největším rizikem **e-mailový spam**, který by poslal útočník s úmyslem infikovat uživatele.

Ochrana proti e-mailovému spamu

U uživatele Jana je navrhováno, aby si stáhnul a nainstaloval poštovního klienta. Konkrétně klienta, který se nazývá Mozilla Thunderbird. Tento klient nabízí příjemné uživatelské rozhraní a vlastní antispamový filtr. Uživatel může spravovat svůj e-mail přes tohoto klienta a nemusí používat webové rozhraní, což mu usnadní práci s e-maily, ale také pomůže lépe zabezpečit svojí e-mailovou schránku.

I přes všechny antispamové filtry se k uživateli může dostat e-mailový spam, který by ho mohl ohrozit. Proto je nutné samotného uživatele proškolit. Nejdříve je mu potřeba sdělit, jaké nebezpečí takový e-mailový spam může představovat. Potom je nutné vysvětlit, jak takový uživatel může sám daný e-mailový spam identifikovat.

Ochrana proti nebezpečným stránkám

Proti ohrožení vstupem na nebezpečné stránky je navrženo, aby se uživateli vysvětlilo, jak identifikovat nebezpečné stránky, jelikož s uživatelem sdílí počítač také jeho manželka, je tedy nutné v této oblasti proškolit také ji.

Jak ochranu proti vstupu na nebezpečnou stránku, tak také celkovou ochranu posílí ještě antivirový program Avast Premier 2017.

Jedná se o placenou verzi tohoto antivirové programu, který nabízí na rozdíl od neplacené verze například funkci Ověřené weby, která uživatele chrání před podvodnými weby, které se vydávají za skutečné.[3]

Uživatel bude používat výhradně prohlížeč nazvaný SafeZone Browser. Především proto, že například funkce Ověřené weby funguje pouze na tomto prohlížeči.[3]

Ochrana proti infikovanému přenosnému paměťovému zařízení

Poslední věcí, kterou je potřeba zabezpečit je riziko spojené s používáním cizích USB Flash disků.

Uživatel musí dodržet pravidlo, že nesmí vkládat, žádný USB Flash disk od nedůvěryhodných osob, nebo dokonce, který by někde nalezl, protože se na nich můžou objevit různé škodlivé programy, které se okamžitě po vložení do počítače sami mohou nainstalovat.

Pokaždé, když vloží uživatel USB Flash disk do počítače, tak ho prověří pomocí antivirového programu Avast Premier 2017, jestli se na něm nenachází škodlivý program.

Náklady na zvolené řešení

Náklady na zvolené řešení pro uživatele Jaroslava jsou pouze za koupi licence antivirového programu Avast Premier 2017. Cena roční licence je podle oficiálních stránek výrobce 1690kč.[1]

3.3.2 Návrh ochrany pro uživatele Jaroslava

Pro uživatele Jaroslava je největším rizikem útok e-mailovým spamem a přenosným paměťovým zařízením.

Ochrana proti e-mailovému spamu

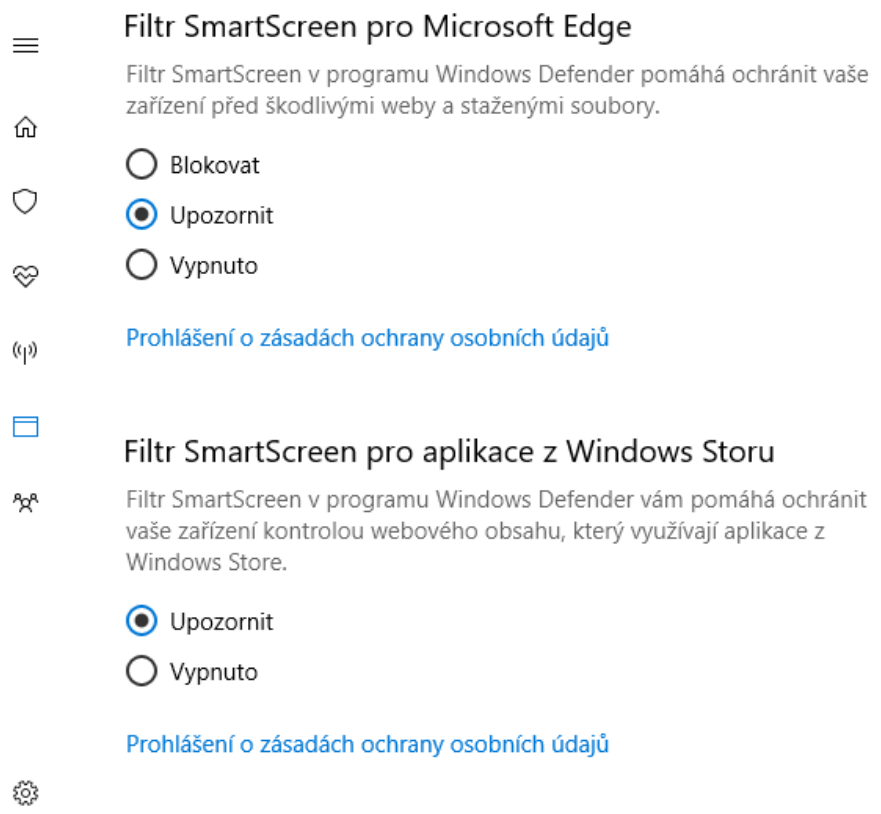
Také pro uživatele Jana je navrženo, aby si stáhnul a nainstaloval poštovního agenta Mozilla Thunderbird. Dále je nutné, aby e-mail, který má uvedený na firemních stránkách byl uveden, tak aby ho útočník pomocí „spambota[2]“ nemohl zneužít. Například nahrazením znaku @ v e-mailové adrese napsané na stránkách firmy slovem zavináč. Klient pochopí, že slovo zavináč má nahradit znakem, ale „spambot“ pravděpodobně ne.

