Česká zemědělská univerzita v Praze

Technická fakulta

Internetová kriminalita

Bakalářská práce

Autor práce: Pavel Myslík

Vedoucí práce: Ing. Zdeněk Votruba, Ph.D.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pavel Myslík

Zemědělské inženýrství
Informační a řídicí technika v agropotravinářském komplexu

Název práce

Internetová kriminalita

Název anglicky

Internet criminality

Cíle práce

Cílem práce je shrnout rizika spojená s použitím Internetu jak z pohledu běžného uživatele, tak i z pohledu komerční firmy. Základem práce je rozbor kritických oblastí a činností včetně porušování autorských práv. Zpracována je základní legislativa postihující počítačovou kriminalitu a na základě vybraných kauz demonstrována příslušná rizika. V závěru práce jsou vyjádřena doporučení minimalizující rizika plynoucí z popsané kriminální činnosti.

Metodika

1. Úvod
2. Cíl a metodika
3. Historie Internetu a nástup internetové kriminality
4. Druhy internetové kriminality
5. Pachatelé internetové kriminality
6. Vybrané způsoby napadení
7. Autorská práva a jejich porušování
8. Legislativa a instituce
9. Doporučení a závěr

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

počítačová kriminalita, vir, spam, spyware, legislativa

Doporučené zdroje informací

JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

Joel Scambray, Stuart McClure, George Kurtz: Hacking bez tajemství, COMPUTER PRESS,

KIM, P.: Hacking – praktický průvodce penetračním testováním, Zoner Press, 2015, ISBN: 25845970

Klimek, L.; Záhora, J.: Počítačová kriminalita v európskych súvislostiach , Wolters Kluwer (Iura Edition), 2016. ISBN:25845970

Předběžný termín obhajoby

2019/2020 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 7. 1. 2019

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 15. 2. 2019

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 03. 04. 2020

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Internetová kriminalita“ vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.
Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.
Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.
Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne 9.4.2020 _____

Pavel Myslík

Poděkování

Rád bych touto cestou poděkoval mému vedoucímu práce Ing. Zdeňku Votrubovi, Ph.D., za jeho odborné rady, připomínky a pomoc při psaní této bakalářské práce.

Internetová kriminalita

Abstrakt

Bakalářská práce popisuje různé druhy útoků, které hrozí při využívání Internetu. Na začátku práce je popsána historie Internetu, jeho vznik a vývoj v České republice. Následuje rozlišení pojmů počítačová, internetová a kybernetická kriminalita. Dále jsou definováni a rozděleni pachatelé internetové kriminality a také podrobně popsány jednotlivé druhy této kriminality. Na ty navazuje základní legislativa České republiky postihující kriminalitu v online prostředí a poté jsou uvedeny organizace a projekty bojující proti internetové kriminalitě. Cílem práce je upozornit na rizika a hrozby spojené s používáním Internetu a také uvést možnosti obrany. V závěru práce jsou uvedeny doporučení pro snížení rizika napadení.

Klíčová slova: počítačová kriminalita, vir, spam, spyware, legislativa

Internet criminality

Summary

Bachelor thesis describes various types of attacks that threaten to use the Internet. At the beginnig of the thesis is described the history of the Internet, its origin and development in the Czech Republic. The following is a distinction between the terms computer, internet and cyber crime. Furthermore, the perpetrators of the internet criminality are defined and divided and also individual types of this criminality are descriped in detail. These are followed by the basic legislation of the Czech Republic and then organizations and projects fighting Internet crime are listed. The aim of this thesis is to point out the risks and threats associated with using the Internet and also to mention the possibilities of defense. At the end of the work are recommendations for reducing the risk of attack.

Keywords: computer crime, virus, spam, spyware, legislation

Seznam obrázků

Seznam použitých zkratek

ARPA	Advanced Research Projects Agency
BBN	Bolt, Beranek and Newman
BSA	Business Software Aliance
CERN	The European Organization for Nuclear Research
CESNET	Czech Educational and Scientific Network
ČR	Česká republika
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DRDoS	Distributed Reflected Denial of Service
EARN	Europian Academic and Research Network
EC3	European Cybercrime Centre
FERNET	Federal Educational and Scientific Network
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IMP	Interface Message Processor
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NCP	Network Control Protocol
NCSA	National Center for Supercomputing Applications
SANET	Slovak Academic NETwork
TCP/IP	Transmission Control Protocol/Internet Protocol
UCLA	University of California Los Angeles
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
WWW	Word Wibe Web

Obsah

1 Úvod

V současné době využívá Internet více než 4 miliardy lidí na světě a počet stále roste. Tento nárůst je daný také díky rozvoji informačních technologií, jako jsou notebooky, počítače a chytré mobilní telefony, které využívá čím dál, tím víc lidí, a to v každé věkové kategorii. Pro většinu z nás představují informační technologie nezbytnou součást života. Každá nová technologie však přináší i negativní stránku používání.

V síti Internet s rostoucím počtem uživatelů přibývá také obětí internetové kriminality. Je to dáno zdokonalujícími technikami pachatelů a neznalostí uživatelů bránit se proti internetovým hrozbám. Útoky v prostředí Internetu mohou být páchány na jednotlivcích, společnostech, ale i vládách.

Na začátku této bakalářské práce, která se zabývá právě problematikou internetové kriminality, je nejprve definován Internet a následně popsána jeho obecná historie a vývoj v České republice. Dále jsou rozlišeny pojmy počítačová, internetová a kybernetická kriminalita. Poté jsou zmíněni pachatelé internetové kriminality a její jednotlivé druhy, jako jsou hackerské nástroje, malware, spam nebo také kyberšikana.

Závěr práce je věnován základní legislativě v České republice, která postihuje tento druh kriminality a jsou zde také zmíněny projekty a organizace bojující proti internetové kriminalitě.

2 Cíl a metodika práce

Cílem mé práce bude upozornit na rizika a hrozby spojené s používáním Internetu, a to jak z pohledu jednotlivých uživatelů, tak z pohledu firem. Důležitou součástí práce budou také možnosti obrany či opatření, jak jednotlivým druhům napadení předcházet.

Metodikou této práce bude nastudovat českou i zahraniční literaturu a na základě zjištěných informací nejprve definovat Internet a jeho vznik. Základem práce bude popsání jednotlivých druhů internetové kriminality a jejích pachatelů. Pro lepší porozumění a seznámení s problematikou budou u vybraných napadení použity obrázky s ukázkami konkrétních útoků. Zmíněna bude také základní legislativa České republiky.

3 Internet

Internet je celosvětový systém propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí přenosových protokolů TCP/IP. Cílem všech lidí využívajících Internet je vzájemná komunikace neboli výměna dat. [5]

3.1 Historie

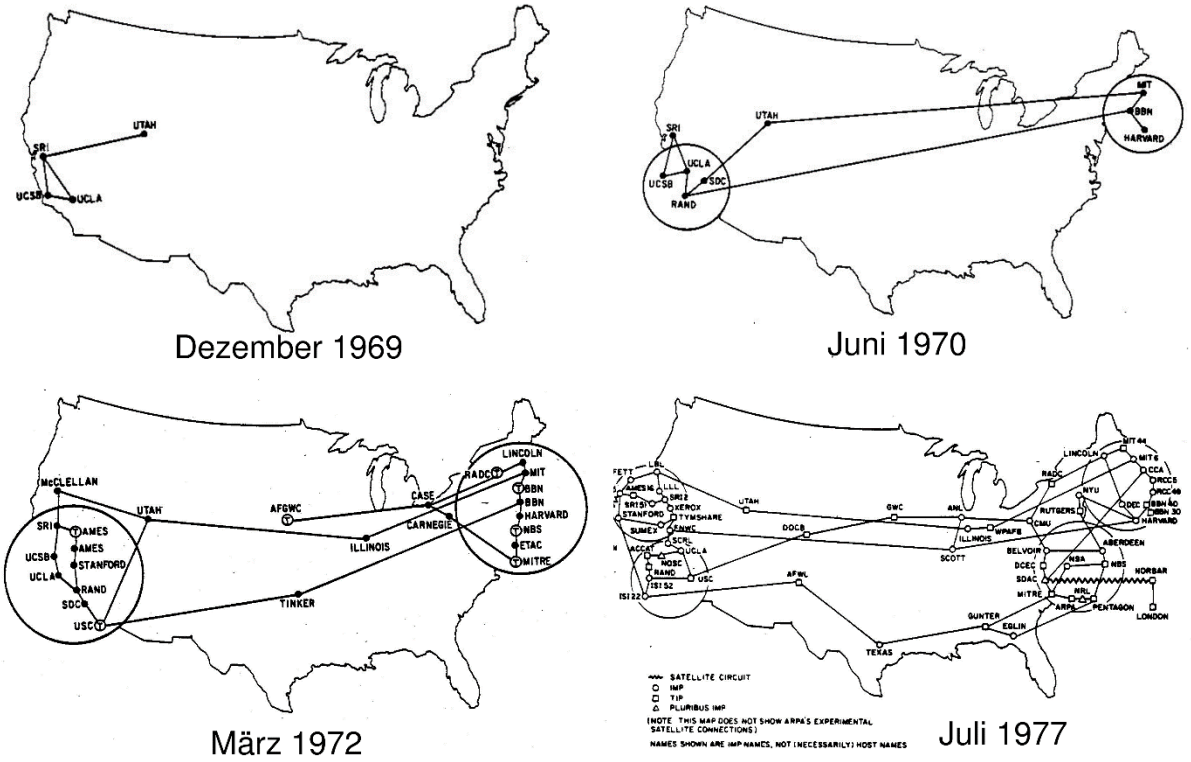
Počátky Internetu lze vysledovat až k šedesátým létům, kdy v roce 1957 Sovětský Svaz vypustil první umělou vesmírnou družici Sputnik 1, což dost šokovalo americké vědce, inženýry a politiky. Proto 7. února 1958 americké ministerstvo obrany založilo Agenturu moderních výzkumných projektů (Advanced Research Projects Agency, ARPA). Tímto chtěli udržet technologický náskok ozbrojených sil USA a předejít tak „překvapením“, kterým byl Sputnik 1.

Úřad ARPA připravil programový plán, který podrobně popisoval procesor IMP (Interface Message Processor). Podle Michaela Haubena (2003) je IMP definováno jako: „*hardwarové zařízení, které rozhodovalo o metodě spojení zúčastněných počítačů přes telefonní linky a řídilo komunikaci*“. První čtyři IMP vyrobila a dodala v roce 1969 společnost BBN (Bolt, Beranek and Newman). Téhož roku byly jednotlivě tyto IMP (uzly) připojeny, a tak vznikla síť ARPANET, kterou na konci roku 1969 tvořily čtyři uzly, viz Obrázek 1. První uzel byl připojen v září 1969 na Kalifornské univerzitě v Los Angeles (University of California Los Angeles, UCLA). Ke komunikaci mezi jednotlivými uzly byl využíván protokol NCP (Network Control Protocol). Přenos souborů po síti ARPANET probíhal pomocí protokolu FTP (File Transfer Protocol), který byl dokončen v 1972.

V roce 1973 byl navrhnut protokol s názvem "Protocol for Packet Network Intercommunication", který sloužil k síťové komunikaci neboli připojení sítě ARPANET k jiným sítím. Takto navrhnutý protokol fungoval jako určitá obálka, jejíž funkce byla zajistit přenos jednotlivých částí dopisu nazvané jako „datagramy“ a byl nazván protokolem řízení přenosu TCP (Transmission Control Protocol). V létě roku 1977 Vint Cerf a Bob Kahn demonstrovali využití TCP při poslání paketu třemi různými sítěmi. Paket cestoval ze San Francisca do Londýna a odtud zpět na Univerzitu jižní Kalifornie, aniž by ztratil jediný bit. Později bylo rozhodnuto rozdělit původní protokol TCP na protokol transportní vrstvy TCP a

protokol síťové vrstvy IP (Internet Protocol). Transportní vrstva zajišťuje spolehlivý přenos paketů, síťová vrstva jejich směřování a adresování. V roce 1983 ARPANET přešel z protokolu NCP na soubor protokolů TCP/IP a následně se rozdělil na veřejnou síť, nazývanou Internet a vojenskou síť nazývanou Milnet.