[2] Robota, který je naprogramován k hledání e-mailových adres a rozesílání spamů.

Ochrana proti nebezpečným stránkám

U uživatele Jaroslava je velmi nízké riziko, že bude infikován přes nebezpečné stránky, proto postačí, když bude chráněn již nainstalovaným antivirovým programem, který je součástí již zmíněného operačního systému Microsoft Windows 10 Home, tento antivirovým program se jmenuje Windows Defender. Před nebezpečnými stránkami bude chránit uživatele především funkce firewall. Uživatel bude pravidelně kontrolovat, zda je firewall zapnutý.[14]

Uživatel Jaroslav si nastaví filtr SmartScreen podle obrázku 3, tak bude tento filtr upozorňovat na škodlivé weby. Tato funkce funguje pouze na prohlížeči Microsoft Edge, který je součástí operačního systému Microsoft Windows 10 Home. Uživatel bude používat pouze tento prohlížeč.[14]



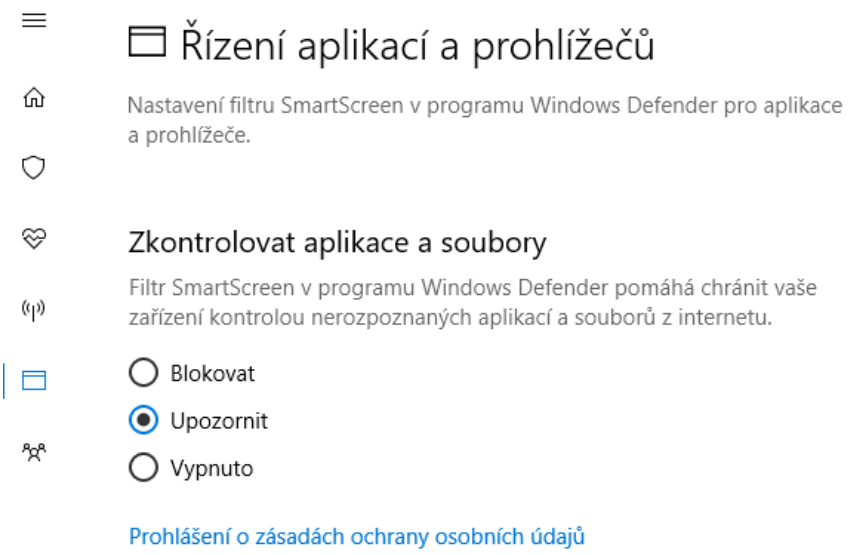
Obrázek 3: Nastavení filtru SmartScreen

Zdroj: vlastní zpracování

Ochrana proti trojskému koni

Proti nainstalování trojského koně bude chráněn uživatel stejně jako proti navštěvování nebezpečných stránek, tedy pomocí antivirového programu Microsoft Defender. Uživatel si

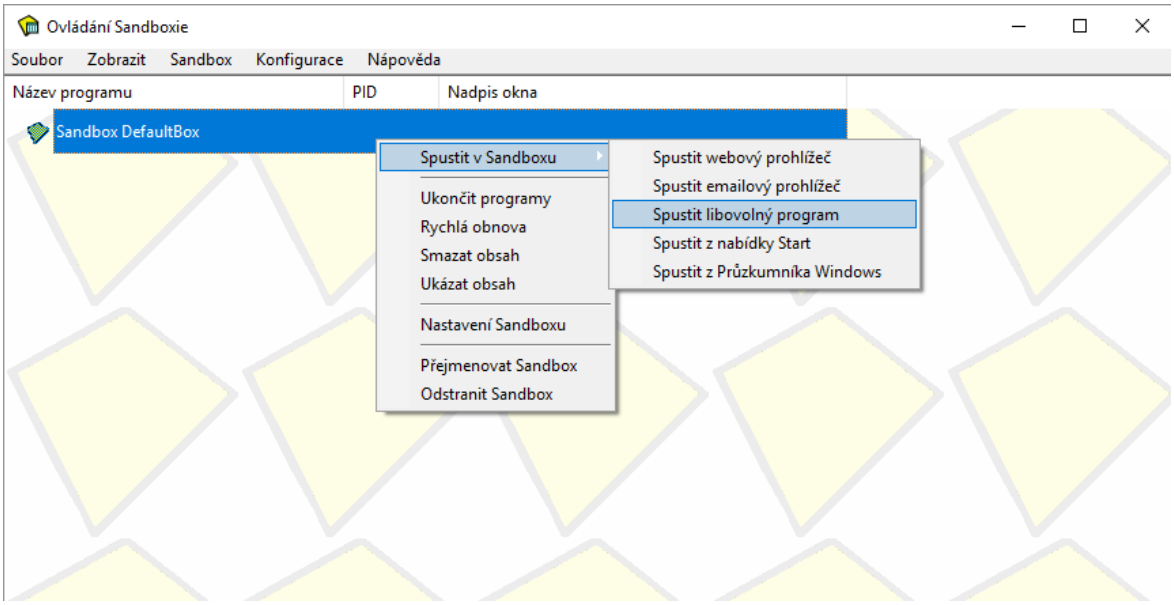
nastaví antivirový program podle obrázku 4. Tím bude uživatel upozorňován na nebezpečné aplikace, které by mohli například obsahovat trojského koně.



Obrázek 4: Nastavení kontroly aplikací

Zdroj: vlastní zpracování

Uživatel si také nainstaluje program, který se jmenuje Sandboxie. Tento program umožní uživateli ve virtuálním prostředí otestovat, zda program, který chce nainstalovat je skutečně bezpečný. Ukázka, jak lze provést kontrolu podezřelého programu je na obrázku 5. Tento program je zcela zdarma. [9]



Obrázek 5: Sandboxie

Zdroj: vlastní zpracování

Dále bude uživatel každý týden provádět úplnou antivirovou kontrolu právě pomocí programu Microsoft Defender.

Ochrana proti infikovanému přenosnému paměťovému zařízení

Nebude používat USB Flash disk od nedůvěryhodných osob. Pokaždé když bude vkládat do svého počítače, tak prověří zařízení pomocí antivirového programu Microsoft Defender.

Náklady na zvolené řešení

Pro uživatele Jaroslava nejsou žádné náklady na zvolené řešení.

3.3.3 Návrh ochrany pro uživatelku Lucii

Pro uživatelku Lucii jsou největšími riziky útoky přes sociální sítě, trojské koně a nebezpečné stránky.