Obrázek 1: Mapa vývoje ARPANETU v USA



Zdroj: http://www.fibel.org/linux/lfo-0.6.0/arpanet.png

S nárůstem připojených počítačů k Internetu vyvinula v roce 1983 společnost BBN za účelem usnadnění jejich vzájemné komunikace, systém doménových jmen (Domain Name System, DNS). Ve stejném roce došlo také k rozvoji adresovacího protokolu IPv4, který využíval 32bitové adresy. To se tehdy nezdálo jako dostatek a docházelo k obavám, že adresy dojdou kolem roku 2005. Aby bylo k dispozici více adres, došlo později k vyvinutí IPv6, který využíval 128 bitové adresy. Podle Jaroslava Hrstky (2014) došlo k prvnímu komerčnímu využití IPv6 1. dubna 2002 společností NTT. Mezi lety 1985 a 1986 vznikla spojením šesti superpočítačových center síť NSFNET. Provoz ARPANETU byl oficiálně ukončen v roce 1990, kdy jeho služby převzala právě síť NSFNET. [1, 6]

V roce 1989 se britský počítačový vědec Tim Berners-Lee pracující pro jaderný výzkum CERN vrátil ke své dříve navržené myšlence hypertextu, což mělo usnadnit sdílení informací mezi fyziky po celém světě. Nejprve začal vývojem jazyka HTML a během následujících dvou let vyvinul společně s Robertem Caillau hypertextový přenosový protokol (HTTP) a univerzální zdrojový lokátor (URL). Koncem roku 1990 zavedl Tim Berners-Lee technologii World Wide Web (WWW), která označuje distribuovaný hypertextový informační systém. World Wide Web byl nejdříve navrhnut pro spolupráci fyziků, brzy se však rozrostl a dnes je nejrozšířenějším nástrojem Internetu. V roce 1992 byl Marcem Andreesenem a jeho kolegy z Národního střediska pro aplikace superpočítačů (NCSA) vyvinut první internetový prohlížeč Mosaic. První verze byla uvedena zdarma v dubnu roku 1993 a následně se prohlížeč rychle komerčně prosadil. Díky webovému prohlížeči začalo Internet využívat miliony počítačů po celém světě. Hranice 50 miliónů uživatelů na Internetu byla dosažena za necelé čtyři roky po zavedení WWW v roce 1992, kdežto například u televize byla tato hranice dosažena až po 13 letech a u telefonní služby dokonce po 75 letech. [1, 4, 6]

3.2 Vývoj Internetu v České republice

Počátek českého Internetu se píše do roku 1990, kdy byla po listopadu roku 1989 odstraněna zábrana v komunikaci se západem. Jako první síť se v březnu roku 1990 dostává do České republiky FidoNET. V květnu stejného roku přichází síť EUNet, která propojuje zejména unixové počítače. Obě sítě fungovaly na základě klasické telefonní linky. [7]

3.2.1 EARN

V říjnu roku 1990 se k nám dostává síť EARN (Europian Academic and Research Network), což byla odnož evropského BITNETU. EARN zpočátku fungoval s velmi malou přenosou rychlostí a jeho hlavní službou byl přenos elektronické pošty a souborů. První uzel byl k této síti připojen na ČVUT v Praze. Konkrétně se jednalo o střediskový počítač IBM 4381, který byl připojen do rakouského Lincu pevnou linku o přenosové rychlosti 9600 bit/s. Do této doby se datuje pouze neoficiální připojení České republiky k Internetu. Takto bylo připojeno pouze jedno pracoviště, ale v České republice byly desítky akademických pracovišť, která by měla být napojena na síť EARN. EARN se velmi rychle rozšířil v Praze, kde nebyly velké poplatky a vzdálenosti mezi jednotlivými pracovišti, dále se dostal pouze do Brna a Banské Bystrice. Připojení pevnou linkou ostatních měst v České republice nebylo

možné kvůli ceně pronájmu a malé přenosové rychlosti, proto musela být připojena pomocí komutované telefonní linky s přenosou rychlostí 2400 bit/s nebo 9600 bit/s. Jednalo se o velmi nákladné a nekomfortní řešení a začalo se jasně ukazovat, že EARN není perspektivní síť. [7, 8]

3.2.2 CESNET

Aby mohlo dojít k propojení akademických pracovišť, byl v polovině roku 1991 podán návrh na vybudování celostátní páteřní sítě, která měla sloužit pro akademická pracoviště a pokrývat území dřívějšího Československa. V Československu tedy vznikly dva projekty, které sloužily k vybudování národních páteřních sítí. Na Slovensku se začal budovat projekt SANET (Slovak Academic NETwork). Český projekt se měl původně jmenovat FERNET (Federal Educational and Research Network), ale kvůli odpůrcům tohoto názvu byl později zvolen název FESNET (Federal Educational and Scientific Network). Dne **13.2.1992** probíhá na pražském ČVUT oficiální připojení České republiky k Internetu. V červnu roku 1992 byl tento projekt oficiálně schválen ministerstvem školství, které na realizaci uvolnilo 20 miliónů korun. Ve druhé polovině tohoto roku byl název projektu změněn na CESNET (Czech Educational and Scientific Network). [7, 8]

Topologie sítě CESNET byla nejprve hvězdicová se dvěma uzly v Praze a v Brně, které byly propojeny pevnou linkou s přenosovou rychlostí 64 kb/s. K těmto uzlům byly postupně připojovány další uzly nacházející se v akademických městech a v březnu roku 1993 byla síť CESNET k dispozici v 11 městěch České republiky. Všechny tyto spoje měly přenosovou rychlost 19,2 kb/s, kromě již zmíněného spoje Praha – Brno (64 kb/s). Dochází také ke vzniku linek směřujících z České republiky. Nejprve byl vytvořen spoj Praha – Vídeň z původního spoje vedoucího z Prahy do Lince. Později přibývá spojení Praha – Amsterodam s přenosvou rychlostí 64 kb/s a s rozpadem Československa vzniká linka na trase Praha – Banská Bystrica.

Ačkoli byl CESNET původně vytvořen jako páteřní síť, která měla sloužit pro akademické účely, stal se později i poskytovatelem připojení k Internetu, nebyl ovšem jediným. Prvním komerčním poskytovatelem připojení k Internetu byla firma COnet, která provozovala síť CZnet vzniklou ze sítě EUnet. [8]

4 Počítačová, internetová a kybernetická kriminalita

S rozvojem výpočetní techniky a snahou jejího maximálního využití přichází také negativní stránka. Když vznikne nový vynález, je obecně známo, že se objeví i tací lidé, kteří ho využijí k nelegální činnosti. Jinak tomu není ani u informačních technologií. [11]

4.1 Počítačová kriminalita

Název počítačová kriminalita byl odvozen od zneužití spojeným s osobním počítačem. Jedná se tedy o trestné činy, v nichž je počítač využíván jako nástroj nebo jako předmět útoku. Je charakteristická pro zneužívání osobních údajů nebo finančními ztrátami napadených. Později bylo navrhnuto také označení kriminalita spojená s počítači (computer-related crime). [3]

Počítačová kriminalita se liší od klasické kriminality tím, že se neobjevují zbraně, násilí, újma na zdraví apod. Dále může být trestný čin spáchán během několika sekund a pachatel nemusí být na místě činu. [11]

4.2 Internetová kriminalita

Když v roce 1969 došlo ke vzniku sítě ARPANET, nikdo neočekával velký rozvoj síťových technologií propojujících miliony uzlů. Při návrhu protokolu TCP/IP, který je dnes nejrozšířenější, nebyl očekáván tak velký dosah Internetu. Proto nebyl kladen takový důraz na bezpečnostní charakteristiky sítí a protokolů, jako je tomu dnes. [2]

S rozvojem a vznikem nových zařízení, jako byly například mobilní telefony, tablety apod., jejichž společným jmenovatelem se stala komunikační síť a data, vznikl také pojem kriminalita informačně-komunikační technologie. Elektronických komunikačních sítí máme dnes několik druhů, ale existuje jeden speciální typ sítě, kterým je Internet. Jak již zmiňuji v kapitole 3, Internet ke komunikaci využívá speciální protokol (IP – internet protocol) a poskytuje několik služeb. Mezi tyto služby patří již zmíněný WWW (world wide web), dále také elektronická pošta, internetový chat v reálném čase, internetové telefonování (VoIP – voice over internet protocol), apod. Využíváním těchto služeb a páchání nelegální činnosti na Internetu vznikl pojem Internetová kriminalita. [3]

4.3 Kybernetická kriminalita

Kybernetická kriminalita označována také jako kybernalita je odvozena od pojmu kyberprostor, ve kterém k této kriminalitě dochází. Kyberprostor je dle Policie ČR „*virtuální prostředí, které nemá začátek ani konec, nezná hranice národních států a nelze určit, jak rozsáhlý je*.“ [2, 9]

Podle Jirovského (2007) je kybernetická kriminalita činnost, která porušuje zákon a může být namířena přímo proti počítačům, jejich hardwaru, softwaru, sítím, datům apod. Nebo v ní figuruje počítač pouze jako prostředek pro páchání trestné činnosti, popřípadě počítačová síť a k ní připojená zařízení jsou prostředím, kde se taková činnost odehrává. [2]

Završnik (2017) ve své knize uvádí, že jednotná definice kyberkriminality neexistuje v teorii ani legislativě a Úmluva Rady Evropy o kyberkriminalitě z roku 2001 (budapešťská úmluva) rozlišuje:

1) Trestné činy proti důvěrnosti údajů, ucelenosti a dostupnosti počítačových údajů a systémů (respektive „pravá“ kyberkriminalita)
2) Trestné činy spojené s počítačem: počítačové padělání a počítačové podvody
3) Trestné činy spojené s obsahem: různé formy trestných činů spojených s dětskou pornografií
4) Trestné činy spojené s porušováním autorských práv a práv příbuzných

Dále uvádí, že kyberkriminalitu definují tři hlavní novinky:

1. Uskutečňuje se v novém virtuálním prostoru
2. Obsahuje nová deviantní chování
3. Novinky v trestněprávních reakcích (například digitální forenzní analýza) [3]

Sledování kybernetické kriminality je dle Jirovského (2007) velice obtížné, protože ji můžeme pozorovat pouze přístroji, které nám umožní přístup do kyberprostoru. [2]

5 Pachatelé

Podle Látala (1998) jsou obvykle pachateli trestných činů v informačních technologiích lidé se středoškolským, vyšším, nebo vysokoškolským vzděláním v oboru informačních technologií. Často bývají nadprůměrně inteligentní a vynalézaví v programátorské oblasti. Jejich protiprávní jednání neobsahuje prvky násilí a jednají individuálně. Motivem pachatele nejčastěji bývá touha po zisku, dále také motivy získání převahy nad zaměstnavatelem, zneužívání osobních dat, nedostatečné ocenění práce nebo také touha po dobrodružství. Látal (1998) dále dělí pachatele z hlediska jejich vztahu k informacím na:

- Amatéry, mezi které řadí hackery, crackery a ostatní typy
- Profesionály, kam zařazuje pracovníky speciálních tajných služeb, detektivy, žurnalisty, podnikatele všeho druhu, specialisty informatiky a teroristy

Amatéry definuje jako „*osoby pronikající náhodně nebo cílevědomě do informačních systémů tak, že vyhledávají zranitelná místa.*“ Také uvádí, že se jedná o lidi s vyšší inteligencí, kteří mají schopnost rychle se naučit pracovat s počítačem. Profesionálové jsou podle Látala (1998) osoby, jejichž zaměstnáním je získávání, analyzování a využívání informací. Tyto činnosti většinou vykonávají pouze pro zaměstnavatele, nikoli pro sebe. [11]

5.1 Hackeři

„*Lidé často rozdíl mezi crackery a hackery nevidí a tyto termíny si pletou. Je to způsobeno také novináři, kteří slovem hacker označují i ty, kteří kradou data a peníze prostřednictvím internetu.“* [10]

5.1.1 Definice

V padesátých letech 20. století vznikly v komunitě radioamatérů termíny „hacker“ a „hacking“. Byly tak nazývány technicky nadané osoby, schopné hledat nové zapojení a metody, které vedly ke zlepšení výkonu a dosahu jejich vysílače. [2]

Zatímco média prezentují hackery jako kriminálníky nebo jako nebezpečné jedince, Jirovský (2007) uvádí následující rysy hackera:

- Člověk, který s nadšením programuje, dokonce je programováním posedlý, anebo dává přednost praktickému programování před teoretickými úvahami o programování

- Jedinec, který vyniká v rychlém programování nebo je expertem ve využívání konkrétního programu
- Osoba, která dokáže ocenit „hack value“, tedy hodnotu ztvárněného technologického řešení
- Obecně osoba, která je expertem nebo nadšencem v daném vědním oboru

Policie definuje hackera jako člověka, který proniká do chráněných systémů bez zájmu získání nebo zničení informací. K uspokojení nepotřebují, aby o jejich činech věděla veřejnost, stačí když se o nich mluví v jejich komunitě. U počítače tráví hodiny a získaná data používají pouze pro svou potřebu.

Přestože jsou hackeři většinou introverti a neradi komunikují, vytvářejí své vlastní komunity. Mezi sebou většinou komunikují písemně svým specifickým jazykem, který spočívá v grafické úpravě běžných slov. Také používají vlastní slang a specifický humor, kterému běžní lidé nerozumí. Hackerská etika je dle Jirovského (2007) rozdělena na těchto osm pravidel:

1. Přístup k počítačové technologii je pro všechny bez rozdílu a zdarma.
2. Všechny informace zdarma.
3. Nedůvěřujeme vládě a obecně mocenským autoritám, podporujeme decentralizaci.
4. Hackeři mají být posuzováni podle jejich dovedností jinými hackery, a ne nějakou formální organizací nebo jinými nerelevantními kritérii.
5. Na počítači je možné vytvořit i umění a krásu.
6. Počítače mohou změnit život k lepšímu.
7. Hacker nikdy nepoškodí systém.
8. Hacker se nikdy neprolamuje do státních počítačů. [2]

Podle Raymonda (2004) vytvořili Internet právě hackeři. Také uvádí, že hackeři udržují v provozu World Wide Web. [12]

5.1.2 Rozdělení hackerů

Hackeři se rozlišují podle motivace získání přístupu do systému, způsobu provedení průniku a také podle toho, jak s případně získanými daty zacházejí. Hackeři jsou rozděleni pomocí tzv. kloboukového dělení, které je odvozeno od barev klobouků hrdinů ve westernu.