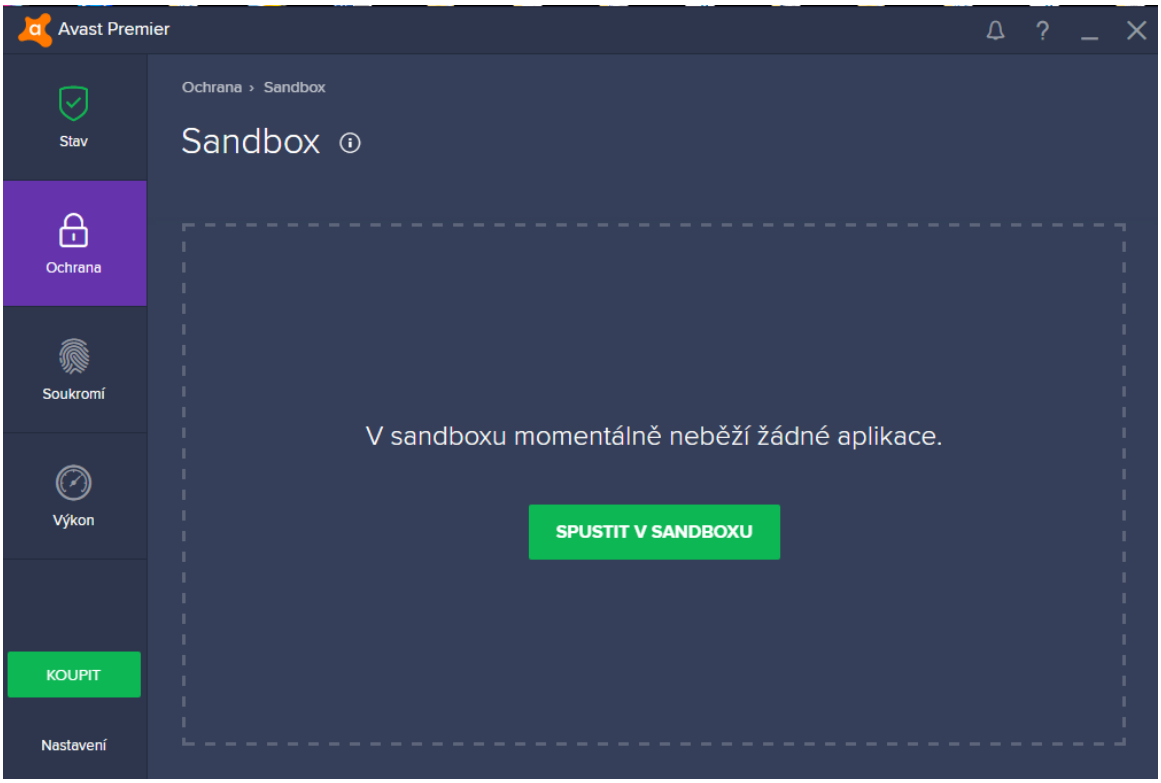
Ochrana proti útoku přes sociální sítě

Uživatelka Lucie bude muset především hlídat, s kým komunikuje přes sociální sítě. Dále musí být proškolena z hlediska nebezpečí jaká mohou skrývat sociální sítě. Je nutné, aby byla proškolena také z hlediska možnosti, že osoba, která je prověřená může být ve skutečnosti útočník, který se zmocnil cizího účtu. Je nutné, aby uživatelka důkladně zvažovalo chování jednotlivých svých přátel ze sociálních sítí, jestli nevykazují neobvyklé chování.

Ochrana proti trojskému koni

Jak již bylo zmíněno, uživatelka Lucie často instaluje různé programy, které jsou většinou volně ke stažení, proto je nutné, aby stejně jako uživatel Jan také ona zakoupila antivirový program Avast Premier 2017.

Uživatelka Lucie bude každý nový program podrobovat důkladnému testu v Sandboxu. Jedná se o funkci antivirového programu, která umožní nainstalovat program na virtuálním počítači a vyzkoušet ho, jestli je bezpečný také pro skutečný počítač. Jak ukazuje obrázek 6 stačí pouze kliknout na tlačítko spustit v Sandboxu, potom se spustí dialogové okno, kde uživatelka vybere program, který chce testovat.[3]



Obrázek 6: Avast Sandbox

Zdroj: Vlastní zpracování

Ochrana proti nebezpečným stránkám

Ochranu proti nebezpečným stránkám bude zajišťovat stejně jako u uživatele Jana již zmíněná funkce Ověřené weby, která je součástí antiviru Avast Premier 2017. Uživatelka Lucie bude používat výhradně prohlížeč SafeZone, který je také součástí antivirového programu.[3]

Ochrana proti e-mailovému spamu

U uživatelky Lucie není příliš velké nebezpečí z hlediska útoku pomocí spamu, protože uživatelka e-mail příliš často nepoužívá. Bude tedy stačit, když dále bude používat pro přístup k e-mailu webové rozhraní.

Přesto je nutné, aby uživatelka byla proškolena v oblasti rozpoznávání spamu. Především je nutné, aby byla poučena o nebezpečí, které se může ve spamu skrývat.

Ochrana proti infikovanému přenosnému paměťovému zařízení

U uživatelky Lucie je navrženo, aby stejně jako uživatelé Jan a Jaroslav nepoužívala, žádné zařízení od neznámé osoby, které nedůvěřuje.

Pokaždé když uživatelka Lucie vloží USB Flash disk, tak prověří pomocí antivirového programu Avast Premier 2017, zda se na něm nenacházejí škodlivé programy.

Náklady na zvolené řešení

Náklady na zvolené řešení pro uživatelku Lucii stejně jako u uživatele Jana jsou pouze za koupi licence pro antivirového programu Avast Premier 2017. Cena roční licence je podle oficiálních stránek výrobce 1690kč.[1]

3.4 Shrnutí

Uživatelé v těchto případových studií nejsou ohroženi úplně stejnými riziky, což je dáno především jejich způsobem využití počítače. Také znalosti a zkušenosti jsou u jednotlivých uživatelů rozdílné, proto liší způsoby zabezpečení.