Zatímco kladní hrdinové často nosili bílé nebo světlé klobouky, záporní nejčastěji nosili černé nebo tmavé klobouky. Podobně je tomu tak i u hackerů, kteří se dělí do tří základních skupin následovně:

- **White hats** (bílé klobouky) – jsou hackeři, kteří na žádosti společností podnikajících v oblasti informačních technologiích pronikají do bezpečnostních systémů za účelem odhalení slabin systémů. Následně vytvářejí bariéry, které by měly těmto útokům zabránit. Jejich průniky nejsou nijak škodlivé, naopak by měly upozornit na bezpečnostní chyby v systému. Tato skupina se může také označovat jako „sneakers" či „tiger-team".
- **Black hats** (černé klobouky) – jsou v podstatě opakem skupiny White hats. Cílém této skupiny je získat data napadeného systému a mnohdy se snaží uškodit i jeho uživateli. Hackeři této skupiny jsou často najímáni nelegálními organizacemi, kterým poskytují získaná data.
- **Grey hats** (šedé klobouky) – jedná se o skupinu hackerů, kteří se pohybují na pomezí obou skupin. Ačkoli není jejich primárním cílem škodit, mohou občas porušit práva nebo jiné morální principy. Do této skupiny jsou také řazeni hackeři, kteří nemají jasný svůj budoucí úkol. [2, 13]

Jirovský (2007) dále uvádí skupinu, která sama sebe označuje jako „brilantní programátory". Jedná se o hackery, kteří rádi programují a mají rozsáhlé znalosti o bezpečnostních systémech a jejich bariérách. Na základě přístupu k řešení problému má tato skupina dvě podskupiny:

- Guru – hacker, který je schopen svými zkušenostmi stanovit správné řešení zadaného problému.
- Wizard – hacker neboli „čaroděj" dokáže řešit zadaný problém způsobem, který ostatní zcela nechápou. Řešení hackerů této skupiny nemusí však vždy správně fungovat, zejména v okrajových situacích.

Výše zmíněné skupiny patří mezi základní dělení hackerů. Dále však mohou být skupiny jako Script-kiddies, profesionální hackeři, začátečníci, nespokojení zaměstnanci apod. [2]

5.1.3 Nejznámější hackeři a hackerské skupiny

Podle Jirovského (2007) a většiny zahraničních i českých serverů je za nejznámějšího hackera všech dob považován Kevin David Mitnick. Několikrát se mu podařilo nabourat do sítě Pentagonu a svými průniky do jiných společností způsobil škodu za téměř 300 milionů dolarů. V roce 1995 byl za své činy dopaden a zatčen. Po propuštění v roce 2000 mu byla přidělena podmínka se zákazem používání počítačů a Internetu po dobu tří let. Nyní vlastní společnost Mitnick Security Consulting, která se zabývá systémovým zabezpečením proti lidem, mezi které dříve patřil on sám. Ostatní známí hackeři jsou například Robert Tappan Morris, Kim Schmitz nebo Kevin Poulsen, kterému se podařilo nabourat několik systémů na síti Arpanet. [2, 14]

Podle Koloucha (2016) je nejznámější hackerskou skupinou Anonymous, jejichž vlajka je znázorněna na Obrázku 2. Ti sami sebe popisují jako skupinu lidí na Internetu, kteří chtějí spravedlnost pro každého občana na světě. Přesto se jedná o skupinu hackerů, kteří „sestřelují“ weby. Podařilo se jim hacknout webové stránky firmy Sony, televizní stanice Fox a mnoho dalším. Jako další známé skupiny Kolouch (2016) uvádí Lizard Squad, The Level Seven Screw, Chaos Computer Club, Globalhell a další. [13, 15]

Obrázek 2: Vlajka skupiny Anonymous

Zdroj: https://cs.wikipedia.org/wiki/Anonymous_(skupina)

5.2 Crackeři

Za crackery často bývají označováni hackeři ze skupiny Black hats. Crackeři však zneužitím hackerských metod většinou způsobují kriminální činnost. Cílem útoku je získání

dat ze systému, které mnohdy nevyužijí ani pro svůj prospěch. Často data pouze neoprávněně pozmění, ale jde jim spíše o destrukci systému. Mezi crackery se řadí i osoby, které zneužívají Internet a metody pro finanční podvody, vandalismus, teroristické činnosti a další nelegální aktivity. [2, 16]

Crackeři zpravidla pracují ve skupinách, ve kterých jsou členové děleni na jednotlivé pozice a každý má na starost konkrétí činnost. Jedná se o pozice např. prezidenta, webmastera, manažera, mluvčího apod. Tyto skupiny také mají odlišné specializace. Crackeři se často považují za hackery, kterými ale nejsou. Jejich znalosti v oblasti programování a informačních systému nejsou na tak vysoké úrovni jako u hackerů. Do bezpečnostních systémů většinou pronikají pomocí zveřejněných slabin, na které administrátoři ještě nezareagovali. [16]

5.2.1 Podskupiny crackerů

Crackeři se na základě jejich činnosti dělí na další podskupiny. První podskupinou jsou **Warez**. Členové Warez se zabývají překonáním ochrany proti kopírování, úpravou komerčních programů a také distribucí chráněného softwaru.

Dalšími jsou Phreakři neboli **Phrackeři**, jejichž činnost je zaměřena na vnikání do telekomunikačních služeb. Také se zabývají napichováním hovorů, sběrem a využíváním ukradených telefonních informací. Hackeři nechtějí mít s touto skupinou nic společného.

Rhybáři jsou další podskupinou a navazují na činnost Phrackerů. Jejich cílem však není krádež čísel telefoních karet, ale citlivějších a osobnějších dat napadeného. Jedná se zejména o údaje platebních karet nebo získání přístupových údajů bankovního účtu. [16]

6 Jednotlivé druhy internetové kriminality

6.1 Hacking, Cracking

Hacking, jak již vyplývá z činnosti hackera, znamená průnik do systému nestandartní cestou. Dochází tedy k obejití, u crackerů k prolomení bezpečnostní ochrany systému. [17]

6.1.1 Hackerské programové nástroje

Hackeři používají technologie, které musí mít programové nebo hardwarové nástroje, aby byly ovladatelné. Podle typu použití Jirovský (2007) rozlišuje tyto hackerské techniky na:

- Hardwarové nástroje, kam patří např. techniky hledání bezpečnostních děr v čipových kartách. Bylo by mylným předpokladem do hackerské komunity zahrnout pouze programátory. První techniky phreackerů byly v podstatě hardwarové blue-boxy a tímto označením se mnoho technických zařízení pro neoprávněný přístup označuje dodnes.
- Softwarové neboli programové nástroje, které v hackerské komunitě převažují.
- Sociální inženýrství neboli techniky zneužití lidského elementu.

Prolamovače hesel

Označovány také jako „Password crackers“ patří mezi nejstarší hackerské nástroje. Pomocí těchto nástrojů dochází k prolomení ochrany nebo autorizace, která je prováděna heslem. V podstatě hledají na základě různých kombinací znaků správné heslo, které je po nalezení odesláno hackerovi. Jirovský (2007) uvádí dva druhy útoku způsobené prolamovačem hesel:

- Slovníkové útoky (dictionary attack), které se pokoušejí použít známá slova z vlastní databáze.
- Útoky hrubou silou (brute-force attack) postupně generují všechny možné kombinace potřebné délky z vybraných znaků a zkouší, zda vyhovuje zadanému heslu či nikoliv.

Pro rychlejší nalezení shody kombinace znaků s potřebným heslem jsou u kvalitnějších prolamovačů využívány slovníky. Slovník používá pouze reálné znakové kombinace, tím pádem dochází k odstranění nesmyslných kombinací.

Rychlost prolamovačů je v dnešní době obrovská, kvalitnější z nich jsou schopni ověřit až milion hesel za sekundu. V síti se však prolamovače nedají použít přímo, protože se zde využívá ochranný algoritmus. Při autorizaci je dán časový interval po každém zadání hesla a tím je omezen počet zadávání pokusů v krátkém časovém intervalu. [2]

Backdoors

Neboli „zadní vrátka“ jsou kódy, které slouží k ovládání vzdáleného počítače, na kterém jsou nainstalovány. Tento nástroj je hackery velice využívaný, protože snižuje riziko odhalení útočníka. Většinou má každý hacker několik vzdálených počítačů, pomocí kterých vede útok na cílový stroj. Jedná se o velmi nebezpečný nástroj, protože umožňuje úplnou kontrolu nad napadeným počítačem. [2]

Sniffery

Jelikož se slovo „sniff“ přeloží jako „čmuchat“, jedná se o program, který odposlouchává na síti, zejména na Internetu. Sniffery umožňují zachytávat komunikaci, která prochází přes daný uzel sítě. Mohou tak získat přístupová hesla, znění emailů a ostatní údaje. Ačkoliv se jedná o nelegální činnost, nejedná se o útok. Hackeři se sniffingem spíše připravují k útoku na základě získaných dat. [2, 17]

Jako ochranu před sniffery Matějka (2002) doporučuje důkladné šifrování komunikace po Internetu. [17]

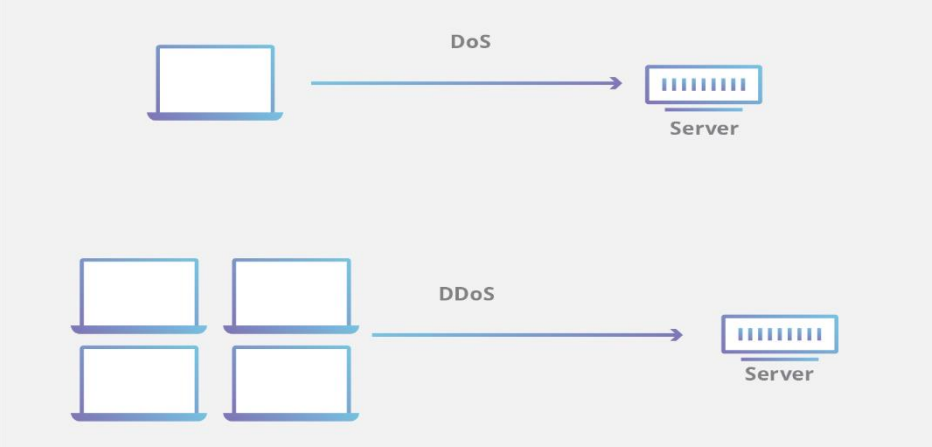
DoS a DDoS útoky

„Denial of Service“ je přeloženo jako potlačení či odepření služby. Jedná se o nástroje, kterými se útočí na (Internetovou) službu. Cílem útoku je snížení výkonu napadeného zařízení nebo jeho úplné vyřazení z činnosti. Jirovský (2007) uvádí, že myšlenka tohoto útoku je jednoduchá – pokud nelze zaútočit na cílový stroj, zaútočí se na jeho spojovací cesty. U napadeného systému dochází ke zpomalení služby nebo např. k nedostupnosti webových stránek. [2, 13]

Na Obrázku 3 je vidět rozdíl mezi DoS a DDoS útoky, který spočívá v počtu využitých počítačů k útoku. DoS (Denial of Service) používá jeden zdroj útoku a je relativně snadné se tomuto útoku ubránit. U DDoS (Distributed Denial of Service) neboli distribuovaného

odepření služby dochází k odesílání paketů z více různě rozmístěných počítačů, což stěžuje obranu.

Obrázek 3: Rozdíl mezi DoS a DDoS útokem



Zdroj: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Existují také útoky **DRDoS** (Distributed Reflected Denial of Service). Při tomto útoku dochází rozeslání požadavků na spojení na spoustu počítačových systémů. Jako zdrojová adresa u těchto podvržených požadavků je použita adresa oběti, která poté obdrží velké množství odpovědí a dojde k zahlcení systému.

Kolouch (2016) uvádí jako základní a nejznámější metody DoS či DDoS útoku tyto:

- **Zahlcení příkazem ping** (Ping-Flood) – Použitím příkazu „ping“ na adresu cílového počítače a následnými odpovědmi na tento příkaz dochází k zahlcení cílové počítače.
- **Zahlcení volných systémových prostředků** (SYN-Flood) – Posláním paketů s příkazem SYN na cílový počítač dochází k vyčerpání systémových zdrojů.
- **Falšování zdrojové adresy** (IP spoofing) – Je typickým spíše pro DRDoS a při jeho použití se zesilují DoS a DDoS útoky. IP spoofing spočívá ve falšování zdrojových adres odesílaných paketů.
- **Smurf attack –** K tomuto útoku dochází při špatné konfiguraci systému. Skrze broadcast adresu se rozešlou pakety všem počítačům v síti. [13]

Nástroje průzkumu sítě

Pro hackera či crackera je důležité naplánování útoku a prozkoumání „terénu“. Spoustu informací lze však zjistit pouze použitím prohlížeče. Pokud je veden útok na nějakou firmu, na jejích webových stránkách bývají často důležité informace o majiteli či topologii sítě. Útočník si také může otevřít zdrojový kód stránky, kde pro něho mohou být další zajímavé informace, které následně zneužije. Takto jednoduše se mohou pachatelé dostat k datům, které jim velice usnadní útok.

Pro získání informací o cílové síti si hackeři automatizovali nástroje průzkumu sítě. Jedná se o jednoduché programy, které jsou schopni zjistit propojení a vlastnosti zařízení v cílové síti. Nejsnadnějším cílem útočníka jsou špatně nakonfigurované DNS servery se záznamy o struktuře celé obsluhované sítě. [2]

6.1.2 Ochrana před útoky hackerů

Je několik možných způsobů, jak se bránit před útoky hackerů a ochránit tedy svá data, a hlavně sami sebe. Bude tedy uvedeno několik typů, jak se před útoky bránit. Samozřejmě někdy ani kvalitní zabezpečení není pro hackery dostatečnou překážkou k našim datům.

První pravidlo, které by měl každý dodržovat, je ochrana svých údajů. Rozhodně není vhodné sdílet s kýmkoliv na Internetu důležitá data, jako jsou informace o platební kartě či přihlašovací údaje. Velice důležité je využití antivirových programů, které identifikují největší hrozby a umožňují odstranění škodlivého softwaru ze zařízení. Ke zvýšení bezpečnostni také vedou pravidelné aktualizace operačních systémů zařízení a dalších softwarových programů využívajících Internet. Pokud zrovna nevyužíváme Internet, je vhodné vypnout funkce Wi-Fi či Bluetooth. Tím totiž zabráníme pachatelům v používání naší sítě nebo v přístupu k našemu zařízení. [18]

6.2 Malware

Termín malware vznikl složením slov malicious software, což znamená škodlivý software. Jedná se o program nebo část kódu, který se využívá k vniknutí do počítačového systému. Nejčastěji se šíří Internetem a e-mailem, kde je součástí příloh. Útočník následně

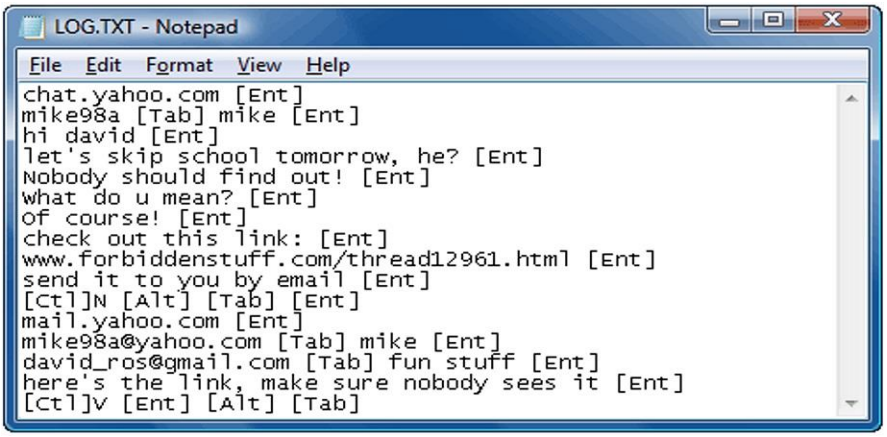
může počítačový systém poškodit, odcizit data nebo sledovat napadeného uživatele. Nejznámější typy malwaru jsou jednotlivě popsány níže. [13, 19]

6.2.1 Spyware

Jedná se o typ malwaru, který slouží ke sledování uživatele. Jelikož je tento typ napadení těžké odhalit, většinou oběť neví, že je sledována. Spyware získává data o chování uživatele na Internetu, například navštívené webové stránky, spuštěné aplikace nebo osobní data jako jsou čísla platebních karet a následně je odesílá útočníkovi. [13, 20]

Zajímavým typem spyware je **keylogger**, který zaznamenává stisky kláves napadeného. Nejčastěji slouží ke zjištění přihlašovacích údajů, kterými jsou pachateli zpřístupněny účty napadeného počítačového systému. Na Obrázku 4 je ukázka výstupního textu keyloggeru neboli získaných dat o oběti. [13, 21, 22]

Obrázek 4: Výstup keyloggeru



Zdroj: https://www.internetembezpecne.cz/internetem-bezpecne/malware/keylogger/

6.2.2 Adware

Tento název je tvořen spojením anglických slov „advertising supported software“, což se přeloží jako software podporující reklamu. Jedná se tedy o software, který na napadeném zařízení zobrazuje reklamu. Ačkoliv není adware nijak zvláště nebezpečný, uživatele může obtěžovat zobrazování reklam v prohlížeči nebo ve vyskakovacích oknech, viz Obrázek 5. [13, 23]

Obrázek 5: Adware

Zdroj: https://searchsecurity.techtarget.com/definition/adware

6.2.3 Viry

Jako vir je označován škodlivý software nebo část kódu, který v podstatě ničí napadené zařízení. Většinou bývá součástí nějakého souboru či softwaru, po jehož spuštění dojde k napadení. Těmito napadenými soubory (hostiteli) se také bez vědomí uživatele sám šíří mezi počítačovými systémy. Počítačový vir se nejčastěji projevuje zpomalením systému, výpadky internetového připojení nebo změnami či mazáním dat. [13, 24]

Extistuje několik druhů počítačových virů, které se dělí podle mnoha faktorů. Může to být podle hostitele neboli souboru, který jej přenáší. Dalé také podle způsobu, kterým se projevují v systému. Kolouch (2017) uvádí dělení virů dle napadeného souboru na:

- Boot viry – napadají systémové oblasti
- Souborové viry – napadají pouze soubory
- Multiparitní viry – napadají soubory i systémové oblasti
- Makroviry – napadají aplikace pomocí maker [13]

Matějčík (2018) uvádí, že jedním z nejznámější a ve své době i nejničivějším virem je virus ILoveYou z roku 2000. Byl součástí e-mailu s předmětem ILOVEYOU a textem „kindly check the attached LOVELETTER coming from me“, což je přeloženo jako „zkontrolujte si laskavě milostný dopis ode mě“, viz Obrázek 6. Milostným dopisem byla

myšlena příloha, po jejímž otevření došlo ke spuštění viru, který následně mazal fotografie, dokumenty a hudební soubory. Tento vir napadl až 10 % počítačů v internetové síti a způsobené škody se odhadují na více než 5 miliard dolarů. [25]

Obrázek 6: Virus ILoveYou

Zdroj: https://en.wikipedia.org/wiki/ILOVEYOU

Jelikož v dnešní době existují kvalitní antivirové programy, které snadno odhalí a zneškodní vir, jsou počítačové viry na ústupu. Více se tedy využívají ostatní formy útoku. [26]

6.2.4 Počítačoví červi

Počítačový červ neboli „worm“ je škodlivý vir, jehož úkolem je infikovat co nejvíce počítačů. Červ se však na rozdíl od viru dokáže šířit bez hostitele. V podstatě z napadeného zařízení sám sítí odešle svou kopii do dalšího počítačového systému. Dokáže se šířit velice rychle, což může vést až k zahlcení počítačové sítě. Červi jsou také naopak schopni zjistit bezpečnostní slabiny systému, proto jsou často využíváni ke hledání bezpečnostních mezer systému. [13, 26]

První červ byl vypuštěn v roce 1988 Robertem Morrisem při experimentování s autoreplikovanými kódy. Podařilo se mu nakazit několik tisíc počítačů a následně byl odsouzen ke třem letům vězení. [2]

K nakažení červem nejčastěji dochází otevíráním e-mailových souborů, ve kterých je obsažen, nebo navštěvováním nebezpečných webových stránek. Napadený systém se nejčastěji projevuje výrazný zpomalením nebo úplnou nefunkčností. [27]

6.2.5 Trojské koně

Bývají označovány také jako Trojani. Jedná se o nebezpečné programy, které jsou nejčastěji součástí e-mailových příloh. Trojský kůň může být ukryt také ve volně stažitelných aplikacích a hrách. Zpočátku se jeví jako užitečná funkce či aplikace, nicméně opak je pravdou. Po jeho aktivaci dochází k manipulaci a mazání dat, monitorování napadeného počítače, získávání hesel apod. Ke svému šíření potřebují trojské koně na rozdíl od virů „pomoc“ uživatele. [2, 13]

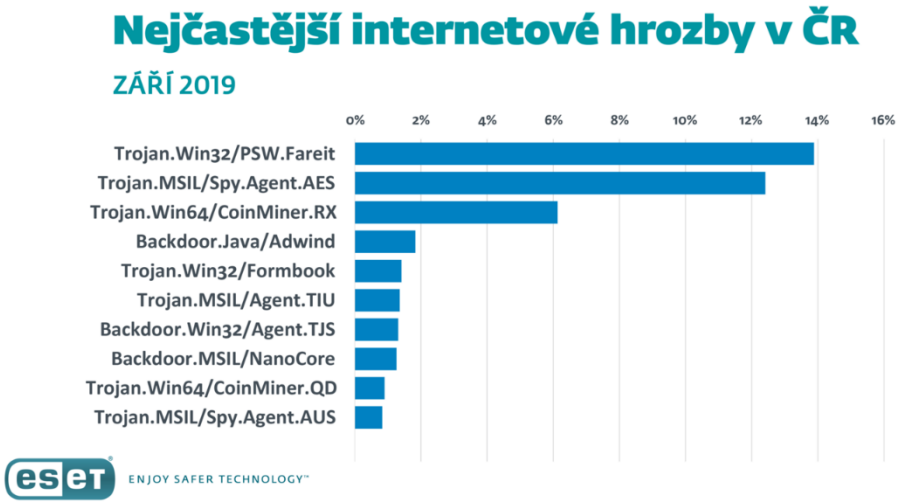
Jako zajímavou variantu trojských koní Jirovský (2007) uvádí „dataminery“, což jsou programy sledující činnost uživatele a následně odesílají potřebné údaje pachateli. Dále také uvádí, že existují nástroje umožňující vytvoření trojského koně. Konkrétně zmiňuje nástroj eLiTeWrap, který spojením trojského koně a nosného programu vytvoří novou modifikaci trojského koně. [2]

První útok trojským koněm byl program ANIMAL, vydaný v roce 1975. Jednalo se o hru, ve které se odpovídalo na dvacet otázek. Ačkoliv se jednalo spíše o neškodný žert, hra se ukládala do sdílených adresářů, odkud se mohla šířit celou počítačovou sítí. [28]

Napadení trojským koněm v roce 2019 v České republice představovalo největší hrozbu ze všech útoků. Společnost ESET v říjnu roku 2019 sestavila žebříček nejčastějších internetových hrozeb za tento rok a první tři místa obsadili trojské koně, viz Obrázek 7. První místo obsadil trojký kůň s názvem PSW.Fareit. ESET uvádí následující definici: „*Tento malware se zaměřuje na odcizení přístupových údajů z prohlížečů Chrome, Firefox, Opera či Internet Explorer. Data následně odešle útočníkům na vzdálený server a z infikovaného zařízení se sám vymaže. Tento fakt sám o sobě komplikuje detekci, respektive uživatel se*

nemusí dozvědět, že se jeho hesla dostala ne nepovolaných rukou.“ Na druhé příčce skončil trojský kůň Spy.Agent.AES, kterým útočníci stejně jako u předešlého získávají přístupové údaje z prohlížečů Chrome a Firefox. A na třetím místě se umístil trojský kůň CoinMiner.RX, pomocí kterého pachatelé těží kryptoměny. [29]

Obrázek 7: Internetové hrozby v ČR



Zdroj: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/nejvaznejsihrozbou-pro-ceske-uzivatele-zustavaji-trojske-kone-kradouci-hesla/

U napadeného zařízení trojským koněm dochází k zatížení procesoru a tím k výraznému zpomalení zařízení. Ke snížení rizika napadení je doporučeno neotvírat neznáme přílohy e-mailu. Trojské koně jsou nejčastěji součástí příloh s příponami .exe, .vbs, .bat. Také se doporučuje využívat funkci firewall a být ostražitý při využívání webů nabízejících bezplatné filmy či hry. [30]