V případových studií bylo uvedeno, že nebezpečí ze strany e-mailového spamu je problémem, který se týká všech zmíněných uživatelů, a ochranu je možné zajistit jedině tak, že sám uživatel se naučí rozpoznávat spamy. Na základě tohoto jsem se rozhodl, že v následující kapitole uvedu příklad spamu a také možnosti, jak rozpoznat, že se jedná o spam.

Velké riziko pro uživatele představuje také paměťové zařízení konkrétně USB Flash disky. Uživatelé totiž často používají toto zařízení, ale neuvědomují si, jaké může skrývat nebezpečí pro jejich počítač. Proti této hrozbě je nutné se chránit také pomocí chování uživatele, který bude dodržovat bezpečnostní pravidla.

Důležitou ochranou před jednotlivými hrozbami jsou antivirové programy, které mohou být také zcela zdarma, ale to doporučuji především u uživatele Jaroslava, protože je velmi

zkušeným uživatel a zbytečně se nevystavuje nebezpečí jako uživatelka Lucie a Jan, pro které navrhuji antivirový program, který představuje určité náklady.

I když byly navrženy příklady řešení, které by mohli uživatele zabezpečit. Nelze říci, že se dá označit za naprosté zamezení možnosti zneužití ze strany útočníka, například proto, že jsou tyto řešení často založena na uživatelovi samotném, který může udělat chybu, nebo jeho chování se může změnit. V kapitole 5 jsem se rozhodl uvést možnosti, jak detekovat zneužívání ze strany útočníka. Je to možnost, když ostatní zabezpečení selžou a počítač uživatele bude infikován.

4 PŘÍKLAD E-MAILOVÉHO SPAMU

V této časti uvedu příklad e-mailového spamu, na kterém vysvětlím, jak můžeme rozpoznávat spamy a jakých detailů je třeba si všímat, aby bylo možné předejít infikování nebezpečným škodlivým programem.

Jedná se o typ spamu, který využívá techniky, která je známá jako “phishing”, tento e-mail nutí příjemce, aby například udělal něco, čím se ochrání před možným rizikem, ale provedení toho, co útočník radí, se naopak vystaví uživatel riziku.

Jedná se o modelový e-mailový spam, kterým chci poukázat, jak takové podvodné e-maily vlastně vypadají.

4.1 Příklad spamu

Odesílatel: admin@email.cz

Předmět: Ochrana před novým typem viru

Vážený kliente,

zasíláme Vám naléhavou zprávu, týkající se nového viru, který napadá zákazníky naší banky. Běžné antivirové programy na něj bohužel nestačí. My Vám, ale před tímto virem nabízíme ochranu zcela zdarma. Stačí abyste program, který je v příloze tohoto e-mailu neprodleně nainstalovali.

S pozdravem,

Jan Kotalík

Vedoucí odboru IT

4.2 Rozbor spamu

V první řade je nutné se podívat na adresu odesílatele. V tomto případě je adresa odesílatele admin@email.cz. Na jménu admin není samozřejmě nic podezřelého. Problém je spíše v doméně, která zní email.cz. Pod touto doménou si útočník muže zaregistrovat e-mailovou schránku velmi snadno, ale téměř všechny společnosti, které mají své webové stránky, posílají e-maily s doménou právě svých stránek, proto je nutné si vždy všímat doménového jména u všech e-mailů.

V e-mailu se nenachází jméno společnosti a logo, kterým je příjemce zákazník. To je velmi neobvyklé a napovídá to o tom, že se jedná o podvod. Může se, ale stát, že útočník

zvolí jednu ze společností náhodně, nebo se mu podaří zjistit, jakou společností je majitel e-mailu zákazník. Například u bank není úplně složité si vybrat jednu, která má v současné době nejvíce zákazníků a jméno této banky vložit do svého podvodného e-mailu. Naštěstí toto však není příliš časté, když útočníci chtějí infikovat nejvíce uživatelů.

Dále je nutné se zaměřit na obsah. Mnohdy stačí zapojit jen zdravý rozum na rozpoznání podvodného e-mailu. V tomto e-mailu například varuje útočník uživatele před nebezpečím, který představuje nový virus, který napadá zákazníky a nabízí ochranu pomocí nějakého programu, ale v e-mailu například chybí, co vlastně ten virus dělá, a hlavně jak nový program pomůže uživateli se bránit.

Pokud uživatel bude mít přesto pocit, že program, který je mu poslán může zamezit nějakému viru může podrobit testu, jak jsem uvedl v případových studiích může použít například program Sandboxie, který otestuje, daný program na virtuálním počítači, avšak toto vyžaduje určité zkušenosti ze strany uživatele.

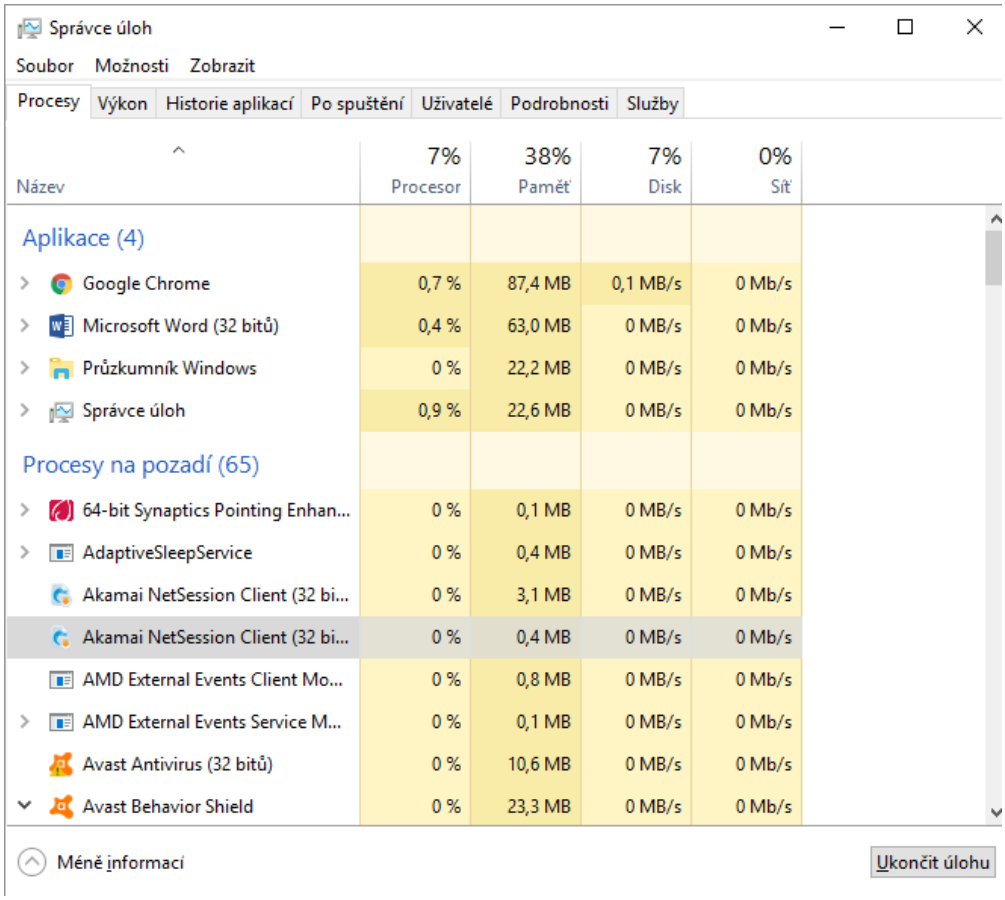
Kdyby si uživatel nebyl jistý, že se jedná o podvod. Může si také ověřit u samotné společnosti, zda je nutné se před nějakou hrozbou chránit a zda rozesílají program, který před touto hrozbou chrání. Informovat společnost o možnosti podvodného e-mailu je důležité také proto, že společnost může varovat ostatní zákazníky.

5 DETEKOVÁNÍ ZNEUŽITÍ

U útoku, kdy se využívají uživatelé se útočník snaží, aby škodlivým program, kterým infikuje uživatelský počítač nebyl vidět, proto může být obtížná detekce takovéhoto skrytého programu.

Uživatel může například zjistit, že jeho počítač nemá takovou rychlost, jakou by měl vzhledem k puštěných programů mít, nebo se podezřele dlouho načítají stránky na webovém prohlížeči. To vše může být právě příkladem činnosti skrytého škodlivého programu, který zřejmě firewall nebo antivirový program automaticky nezaznamenal.

Je tedy nutné, aby sám uživatel se pokusil detekovat možné zneužívání jeho počítače útočníkem. K tomu může uživatel použít například task manager (správce úloh). Pro rychlý přístup může využít klávesové zkratky (Ctrl+Shift+Esc), jakmile uživatel stiskne najednou klávesy control, shift a escape, tak se mu otevře okno s touto aplikací, která je zobrazena na obrázku 7.