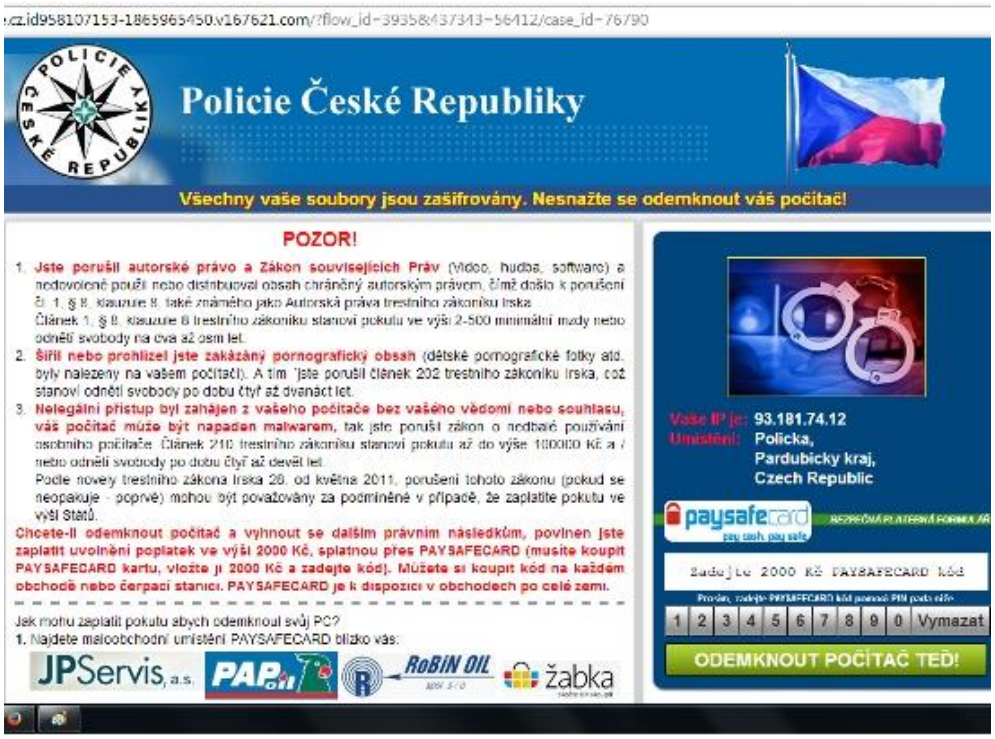
6.2.6 Ransomware

Jedná se o tzv. vyděračský malware, který zamezí uživateli přístup k jejich počítačovému systému nebo datům. Následně za obnovení přístupu vyžaduje výkupné. [13]

Kolouch (2016) uvádí, že nástup velkého počtu ransomware proběhl v roce 2011, kdy se celosvětově šířil tzv. „policejní“ ransomware. První verze tohoto ransomware se v České republice objevila právě koncem roku 2011, může se však objevit i dnes. Jedná se o typ ransomware, který se zobrazí při navštěvování webových stránek. Útok spočívá v zobrazení

nového okna prohlížeče, kde je uživatel nařknut za prohlížení nevhodného obsahu, viz Obrázek 8. Poté dochází k zablokování osobních dat nebo jen daného prohlížeče a pro odblokování je vyžadováno zaplacení částky, která se v České republice běžně pohybuje v rozmezí 2 000-4 000 Kč. Ačkoliv se to může zdát zarážející, tuto částku někteří uživatelé skutečně zaplatili, aniž by si ověřili, komu peníze odesílají. [13, 31]

Obrázek 8: Policejní ransomware



Zdroj: *https://www.policie.cz/clanek/objevuje-se-vam-na-monitoru-podezrele-hlaseni.aspx*

František Doupal (2020) ve svém článku uvádí, že největší nárůst ransomwarů proběhl v roce 2017. V té době se šířil zejména ransomware WannaCry, který napadl více než 230 000 počítačů s Windows po celém světě a jedná se tak o největší útok s využitím tohoto malware. K napadení došlo také ve státních úřadech a nemocnicích. Napadení WannaCry (označován také WanaCryptOr 2.0) způsobí zašifrování souborů a narozdíl od běžných ransomwarů vyžaduje výkupné v bitcoinech.

Následně však začali firmy a jednotliví uživatelé investovat do ochrany proti tomuto malware a jeho výskyt tak začal klesat. Doupal (2020) uvádí, že se v roce 2019 v České republice výrazně snížil počet napadení ransomwarem, ale i přesto zůstává rizikový pro uživatele i firmy. Také přidává následující vysvětlení Martina Jirkala, vedoucího analytického

oddělení pražské pobočky ESETu: *„Důvodem poklesu detekcí ransomware byl zřejmě náročný vývoj a z toho plynoucí nižší zisky útočníků. Řada firem má dnes kvalitně řešené zálohy a platit výkupné tak jednoduše nemusí. Ke konci roku se však objevilo několik výrazných útoků cílených na Českou republiku, které získaly významnou mediální pozornost, a může se jednat o začátek nového trendu, kdy se s ransomwarem začneme potkávat opět častěji.“* [32]

K napadení nemusí docházet jen u počítače, ale také u mobilních telefonů, serverů či u IoT (Internet věcí). Napadený uživatel odhalí ransomware celkem jednodušše, nejčastěji nebude mít přístup ke svým souborům. K nákaze většinou dochází přes e-mail, konkrétně stažením nevhodné přílohy nebo kliknutím na odkaz, který je obsažen ve zprávě e-mailu.

Jako vhodná ochrana před tímto napadením je ostražitost při stahování e-mailových příloh. U firem je vhodné školení zaměstnanců, jak rozpoznat nevhodné e-maily. Dále využití softwarové ochrany, aktualizace softwaru a operačního systému. Některé firmy často mají zabezpečení za stovky tisíc korun, ale už nemají člověka, který by se o daný software a aktualizace staral. Proto i u takových firem může dojít k napadení. [33]

6.3 Spamming

Téměř každý uživatel využívající e-mail musel ve své schránce nalézt nevyžádanou poštu, která se nazývá spam.

Kolouch (2016) definuje spam jako: „*hromadné šíření nevyžádaného sdělení nejčastěji reklamního charakteru pomocí Internetu, nejčastěji prostřednictvím elektronické komunikace.“* Dále uvádí, že se jedná o veškerou nevyžádanou poštu, například zprávy obsahující viry, trojské koně apod. [13]

Ačkoliv se spam nemusí jevit nebezpečně, není to vždy pravda. Obsahem spamových e-mailů totiž může být malware. Pravidelný příjem nesmyslných zpráv a reklam je pro uživatele mnohdy obtěžující, zejména když dostává stejnou zprávu několikrát týdně. Při rozesílání spamů také dochází k zatěžování linek a serverů, a to i přesto, že jejich výkonnost stále roste. [34]

Pokud se nevyžádaná pošta objeví v e-mailové schránce, je vhodné ji vůbec neotevírat, nahlásit a následně smazat. Uživatelé by měli být ostražití při zveřejňování e-mailové adresy. Pokud však uživatel musí uvést svou e-mailovou adresu, je vhodné ji uvádět v následujícím tvaru: „název(zavináč)doména.cz.“ Je to kvůli programům, které sbírají e-mailové adresy za účelem zasílání spamu, nicméně takto zadanou adresu přeskočí. Častým problémem příchozího spamu bývá nepozornost při registraci v jakékoliv internetové službě, kdy uživatelé odsouhlasí zasílání reklamního sdělení. Zbavení takového spamu bývá velice jednoduché, většinou se stačí pouze odhlásit od těchto oznámení a znovu nepřijdou. [35]

Jirovký (2007) uvádí, že přes všechna opatření a návrhy vydané proti spamu, je jeho nárůst téměř nezastavitelný. [2]

Jak jsou na tom Češi se spamem?

Podle výzkumu společnosti Mailkit z roku 2018, který zveřejnil portál tyinternety.cz, přijde 28 % Čechů maximálně 5 spamů týdně. Stejnému procentu lidí za stejné období dorazí 6-15 spamů. 32 % lidí najde ve své schránce 16-50 spamů a více jak 51 spamů obdrží 12 % dotázaných.

Jako nejčastější metodu boje proti spamu Češi využívají označení zprávy jako spam. Takto se zachová 68 % dotázaných, 66 % si nastaví pravidla pro ukládání spamu v e-mailové schránce. 63 % lidí se odhlásí od obdržování zpráv odesílatele. Dalších 21 % e-mail pouze smaže. 14 % dotázaných kontaktuje odesílatele, aby jim přestal zprávy posílat a 0,8 % Čechů podalo stížnost na úřad pro ochranu osobních údajů. [36]

6.3.1 Hoax

Jedná se o poplašnou zprávu, která se šíří internetovou komunikací. Nejčastěji varuje před neexistujícím nebezpečím, prosí o pomoc nebo chce pouze pobavit. Za hoax je považována také šířená zpráva, která obsahuje nepřesné informace nebo účelové lži. Hoax je řetězová zpráva, to znamená, že obsahuje výzvu k přeposlání zprávy dalším přátelům. Zejména podle této výzvy se nejčastěji pozná, že jde právě o hoax.

Účely rozesílání hoaxu mohou být různé. Většinou jde však o vyvolání strachu, šíření falešných rad, poškození dané společnosti nebo pouze o přilákání pozornosti. [37]

Pokud uživatel obdrží poplašnou zprávu, jako první by si měl ověřit její pravdivost. Dále je vhodné informovat a ponaučit uživatele, který tuto zprávu odeslal. Někteří lidé totiž bez přemýšlení zprávu s nepravdivými informace rozesílají dále, aniž by si to sami uvědomili. Jakmile se však potvrdí, že se jedná o hoax, je vhodné zprávu smazat nebo označit jako spam a dále ji hlavně nepřeposílat. [37, 38]

Šíření hoaxu v České republice

Portál e-bezpeci.cz zveřejnil výzkum z roku 2017, kterého se zúčastnilo 1072 lidí a zabýval se šířením hoaxů. E-maily, které varují před nebezpečím šíří 35 % osob ve věku 55-64 let a 47 % dotázaných starších 65 let, což je čtyřikrát více než u lidí ve věku 35-44 let. Pravdivé i nepravdivé zprávy o politickém dění šíří senioři šestkrát více než osoby mladší. Z výzkumu tedy plyne, že nejaktivnějšími šiřiteli jsou senioři starší 65 let.

Podle vysvětlení Mgr. Kamila Kopeckého zveřejněného na stejném portálu je to dané tím, že si senioři informace, které sami šíří, vůbec neoveřují a věří odesílateli. Proto lze starší uživatele snadno ovlivnit a ti následně ovlivňují své přátelé šířením hoaxu. [39]

Dle portálu internetembezpecne.cz se oběťmi hoaxu často stávají děti, protože si neověřují informace získané z Internetu a následně šíří nesmyslné a nepravdivé zprávy dál. [37]

6.4 Warez

Warez je dle Rosteckého (2012): *„slangové označení pro činnost šířící a odstraňující ochranné prvky autorských děl, včetně jejich používání, šíření a jiné nakládání v* rozporu s *autorských právem. Jinými slovy je to používání, šíření a upravování software a obcházení tak nutnosti zaplatit si všechny jeho funkce.“* [40]

Jirovský (2007) tvrdí, že se jedná o trestnou činnost, která je delší než historie Internetu. K prvnímu kopírování hudby docházelo pomocí audio kazet a k pirátskému šíření

filmů sloužily videokazety. Dále uvádí, že opravdový nástup warezu přišel až s rozvojem rychlého Internetu. V dnešní době je možné získat pirátské kopie i týdny před vydáním originálu. [2]

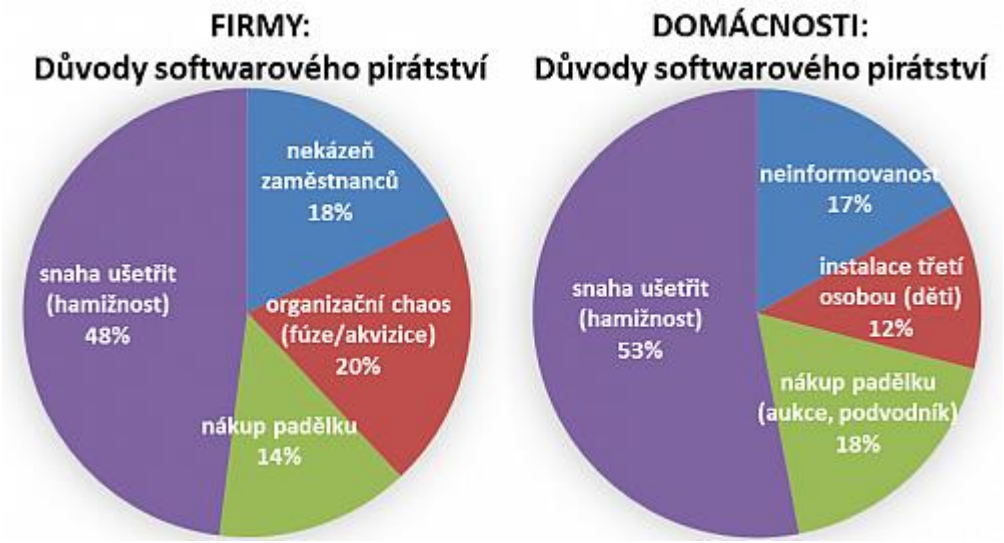
Legálností warezu v České republice se zabývá následující článek z portálu myprovas.cz: *„V Česku je kopírování (tedy i stahování) autorských děl (nikoli však softwaru či databází) pro vlastní (osobní) potřebu zcela legální. Nelegální je však šíření (sdělování veřejnosti) takových děl bez povolení autora. Takové počínání je dle autorského zákona trestný čin (Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi, § 270 TrZ), který se trestá odnětím svobody až na dvě léta (nebo na šest měsíců až pět let, pokud tak pachatel konal ve značném rozsahu) nebo peněžitým trestem nebo propadnutím věci. Použití jiného autorského díla než programu či elektronické databáze pro vlastní potřebu je v Česku zcela legální i bez svolení autora. Tedy např. stažením filmu a jeho užitím pro vlastní potřebu není český zákon porušen, třebaže film je šířen v rozporu se zákonem.“* [41]

6.4.1 Proč Češi používají warez?

Průzkum protipirátské organizace BSA (Business Software Alliance), který zveřejnil v roce 2016 portál cnews.cz, se zabýval zjištěním důvodu, proč české domácnosti a firmy využívají nelegální software. Bylo zjištěno, že hlavním důvodem je u obou případů ušetření peněz. V domácnostech se snaží ušetřit 53 % lidí a ve firmách 48 %, dále viz Obrázek 9. Častým problémem v domácnostech bývá neinformovanost. Někdy lidé ani nevědí, že používají warez, protože ho stáhly nebo nainstalovaly děti. Ve firmách bývají častým problémem zaměstnanci, kteří nelegální software přinášejí. Dalším a zároveň nebezpečným problémem je nákup padělku, kdy si jednotlivci nebo firmy pořídí levnější software, ale ve skutečnosti se jedná o pirátskou kopii.