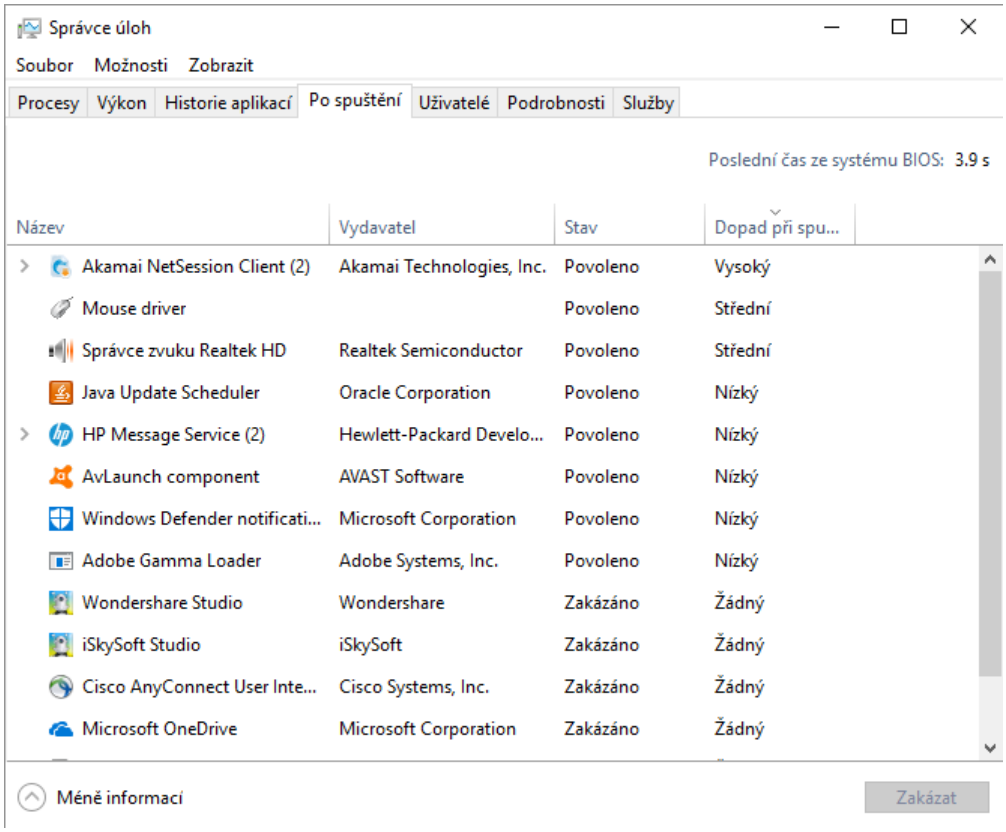
Obrázek 7: Správce úloh

Zdroj: vlastní zpracování

Uživatel má tedy určitý přehled o tom, jaké aplikace jsou spuštěny a jaké procesy probíhají na jeho počítači. To mu může umožnit zjistit, že na jeho počítači jsou spuštěny například programy, které jsou podezřelé nebo probíhají procesy, které by zřejmě probíhat neměli.

Samozřejmě většina uživatelů nezná všechny procesy, které probíhají na jejich počítačích. Proto je nutné, aby použili při detekování podezřelé aktivity svého počítače například také antivirový program a spustili test celého systému.

Uživatel také může zkontrolovat jaké aplikace se spouštějí při startu systému. Stačí, když ve Správci úloh klikne na záložku Po spuštění. Jak je vidět na obrázku 8. Zde uživatel vidí, jaké aplikace se spouští po startu systému. Zároveň je zde vidět jaký mají dopad jednotlivé aplikace na rychlost spouštění systému. Jak již bylo zmíněno v kapitole 1.1.5 některé druhy trojských koní se spouští se startem systému, tímto způsobem může například uživatel odhalit škodlivý program.



Obrázek 8: Správce úloh, záložka Po spuštění

Zdroj: Vlastní zpracování

Další možností, jak detekovat možné zneužití jsou některé antivirové programy, které nabízí štíty, které sledují podezřelou aktivitu na počítači, a potom jí uživateli hlásí, nebo jí přímo eliminují.

Těmto programů se může podařit automaticky bez přičinění uživatele odhalit škodlivý program, ale také nemusí, proto je nutné provádět pravidelné testování systému a aktualizace.