Na stejném portálu je také následující vyjádření BSA k této problematice: *„Nejčastěji se pirátsky užívá kancelářský software a operační systémy (výrobce Microsoft), grafické a návrhářské programy (Adobe), CAD aplikace (Autodesk) či utility, například antivirové systémy (Symantec). Stíhané firmy mají většinou méně než 150 zaměstnanců a podnikají v oblasti služeb, výroby, designu, inženýrství a architektury.“* [42]

Obrázek 9: Důvody softwarového pirátství v ČR



Zdroj: https://www.cnews.cz/proc-warez-polovina-domacnosti-i-firem-pirati-proto-ze-se-jim-za-software-nechce-platit/

6.5 Phishing

Phishing neboli rhybaření označuje podvodné jednání, které slouží k získání citlivých údajů uživatele, nejčastěji za účelem obohacení pachatele. Nejčastěji jsou to přihlašovací údaje k různým webům, jindy to mohou být čísla platebních karet. K získávání údajů pachatelé využívají falešné webové stránky (např. web internetového bankovnictví), kde se uživatel přihlásí. Další možností je vyžadování údajů napřímo, tzn. zaslání formuláře s požadavkem k jeho vyplnění. Dle Koloucha (2016) není phishing zaměřen pouze na e-maily, ale je využíván i v rámci sociálních sítí, SMS a MMS zpráv, instant messages (Skype, ICQ), atd. [13, 43]

6.5.1 Princip útoku

V prvotní fázi je využita metoda sociálního inženýrství, které je dle Jirovského (2007) definováno jako: *„umění, jak přimět ostatní lidi, aby splnili Vaše přání.“* Samotným principem útoku je věrohodné napodobení žádosti, např. banky a následné „donucení“ k vyplnění přihlašovacích údajů oběti. Tyto zprávy obsahující žádosti jsou nejčastěji odesílány e-mailem. Součástí e-mailu (spamu) je také odkaz, který uživatele přesune na falešné webové stránky zmíněné instituce, kde je vyžadováno přihlášení uživatele. Pokud uživatel vyplní své přihlašovací údaje, v podstatě je předává pachateli a ten je může využít ke

svému prospěchu. Falešné webové stránky je velice obtížné rozeznat od skutečných, a proto i zkušení uživatele mohou být napadeni touto formou útoku. [2, 43]

Dle portálu internetembezpecne.cz lze kombinaci spamu obsahujícího sociální inženýrství a následného phishingu označit za jednu ze spolehlivých cest k osobním údajům oběti, a to včetně přístupů do bankovních účtů. [43]

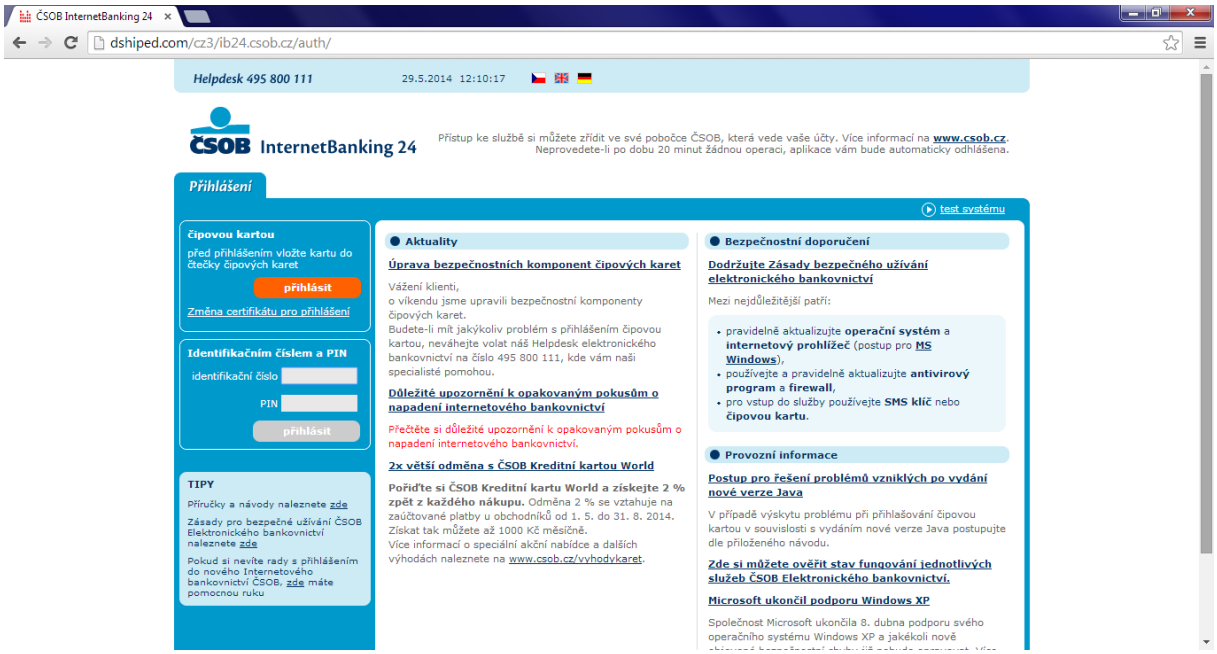
6.5.2 Ukázka phishingového útoku

Následující obrázky ukazují konkrétní útoky phishingu. Na Obrázku 10 je vidět využití metody sociálního inženýrství a odkaz na falešný web. Na Obrázku 11 a Obrázku 12 je porovnání skutečných a falešných webových stránek ČSOB.

Obrázek 10: Phishingový e-mail

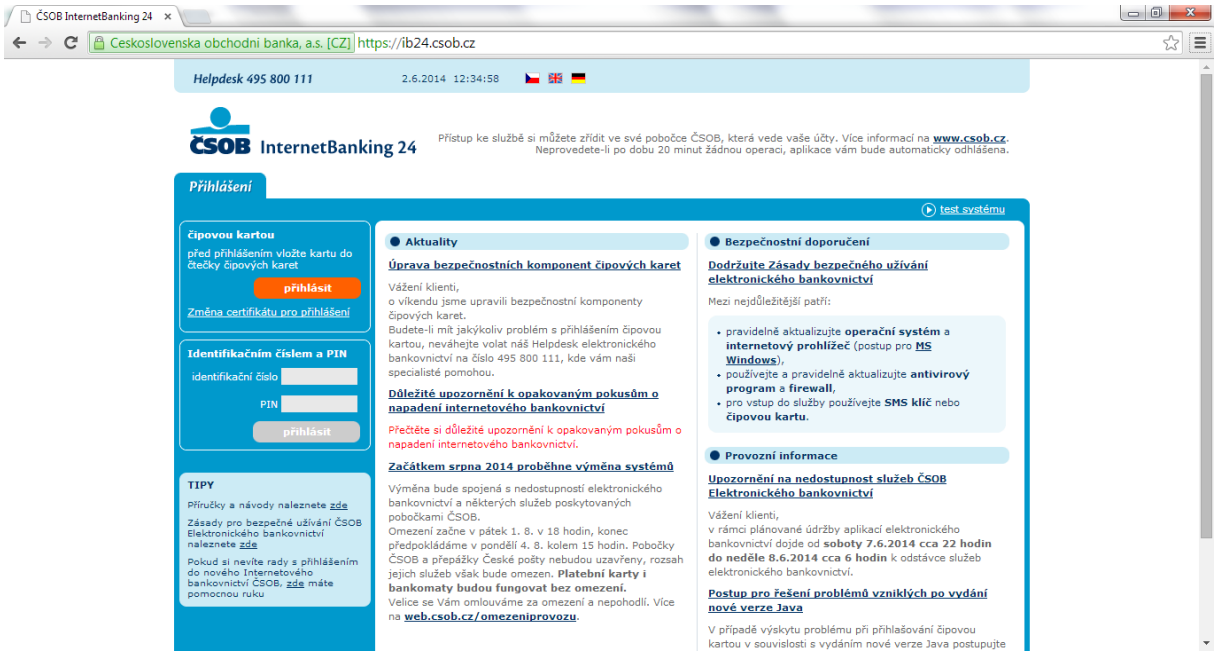
Zdroj: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/

Obrázek 11: Ukázka falešný webových stránek ČSOB



Zdroj: https://support.zcu.cz/images/4/48/Novinka-PhishingCSOB-2.png

Obrázek 12: Skutečné webové stránky ČSOB



Zdroj: https://support.zcu.cz/images/6/6f/Novinka-PhishingCSOB-1.png

Na první pohled není rozdíl webových stránek viditelný, nicméně falešný web lze poznat dle URL adresy a ověření certifikátu.

6.5.3 Proč je phishing stále tak nebezpečný a jak se chránit?

Společnost ESET se problematikou a nebezpečím phishingu zabývá v jednom ze svých článků. Uvádí, že v roce 2018 stál phishing za třetinou bezpečnostních incidentů ve firmách, a to i přesto, že se poskytovatele elektronických stránek snaží uživatele chránit. Jen společnost Google každý den zablokuje více než 100 miliónů phishingových e-mailů.

Útoky phishingem jsou preciznější a neustále se vyvíjí, a to je hlavním důvodem, proč se uživatelé stávají oběťmi. Dalším důvodem je umění přesvědčit v e-mailu, a i to se daří, protože se z útočníků stali dobří manipulátoři. Existují různé faktory, které dokážou napadení ovlivnit. „*Například, jsme-li v dobré náladě a hormonální hladina oxytocinu, serotoninu a dopaminu je vysoká, je pravděpodobnější, že budeme podvedeni. Když je ale vysoká hladina kortizolu (obvykle to je spojeno se stresem), budeme opatrnější a ostražitější*.“ [44]

Jako vhodná ochrana před phishingem je kontrola webové adresy, kde se uživatel nachází a vyplňuje své údaje. Je dobré si uvědomit, že banka ani žádná podobná instituce nikdy po uživateli nevyžaduje žádné z osobních údajů prostřednictvím e-mailu. Ověřením odesílatele nebo smazáním podezřelého e-mailu se také snižuje riziko napadení. Phishingové útoky ze zahraničí se nejčastěji poznají podle špatné češtiny v textu. V některých případech může pomoci i prohlížeč, který upozorní, že se jedná o phishing. [43]

6.6 Kyberšikana

Podle portálu internetembezpecne.cz je definována jako: *„Druh šikany využívající informační a komunikační technologie (počítače, tablety, mobilní telefony, sociální sítě, emaily apod.) k ublížení druhému (vydírání, ubližování, ztrapňování, obtěžování, ohrožování, zastrašování apod.).“* Její cíl je tedy stejný jako u klasické šikany-ublížit. Problémem ale je, že ve virtuálním prostředí jsou mnohdy pachateli k dispozici nástroje, které mohou mít na oběť mnohem větší dopad než v reálném světě. Často také dochází k propojení kyberšikany a klasické šikany. Typickým příkladem je umístění videa či fotky, jejíž obsahem je fyzické napadení oběti, na web. [13, 45]

Kolouch (2016) uvádí následující projevy kyberšikany:

1. Pomlouvání, zastrašování, urážení, zesměšňování, či jiné ztrapňování (sociální sítě, e-mail, SMS, chat, ICQ, Skype, hry aj.).
2. Pořizování zvukových záznamů, videí či fotografií, jejich grafické či jiné upravování a následné zveřejňování s cílem poškodit (zesměšnit) vybranou osobu.
3. Natáčení a zveřejnění videí, při kterých je oběť napadána fyzicky či jinak psychicky týrana a zesměšňována.
4. Vytváření internetových stránek, sociálních účtů (úprava původních či vytváření nových profilů), diskusních portálů, které urážejí, pomlouvají nebo ponižují konkrétní osobu.
5. Zneužívání cizího účtu-krádež identity (e-mailového, diskuzního apod.)
6. Provokování a napadání uživatelů v diskuzních fórech, tapetování (chatovací místnosti apod.)
7. Odhalování cizích tajemství.
8. Vydírání pomocí mobilního telefonu nebo Internetu.
9. Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním. [13]