ZÁVĚR

Ve své práci jsem se zabýval, stále se zvětšujícím problémem bezpečnosti uživatele před útoky, které nejsou zaměřeny přímo na uživatele, ale pouze ho využívají k útoku na služby v síti Internet.

Pokusil jsem se navrhnout řešení zabezpečení před možným zneužitím pro jednotlivé uživatele. Mezi jednotlivými uživateli jsem našel určité rozdíly, proto také jejich rizika jsou jiná a samozřejmě také řešení týkající se jejich zabezpečení jsou tedy odlišná.

Dále jsem navrhl příklad e-mailového spamu, na kterém jsem se pokusil vysvětlit způsoby, jak ho normální uživatel může rozpoznat.

V poslední časti jsem navrhl způsob, jak lze detekovat možné zneužití ze strany útočníka, pokud uživatel zaznamená podezřelou aktivitu na svém počítači.

POUŽITÁ LITERATURA

[1] Antispam. *antivirovecentrum.cz* [online]. [cit. 2017-08-10]. Dostupné z: https://www.antivirovecentrum.cz/antispam.aspx

[2] Antivirové programy. *antivirovecentrum.cz* [online]. [cit. 2017-08-10]. Dostupné z: https://www.antivirovecentrum.cz/antiviry.aspx

[3] Avast Premier. *Avast* [online]. [cit. 2017-08-02]. Dostupné z: https://www.avast.com/cs-cz/premier

[4] CO JE TO HOAX. *Hoax.cz* [online]. [cit. 2017-04-07]. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax

[5] CSIRT.CZ. *CSIRT.CZ* [online]. [cit. 2017-08-02]. Dostupné z: https://csirt.cz/

[6] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP: bezpečnost. 2. aktualiz. vyd*. Praha: Computer Press, 2003. ISBN 80-7226-849-x.

[7] HALLER, Martin. *Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků*. [online]. 2006 [cit. 2017-06-04]. Dostupné z: https://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-1/

[8] HALLER, Martin. *Denial of Service (DoS) útoky: záplavové typy*. [online]. 2006 [cit. 2017-06-04]. Dostupné z: https://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/

[9] How It Works. *Sandboxie* [online]. [cit. 2017-04-07]. Dostupné z: https://www.sandboxie.com/index.php?HowItWorks

[10] HUB, Miloslav. *Bezpečnost a ochrana informací v prostředí internetu.* 1. Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[11] JIROVSKÝ, Václav. *Kybernetická kriminalita.* 1. Praha: Grada, 2007. ISBN 978-80247-1561-2.

[12] KRATOCHVÍL, Petr. *Nejbezpečnější e-mail světa pod těžkým DDoS útokem* [online]. 2015 [cit. 2017-06-04]. Dostupné z: http://www.chip.cz/novinky/nejbezpecnejsi-e-mail-sveta-pod-tezkym-ddos-utokem

[13] MALINKA, Kamil a Radim PEŠTA. *Zase ty viry*. Zpravodaj ÚVT MU [online]. 2009, 14.11.2011, XIX (5) [cit. 2017-04-08]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/620.html#lit1

[14] Windows Defender. *Microsoft* [online]. [cit. 2017-04-07]. Dostupné z: https://www.microsoft.com/en-us/windows/windows-defender

[15] MOIR, Robert. *Defining of malware* [online]. 2003 [cit. 2017-06-04]. Dostupné z: https://technet.microsoft.com/en-us/library/dd632948.aspx

[16] PATRIKAKIS, Charalampos, MASIKOS, Michalis, ZOURARAKI, Olga, *Distributed Denial of Service Attacks*. [online]. 2004 [cit. 2017-06-04]. Dostupné z: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

[17] PŘIBYL, Tomáš. *Jak vás ochrání antispamové filtry?* [online]. 2005 [cit. 2017-06-04]. Dostupné z: http://technet.idnes.cz/jak-vas-ochrani-antispamove-filtry-dug-/software.aspx?c=A050221_163205_bezpecnost_vse

[18] Phishing. *Hoax.cz* [online]. [cit. 2017-04-07]. Dostupné z: http://www.hoax.cz/phishing

[19] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

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

[21] Seznamte se – DoS a DDoS útoky. *Security-portal* [online]. 2013 [cit. 2017-06-04]. Dostupné z: http://www.security-portal.cz/clanky/seznamte-se---dos-ddos-útoky

[22] SCHILLER, Craig A. *Botnets: the killer web APP*. s.l.: Syngress, 2007. ISBN 978-1-59749-135-8.

[23] TANENBAUM, Andrew S. Computer networks. 4th ed. New Jersey: Prentice-Hall, c2003. ISBN 0-13-038488-7.