Kvůli anonymitě jsou pachatele kyberšikany na Internetu často odvážnějšími než v reálném světě. Mnohdy využívají falešná jména, vytvářejí si falešné profily na sociálních sítích a následně používají agresivnější formy útoky. Nicméně odhalení takového pachatele není v dnešní době pro Policii ČR problém. Problémem může být pouze to, že kyberšikana není právně nijak vymezena. Proto může být pro policejní orgán obtížné získat důkazní materiál. [45]

6.6.1 Výzkum rizikového chování dětí na Internetu

Tento výzkum realizoval v roce 2014 projekt e-bezpečí a zúčastnilo se ho 28 232 dětí, z toho bylo 55,54 % ve věku 11-14 let a 44,46 % ve věku 15-17 let. Celkem se obětí kyberšikany stalo 50,90 % dětí. Nejčastěji se jednalo o průnik na účet (34,80 %), verbální útoky (34,33 %) a obtěžování prozváněním (26,36 %). 54,30 % dotázaných komunikuje s neznámými lidmi přes Internet a 40,22 % dotázaných by bylo schopno jít na schůzku s

„kamarádem“ z Internetu. Takové jednání považuje za nebezpečné a riskantní 58,25 % dětí. [46]

7 Legislativa v České republice

Českou legislativu v oblasti kybernetické kriminality upravuje zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších změn a předpisů. Tento zákon vstoupil v platnost 1.1.2010. Většina trestných činů proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů je zasazena v Trestním zákoníku do hlavy V-Trestné činy proti majetku. [47]

Policie ČR na svém webu uvádí nejčastější trestné činy kybernetické kriminality s odkazem na trestní zákoník:

1. Trestné činy upravené zákonem č. 40/2009 Sb., o trestní zákoník, ve znění pozdějších změn a předpisů, páchané ve vztahu k datům (uloženým informacím):
    - Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230),
    - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231),
    - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232)

2. Trestné činy upravené zákonem č. 40/2009 Sb., o trestní zákoník, ve znění pozdějších změn a předpisů, páchané ve vztahu k datům (uloženým informacím), při nichž je počítač prostředkem k jejich páchání:
    - Šíření pornografie (§ 191),
    - Výroba a jiné nakládání s dětskou pornografií (§ 192),
    - Navazování nedovolených kontaktů s dítětem (§ 193b),
    - Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270),
    - Hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355),
    - Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§356),
    - Šíření poplašné zprávy (§ 357),
    - Pomluva (§ 184),
    - Vydírání (§ 175), a mnohé další. [47]

V předešlých ustanoveních implementuje trestní zákoník závazky z Úmluvy Rady Evropy o kybernetické kriminalitě, což je nejvýznamnější právní dokument týkající se kyberkriminality a vznikl za účelem sjednocení národní právní úpravy právě v této oblasti. Česká republika podepsala Úmluvu o kyberkriminalitě 9.2.2005 a v platnost v ČR vstoupila 1.12.2013. [13, 47]

Kolouch (2016) uvádí mimo zákon č. 40/2009 Sb., trestní zákoník i následující právní normy ČR, které mají vztah k problematice kyberkriminality:

- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízeni proti nim
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích navrzích
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon kybernetické bezpečnosti) [13]

8 Projekty a organizace bojující proti internetové kriminalitě

8.1 BSA | The Software Alliance

BSA | The Software Alliance je světová organizace, která se zabývá legálním využíváním softwaru a podporou růstu digitální ekonomiky. Také hájí zájmy softwarového odvětví u vlád a na mezinárodním trhu. BSA sídlí ve Washingtonu DC a působí ve více než šedesáti zemích. V České republice byla její pobočka již zrušena. Jejími členy jsou společnosti, které vyvíjejí software zlepšující moderní život. Mezi nejznámější patří Microsoft, Adobe, Intel, IBM a mnoho dalších. [48]

BSA se také zaměřuje na připravenost vlády čelit kybernetickým bezpečnostním hrozbám. To dle portálu bsa.org zahrnuje partnerství mezi veřejnými a soukromými entitami, posilování kybernetické bezpečnosti na pracovištích, zavádění rámců efektivního sdílení informací, politiku podporující rozvoj špičkových technologií kybernetické bezpečnosti a další kroky pro zabezpečení a ochranu informační infrastruktury. [49]

Stejný portál také upozorňuje, že pokud české firmy chtějí snížit riziko kybernetických útoků, měly by ze své počítačové sítě odstranit veškerý nelegální software. [50]

8.2 Evropské centrum pro kyberkriminalitu (EC3)

Toto centrum bylo zřízeno v roce 2013 Evropským policejním úřadem neboli Europolem. Cílem centra je posílit reakci orgánů na počítačovou trestnou činnost v EU. Tím chce pomoci chránit evropské občany, podniky a vlády před online trestnou činností.

EC3 se zaměřuje na následující typy kybernetické kriminality:

- Kybernetický zločin
- Sexuální zneužívání dětí
- Platební podvody

Od svého založení EC3 analyzovalo stovky tisíc souborů, z nichž byla většina škodlivá, a tím se významně podílelo na boji proti kyberkriminalitě. Centrum se také podílelo na

desítkách významných operací a stovkách nasazení, které vedlo k zatčení mnoha pachatelů. [51]

8.3 Projekt Internetem Bezpečně

Jedná se o projekt, jehož cílem je na základě různých vzdělávacích aktivit zvýšit povědomí uživatelů o nebezpečí v internetovém prostředí. Zaměřuje se na nové hrozby v online prostředí, o kterých informuje na svých webových stránkách a vzdělávacích akcích. Tím se snaží předcházet nebezpečným následkům těchto hrozeb, případně snížit počet útoků páchaných v kyberprostoru. Cílové skupiny projektu jsou děti a máděž, rodiče, pedagogové, pracovníci bezpečnostních složek a mnoho dalších.

Na svých webových stránkách internetembezpecne.cz uvádí následující vzdělávací aktivity, které jsou nezbytnou součástí projektu:

- provoz webových stránek internetembezpecne.cz,
- provoz facebookové stránky Internetem Bezpečně,
- realizace odborných přednášek,
- vydávání odborných publikací a dalších vzdělávacích materiálů.

V rámci těchto aktivit využívají moderní výukové metody a trendy. Součástí jsou také praktické ukázky kybernetických hrozeb a konkrétní návody, jak se před nimi bránit. [52]

8.4 Projekt E-Bezpečí

Jde o celorepublikový certifikovaný projekt, který se zabývá vzděláním, výzkumem a prevencí v oblasti rizikového chování na Internetu. V posledních letech se také zaměřuje na pozitivní využití informačních technologií ve vzdělání a běžném životě.

Základní činnosti projektu E-Bezpečí jsou terénní práce s různými cílovými skupinami, odborné přednášky, vzdělávací akce apod. Projekt je zaměřen zejména na žáky a studenty (od 1. stupně ZŠ), učitele, policisty, vychovatele a také rodiče. Mezi jeho hlavní specializace patří zejména:

- kyberšikana a sexting,
- kybergrooming (komunikace s neznámými uživateli internetu vedoucí k osobní schůzce),

- kyberstalking a stalking (nebezpečné pronásledování s použitím ICT),
- rizika sociálních sítí (zejména Facebook),
- hoax, spam a další.

Projekt mimo jiné také realizuje pravidelné celorepublikové výzkumy, které jsou zaměřené na rizikovou komunikaci v online prostředí. Dále také provozuje online poradnu a vydává řadu zajímavých tiskovin pro žáky a učitele. [53]

8.4.1 Současnost

Projekt E-Bezpečí je v současnosti národním preventivním projektem, který poskytuje pomoc velkému počtu uživatelů Internetu. Také nabízí pomoc obětem, které se kvůli internetovému prostředí dostali do obtížné situace a je důležitou součástí v oblasti prevence online kriminality. Jedná se o uznávaný projekt podporovaný ministerstvem vnitra, ministerstvem školství a Policií ČR.

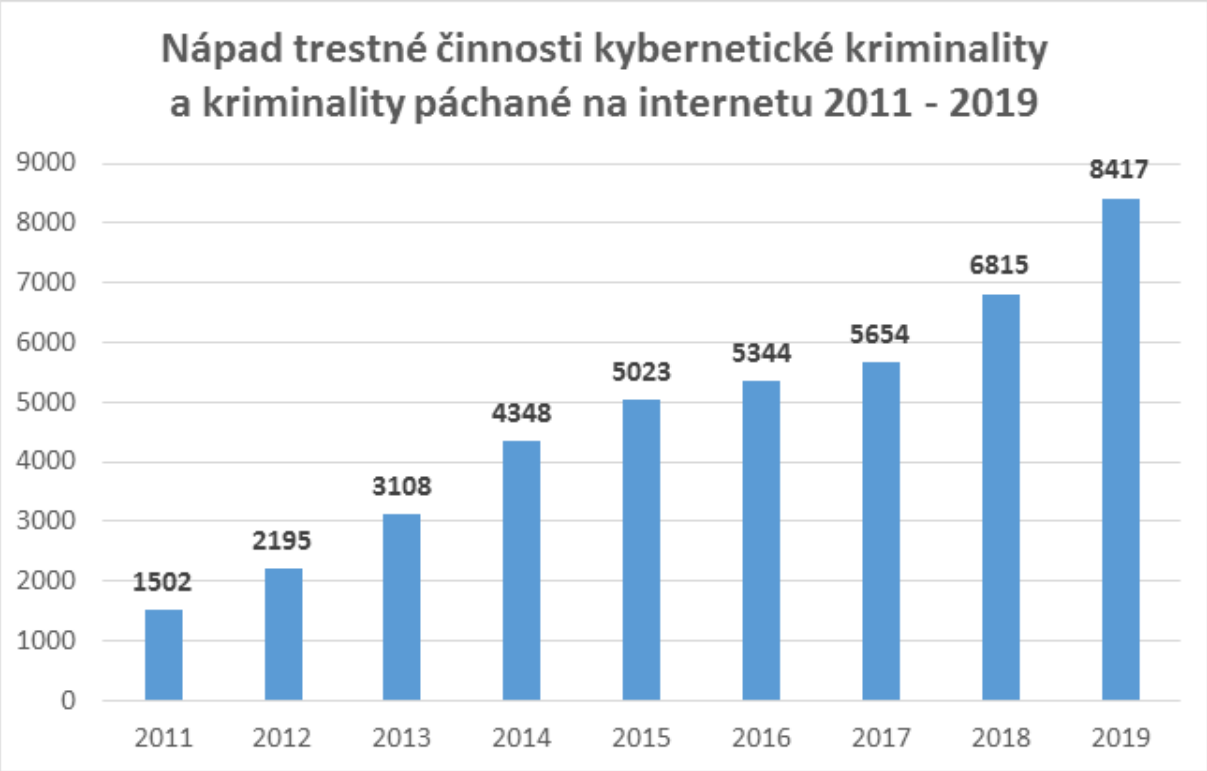
Doposud výcvikem projektu E-Bezpečí prošlo více než 60 000 žáků základních a středních škol, proškoleno bylo přes 10 000 zaměstnanců a pomoc byla poskytnu více než 2 500 obětem kybernetické kriminality. [53]

9 Závěr

Využívání Internetu a informačních technologií má pro lidstvo velký přínos a jejich vývoj jde neustále dopředu. Přesto však s jejich používáním přicházejí také oběti internetové kriminality. Mnoho uživatelů si ani neuvědomuje rizika a nebezpečí spojená s online prostředím.

Internetová kriminalita je celosvětovým problémem a počet jejích obětí se neustále zvyšuje. Přibývající počet trestných činů v síti Internet lze pozorovat i v České republice. Touto problematikou se zabývá Policie ČR, která přesná čísla znázorňuje ve svém grafu, viz. Obrázek 13. Oběťmi nejsou pouze jednotliví uživatelé, ale i vlády, velké společnosti, nebo také státy. Na téma internetová kriminalita již bylo vydáno mnoho publikací, článků a ostatní literatury, z toho je patrné, že se veřejnost touto problematikou zabývá.

Obrázek 13: Graf internetové kriminality v ČR



Zdroj: https://www.policie.cz/clanek/kyberkriminalita.aspx

Tato bakalářská práce popisuje historii vzniku Internetu společně s jeho rozvojem v České republice, uvádí problematiku nejběžnějších typů kriminality, jejich pachatele a účinnou obranu proti těmto napadením. Pro názornou ukázku jsou v práci vloženy obrázky s

jednotlivými typy napadení spojené s internetovou kriminalitou. V další části je uvedena česká legislativa zahrnující trestné úkony proti těmto zločinům.

Cílem této práce bylo upozornit uživatele Internetu na stále rostoucí hrozby možného nebezpečí spojené s jeho používáním a také vytvořit přehled vybraných druhů internetové kriminality. Cíl práce byl tedy splněn.

Jako preventivní opatření proti internetové kriminalitě je doporučeno používat antivirové programy, nenavštěvovat neznámé internetové stránky, také stránky s nevhodným obsahem, neotervírat internetovou poštu bez uvedeného adresáta, či poštu se zavádějícím jménem adresáta. V oblasti Internetu se pohybovat ostražitě, jelikož je toto prostředí nebezpečné jako každé jiné. Ani jedno z tohoto doporučení nezaručuje stoprocentní ochranu, ale je lepší se chránit alespoň nějakým způsobem než vůbec.

Na úplný závěr bych chtěl uvést svůj osobní názor, že se internetovou kriminalitu nikdy nepovede zcela odstranit, stejně jako jiné druhy kriminality, ale je důležité ji omezit a umět se před ní bránit. V současné době žijeme každý na velmi slušné materiální úrovni, kdy je dostatek práce, jídla a také finančních prostředků. Mnoho lidí v České republice si nedovede představit život bez mobilních telefonů, počítačů nebo jiných technologií s přístupem k Internetu. V budoucnosti bude mít tento trend tendenci vzrůstat a mnohem více lidí bude využívat internetové služby, což bude pro pachatelele znamenat více obětí jejich činů. Bohužel si myslím, že období stabilní situace brzy skončí a v nejbližší době přijde ekonomická krize, která zapříčiní, že trestná činnost v rámci oblasti Internetu bude páchána v mnohem větší míře, než byla páchána doposud.

Jak již dnes můžeme pozorovat v rámci šíření viru COVID-19 se ekonomika nejen České republiky, ale i okolních států bortí. Lidé nemohou chodit do práce, děti do škol, jsou uzavřeny hranice, tudíž země trpí také nedostatkem financí z cestovního ruchu. Lidé, kteří jsou nuceni být doma v karanténě si svůj čas krátí sledováním online filmů či videí, nakupují přes Internet, svou práci řídí z domova a komunikují pomocí internetové pošty a své pohledávky hradí pomocí internetového či mobilního bankovnictví. Všechny tyto činnosti usnadňují pachatelům vykonávat jejich činy. Z tohoto důvodu usuzuji, že to nejhorší v oblasti

internetové kriminality je stále před námi a nebude trvat dlouho, kdy nás tato velmi nepříjemná situace dostihne.

10 Literatura

1) HRSTKA, Jaroslav. Historie a počátky Internetu. *Sdělovací technika: telekomunikace, elektronika, multimédia*. Praha: Sdělovací technika. 2014, 8-12, ISSN 0036-9942.
2) JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s, 2007. ISBN 978-80-247-1561-2.
3) ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-758-5
4) KODÝTEK, Pavel. *Historie Internetu* [online]. [cit. 20.12.2019]. Dostupné z: http://www.webdesign.paysoft.cz/clanky/2006/historie-internetu/
5) *Internet* [online encyklopedie]. [cit. 2.2.2020]. Dostupné z: https://cs.wikipedia.org/wiki/Internet
6) HAUBEN, Michael. *Historie sítě ARPANET/Internet* [ebook]. 2003 [cit. 4.2.2020].
7) ZANDL, Patrick. *Historie českého Internetu II*. [online]. 2003 [cit. 4.2.2020]. Dostupné z: https://www.lupa.cz/clanky/historie-ceskeho-internetu-ii/
8) CHLAD, Radim. *Historie internetu v České republice* [online]. [cit 5.2.2020]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm?fbclid=IwAR0UV7_1ziow3Zx-SCk78TRotGnvmVhp2nK7DVtwy-w-ZVsfJcCeBeC6PyM
9) POLICIE ČR. *Kyberkriminalita* [online]. [cit 7.2.2020]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
10) HAVLOVÁ, Alžběta, Ondřej BOUDA a Marína DVOŘÁKOVÁ. *Crackeči a hackeři: Jedni na internetu kradou, druzí jen protestují* [online]. 2013 [cit 9.2.2020]. Dostupné z: https://www.irozhlas.cz/veda-technologie_technologie/crackeri-a-hackeri-jedni-na-internetu-kradou-druzi-jen-protestuji_201303120538_kpracharova
11) LÁTAL, Ivo. *Počítačová (informační) kriminalita a úloha policisty při jejím řesení* [online]. 1998 [cit. 8.2.2020]. Dostupné z: http://www.scritub.com/limba/ceha-slovaca/Potaov-informan-kriminalita-a-1513463.php
12) S. RAYMOND, Eric. *Jak se stát hackerem* [ebook]. 2004 [cit 10.2.2020].
13) KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8.
14) KOSPERTOVÁ, Lenka. *Nejslavnější hackeři světa: začali útočit už v dětském věku!* [online]. 2017 [cit. 14.2.2020]. Dostupné z: https://epochaplus.cz/nejslavnejsi-hackeri-sveta-zacali-utocit-uz-v-detskem-veku/

15) OLSONOVÁ, Parmy. *Jsme Anonymous*. Praha: Práh, 2012. ISBN 978-80-7252-400-6.
16) VONDRUŠKA, Pavel. *Hackeři, Crackeči, Rhybáři a Lamy? (2. díl)* [online]. 2004 [cit.18.2.2020]. Dostupné z: https://www.idnes.cz/technet/software/hackeri-crackeri-rhybari-a-lamy-2-dil.A040812_5271894_bezpecnost
17) MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. ISBN 80-7226-419-2.
18) ELLISON, Keith. *Internet Safety: How to Protect Yourself Against Hackers* [online]. [cit. 25.2.2020]. Dostupné z: https://www.ag.state.mn.us/Consumer/Publications/HowtoProtectYourselfAgainstHackers.asp
19) ESET software spol. s.r.o. *Malware* [online]. [cit. 25.2.2020]. Dostupné z: https://www.eset.com/cz/malware/
20) AVAST Software s.r.o. *Spyware* [online]. [cit. 26.2.2020]. Dostupné z: https://www.avast.com/cs-cz/c-spyware
21) AVAST Software s.r.o. *Keylogger* [online]. [cit. 26.2.2020]. Dostupné z: https://www.avast.com/cs-cz/c-keylogger
22) Keylogger, *Internetem Bezpečně* [online], [cit. 26.2.2020]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/keylogger/
23) AVAST Software s.r.o. *Adware* [online]. [cit. 26.2.2020]. Dostupné z: https://www.avast.com/cs-cz/c-adware
24) AVAST Software s.r.o. *Počítačový virus* [online]. [cit. 27.2.2020]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus
25) MATĚJÍČEK, Pavel. *Deset nejznámějších virů historie* [online]. 2018 [cit. 27.2.2020]. Dostupné z: https://computerworld.cz/software/deset-nejznamejsich-viru-historie-54722
26) POČÍTAČOVÉ VIRY, ČERVI A TROJSKÉ KONĚ, *Internetem Bezpečně* [online], [cit. 27.2.2020]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/
27) AVAST Software s.r.o. *Počítačový červ* [online]. [cit. 28.2.2020]. Dostupné z: https://www.avast.com/cs-cz/c-computer-worm
28) *TROJAN: All about Trojans* [online]. [cit. 28.2.2020]. Dostupné z: https://www.malwarebytes.com/trojan/

29) ESET software spol. s.r.o. *Nejvážnější hrozbou pro české uživatele zůstávají trojské koně kradoucí hesla* [online]. [cit. 1.3.2020]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/nejvaznejsi-hrozbou-pro-ceske-uzivatele-zustavaji-trojske-kone-kradouci-hesla/
30) AVAST Software s.r.o. *Trojský kůň* [online]. [cit. 1.3.2020]. Dostupné z: https://www.avast.com/cs-cz/c-trojan
31) Ransomware, *Internetem Bezpečně* [online]. [cit. 2.3.2020]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/ransomware/
32) DOUPAL, František. *Jak se vyvíjel malware v České republice v roce 2019?* [online]. 2020 [cit. 3.3.2020]. Dostupné z: https://www.rmol.cz/novinky/jak-se-vyvijel-malware-v-ceske-republice-v-roce-2019
33) ESET software spol. s.r.o. *Jak se může firma bránit ransomware?* [online]. 2019 [cit. 4.3.2020]. Dostupné z: https://www.eset.com/cz/blog/hrozby/jak-se-muze-firma-branit-ransomware/
34) Hoax: Čím hoax škodí? *ho@x.cz* [online]. [cit. 6.3.2020]. Dostupné z: https://www.hoax.cz/hoax/cim-hoax-skodi
35) Spam, *Internetem Bezpečně* [online]. [cit. 6.3.2020]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/spam/
36) Infografika: Jak jsou na tom Češi se spamem? Nejvíce se ho snaží potírat Pražané, 2019. *Tyinternety.cz* [online]. [cit. 6.3.2020]. Dostupné z: https://tyinternety.cz/prirucka-marketera/infografika-jak-jsou-na-tom-cesi-se-spamem-nejvice-se-ho-snazi-potirat-prazane/
37) Hoax, *Internetem Bezpečně* [online]. [cit. 7.3.2020]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/hoax/
38) Co je to hoax a jak se mu bránit? *PC PORADENSTVÍ.CZ* [online]. [cit. 7.3.2020]. Dostupné z: http://www.pcporadenstvi.cz/co-je-hoax-jak-se-mu-branit
39) Starci na netu (2018): Pravdivé i nepravdivé zprávy emailem šíří nejvíce senioři, 2018. *Ebezpečí* [online]. [cit. 8.3.2020]. Dostupné z: https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/starci-na-netu-vyzkum-2018

40) ROSTECKÝ, Jiří. I*nternetová kriminalita: Ve šlépějích warezu za porušováním autorských práv* [online]. 2012 [cit 10.3.2020]. Dostupné z: https://www.objevit.cz/internetova-kriminalita-ve-slepejich-warezu-za-porusovanim-autorskych-prav-t8938?fbclid=IwAR3dfiYtZY-gdiJE--QsowIeJ2tM9hYXv0hGq6NifZWHTDEwtUd5rgm2ihE
41) Co je to: Warez, *myprovas.cz* [online]. 2015 [cit 10.3.2020]. Dostupné z: https://www.myprovas.cz/co-je-to-warez/?fbclid=IwAR3erTnkYmf1RAanjfZLXfOM5Ic7yKaVyWxCDpwjmRHqipz9iyOL0EX7xPk
42) VÁCLAVÍK, Lukáš. *Proč warez? Polovina domácností i firem pirátí proto, že se jim za software nechce platit* [online]. 2016 [cit 11.3.2020]. Dostupné z: https://www.cnews.cz/proc-warez-polovina-domacnosti-i-firem-pirati-proto-ze-se-jim-za-software-nechce-platit/?fbclid=IwAR2MCmt2_oKN_BdGvcEWCdyrm_lpPZ4iULU97Er1RT7kvHE-C2FeL_PbrYc
43) Phishing, *Internetem Bezpečně* [online]. [cit. 12.3.2020]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/?fbclid=IwAR0Vx57VJJgSb7jOJ15b76NL1e_vtfgbe2655T-eFBvzybLTxhfj3dn0eMw
44) ESET software spol. s.r.o. *Jak je možné, že je phishing stále tak nebezpečný* [online]. 2019 [cit. 12.3.2020]. Dostupné z: https://www.eset.com/cz/blog/hrozby/jak-je-mozne-ze-je-phishing-stale-tak-nebezpecny/?fbclid=IwAR1SfuXhMPKXeEF0lXFHMDXLC3_21GZ7lQ-D-jHofeHIYrttdBQ0n9hYWz8
45) Kyberšikana, *Internetem Bezpečně* [online]. [cit. 14.3.2020]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/?fbclid=IwAR2EKhdSEHA2hTwXkG-3KZiRm9lEuQ_f61LIOt4BIoby6CqTFmKM9g25u4g
46) Výzkum rizikového chování českých dětí v prostředí internetu (2014), *Ebezpečí* [online]. 2014 [cit. 15.3.2020]. Dostupné z: https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/rizikove-chovani-ceskych-deti-2014

47) Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník, *Policie ČR* [online]. [cit. 17.3.2020]. Dostupné z: https://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx?fbclid=IwAR36s0duegfgfGY3YhzpCetcujAVIL3K_ELvbNNnshu835PT66OCxVy6v5k
48) O BSA a jejích členech, *BSA | The Software Alliance* [online]. [cit. 18.3.2020]. Dostupné z: https://ww2.bsa.org/about-bsa
49) Programové cíle BSA: Soukromí a bezpečnost dat, *BSA | The Software Alliance* [online]. [cit. 18.3.2020]. Dostupné z: https://ww2.bsa.org/policy/data
50) Novinky: V Česku se užívá 32 % nelicencovaného softwaru, nejméně v historii, hlavně kvůli strachu firem z kybernetických útoků a ztráty dat, 2018. *BSA | The Software Alliance* [online]. [cit. 19.3.2020]. Dostupné z: https://ww2.bsa.org/news-and-events/news/2018/june/gl06052018gss
51) About Europol, *EUROPOL* [online]. [cit. 19.3.2020]. Dostupné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3?fbclid=IwAR26wnx-mYHTEvds7tvksyPPFdhKP2PEeEq7XX3BHKYuN_mF0eDee8D73KM
52) O nás: O projektu, *Internetem Bezpečně* [online]. [cit. 20.3.2020]. Dostupné z: https://www.internetembezpecne.cz/o-projektu/
53) O projektu: Informace o projektu, *Ebezpečí* [online]. [cit. 20.3.2020]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu