Univerzita Palackého v Olomouci

Fakulta tělesné kultury

Bezpečnost společnosti v éře kybernetiky

Bakalářská práce

Autor: Jiří Odvářka

Vedoucí práce: doc. Ing. Jaromír Novák, CSc.

Olomouc 2020

Bibliografická identifikace

Jméno a příjmení autora: Jiří Odvářka

Název bakalářské práce: Bezpečnost společnosti v éře kybernetiky

Katedra: Aplikovaných pohybových aktivit (APA)

Vedoucí bakalářské práce: doc. Ing. Jaromír Novák, CSc.

Rok obhajoby: 2020

Abstrakt: Bakalářská práce pojednává o problematice kybernetických útoků v kyberprostoru. Cílem bakalářské práce je představit kyberterorismus a kyberkriminalitu jako novou hrozbu lidstva, vytvořit přehled stavu softwarových technologií určených pro kyberprostor a obeznámit s jejich prevencemi či řešením. Práce dále obsahuje názorný způsob napadení v kybernetickém prostoru. Dílčím cílem je srovnání způsobů projevů kybernetické kriminality prostřednictvím dotazníkové analýzy, na jejímž základě statisticky znázorňuje znalost populace v tomto odvětví.

Klíčová slova: monitoring, kylogger, spyware, kyberterorismus, kyberkriminalita, hacking, phishing, darkweb malware

Bibliographical identification

Autor's first name and surname: Jiří Odvářka

Title of the thesis: Security of society in the age of cybernetics

Department: Aplikovaných pohybových aktivit (APA)

Supervisor: doc. Ing. Jaromír Novák, CSc.

The year of the presentation: 2020

Abstract: The bachelor's thesis is concerned with the issue of cyber attacks in cyberspace. The purpose of the thesis is to introduce cyber terrorism and cybercrime as a contemporary menace to humanity, to summarize the number of software technologies designed for cyberspace, and furthermore, to familiarize with it's prevention and solution. In addition, the work contains a process of an intervention in cybernetic space. A partial target is the comparison of various forms of cybernetic crime and it's impact concluded from a questionnaire analysis, which statistically displays the amount of knowledge population possesses of this field.

Keywords: monitoring, kylogger, spyware, cyberterrorism, cybercrime, hacking, phishing, darkweb, malware

Prohlašuji, že jsem bakalářskou práci na téma Bezpečnost společnosti v éře kybernetiky vypracoval samostatně pod vedením doc. Ing. Jaromíra Nováka, CSc., citoval jsem všechny použité zdroje a řídil se zásadami vědecké etiky.

V Prostějově dne 22.05. 2020 …….

Jiří Odvářka

Tímto bych chtěl poděkovat vedoucímu mé bakalářské práce doc. Ing. Jaromíru Novákovi, CSc. za odborné vedení, poskytnutí cenných rad a připomínek, které jsem využil při její tvorbě.

Obsah

1 ÚVOD

Svět v době obrovského technologického rozvoje má v boji proti fenoménu kybernetických hrozeb, zejména počítačové kriminality a počítačového terorismu jako nové formy hrozeb 21. století, mnoho výzev. Informace jsou velmi dlouhou dobu považovány za významný aspekt moci či diplomacie. Od 90. let se však informační role v mezinárodních vztazích a bezpečnosti diverzifikovala a její význam se zvýšil, zejména kvůli masivnímu nárůstu informačních a komunikačních technologií. Vezmeme-li v potaz faktor lidské povahy a vyspělé možnosti kyberprostoru, je tohle onen důsledek toho, proč se záležitosti kybernetické bezpečnosti staly bezpečnostním problémem, které zasahují do všech sfér společnosti.

Nastala doba Hi-Tech zařízení, bez které si lze jen těžko dnešní svět představit. Spousta lidí se často novým změnám brání a jednoduše jej neakceptují. Z důvodu ochrany bezpečnostního systému před potenciálními hrozbami jsem přesvědčen, že je třeba provést přiměřené zabezpečení v oblasti kybernetického terorismu i počítačové kriminality a umět adekvátně reagovat.

V teoretické části bakalářské práce vysvětlím a charakterizuji veškeré pojmy vztahující se k problematice daného tématu práce. Objasním pojmy, jako jsou kyberterorismus, kyberkriminalita, kyberprostor aj. Dále se budu věnovat nejen projevům kybernetické kriminality, ale i jejich prevenci či řešením, kdy se dostávám také k části praktické.

V praktické části se budu věnovat prevenci proti všemožným kybernetickým útokům hrozícím v kyberprostoru a u některých typů objasním řešení už stávajícího problému, a to vše se zaměřením na domácího uživatele. Následovat bude praktický test způsobu napadení uživatele v čele s únikem soukromí a dále se budu věnovat dotazníkovému šetření. Mimo dotazníkové šetření se teoretická část prolíná s částí praktickou z důvodu přehlednosti, protože různé druhy útoků mají ihned vysvětlenou prevenci nebo způsoby řešení.

2 PŘEHLED POZNATKŮ

2.1 Kybernetický prostor

Jedním z mnoha národních strategických cílů, které by měly být ve strategii obrany zemí obecně formulovány, je ochrana kybernetického prostoru s cílem, chránit kritickou infrastrukturu a redukovat možnost zasažení v oblasti kyberprostoru, ale také snížit následky škod způsobené kybernetickými útoky. Důležité je vzít v potaz využití vládních služeb závisejících na kybernetickém prostoru v tom smyslu, že jeho prostřednictvím se zprostředkovávají služby v oblasti bankovnictví, financí, zdravotnictví, informačních a komunikačních služeb apod. Ministerstvo obrany (2006) definuje kyberprostor jako „globální doménu v informačním prostředí skládající se ze vzájemně závislé sítě infrastruktur informačních technologií, včetně internetu, telekomunikačních sítí, počítačových systémů a vestavěných procesorů a kontrolérů“ (Congressional Research Service, 2020).

Z výše uvedených argumentů je bezpečnost v kybernetickém prostoru nejdůležitější z důvodu trvalého využívání vládních služeb a zvyšování důvěry veřejnosti v informační systémy.

Díky těmto informacím jsem dospěl k závěru, že je nezbytné chránit národní kritickou infrastrukturu před vniknutím a kybernetickými útoky z toho důvodu, že „hackeři“ a další vetřelci mohou kritickou infrastrukturu zneužít jako nástroj k provedení svých útoků. Optimální komunikace v kybernetickém prostoru je důležitá pro výměnu informací mezi propojenými vládními institucemi. Kvalitní propojení mezi institucemi umožňuje zrychlit detekci a řešit problémy s IT jako jsou viry, malware a jiné typy počítačových útoků, kterým se budu věnovat v pozdějších kapitolách.

2.1.1 Internet

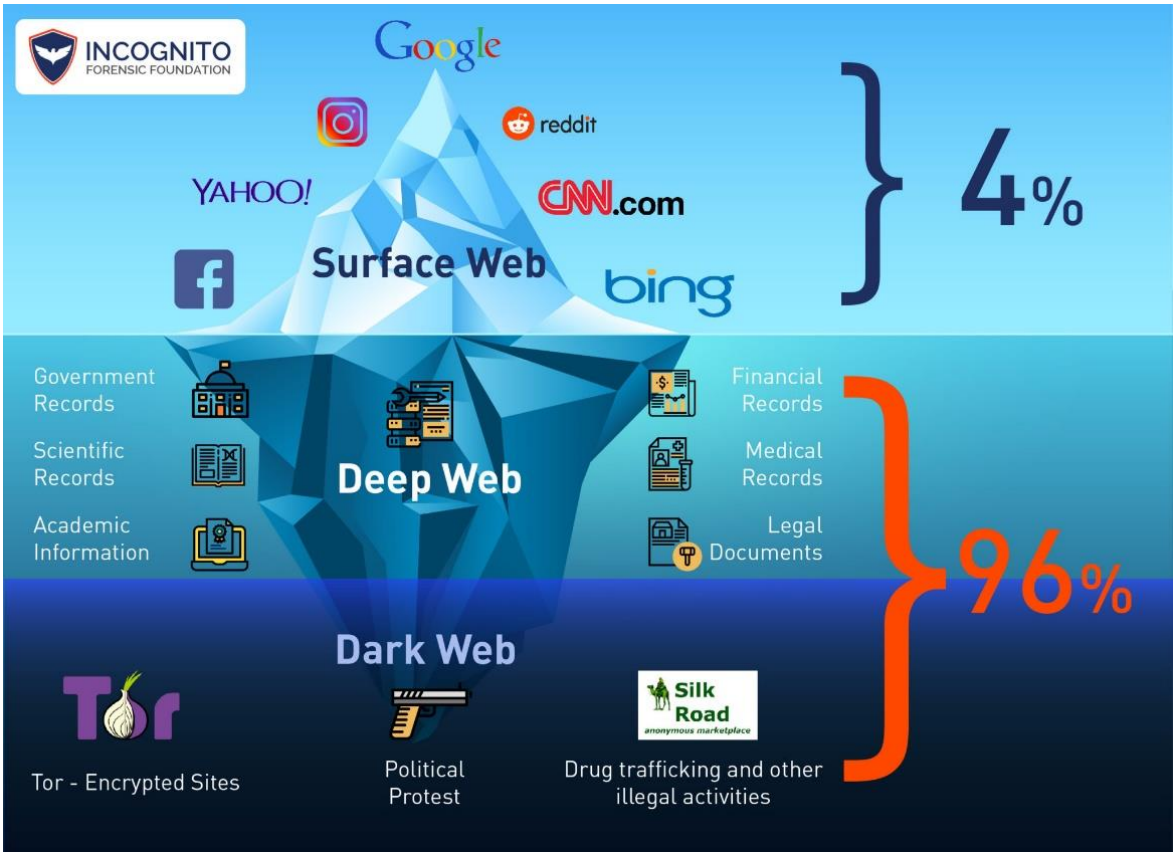
K internetu se váže nespočetné množství informací, které nelze shrnout do jedné kapitoly, avšak pro pochopení následujících pojmů je nezbytné chápat, jakým způsobem internet funguje. V dnešní době snad už není zapotřebí zmiňovat, že se jedná o celosvětový systém navzájem propojených počítačových sítí, kde zařízení mezi sebou komunikují prostřednictvím protokolu TCP/IP[1]. Cílem internetu je bezproblémová komunikace neboli výměna dat. Služba internetu, ve které ji známe dnes, je bezpochyby nejrozšířenější WWW (World Wide Web). Napsaný programovacím jazykem HTML[2]. Důležitým faktem je

uvědomění, že odkazy na webu nám umožňují kamkoliv přecházet. K dispozici jsou prakticky kdykoliv, jelikož jsou uloženy na permanentně běžících webových serverech[3].

Rozdělit internet lze na 3 základní skupiny:

- Surface web
- Deep web
- Darknet (Dark web)

Obrázek 1 - Rozdělení internetu



Zdroj: ifflab.org

2.1.2 Surface web

Jedná se o takovou část internetu, která je přístupná pro všechny uživatele internetu, prostřednictvím standardních prohlížečů (Google Chrome, Internet Explorer, Opera, Safari)

a lze ji vyhledávat na běžně dostupných webových vyhledávačích (Google, Seznam, Centrum, Atlas). Lze jej považovat za přímý opak dark webu, který není indexovatelný pomocí běžného webového vyhledávače. Dle serveru IFFLAB je procentuální poměr obsahu mezi „viditelným“ a „neviditelným“ internetem 4:96 ve prospěch dark webu a deep webu.

2.1.3 Deepweb

Do deepwebu patří všechen obsah vyhledávatelný prostřednictvím tradičních „WWW“ vyhledávačů a ve výjimečných případech je důležité vlastnit odkaz pro přesměrování na danou adresu. Jedná se o takový obsah, ke kterému jsou zapotřebí přihlašovací údaje (Facebook, Instagram, Twitter, E-mail).

2.1.4 Darknet (Darkweb)

Mnohdy nazývaný jako „temná strana internetu“. Darkweb je součástí internetu samotného, ovšem původní myšlenka stvoření darkwebu nespočívala v porušování zákonů, ale byl vytvořen za stejným účelem jako internet a původně si našel využití v akademických účelech či vládních institucích. I přes fakt, že internet a darkweb mají téměř totožné datum vzniku, druhý zmiňovaný je veřejnosti mnohem méně známý a novější. Největší rozmach zažil v roce 2011, kdy spatřilo světlo světa virtuální tržiště zvané Silkroad, kde zájemci měli a nadále mají možnost zakoupit ilegální látky, zbraně či služby nájemných vrahů. První verze označená Silkroad 1.0 vznikla v únoru 2011 a byla zavřena federálním úřadem FBI v říjnu 2013. Téhož roku v listopadu byla spuštěna druhá verze Silkroad 2.0, která byla pod vedením jednoho z původních administrátorů Silkroad 1.0. Druhá verze skončila zavřením v roce 2014 a následně byla vytvořena Silkroad 3.0, která funguje dodnes (Wikipedie, 2020). Dnes v době velkého rozmachu využívání anonymních VPN[4] či proxy serverů[5] je boj proti tomuto druhu ilegality velice obtížný, mnohdy téměř nemožný.

2.2 Kybernetická kriminalita (IT crime, cybercrime)

Počítačová trestná činnost zahrnuje jakýkoli trestný čin týkající se počítačů a sítí. Kromě toho kybernetická trestná činnost zahrnuje také tradiční trestné činy vedené přes internet. Například: zločiny z nenávisti, telemarketing, internetové podvody, krádeže identity a krádeže

účtů na kreditních kartách se považují za počítačové trestné činy, pokud jsou nezákonné činnosti spáchány pomocí počítače a internetu (ResearchGate, 2001).

Některé útoky v kybernetickém prostoru nemají specifické cíle, protože útoky proti počítačům či skupině počítačů jsou stále běžnější. Útočníci prostřednictvím počítačů mohou navíc způsobit poškození Národní kritické infrastruktury (CNI), která zahrnuje pohotovostní služby, distribuci energie, zdraví, finance a další služby závisející na IT. Mnoho IT systémů, které dříve byly izolovány od internetu, nyní přístup k internetu postupně dostávají a jejich možnost napadení se zvyšuje.

Podle Achkoski & Dojchinovski (2000) existují dva hlavní způsoby jakými mohou být počítače zapojeny do trestné činnosti:

1) Staré typy trestní činnosti prováděné prostřednictvím počítačů jako například obtěžování pomocí mobilních telefonů nebo nezákonné stahování hudby, filmů a další formy pirátství. Dalším příkladem je „phishing“ – triky založené na důvěře jedince zahrnující podvodné e-maily nebo weby k získání citlivých informací.
2) Nové typy trestné činnosti umožněné specifickými technologiemi. Například útoky DoS, které brání internetové službě či stránce k přístupu ostatním uživatelům. Další trestné činy zahrnující útok na počítač jsou často „hackování“ či neoprávněné získání přístupu do počítačového systému nebo psaní virů k odstranění uložených dat.

2.2.1 Kybernetická kriminalita ve světě

Vezmeme-li v potaz počítačovou kriminalitu ve světě a budeme-li chtít ji porovnávat, musíme vzít v úvahu řadu zásadních faktorů, které tento jev mohou ovlivňovat. Jako jeden z nejdůležitějších aspektů jsou ekonomické rozdíly států, které se zrcadlí do technologické vyspělosti. Tím pádem nelze objektivně porovnat jednotlivé státy mezi sebou. Nabízí se zde porovnání pouze relativní, a to u takových států, které jsou ve svém technologickém rozvoji na srovnatelné úrovni.

Dle serveru Buguroo (2018) patří mezi státy s nejvíce rozšířenou kyberkriminalitou Rusko, Brazílie a Čína.

2.2.1.1 Rusko

Z analýzy sociálních sítí se Rusko řadí mezi státy s největší technologickou vyspělostí a kreativitou, která zaručuje být o krok napřed. Mezi oblíbené oběti patří obyvatelé Evropy a USA, kteří se těmto útokům snaží adekvátně přizpůsobit bezpečnostní opatření. Tato opatření zahrnují především vyšší bezpečnost bankovních účtů a zvýšit počet dvoufaktorového ověření. Tzv. „škola ruských hackerů" je jednou z nejznámějších díky množství kybernetických útoků. Většina je politicky motivována a jejich „hackerská komunita" nemluví o kyberkriminalitě, ale spíše o kybernetické válce. Skutečnost, že se Rusko roky řadilo na první místo seznamu, vede vědce k pochybnostem a také to, kde stojí klíč k tomuto „úspěchu". Dle mých poznatků se jedná o vzdělávací systém Země, který od dob Sovětského svazu řídí studium vědy, matematiky, a především vědecká zvídavost.

2.2.1.2 Brazílie

Brazilská „hackerská škola" narůstá v globálním měřítku především díky dopadu svých činů, což z ní dělá podobně nebezpečnou jako je ta Ruská. Dle serveru *Igarape.org.br* patří Brazílie mezi nejvíce napadané země. Díky tomuto faktu je více než jasné, proč brazilské banky vyvíjí stále sofistikovanější ochranné systémy zaměřující se na ověřování identity zařízení, které zákazníci využívají k přihlášení na své webové servery. To je důvod, proč kybernetické zločince nutí k vývoji technik řízení vzdáleného přístupu za účelem odcizení účtu uživatele. Jsem přesvědčen, že brazilští kybernetičtí zločinci se inspirují Rusy a dále způsoby rozvíjí ve své zemi.

2.2.1.3 Čína

Oblíbené oběti čínských zločinců se nacházejí především v Asii, Tichomoří a Austrálii. Bezpečnostní opatření v těchto oblastech jsou velmi podobná těm evropským, proto čínští kybernetičtí zločinci začlenili techniky používané Rusy, které jsou proti těmto cílů účinné. Je ironií, že velká část čínských infrastruktur kybernetického zločinu je umístěna mimo zemi.

Domnívám se, že můžou úzce souviset s přísnými právními předpisy Číny, kde je komunikace vysoce monitorována.

2.2.2 Kybernetická kriminalita na přelomu tisíciletí

Přelom nového tisíciletí není zvolen čistou náhodou. V kybernetice se lze snadno orientovat v období podle významných událostí, které zasáhly globální sféru počítačových systémů. S blížícím se rokem 2000 se objevil problém strhující paniku, který byl později známý jako Y2K problém. Předpokladem byla nemožnost zobrazit takové datum. Potvrzujícím faktem byly přepisy hodnot z čísla 1999 na 1900 či 19100. Většina programů roky interpretovala chybně. Jedny z nejhorších prognóz spekulovaly o katastrofických scénářích, kdy má dojít k vynulování účtu v bankách, výpadkům, či dokonce haváriích jaderných elektráren, leteckého provozu nebo všech počítačových systémů. Tento problém se s příchodem roku 2000 uvedl jako „global fake news“ a mimo pár potřebných aktualizací se prakticky nic nestalo (Javůrek, 2009).

Rok se nesl v éře problémů tisíciletí. Objevil se další problém označovaný názvem „I love you“ a jednalo se o počítačového červa vytvořeného v jazyce VBScript[6]. Infikoval 50 milionů počítačů a škody způsobené za zhruba 5-8 miliard amerických dolarů. Weimann (2008) uvádí, že může nastávající generace teroristů způsobit více škody mobilním telefonem než prostřednictvím bomby. Tento červ byl vstup do sociálního inženýrství, který podle diskuzí s mými kolegy, kteří se zabývají IT, byl jeden z prvních. Jednalo se o virus z Filipín, kde vznikl pro zábavu. Oběti obdržely e-mail, který po otevření přílohy aktivoval protokol, který poštu posílal dalším obětem. Z důvodu absence legislativní normy upravující tento čin, nikdo nebyl potrestán.

Nastávající rok byl ve znamení virů, trojských koní a červů, které se zaměřovaly na emailovou poštu. Známý virus MiMail[7], který své obdobné verze drží dodnes, obsahující primitivní kód tehdejší doby, proto většina aktuálních antivirových programů tento vir identifikuje ihned. Šířil se pomocí e-mailové pošty, kde pomocí zprávy měl za úkol získat důvěru oběti. E-mail obsahoval falešný odkaz, který uživatele přesměroval na webovou stránku s formulářem, která na první dojem vypadala jako platební systém PayPal, jednalo se však o povedený grafický klam. Následující kroky už učinil sám uživatel, který nebyl schopen rozpoznat, kam své údaje o kreditní kartě zadává. Po potvrzení se údaje odeslaly na předem danou e-mailovou adresu. Útočník během krátké chvíle byl schopen získat o oběti citlivé informace bez jejich vědomí. Lze snadno odhadnout, že útočník svůj čin provedl vědomě za účelem finančního zisku.

Obrázek 2 Teroristický útok 11. září 2001 v USA.

Zdroj: google.cz

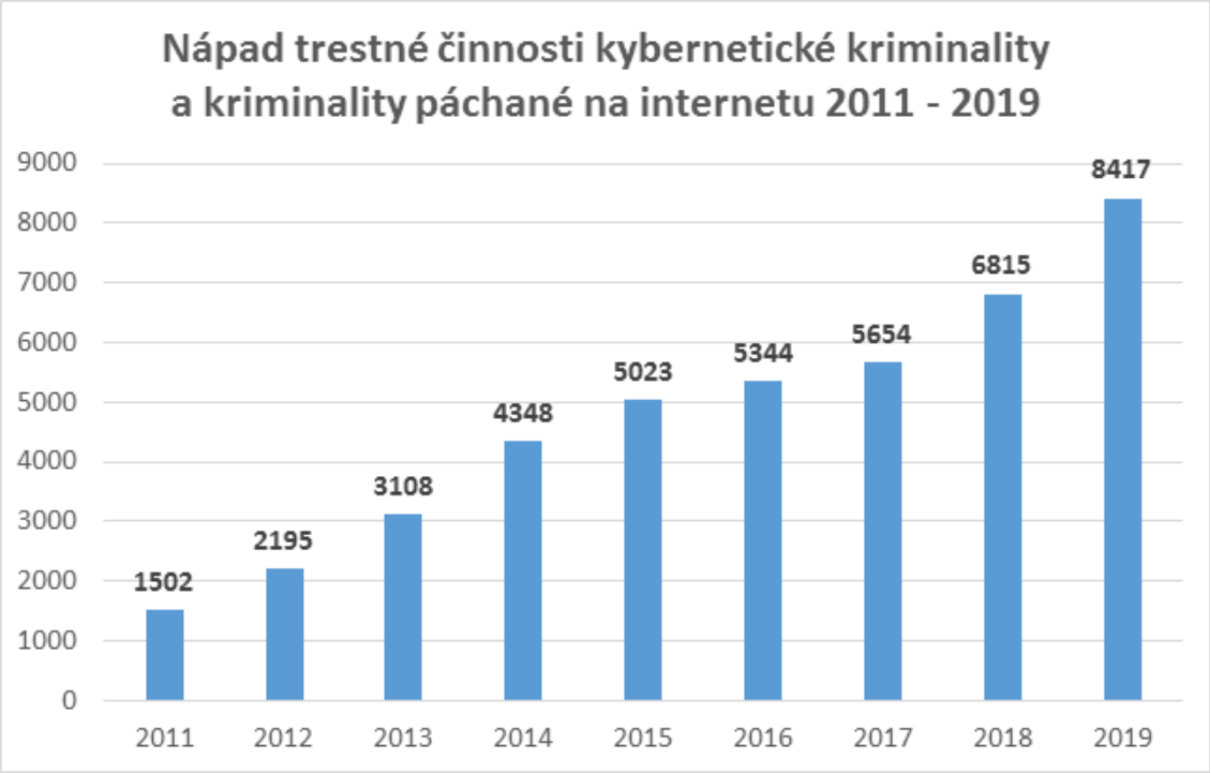
Klíčové události se odehrály 11. září 2001, které navždy změnily dějiny. Teroristické útoky spáchané ve Spojených státech amerických, známé jako „September 11 Attacks“, kde havarovaly čtyři letadla amerických aerolinek a zasáhla postupně Světové obchodní centrum v New Yorku, Pentagon a poslední letoun se zřítil u města Shanksville v Pensylvánii.

Na základě názoru nebylo možné zrealizovat plány o takovém rozsahu právě bez moderních technologií (Harrison, 2016). Už neexistuje naděje, že některých věcí se člověk není schopen dopustit (Zuna, 2010).

2.2.3 Kyberkriminalita v ČR

Policie ČR od roku 2011 monitoruje počet trestných činů spáchaných v kyberprostoru. Jedná se především o internetovou síť. V grafu lze zaznamenat graduální nárůst případů kybernetické kriminality. Počínaje rokem 2011, kdy záznam ustanul na 1502 trestných činech a v roce 2019 se téměř 6x znásobil.

Obrázek 3 Kyberkriminalita za období 2011 – 2019.



Zdroj: Policie ČR

Dle Policie ČR páchané kybernetické kriminality v roce 2019 narostlo na 8417 trestných činů a v porovnání s předchozím rokem je potvrzený skok o 1600 činů. Do skupiny nejvíce zneužívaných způsobů kybernetické kriminality prostřednictvím internetu se řadí různé typy podvodného jednání, kde množství evidovaných trestných činů dle statistiky zahrnuje více než polovinu.

Důležité je upozornit na riziko hackingu, které v roce 2019 „předehnalo“ značným způsobem mravnostní trestné činy. Jedná se o neoprávněné vniknutí do počítačového systému a sběr informací. Díky technologicky vyspělejším systémům, softwaru a stále se rozšiřujícímu kybernetickému světu stoupá nárůst hazardních her prostřednictvím internetu u osob mladších 18 let, která převyšuje ostatní druhy kybernetické kriminality obecně (Policie ČR, 2020).

2.3 Formy terorismu

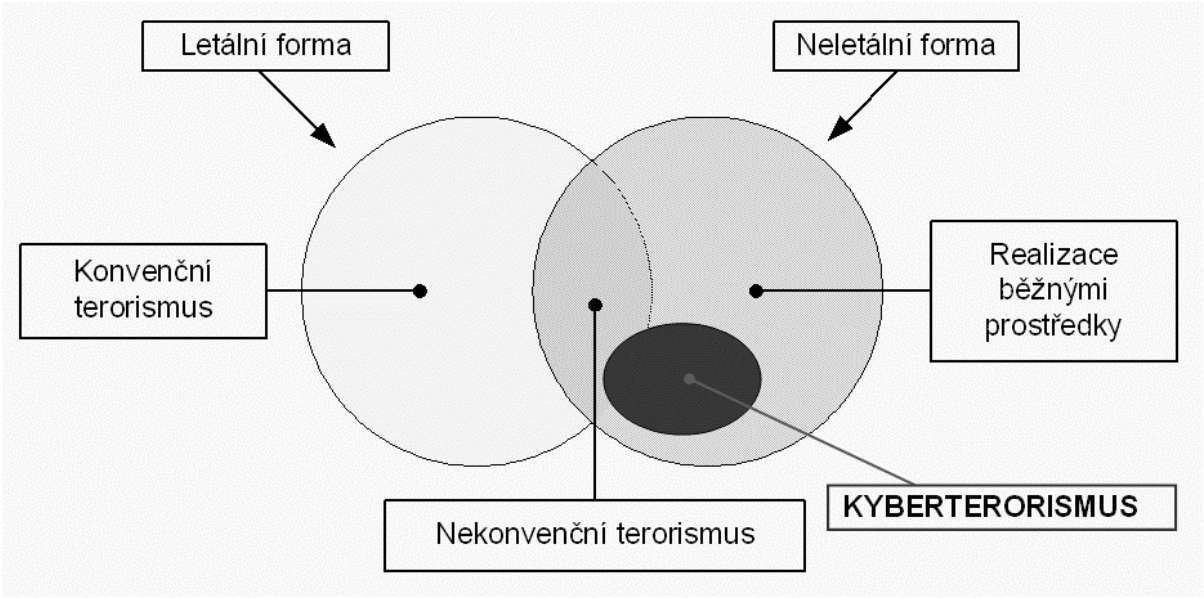
I přes značnou změnu zaznamenaného nižšího počtu teroristických útoků, materiální škody a počet obětí neustále narůstá. Nárůst je úzce spojován s množstvím využívaných forem. Tyto formy členíme dle Jirovského (2007) do dvou skupin:

- Letální formy
- Neletální formy

2.3.1 Letální formy terorismu

První skupina tedy letální forma terorismu se vyznačuje použitím běžných prostředků pro realizaci násilí. Dále je členěna na dvě podskupiny, lišící se použitými prostředky, na konvenční a nekonvenční terorismus. Do podskupiny konvenčních forem letálního terorismu se řadí útoky páchané pomocí běžně dostupných bojových prostředků, např. střelných zbraní, zatímco mezi nekonvenční formu zneužití nebezpečné zbraně hromadného ničení.

Obrázek 4 Letální a neletální formy terorismu a jejich vztah



Zdroj: JÍROVSKÝ, V. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koní bez tajemství 2007.

2.3.2 Neletální formy terorismu

V kyberprostoru se však běžněji vyskytují neletální formy či útoky, při kterých jsou uplatňovány nástroje sofistikovaného typu v kombinaci s letálními prostředky. Konvenční forma neletálního terorismu zahrnuje tyto podskupiny:

- Neozbrojený terorismus nebo-li „unarmed terrorism“ – způsob vedení teroristických akcí, při nichž jsou prostředky každodenního života použity novodobým způsobem tedy jako zbraň či donucovací prostředek.
- Kyberterorismus patřící mezi prvenství největších hrozeb 21.století zneužívá výpočetní a telekomuinikační technologie, především internet jako prostředek pro realizaci teroristického útoku. Jedná se o plánovanou činnost, zpravidla motivovanou náboženskými či politickými ideologiemi a realizované jsou většinou menšími skupinami nežli vojenskými strukturami.
- Mediální terorismus je často označovaný jako psychologický terorismus. Zahrnuje především plánované zneužívání mediálních prostředků pro přenos dat. Hlavním cílem je ovlivnit názor celé populace nebo cílených skupin obyvatelstva (Jirovský, 2007).

2.4 Kybernetický terorismus (kyberterorismus)

Pojem kyberterorismus na konci minulého století zaznamenal s příchodem internetu globální rozmach. Kyberterorismus označuje užití internetu pro teroristické účely, které bývají ve většině případů politicky či ideologicky zabarvené. Počítačový terorismus vytvořil otázku změny tváře dnešního terorismu. Protíná dva světy, a sice fyzický s virtuálním.

Ať už se jedná o domácí přístroje jako mikrovlnná trouba, vysavač nebo mobilní telefon, vztahuje se i na velké průmyslové systémy jako jsou elektrárny, vodní přehrady nebo továrny. Téměř vše se řídí informačními technologiemi, které se s postupem času ukázaly být vysoce efektivní. S tím přichází spousta možností, kde systémy mohou selhat a ovlivnit tak nespočet lidí v každodenním životě.

V současné době neexistuje přesná definice v širším slova smyslu vymezující význam kybernetického terorismu.

Obecné definice:

- definice kyberterorismu podle A. Colarika a L. Janczewskiho:

„Kybernetický terorismus lze definovat jako představitele aktivit vedených nebo koordinovaných státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka.“

- definice kyberterorismu dle P. Everarda:

„Kybernetický terorismus je kybernetický útok užívající či zneužívající počítač nebo telekomunikační sítě za účelem způsobení dostatečné škody s cílem zastrašit společnost a mající ideologický podtext.“

- definice kyberterorismu dle Ministerstva vnitra Spojených států amerických publikovaná P. Everardem:

„Kybernetický terorismus je kriminální akt vedený za pomocí počítače nebo telekomunikačních prostředků. Cílem je pak způsobit zmatek a nejistotu za účelem ovlivnit vládu či populaci k přijetí určitých politických, ideologických či sociálních témat.“

Oficiální definici kyberterorismu v užším slova smyslu před nedávnem formulovala americká analytička Dorothy E. Denningová:

„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaných v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.”

Kybernetický terorista je považován za profesionálního, tvůrčího a velmi chytrého. Na místě je hledání neortodoxní a originální metody k dosažení svých cílů. Teroristé preferují tradiční způsob boje s klasickými zbraněmi, avšak v poslední době zavádějí použití stále sofistikovanější „špičkové“ technologie, která znázorňuje, že se z nich stávají „moderní“ válečníci, kteří tempo technologického vývoje akceptují. Pokud je řeč o počítačovém terorismu, existuje skutečné nebezpečí pro informační zdroje, zejména v globálních informačních sítích, což znamená, že pokud jsou teroristy zneužity, může se globální informační síť stát účinnou zbraní pro počítačové útoky. Teroristům také dává úplně nový rozměr boje.

2.5 Vztah mezi hackery a teroristy

Skupiny hackerů jsou četné a dají se rozdělit dle úrovně technologické vyspělosti. Členství ve vysoce technologicky pokročilých skupinách může být často omezené a výhradně povoleno pouze nejzdatnějším jedincům, kteří vyvíjejí nejsofistikovanější kyber-útočné nástroje. Tyto skupiny jsou díky svým dovednostem vysoce anonymní a důvěrné, což zvyšuje efektivitu útoku. I přesto, že některé skupiny mohou být globálního měřítka, mají podobné cíle, často obsahující politický zájem nebo je pojí sociální či náboženská ideologie. Častým motivem skupiny je finanční zisk spojován s organizovaným zločinem. Rovněž je možné se setkat s hackerskými skupinami, které se své výjimečné dovednosti snaží prodat sponzorům. Aby se však předešlo škodám způsobeným teroristickými a zločineckými jednáními, vyvíjí se četné výzkumné projekty, které mají za úkol přispět k nalezení technologií, technik nebo taktik proti kybernetickým hrozbám.

2.6 Rozdíl pojmů kybernetická kriminalita a kybernetický terorismus

V současné době existuje mnoho obecných definic počítačové kriminality a počítačového terorismu, které jsem zmiňoval v přecházejících kapitolách. Před nedávnem došlo ke zmatku, zda nejsou pojmy počítačová kriminalita a počítačový terorismus synonymem. Tímto se společnost autorů definic rozdělila na dva tábory, a to na ty, kteří preferují názor, že tyto dva termíny se shodují a druhý, že nikoli. Z globálního pohledu jsou prioritními definice využívané dle terminologie USA. Hlavním cílem kybernetického terorismu je infiltrace do konkrétního systému, kde může způsobit škody finanční či na majetku a účelně destabilizovat nebo snížit či úplně narušit bezpečnost. Hackeři, kteří jsou vyznavači počítačové kriminality, mají obvykle jako hlavní motivy individuální úspěch v komunitě nebo dosažení finančních prostředků aj. Zatímco počítačoví teroristé, kteří jsou často komplici teroristických organizací (Al-Káida, ETA, IRA atd.), mají motivaci politického charakteru (Lorents & Ottis, 2011).

Kybernetický terorista může útočit na jasně definované cíle, které jsou pro určité země významnými strategickými body. Jako příklad lze uvést elektrárnu, která dodává elektřinu široké oblasti. Kybernetický terorista, který se dopustí tohoto typu útoku, může efektivně přerušit dodávku elektřiny anonymně bez zanechání stop (Achkoski & Dojchinovski, 2000).

Dalším příkladem počítačového terorismu může být hacking nemocničního počítačového systému a změna lékařských předpisů.

Kybernetická kriminalita je v dnešní době pojmem, který se čím dál častěji objevuje v běžné lidské komunikaci, ve sdělovacích prostředcích nebo v policejních statistikách. Jde o takovou trestnou činnost, pro kterou jsou jako nástroj používány moderní informační a komunikační technologie.

„Informační technologie a jejich dynamický rozvoj s sebou přináší nová společensky škodlivá jednání, a proto je kybernetické kriminalitě věnována stále větší pozornost. Pojem kybernetická kriminalita je odvozován od pojmu kybernetický prostor, případně zkráceně kyberprostor. Kyberprostor je virtuální prostředí, které nemá vymezený začátek ani konec, neplatí pro něj hranice národních států, takže nelze určit rozsáhlost.“ (Policie ČR, 2020)

2.6.1 Taxonomie útočníků dle motivace

Kyberteroristická motivace je různorodá a liší se napříč celým světem. Jeden z hlavních záměrů teroristických skupin často bývá iniciace politické změny prostřednictvím změny názorů populace země. Separatistické motivy jsou dalším důvodem, které prostřednictvím nezávislosti či náboženské svobody se snaží odtrhnout od existující entity.

Mezi obecné motivace lze zařadit touhu po slávě či zábavu nebo publicitě a v neposlední řadě jde často o pomstu. Jirovský (2008) uvádí, že více než 50 % hackerských skupin přiznává politickou motivaci.

3 CÍL PRÁCE

Cílem mé bakalářské práce je představit kyberterorismus jako novou hrozbu lidstva, vymezit jeho pojmy, vytvořit přehled stavu softwarových technologií používaných v kyberprostoru a obeznámit s jejich prevencemi či řešením. Dále objasnit, jak lze přistupovat k informacím oběti z pohledu útočníka, a to způsobem znázornění specifického softwaru. Dílčím cílem je srovnání způsobů projevů kybernetické kriminality prostřednictvím dotazníkové analýzy, na jejímž základě statisticky znázornit znalost populace v tomto odvětví.

4 METODIKA

Strategie mé bakalářské práce je heuristická. Práce začíná tematickými poznatky, nutnými pro pochopení dané problematiky, které jsou proložené mými vlastními názory. Dále zmiňuji projevy kybernetických útoků, které jsou rozdělené do několika typů a to takových, které jsou dle mých poznatků nejrozšířenější. Většina kapitol obsahuje doplnění o doporučenou technologickou prevenci, která potenciálním obětem může redukovat riziko napadení v kyberprostoru. Pro případné vzniklé škody uvádím způsoby řešení jednotlivých útoků. Následuje praktický test napadení v kyberprostoru jako názorná ukázka, možnosti krádeže osobních údajů. V poslední části se věnuji dotazníkovému šetření, které jsem publikoval prostřednictvím sociálních sítí, kterého se zúčastnilo 148 respondentů, kde převažoval studentský věk 20-25 let.

5 VÝSLEDKY

5.1 Projevy kybernetických útoků

V následující části se budu věnovat nejčastějším typům útoků, které se nejvíce rozšířily s příchodem sítě internet. Do ustanovení platného trestního zákona spadají určitá protiprávní jednání v internetové síti, kde i přes značnou část činností spadající mezi delikty působnosti příslušných paragrafů, existuje množství deliktů, kde označení za trestné činy se zdá být komplikované či nemožné (Jirovský, 2020).

Se vzestupnou tendencí kybernetických útoků zde figurují čím dál tím více účinnější a sofistikovanější technologie, a to především z důvodu absence trestněprávní ochrany, která na nové protiprávní způsoby jednání není připravená. Osobní počítač, který byl dostupný pro běžného uživatele od roku 1976 se stal nejen cílem útoku, ale současně se stal prostředkem sloužícím k napadení.

5.1.1 Hacking

Nejstarším způsobem napadajícím kyberprostor, u kterého kořeny zasahují do 50. let 20. století, se nazývá hacking. Člověk způsobující tuto činnost je označován pojmem hacker. Původ slova označoval člověka nadmíru nadaného pro schopnost nalézat nová či neortodoxní řešení. Často není o přítomnosti hackera informován ani správce sítě, neboť se tyto útoky provádí anonymně a tzv. „no noise“ (bez hluku). Motivací není způsobení škody či peněžní zisk, ale překonávání výzev a především uznání komunity a respekt z vítězství nad technologií. Dle § 230 trestního zákoníku lze hacking označit za trestný čin.

Definice hackingu dle V. Jirovského: *Hacking označuje proniknutí do počítačového nebo řídícího systému jinou, než standartní cestou při obejití nebo prolomení jeho bezpečnostní ochrany“*

Tzv. „hacking community“ (hackerská komunita) se označuje za: „*Člověka, vyžívajícího se v bádání po detailech programových systémů a překračování jejich schopností. Člověka, který má potěšení z detailní znalosti vnitřních pochodů systému, počítače a sítí. Experta na*

určitý program či experta v jiném oboru. Jako jedince užívajícího si intelektuální výzvy k překonání či obcházení limitů.“ (The Jargon File, 2016)

5.1.1.1 Jak se bránit hackingu?

Vzhledem k individualitě útoků hackerů se proti hackingu jen velice těžko brání, neboť se jedná o útok tzv. „na míru“. Z reportu společnosti M-trends (2019) vyplývá, že odhalení úspěšného útoku trvá ve více než v polovině případů déle než 177 dní. Útočník ze začátku často provádí dlouhý průzkum a během něj střádá informace, ze kterých následně útok vychází. Často se jedná o telefonní čísla, e-mailové adresy nebo zjištění přítomnosti typu zabezpečovacího softwaru.

Nicméně v dnešní době se na trhu nachází celá řada zabezpečovacích softwarů, které obsahují bohaté bezpečnostní databáze všech doposud používaných nástrojů či metod, kterým často mohou zabránit. Rozdíly aplikací se nachází ve funkcionalitě a autonomii, kde je zapotřebí, aby každý uživatel určil své priority. U běžného uživatele tedy přihlédnu k ochraně hesel k účtům či ochraně osobních souborů.

Osobní zkušenost mám velice pozitivní se softwarem Eset Smart Security, kde za období od června 2017 po současnost se v osobním zařízení detekovala jinými analyzátory pouze jedna hrozba.

5.1.2 Cracking

Cracking je termín, kterým je označováno prolamování softwarové ochrany. Funguje na principu odstranění či deaktivace ochrany softwaru, která má za úkol chránit software proti kopírování, možnosti spuštění zkušební „demo“ verze na dobu určitou či opakované využití licenčního klíče. Softwarové prolomení ochrany je často označováno za „pirátský software“.

Pojmem cracking se také označuje neoprávněný průnik do systému. Jirovský (2007) konstatuje, že nejčastějším způsobem je tzv. „password cracking“ a jedná se o metodu zjišťování hesla za použití hrubé síly s pomocí slovníku nejčastěji užívaných hesel. Utilita tedy generuje a zkouší všechny možné kombinace znaků, dokud nenajde správnou. Rychlost generování znaků je závislá na výkonu hardwaru zařízení. S narůstající tendencí

technologického vývoje se zvyšuje hardwarový výkon všech zařízení, které mají čím dál tím vyšší výpočetní výkon pro zvládnutí většího počtu úloh. Dle serveru Avast (2019) anonymní hacker dokázal v roce 2012 naprogramovat skupinu 25 GPU (grafických karet), která umí prolomit jakékoli osmi znakové heslo k systému Windows s možností obsahovat velká či malá písmena, číslice a symboly za méně než 6 hodin. Naprogramovaný software dokáže hádat kombinací znaků s rychlostí 350 miliard pokusů za sekundu.

Vzal jsem v potaz rozdíl osmi let technologického vývoje. Od roku 2012, kdy byl software naprogramován a revoluční pokrok, po současnost. Pro porovnání jsem vybral „vlajkové lodě“ (GPU) roku 2012 s označením (HD 7770) a 2020 (RTX 2080TI). Dle webu *gpu.userbenchmark.cz* je rozdíl těchto grafických karet enormní, a to +1193% nárůstu efektivní rychlosti ve prospěch novějšího modelu. Lze tedy očekávat, že model RTX 2080TI zvládne totožnou úlohu, tedy prolomit osmi znakové heslo v systému Windows téměř 12x rychleji než model z roku 2012.

Společnost *SafetyDetectives* vytvořila pro rok 2020 aktuální žebříček nejlepších „Top 10 Anti-Spyware“, kde se každý software testuje na danou komplexní skupinu Malwaru, Spywaru, Virů aj. Každý jednotlivý software má označení své dominantnosti.

Tabulka 1 Výsledky nejlepších Anti-Spyware pro rok 2020

Norton 360	Best for All-Around Protection
McAfee Total Protection	Best for Extra Anti-Spyware Features
TotalAV	Best New Antivirus Software
Bitdefender Total Security	Best for Secure Banking
Malwarebytes	Best for Ease-of-Use
Avira Antivirus Pro	Best for Keylogger Detection
Adaware Antivirus Total	Best for Securing Personal Information
SUPERAntiSpyware	Best for Additional Spyware Protection
SpywareBlaster	Best for Browsing Protection
Spybot Search and Destroy	Best for Advanced Users

Zdroj: Robert Bateman (safetydetectives.cz)

5.1.3 DDoS útok

DDoS (Distributed Denail of Service). Jedná se o jeden ze tří typů útoků DoS (Denail of Service). Lze přeložit do češtiny jako potlačení služby. Útočník využívající DDoS útok odesílá objemné množství paketů pomocí velkého množství zařízení. Systém sice tyto požadavky má řešit, avšak nikoli v tak rozsáhlém množství. Cílem útoku je omezení funkčnosti některých síťových služeb či jejich vyřazení z provozu (např. webových stránek, serverů apod.).

5.1.3.1 Cíle podle rizika

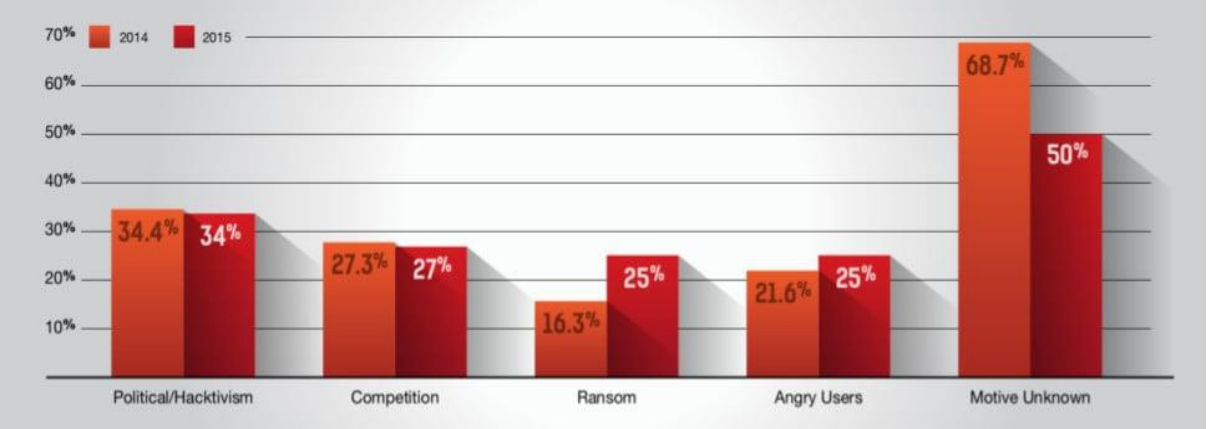
Podle statistiky společnosti Root.cz je možné rozdělit cíle do tří skupin podle míry rizika útoku:

- Vysoké riziko – ISP, hosting, vlády, vzdělávací instituce
- Střední riziko – finance, zdravotnictví, maloobchod, mobilní segment
- Nízké riziko – energie, služby, jednotlivci

Nejčastěji se útočí na služby, které jsou vytvářeny automaticky. „*Nikdy nevíte, kdo si službu objednává a jak ji má zabezpečenou.“* Naopak nejméně jsou ohroženi jednotlivci. *„Viděli jsme počet, ale jedná se o velmi malé množství.“* (Krčmář, 2016).

Zásadní je, že cílem útoku se může stát jakékoliv zařízení připojené k internetu. Důležitým faktorem je, zda jsou služby na takový útok připravené a kolik se do přípravy věnovalo financí a úsilí. „*Máme útoky, které trvají hodiny, ale i takové, které trvají dny.“* (Krčmář, 2016). Záleží dále na tom, zda si můžete dovolit službu na tuto dobu odstavit a počkat, až útok přejde. „*Proti útoku DDoS neexistuje univerzální ochrana, která vám zaručí stoprocentní účinnost. Spousta zákazníků to ale očekává.“* (Krčmář, 2016)

Obrázek 5 Přehled motivu útoků DDoS společnosti Radware



zdroj: root.com

Společnost Radware analyzovala motiv útoku s cílem znepřístupnění služby za rok 2014 a 2015. Nejmenší podíl tvoří dle grafu touha po výkupném. Za to největším známým podílem je politický hacktivismus[8]. Nejvyšší podíl vůbec tvoří ostatní neznámé motivy, které v roce 2014 činily téměř 69 % celkového poměru DDoS útoků. Dá se tedy očekávat, že spousta útoků vzniká za účelem slávy či uznání hackerské komunity, což koresponduje s výše uvedeným názorem v kapitole „Taxonomie útočníků dle motivace“ dle Jirovského (2007). Dalšími motivy jsou tzv. Angry Users (naštvaní uživatelé) nebo „hackerská soutěž“ v jejich komunitě.

5.1.3.2 Jak se proti útoku DDoS bránit?

Podle Amazon.com je důležité zavést omezení šíření nadměrného množství paketů. Ve výsledku server příjme pouze tolik žádostí, kolik dokáže zpracovat.

Další způsob útoku je využití příkazu „ping“. Vysláním příkazu do sítě místo počítače, automaticky přijde odezva od všech zařízení v síti. Odpovědi se přesměrují na IP vybraného zařízení, ten je následně zahlcen.

Poslední způsob je zahlcení volných systémových prostředků. Útočník pošle cílovému zařízení oběti určité množství paketů typu SYN[9] a díky tomu nemá cílený počítač volné prostředky pro spojení (Jirovský, 2007).

Útoky jsou prováděny ve většině případů jednotlivými „nadšenci“ či skupinami z důvodu rychlého nárůstu popularity či upozornění na zranitelnost systémů. Potenciálně

v největším nebezpečí jsou velké firmy, kde odstavení serverů může mít za následek miliardové ztráty. Nejedná se o útok, kde by hlavní aspekt „hrála“ touha po bohatství.

5.1.4 Scam 419 (Nigerijské dopisy)

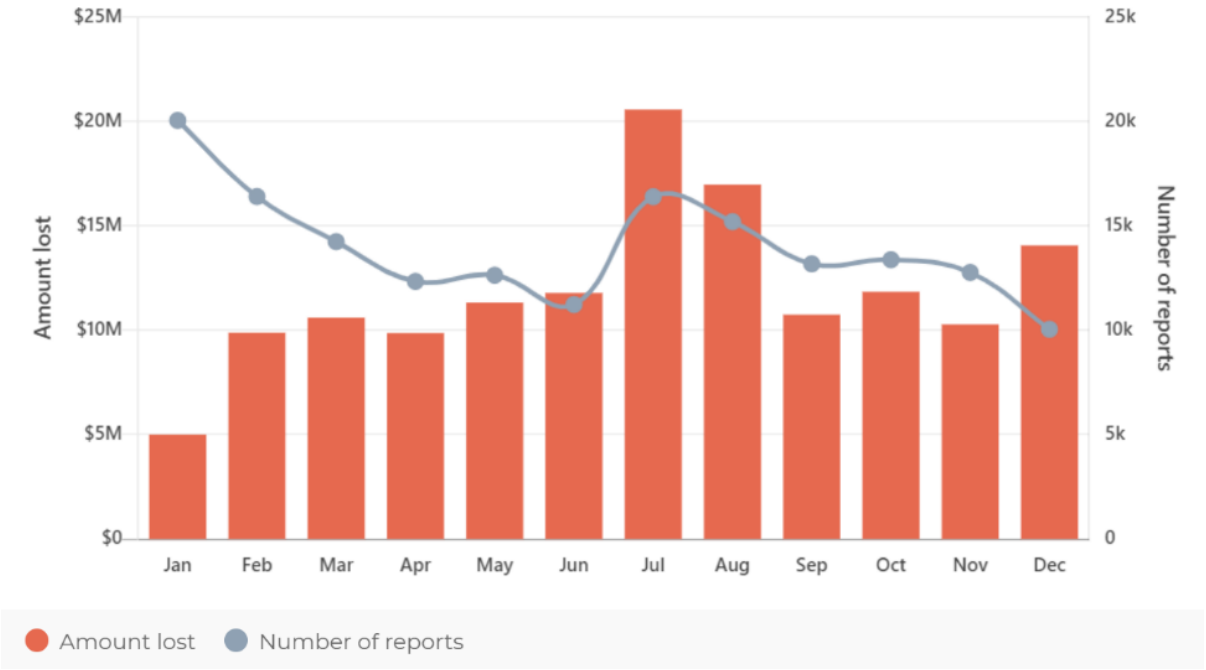
Jedná se o způsob počítačové kriminality, které jsou realizované se záměrem obohacení se. Je to způsob, který má kořeny u klasických dopisů a je ukázkou přenosu běžné kriminality ze světa reálného do světa virtuálního, a proto je považován za jeden z nejstarších, jehož kořeny sahají do 18. století (Hoax.cz, 2020). E-mail a internetová komunikace pomohla pachatelům k enormnímu rozmachu tohoto způsobu. Podle webu Timehosting (2015) se jedná o nejrozšířenější způsob internetového podvodu.

Podvod byl založen na následujícím principu: oběť obdržela dopis s přesvědčivou historkou o nelegálním získání velkého obnosu peněz. Pachatel se potřebuje dostat k informacím o účtu poškozeného. Oběti je nabídnuta odměna ve výši většinou 10-30 %. Naivní poškozený poskytne údaje o svém účtu, aby mohla být provedena transakce, ale místo zaslání peněz jsou z účtu ukradeny. Jsou známy případy, kdy oběť přišla o několik tisíc dolarů.

Jedná se o formu, která je velice riskantní pro pachatele z toho důvodu, že je zapotřebí s obětí komunikovat dlouhodobě a je tedy snadno vystopovatelný. Nicméně podvod vykazuje vysokou latenci, protože pachatel udělá ze své oběti spolupachatele. Málokdo je v takovém případě ochotný podat trestní oznámení s vědomím, že sám bude pravděpodobně podezřelý z podílení se na nelegální činnosti. Proto je velice těžké přesně určit skutečné ztráty, které tento druh podvodů opravdu způsobil a nadále působí.

Úspěšnost typického nigerijského dopisu se těžko odhaduje, nicméně existuje webový server *Scamwatch.gov.au* zabývající se scamy všeho typu. Za rok 2019 je udávaná hodnota úspěšnosti 11.8 % s celkovými ztrátami 142.9 milionu dolarů.

Obrázek 6 Graf úspěšnosti útoků SCAM419 za rok 2019



Zdroj: Scamwatch.gov.au

5.1.5 Hoax

Hoax je označení pro poplašné řetězové zprávy, které uvádějí formu spamu, případně scamu. Jsou následujícího typu: „pošli to dál, pokud to nepošleš 20 dalším lidem, tak se stane…“ aj., které uvádějí zkreslené, nepravdivé či jiné zavádějící falešné informace. Hoax obsahuje často varování před útoky, popisy nebezpečí, prosby o pomoc, výzvy, petice, prohlášení slavných, řetězové dopisy štěstí, žertovné zprávy, obrázky a videa v prezentacích, hrající si zvířata atd.

5.1.5.1 Příklady typu Hoax

Příklad 1:

„Synovec jednoho z mých spolužáků úspěšně vystudoval vysokou školu a nyní pracuje v nemocnici v Shenzhenu. Zapojil se do studie virové pneumonie ve Wu-chanu. Zavolal mi a požádal mě, abych řekl přátelům: Pokud máte rýmu a kašel - nejedná se o pneumonii coronaviru, protože pneumonie coronaviru se projevuje suchým kašlem bez nachlazení! Toto je nejjednodušší způsob identifikace. Předejte informaci svým přátelům, aby se dozvěděli více o identifikaci a prevenci.“

Příklad 2:

„Prosím, aby toto upozornění svým přátelům, rodině a kontakty! V nadcházejících dnech by měli být opatrní: Neotevírejte žádné zprávy s přiloženém dokumentu: Aktualizace systému Windows live "(Windows live aktualizace), kdo to poslat. Jedná se o virus, který korumpuje celý pevný disk. Tento virus přijde od kamaráda, který máte v seznamu adres. Proto bychom měli zaslat tento dopis všem vašim kontaktům. Pokud obdržíte zprávu s názvem: "Aktualizace systému Windows live" (Windows live aktualizace), i když je poslal přítel, neotvírejte nebo vypnout počítač okamžitě. To je nejhorší virus oznámila CNN. Microsoft charakterizovat jako nejničivější virus, který existoval. Včera odpoledne byl rozpoznán virus Mc Afee (antivirový program). Stále není pult pro něj. Jen zničí nulový sektor (sektor Zero) na pevném disku. PAMATUJ: Pokud se tato zpráva odeslána, pomáhá všem-abcd_105, Today, 00:31“

Z důvodu zahraničního původu se často vyskytují gramatické, stylistické či formální chyby a mnohdy nedává z překladu věta žádný smysl. Asi nejspolehlivějším způsobem, jak zjistit, zda se jedná o poplašnou zprávu, je nastudovat druhy poplašných typů hoaxů, které se nejčastěji vyskytují. Dle mého názoru se postupem času lze orientovat v Hoaxu takovým způsobem, že nepravdivé tvrzení lze odhadnout. Vyskytují se samozřejmě i natolik sofistikované a nekonvenční zprávy, které databáze neobsahuje a lze jen těžko určit, zda jsou pravdivé. *Nejrozšířenější Hoaxy je možné nalézt na webové stránce www.hoax.cz.*

5.1.6 Podvodné nabídky

Skutečnost, že lze koupit cokoliv, kdykoliv a kdekoliv, je snad pro každého z nás velice zajímavá, avšak důležité je si uvědomit, že velké množství serverů nabízejí na první pohled lákavé nabídky jen z jednoho důvodu. Díky technologickému vzestupu a obchodování na internetu, stačí zločincům pouze legitimně tvářící se webová stránka a nemusí s osobou přijít vůbec do kontaktu.

Např. server *Hypoindex.cz* pojednává o podvodných nabídkách „výhodných“ úvěrů, kde cílem útočníka je pouze vylákat z oběti tzv. „vratnou“ zálohu od důvěřivých lidí.

5.1.6.1 Příklad inzerátu:

Text inzerátu:

„Perfektní nabídka nebankovního úvěru bez poplatků a bez ručitele od 40.000 Kč až do 1.500.000 Kč. Individuální přístup ke každé žádosti, díky čemuž může úvěr získat téměř každý žadatel. Výše měsíčních splátek a doba splatnosti se dá přizpůsobit vašim možnostem. Tato nabídka platí pro celou ČR. Vytvoření konkrétní nabídky zcela zdarma a nezávazně na emailu.“

Projeví-li potenciální klient zájem o zprostředkování úvěru, následuje zažádání o „vratnou“ kauci za poskytnutí úvěru. Stejně jako zprostředkování bezlicenčních půjček se jedná o postup, který zákon o úvěru spotřebitele zakazuje.

„Před uzavřením smlouvy o spotřebitelském úvěru nevzniká poskytovateli nebo zprostředkovateli právo na odměnu nebo jinou platbu s výjimkou práva na náhradu daní, správních poplatků nebo jiných obdobných peněžitých plnění a účelně vynaložených nákladů na ocenění předmětu zajištění spotřebitelského úvěru.“

Zákon č. 257/2016 Sb., § 83, odst, 1., věta první

Že lidé, kteří zaplatili danou zálohu, své peníze už neuvidí, je více než jasné. Další postup by měl následovat k podání trestního oznámení.

Podvodných nabídek se na internetu vyskytuje plná řada a to různých typů, ať už se jedná o internetový obchod prostřednictvím sociálních sítí, podvodné e-shopy nebo falešné nabídky.

5.1.6.2 Jak rozeznat podvodný e-mail od pravého?

Důležité je vzít v potaz „selský rozum“.

- Podezřelá e-mailová adresa – uživatelské jméno je libovolné a lze v průběhu času měnit, ovšem pokud e-mailová adresa nemá příliš společného s oficiální doménou, je zapotřebí se mít na pozoru.
- Gramatické, pravopisné či stylistické chyby – nachází-li se ve zprávě podezřelé množství chyb, je vysoká pravděpodobnost, že se jedná o internetový podvod.

Z vlastní zkušeností můžu říci, že většina doručených e-mailových podvodů pochází ze zahraničí, tudíž ve velkém množství zpráv je využití „google translate“ zcela běžnou záležitostí a mnohdy může věta postrádat smysl.

- Podezřele výhodné nabídky – může se jednat o enormně nízkou cenu elektroniky, dovolené nebo jazykové kurzy.
- Sdělování osobních údajů e-mailem – Jedná-li se o banky, internetové obchody či jiné online služby, zpravidla nikdy neprobíhá žádost o osobní údaje prostřednictvím e-mailové pošty.

5.1.7 Phishing

Pojem phishing je nejčastěji označován pro podvodné či klamné jednání, jehož cílem je získat citlivá data o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj.

Phishingový útok je mezi kyber-živly velmi oblíbenou technikou, a proto se ji snaží stále vylepšovat a optimalizovat. Dle společnosti Eset (2019) je nejčastějším způsobem pokus o krádež citlivých informací kreditní karty nebo internetového bankovnictví. Útok probíhá prostřednictvím podvodného e-mailu. Oběť obdrží zprávu s odkazem na externí webovou stránku s formulářem na zadání čísla kreditní karty a kód CVV[10]. Pokud oběť danému e-mailu uvěří a následně:

1) zadá své přihlašovací údaje podvodnému webu

2) nainstaluje podvodnou aplikaci, která dokáže obejít i dvoufázové SMS ověření

Pak má útočník všechny potřebné údaje pro vybílení účtu dané oběti.

V minulosti se phishing dal jednoduše odhalit na první pohled, a to především z toho důvodu, byl text psán neformální češtinou, místy nepřeloženými slovy z původní zahraniční zprávy, útočník žádal zadávání přihlašovacích údajů přímo do e-mailu a při podvodném odkazu doména neodpovídala doméně finanční instituce. V dnešní době se lze setkat i s tzv. „dokonalými phishingovými zprávami“, které od běžné komunikace dokáže odhalit pouze velmi pozorný nebo zkušený uživatel.

Upozornění:

1) Platí, že banka po vás nikdy nežádá zadávání citlivých upozornění do emailu.
2) Důležitá je kontrola URL adresy, která musí odpovídat dané instituci.
3) Často může dojít k obecnému či neformálnímu oslovení

Obrázek 7 Příklad phishingu České spořitelny.

Zdroj: securitymagazin.cz

5.1.8 Spearphishing

Jde o pokročilejší metodu phishingu, kde útočník zná všechny potřebné informace o dané oběti a vytvoří phishingový e-mail, přesně „na míru“. Dle společnosti Eset se nejčastěji jedná o manažery a majitele firem a lze jej přirovnat k perfektně vyrobenému padělku. Je tedy zřejmé, že odhalit tak sofistikovaný phishing je obvykle velice obtížné.

5.1.9 Malware

Jedná se o program, který byl vytvořen za účelem poškození nebo vniknutí do počítačového systému. Pojmem Malware se ale nerozumí pouze software samostatný, který je lidmi často takto chápán, ale zahrnuje souhrnné označení pro počítačové viry, červy, špehovací software (spyware), keyloggery, trojské koně, vyděračský software (ransomware) a reklamní software (adware). Obecně lze říci, že se řadí k Malwaru veškerý software, který byl vytvořen se záměrem poškození.

Motivem pro vznik bývá pomsta. Typickým příkladem může být programátor propuštěný ze zaměstnání, který může v systému zanechat tzv. „backdoors“ (zadní vrátka) nebo softwarovou „časovanou bombu“ která umožní například zničit v budoucnu systémy bývalého zaměstnavatele. (Wikipedie, 2017)

5.1.10 Trojský kůň

Z hlediska běžného uživatele je Trojský kůň považován za jeden z nejznámějších kybernetických problémů. Mnohdy fráze „Trojan“ zastupovala obecné slovo „Vir“, kdy si uživatel nebyl jistý z jakého důvodu jeho počítač odmítá příkazy či se nesprávně zobrazuje. Často se tedy podle něj jednalo o Trojského koně. Trojským koněm je označován škodlivý kód, který je ukrytý v počítačovém softwaru a který může budit užitečný dojem. Může se jednat o celou řadu aplikací, a to např. „cracky“ aplikací, kdy uživatel pátrá po licenci dané aplikace, která umožní obejít platební metodu. Často je řeč o softwaru na odstranění malwaru, kde se taktéž může trojský kůň objevit. Aby vytvořil domnění, že původ patří legitimnímu zdroji, často zneužívá oficiální e-mailové klienty či věrohodné webové stránky.

„Paralela v názvu je nalezena v řecké mytologii o dobytí bájné Troje, kde byl dřevěný kůň zdánlivým darem, avšak ve svých útrobách nesl řecké vojáky, kteří se později města Troje zmocnili.“

V počítačovém světě má stejné poslání, protože účelem je získání moci nad samotným počítačovým systémem. Řeč je o citlivých informacích, jako jsou hesla k účtům, osobní soubory nebo vzdálené ovládání systému. Od počítačového viru se liší tím, že se obvykle sám nešíří.

Stejné poslání má i Trojský kůň v počítačovém světě, protože jeho účelem je často získat moc nad systémem, kam byl propašován. Jde o získávání hesel, manipulaci se soubory uživatele, ovládání běžících systémů (vzdálené ovládání systému) apod. Na rozdíl od počítačového viru se zpravidla nesnaží o své „samošíření“.

5.1.10.1 Jak se bránit proti Trojskému koni?

Jedná-li se o „primitivnější“ a nepříliš dokonale promyšlené trojské koně, lze jejich chod zpozorovat ve správci úloh, avšak ve velkém množství případů proces nelze ukončit. U sofistikovanějších trojských koní je aktivita skryta a lze se škodlivého softwaru zbavit prostřednictvím antivirových programů, které obsahují funkce jako „rezidentní štít“, tedy ochranu běžící na pozadí v přítomném čase a chrání zařízení během chodu. Typy bezpečnostních softwarů jsem uvedl v dřívějších kapitolách (viz. tabulka č.1).

5.1.11 Keylogger

Obzvláště nebezpečná utilita pro každodenního uživatele patřící do skupiny špionážní techniky, a to z důvodu rozmanitosti. Ve srovnání s populárními viry se jedná o méně poutavé útoky a jejich literatura existuje jen ve velmi omezené míře, díky čemuž jsou prakticky nevystopovatelné. Jedná se o software zaznamenávající konkrétní stisky kláves (monitoring akcí uživatele) na napadeném počítačovém systému. Nejčastěji bývá využíván k zaznamenávání přihlašovacích údajů k účtům. Keylogger nabízí širokou rozmanitost a software bývá často připojován k souboru „.exe“, přibalován k spywarovým aplikacím nebo ho lze najít ve phishingových e-mailech.

Po detekci dat keyloggerem lze přednastavit e-mailové upozornění, kde útočníkovi dorazí e-mail o úspěšnosti a získaném obsahu. Pokud by nedošlo k detekci potřebných informací pro útočníka, lze také nastavit zasílání informací v nastaveném časovém intervalu nebo dle objemu zaznamenaných dat. Keyloggery se nejčastěji užívají za účelem odhalit hesla uživatelů, čísla platebních karet, čísla bankovních účtů, obsah korespondence a další citlivé údaje. Keyloggery existují také hardwarové, kde se ve většině případů jedná o fyzický flash disk, na kterém je škodlivý kód nahrán. Z důvodu fyzické přítomnosti napadení se jedná o jednoduše odhalitelný postup.

5.1.11.1 Test nepozorované krádeže přihlašovacích údajů

Protože se jedná o legitimní software, má vysoké zastoupení ve velkých společnostech, firmách apod., pro kontrolu svých zaměstnanců. Své zastoupení našel i v kontrole dítěte rodiči, kde rodič získává prostřednictvím monitoringu přehledný obsah o činnosti svého dítěte.

Věnovat se budu zneužití keyloggeru jako nástroje pro detekci osobních údajů, tedy bez souhlasu a vědomí uživatele.

V následující kapitole se věnuji testu legitimního softwaru využívajícího často ve firmách a různých společnostech ke kontrole svých zaměstnanců. Tato kapitola v žádném případě neslouží k zneužití, ale jako ukázka, jakým způsobem může útočník přistupovat k citlivým informacím.

5.1.11.2 Jak nebezpečný může být napadený PC?

Pro svou nebezpečnost a zásah do soukromí běžných uživatelů jsem keylogger vybral jako praktickou ukázku, kde mi konkrétně posloužila 7 denní zkušební verze keyloggeru s názvem All In One Keylogger od RelyTec.

Abych minimalizoval pravděpodobnost vlastního napadení, jelikož samotný keylogger může obsahovat škodlivý kód cizího keyloggeru, využil jsem software VirtualBox[10], prostřednictvím kterého jsem na svém fyzickém PC, vytvořil PC virtuální, kde by za předpokladu napadení útočníkem nebyla pravděpodobnost získání mých osobních informací. Jako příklad jsem zvolil odhalení přístupových údajů e-mailu na www.seznam.cz.

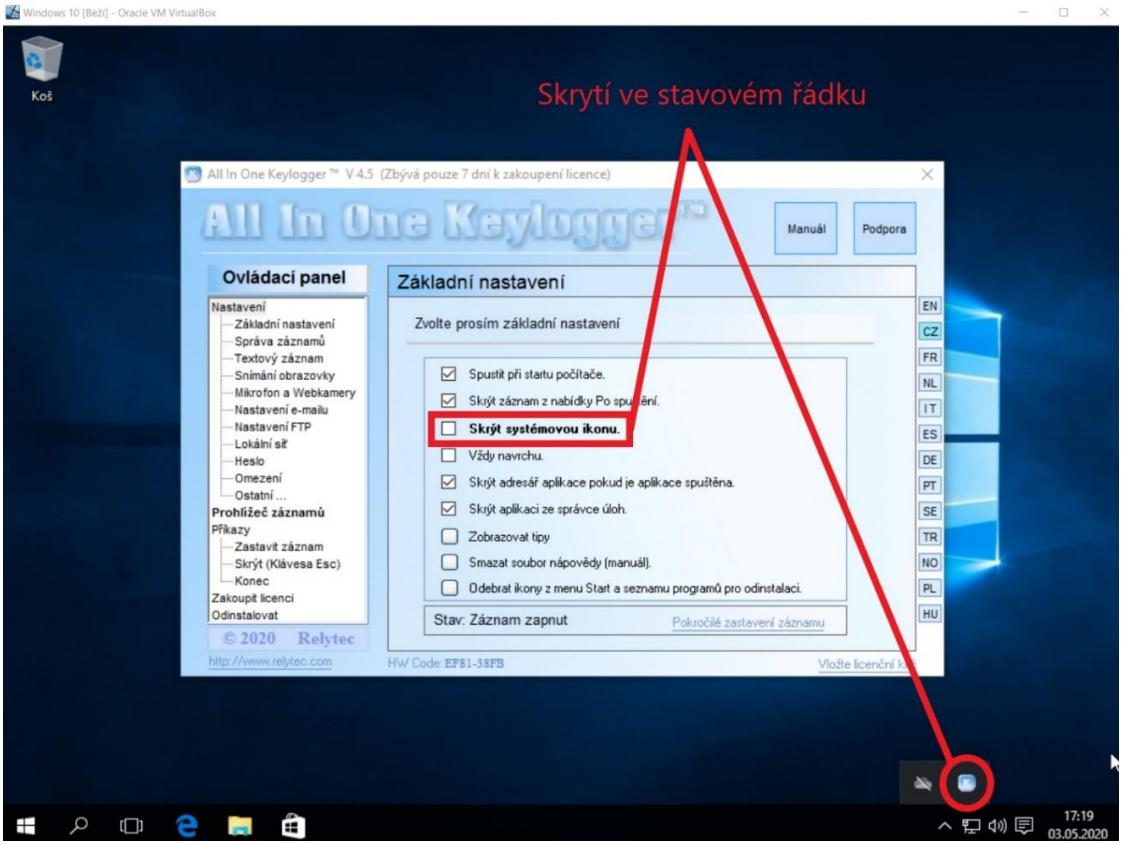
Činnosti oběti:

1. Otevření webového prohlížeče
2. Přesměrování na web www.seznam.cz
3. Zadání přihlašovacích údajů (jako příklad jsem zvolil fiktivní přihlašovací údaje, kde: Login: AUTOBUS, Password: AUTOBUS)

Keylogger:

Oběť na první pohled nemá možnost při kontrole zjistit, zda se na zařízení keylogger nachází. Moderní keyloggery jsou schopny skrýt aktivitu v nabídce procesů a místní soubory samotného softwaru. Při kontrole zaměstnanců se ve většině případů ukládají informace mimo lokální PC, náhradou bývá místní či internetový server.

Obrázek 8 Skrytí aktivity keyloggeru (anonymita pro běžného uživatele)



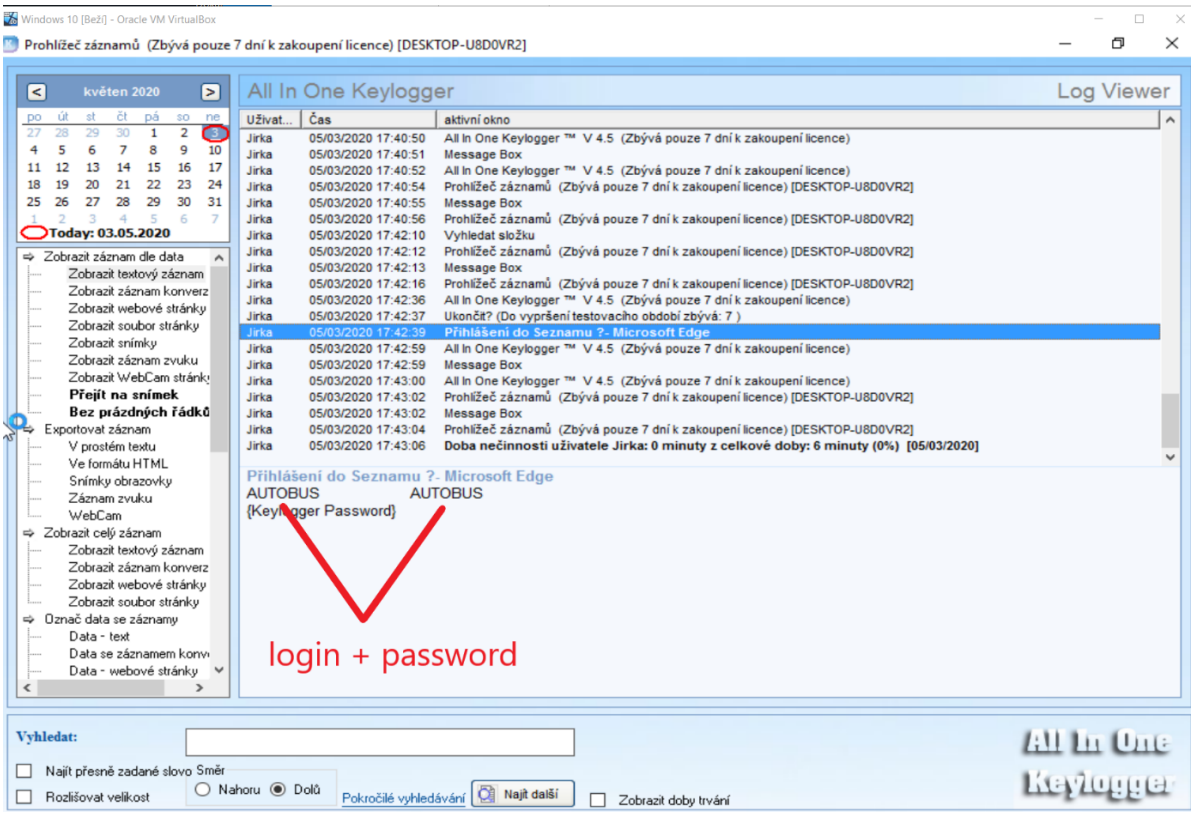
Keyloggery skrývají svoji činnost především z toho důvodu, aby uživatel nemohl software jednoduše vyřadit z provozu. Prostřednictvím mechanismu systému Windows využívají tzv. *hook*. Tento mechanismus vytváří možnost instalace speciálních procedur a monitoring určitého typu zpráv ještě dříve, než dojde ke zpracování samotnou aplikací. V systému Windows se nachází více typů *hooku*. Pro příklad: Když se objeví v systému událost asociovaná určitým typem *hooku*, systém automaticky exportuje zprávu nejbližší proceduře, která je v odpovídajícím seznamu pro danou událost. Prostřednictvím této procedury se provede export následující proceduře v konkrétním seznamu. Vždy export probíhá po jednotlivých

procedurách a vždy dochází buď k monitoringu, nebo změně či ukončení distribuce zprávy a tím zamezí zobrazení procesu ve správci úloh.

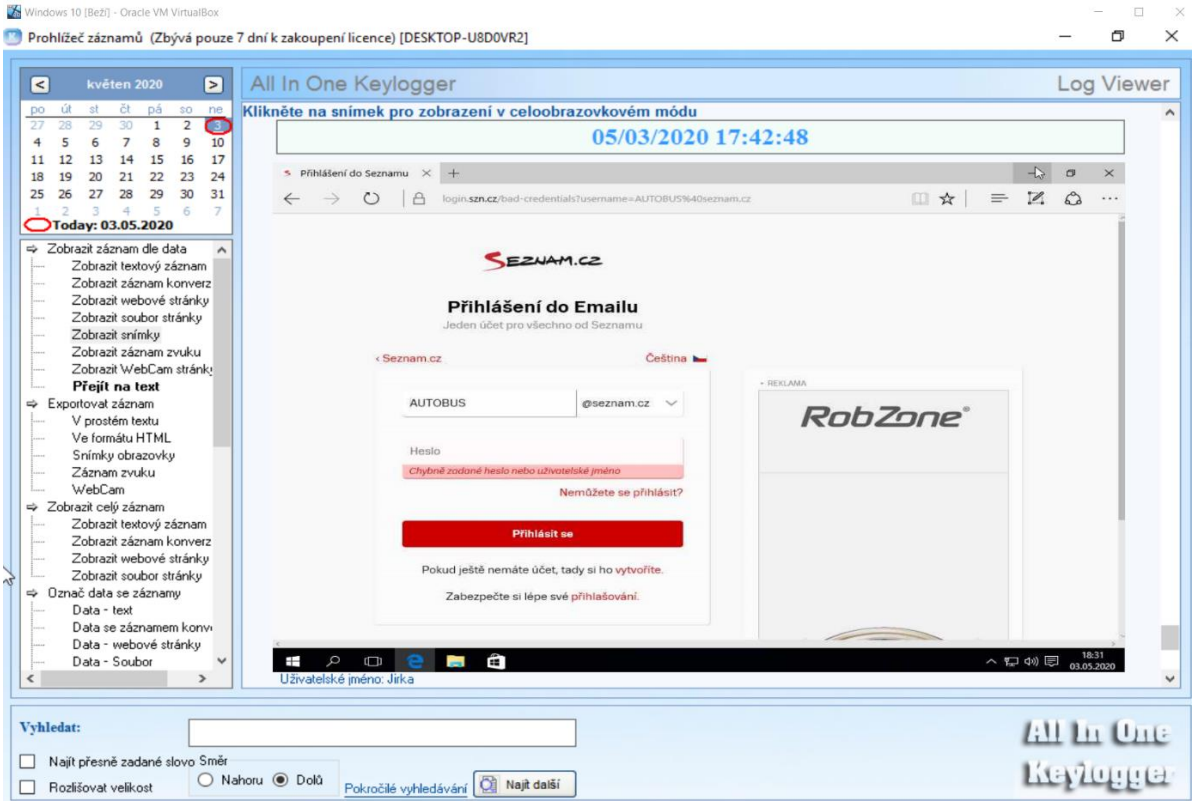
Keylogger All In One má rozsáhlou nabídku možností, kde lze monitoring činností procházet následujícími způsoby:

1. Textový záznam – umožňuje v textovém režimu číst jednotlivé stisky kláves.
2. Snímání obrazovky – umožňuje tzv. screenshot obrazovky, který umožňuje znázornit obrazovku z pohledu oběti.
3. Mikrofon a webkamery – některé typy keyloggerů umí snímat mikrofon i s webkamerou, který obzvláště útočí na soukromí.

Obrázek 9 Zobrazení textového režimu



Obrázek 10 Zobrazení režimu „screenshot“



5.1.11.3 Závěr testu

Davy lidí mohou na tento druh utility nahlížet takovým způsobem, že pokud se útočník dostane k informacím běžné e-mailové schránky, ale dotyčný své soubory uvnitř nepovažuje za důležité, stačí pouze změnit e-mailové heslo a útočník o všechna získaná data přichází. Ovšem podíváme-li se na problematiku z jiného pohledu, tak je důležité vzít v potaz, že *„Pro lenost je člověk pilný“* (Zachar, 2016). Mířím tím na všechny ostatní druhy serverů, kde dotyčný pod stejným registračním e-mailem používá stejné heslo, ke kterým právě onen útočník získal přístup. Lze předpokládat, že většina útočníků míří k finančnímu obohacení a stejný princip využije např. u internetového bankovnictví.

5.1.11.4 Jak se bránit proti keyloggeru?

Vzhledem k povaze funkcí nacházející se v tomto druhu softwaru lze očekávat, že se jedná o nebezpečný nástroj, který čím déle působí, tím více je nebezpečný. Proto níže uvedu typy tzv. *anti-keyloggerů,* které se specializují na odstranění tohoto typu špionážního softwaru.

Mezi nejlepší produkty bych zařadil výše uvedený software Spybot Search and Destroy. Software není primárně určen k vyhledávání keyloggerů, nýbrž jako utilita možná analyzovat primárně Spyware. I přes tento fakt v testu, kde jsem provedl instalaci 3 typů keyloggerů (Spyrix, All In One Keylogger, BlackBox), tento „anti-keylogger“ byl schopný analyzovat a nalézt všechny 3 zmíněné typy keyloggerů. Dle názoru Sergeie Petrenkova v knize Big Data Technologies for Monitoring of Computer Security tedy nelze vyvrátit, že rozšiřování databází bohatým způsobem narůstá.

5.1.12 Sniffing

Sniffing je specifická technika umožňující odposlouchávání počítačů v lokální síti (ukládání a následné čtení TCP paketů), která se používá např. při diagnostice sítě. V rukou crackera může sniffing zajistit zcela jiný rozměr a smysl. Lze např. analyzovat hesla či nikým nerušeně sledovat tok dat na síti příslušné datové komunikace nebo provozu celé sítě, což generuje přínosné informace. Sniffing zcela supluje činnost spywaru (špionáž dat) či keyloggeru (monitoring přihlašovacích údajů). Software zajišťující činnost za pomoci crackera se nazývá sniffer. Důležitého asistenta sniffingu může zastupovat Trojský kůň, protože může obsahovat integrovanou funkci, která je adekvátně upravena pro techniku sniffingu.

6 DOTAZNÍKOVÉ ŠETŘENÍ

V této části bakalářské práce se budu zabývat výsledky svého dotazníkového šetření, které jsem vyhodnotil na základě ankety vyplněné 148 respondenty. Pro přehlednou orientaci jsem některé výsledky exportoval do grafů.

6.1 Otázky dotazníkového šetření:

1) **Pohlaví:**
   a) Muž
   b) Žena

2) **Váš věk?**
   a) Méně, než 15 let
   b) 15–20
   c) 20–25
   d) 25-35
   e) 35-45
   f) 45-55
   g) 55+

3) **Nejvyšší dosažené vzdělání?**
   a) ZŠ
   b) SOU
   c) SŠ
   d) VOŠ
   e) VŠ

4) **Setkal/a jsi se někdy s kybernetickou kriminalitou na internetu?**
   a) Podvodné jednání
   b) Krádež účtu (Sociální sítě, Internetové bankovnictví)
   c) Zločin z nenávisti
   d) Nesetkal/a
   e) Jiné

5) **Jaká si myslíš, že je nejčastější taxonomie útočníků dle motivace? (co útočníky k útoku vede)**
   a) Napište jedno nebo více slov…

6) **Anonymita (1) (vyberte jednu nebo více odpovědí)**
   a) Navštěvuji všechny webové stránky
   b) Navštěvuji jen stránky, které jsou ověřené
   c) Navštěvuji stránky, které potřebuji, bez ohledu na riziko
   d) Používám VPN, Proxy

7) **Anonymita (2)**
   a) Registruji se na všech stránkách
   b) Registruji se pouze na ověřených stránkách
   c) Neregistruji se, protože se nikomu nedá věřit

8) **Kontroluješ si URL adresy navštívených stránek? (stavový řádek)**
   a) Ne
   b) Ano

9) **Navštívil/a jsi někdy tzv. darkweb?**
   a) Ano
   b) Ne
   c) Nevím, co to je
   d) Chci, ale nevím, jak na to

10) **Pokud ano, co tě k tomu vedlo?**
   a) Necenzurované informace
   b) Zvědavost
   c) Objednávky/prodej
   d) Sex, drogy
   e) Nenavštívil jsem

11) Jakou finanční škodu dle tvého názoru způsobil kybernetický terorismus doposud? (tip v CZK, € nebo $)

a) Napište jedno nebo více slov…

12) Říká ti něco pojem Keylogger?

a) Ne

b) Ano

13) Přišel ti tento měsíc hoax typu: pošli to dál, nebo…?

a) Ano

b) Ne

c) Ne, ale tento rok ano

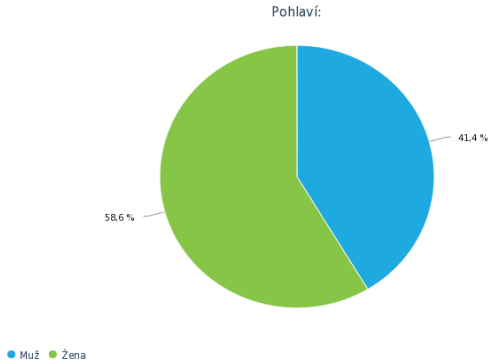
6.2 Vyhodnocení dotazníkového šetření

Otázka 1

Pohlaví:

Dotazníkového šetření se zúčastnilo 148 respondentů. Z toho 58,6 % tvoří ženy a zbylých 41,4 % tvoří muži. Jelikož se jedná o globální problematiku, převaha žen v tomto případě vůbec ničemu nevadí.

Graf 1. Pohlaví respondentů

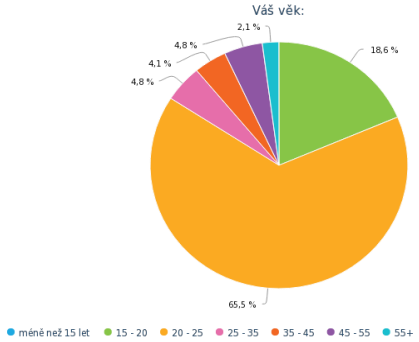


Otázka 2

Váš věk:

Dle *grafu 2* je patrné, že největší podíl zástupců tvoří kategorie 20-25 let, jelikož jsem dotazník sdílel na sociálních sítích, kde se dle mého názoru právě tyto věkové skupiny zdržují. Vzhledem k okolnostem využívání sítě internet se podle očekávání nejmenší zastoupení objevilo v kategoriích patřící lidem ve starším věku. Velké procento zastupuje také věková kategorie 15-20 let.

Graf 2. Věkové zastoupení respondentů

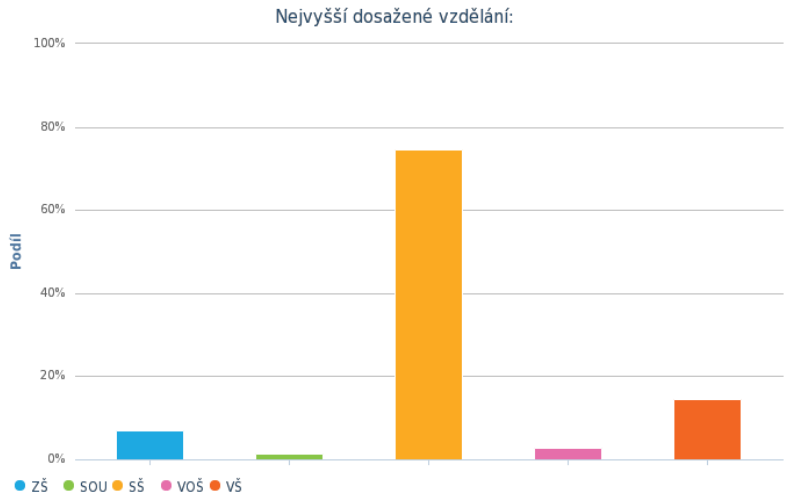


Otázka 3

Nejvyšší dosažené vzdělání?

Tuto otázku jsem zvolil z důvodu přehledu respondentů hlasujících v mém dotazníku, jelikož dle anonymní ankety serveru *PCTuning.cz* největší podíl páchané kyberkriminality tvoří právě lidé se středoškolským vzděláním. Právě tato kategorie tvoří největší podíl a je tedy logické, že přímo-úměrně se může jednat o největší procentuální zastoupení kybernetických útočníků.

Graf 3: Vzdělání respondentů



Otázka 4

Setkal/a jsi se někdy s kybernetickou kriminalitou na internetu?

- Podvodné jednání *(33,1 %)*
- Krádeže účtu (Sociální sítě, Internetové bankovnictví) *(46,9 %)*
- Zločin z nenávisti *(5,5 %)*
- Nesetkal/a *(18,5 %)*
- Jiná *(8,1 %)*

Dle výsledků ankety se podle očekávání nejvíce rozšířeným typem kybernetické kriminality stala krádež účtu a podvodné jednání, kde v součtu hlasovalo *80 %*. S žádným typem kybernetické kriminality se nikdy nesetkalo *18,5 %* respondentů. Pouze jeden respondent se potýkal se zašifrováním dat s následným požadavkem o zaslání dané finanční výše.

Mé poznatky ukazují, že krádeže účtů jsou nejrozšířenějším typem útoků především z toho důvodu, že komplikace zabezpečovacích hesel je u celé řady populace velice „jednoduchá“ pro tzv. „prolamovače hesel“. Web *pctuning.cz* zpracoval žebříček nejpoužívanějších hesel do roku 2018, které jsou následující:

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. 123123
18. dragon
19. passw0rd
20. master
21. hello
22. freedom
23. whatever
24. qazwsx
25. trustno1

Z výše uvedeného seznamu je jednoznačné, že nejčastější typy hesel jsou takové, které jsou snadno zapamatovatelné, avšak dle mého názoru je důležité upozornit, že většina „slovních“ hesel je psána anglicky.

Angličtina se řadí podle statistiky *ESL Stories* na 3. místo nejrozšířenějších jazyků na světě s celkovým počtem 379 milionů aktivně mluvících lidí. Lze tedy očekávat, že nespočetné množství zvolených hesel bude právě v tomto jazyce. Mé doporučení ke správnému zvolení hesla zní, že v poměru snadného zapamatování a vysoké efektivity, je pro česky mluvící populaci výhodné zvolit právě kombinaci českých slov s libovolnými znaky, čísly a využitím diakritiky.

Otázka 5

Jaká si myslíš, že je nejčastější taxonomie útočníků dle motivace? (co útočníky k útoku vede?)

Zdůrazňuji, že tato otázka byla otevřená a nastavil jsem tedy možnost jejího přeskočení. K této otázce se vyjádřilo *78 %* respondentů, 67 respondentů nezávisle na sobě odpovědělo, že se jedná o pomstu, závist a 19 respondentů se zmínilo o politické motivaci, což do jisté míry souhlasí s názorem, který jsem řešil ve výše uvedených kapitolách.

Otázka 6

Anonymita (1):

- Navštěvuji všechny webové stránky.
- Navštěvuji jen stránky, které jsou ověřené.
- Navštěvuji stránky, které potřebuji, bez ohledu na riziko.
- Používám VPN, Proxy.

V této otázce jsem úmyslně uvedl možnost zvolení první i třetí odpovědi (s možností pouze jednoho výběru), jelikož se jedná o synonyma a zvyšuje objektivnost odpovědí. Lze tedy říci, že celých *67,1 %* respondentů navštěvuje jakýkoliv druh webových stránek bez ohledu na riziko.

Z dotazníkové analýzy vyplývá, že mezi oběti kybernetických zločinců se řadí spousta jedinců, kteří jsou nedbalí vůči činnostem, které v kyberprostoru provádějí. Osobně můžu konstatovat, že názor anonymního uživatele kybernetického fóra: „*Vše je založeno na lidské blbosti",* je pravdivý.

Otázka 7

Anonymita (2):

- Registruji se na všech stránkách.
- Registruji se pouze na ověřených stránkách.
- Neregistruji se, protože se nikomu nedá věřit.

Na daný typ otázky odpovědělo *86,1 %* respondentů tak, že se registrují pouze na ověřených webových stránkách, což je zavádějící otázka, jelikož hned další otázka dotazníku byla, zda si respondent kontroluje URL adresy navštívených stránek. Tedy mnoho uživatelů nemá o legitimitě webové stránky sebemenší informace a může se jednat o phishingový útok.

Otázka 8

Kontroluješ si URL adresy navštívených stránek? (stavový řádek)

Ve výše uvedených kapitolách jsem hovořil o faktu, že velké množství populace používá totožná hesla na různých webových stránkách pod stejnými e-mailovými adresami. Tuto otázku jsem zvolil z důvodu průzkumu napadení prostřednictvím „phishingu“, kde *71 %* respondentů odpovědělo, že si své URL adresy nekontroluje, což mě vede k myšlence, že velká část populace není o tomto způsobu napadení příliš informována.

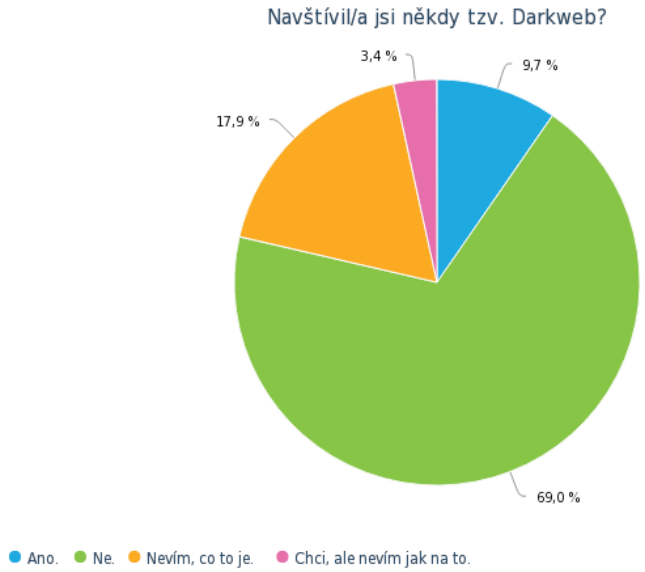
Otázka 9

Navštívil/a jsi někdy tzv. darkweb?

Odpověďmi u této otázky jsem velice spokojený, protože převažující odpovědi tvořící *86,9 %* byly negativní, z čehož *17,9 %* respondentů nemá o tomto pojmu žádné informace, což je přívětivé zjištění v poměru s rizikem, které se na darkwebu vyskytuje.

Dále *13,1 %* respondentů hlasovalo kladně (z toho pouze 1 žena hlasovala pro „ANO“) a *5 %* hlasujících má touhu tuto část internetu navštívit, avšak neví, jakým způsobem se na darkweb dostat. Z výsledků se dá předpokládat, že důvod návštěvy darkwebu by byl i u této menšiny pouhá zvědavost, tedy touha po zjištění, zda informace, které kolují v médiích, jsou pravdivé.

Graf 4: Anketní graf - darkweb



Otázka 10

Pokud ano, co tě k tomu vedlo?

- Necenzurované informace (2,2 %)
- Zvědavost (10,9 %)
- Objednávky/prodej (2,2 %)
- Sex, drogy (2,2 %)
- Nenavštívil jsem (85,4 %)

Média o tomto typu světa hovoří téměř jako o nelegální činnosti, ačkoli pouhé prohlížení darkwebu nepodléhá cenzuře ani zákonům. Z výsledků dotazníkového šetření vyplývá, že množství respondentů, kteří tento prostor navštívili se 10,9 % o darkweb zajímala pouze ze zvědavosti. Ostatní výsledky lze prohlédnout výše.

Otázka 11

Jakou finanční škodu dle tvého názoru způsobil kybernetický terorismus doposud? (tip v CZK, € nebo $)

K této otázce se vyjádřilo 129 respondentů ze 148, kde nejčastější typy odpovědí byly v řádech statisíců, milionů a v nejlepších tipech 1 či 15 miliard CZK. Nejbližší a pouze jeden tip, tedy 20 mld. dolarů se přiblížil na 1/30 celkové reálné částky. Kompletní odhadovaná škoda kybernetickým terorismem se k roku 2020 vyčíslila na 600 mld. amerických dolarů (tedy přes 15 bilionů CZK). Ačkoliv tato otázka není nikoli objektivní, jelikož se jedná o složitější tipovací odpověď, z analýzy této otázky vyplývá, že populace není natolik informována o tomto druhu globální problematiky.

Otázka 12

Říká ti něco pojem Keylogger?

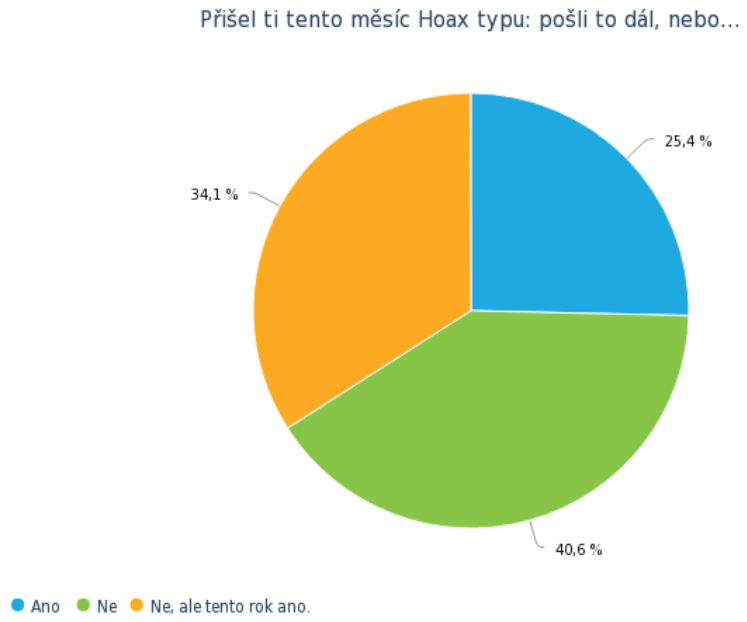
Dokonce až 79 % respondentů hlasovalo, že pojem keylogger jim vůbec nic neříká a nejsou tedy obeznámeni v žádném ohledu s tímto nástrojem, tzn. dá se předpokládat, že by nehledali v počítači žádné stopy této nebezpečné utility, ani nepostupovali obezřetně. Tudíž se může očekávat, že velké množství populace se přihlašuje pod svými přihlašovacími údaji na různých zařízeních a o napadení mnohdy vůbec neví.

Otázka 13

Přišel ti tento měsíc hoax typu: pošli to dál, nebo…?

Ve výše uvedených kapitolách zmiňuji, že hoax je typ nepravdivých či jiných zavádějících falešný informací, které se šíří formou spamu či scamu. Z výsledků dotazníku vyplývá, že 61,5 % hlasujících tento měsíc či rok obdrželo hoax, nutící uživatele dále sdílet obdrženou zprávu nesoucí nepravdivé informace, prostřednictvím citového vydírání nebo vnucení dlouhodobého neštěstí. Ačkoli se nejedná o tak nebezpečný projev kyberkriminality, může se značná část populace „chytit“ falešných informací a následně podle jejich významu jednat.

Graf 5: Anketní graf - hoax



7 ZÁVĚRY

- Analyzoval jsem problémy projevů kybernetické kriminality, se kterými se současný svět potýká a řešil jsem problematiku jejich prevence či řešení.
- Blíže jsem objasnil pojmy jako kybernetický prostor, kybernetická kriminalita a kybernetický terorismus a k nim vztahující se terminologii.
- V neposlední řadě jsem provedl testování specifického softwaru (keyloggeru), který slouží k monitoringu stisknutých kláves a vysvětlil jsem význam a princip, kterým daný software funguje a jakým způsobem je zneužíván.
- Dále jsem vysvětlil myšlenku páchání kybernetického zločinu z pohledu útočníka a uvedl vztah s rozdíly mezi jednotlivými druhy počítačových útoků.
- V poslední řadě jsem analyzoval dotazníkové šetření, ke kterému se vyjádřilo 148 respondentů, z jehož výsledku vzešel závěr, že velké množství obyvatelstva není s problematikou kybernetiky informované a nejedná v kyberprostoru obezřetně.

8 SOUHRN

Úvodní kapitola jasně definovala jeden z primárních cílů této práce, a to představit kybernetické útoky jako novou hrozbu lidstva. Práce dále objasňuje přehled stavu softwarových technologií jako typy projevů kybernetických útoků.

Počet kybernetických operací v kyberprostoru neustále roste. Ať se jedná o sektor státní nebo soukromý, vždy si útočník cestu svou pílí najde, otázkou je pouze „za jak dlouho“. Proto jsem dospěl k názoru, že dnešní společnost je zapotřebí v tomto směru vzdělat natolik, aby byla schopna při nejmenším jednotlivé útoky rozpoznat a stát se vůči nim imunní. Přirovnal bych situaci k efektu motýlích křídel. Jedinec dokáže nevědomky napáchat škodu, která má za následek velké dopady v budoucnu.

Odpovědi dotazníkového šetření přinesly zajímavé poznatky, díky kterým jsem dospěl k závěru, že celá řada populace nedbá na svoji anonymitu na internetu a nezná možnosti následků. Dále anketa přinesla informace o tom, že většina respondentů není obeznámena s nebezpečím, které může na internetu hrozit a je tedy nutné zvýšit informovanost obyvatelstva.

9 SUMMARY

The introductory chapter precisely defined one of the primary objectives of this thesis, to present cyber attacks as a new menace to humanity. The work also contains the summary of the state of software technologies as types of cyber attack effects.

The amount of cyber operations constantly rises. Whether in the state or private sector, the attacker always discovers a new approach, the only question is “in how long”. Therefore I have reached a conclusion. The present-day society is required to be educated in this field in order to perceive individual attacks and to be able to become immune to these assaults. I would equate this situation to the butterfly effect. An individual might unknowingly cause damage, which might induce massive consequences in the future.

The feedback from the questionnaire analysis has lead to intriguing finds, due to which I have reached a conclusion. A significant amount of the population is not cautious about its anonymity on the internet and is not aware of the consequences. The survey also revealed that most of the respondents were not acquainted with the threat, that is present on the internet, and therefore, it is a necessity for the population to become more knowledgeable about this danger.

10 SEZNAM POUŽITÝCH OBRÁZKŮ/ TABULEK/ GRAFŮ

Seznam obrázků:

Seznam tabulek:

Seznam grafů:

11 SLOVNÍK POJMŮ

[1] Protokol TCP/IP – primární přenosový protokol pro komunikaci v síti internet

[2] Jazyk HTML – jeden z hlavních jazyků pro vytváření stránek v systému World Wide Web

[3] Webový server – permanentně běžící počítač, který je zodpovědný za vyřizování požadavků HTTP od klientů

[4] VPN – Virtuální privátní síť, která je prostředkem k propojení nedůvěryhodné počítačové sítě (např. veřejný internet)

[5] Proxy server – funguje jako prostředník mezi klientem a cílovým počítačem

[6] VBSCript – skriptovací jazyk určený pro vkládání kódů do webových stránek

[7] Mimail – vir skrývající se v e-mailové příloze v „.zip“ jako „.jpg“, avšak skutečností je soubor „.exe“.

[8] Hacktivismus – vzniká spojením hackingu, aktivismu, politiky a technologie

[9] Pakety SYN – druh útoku DoS, kdy útočník pošle posloupnost paketů s příznakem SYN, ale dále neodpovídá

[10] Kód CVV – trojmístný ověřovací kód, nacházející se na zadní straně platební karty, který banka žádá automaticky

[11] VirtualBox – multiplatformní virtualizační nástroj distribuovaný pro Windows, Linux i Mac OS

12 REFERENČNÍ SEZNAM

Achkoski, J., & Dojchinovski, M. (2000). *Cyber terrorism and cybercrime.* Retrieved 14. 4. 2020 from World Wide Web: https://core.ac.uk/download/pdf/35329569.pdf

Amazon.cz (2018). *What is a DDoS Attacs?.* Retrieved 6. 5. 2020 from the World Wide Web: https://aws.amazon.com/shield/ddos-attack-protection/

Bateman, R. (2020). *10 Best Anti-Spyware Software for 2020.* Retrieved 30. 3. 2020 from the World Wide Web: https://www.safetydetectives.com/blog/the-best-anti-spyware-software/

Bocij, P. (2004). *Cyberstalking: Harrasment in the Internet Age and How to Protect Your Family.* Westport: Greenwood Publishing Group.

Brenner, S. (2010). *Cybercrime: Criminal Threats for Cyberspace.* California: Greenwood Publishing Group.

Buguroo (2018). *Analyzing the world's top 3 cybercrime countries.* Retrieved 23. 3. 2020 from the World Wide Web: https://www.buguroo.com/en/blog/the-worlds-top-3-cybercrime-and-online-fraud-hotspots

Christensson, P. (2006). *Proxy Server Definition.* Retrieved 20. 5. 2020 from the World Wide Web: https://techterms.com

Congressional Research Service (2020). *Defense Primer: Cyberspace Operations.* Retrieved 9. 2. 2020 from the World Wide Web: https://fas.org/sgp/crs/natsec/IF10537.pdf

Denning, D. E. (2001). *Activism, hacktivism and cyberterorism: The internet as a tool for influencing foreign policy.* Retrieved 28. 3. 2020 from the World Wide Web: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

ESL Stories (2018). *The world's most spoken language by total speakers.* Retrieved 4. 4. 2020 from the World Wide Web: https://blog.esl-languages.com/blog/learn-languages/most-spoken-languages-world/

Forbes (2013). *Meet The Dread Pirate Roberts, The Man Behing Booming Black Market Drug Website Silk Road.* Retrieved 27. 2. 2020 from the World Wide Web: https://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/#48caf9688b73

Harrison, S. (2016). *Evolving Tech, Evolving Terror*. Retrieved 19. 5. 2020 from World Wide Web: https://www.csis.org/npfp/evolving-tech-evolving-terror

Hoax.cz (2020). *SCAM419.* Retrieved 17. 5. 2020 from the World Wide Web: https://www.hoax.cz/scam419/

Hypoindex.cz (2018). *Podvodné úvěry.* Retrieved 19. 5. 2020 from World Wide Web: https://www.hypoindex.cz/clanky/pozor-na-podvodne-nabidky-uveru/

Igarapé institute (2018). *Brazil struggles with effective cyber-crime response.* Retrieved 4. 1. 2020 from the World Wide Web: https://igarape.org.br/en/brazil-struggles-with-effective-cyber-crime-response/

Javůrek, K. (2009). *Nafouknutá bublina Y2K.* Retrieved 1. 3. 2020 from the World Wide Web: https://www.zive.cz/clanky/zive-t-10-nafouknuta-bublina-y2k/sc-3-a-150313/default.aspx

Janczewski, L. J., & Colarik, A. M. (2005). *Managerial guide for handling cyber-terrorism and information warfare.* Retrieved 5. 5. 2020 from the World Wide Web: https://www.researchgate.net/publication/294563593_Managerial_guide_for_handling_cyber-terrorism_and_information_warfare

Jirovský, V. (2007). *Kybernetická kriminalita: Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s.

Jirovský, V. (2008). *Taxonomie kybernetických hrozeb*. Praha: České vysoké učení technické

Kolouch, J. (2016). *CyberCrime.* Praha: CZ.NIC, z. s. p. o.

Lorents, P., & Ottis, R. (2011). *Cyberspace: Definition and implications.* Retrieved 15. 4. 2020 from the World Wide Web:

https://www.researchgate.net/publication/287868009_Cyberspace_Definition_and_implications

McAfee, (2011). *A good decade for cybercrime.* Retrieved 19. 5. 2020 from the World Wide Web: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

NATO Public Diplomacy Division (2007). *Centre of Excellence Defence Against Terrorism, Ankara, Turkey.* Retrieved 11. 5. 2020 from the World Wide Web: https://books.google.cz/books?hl=cs&lr=&id=Eg7vAgAAQBAJ&oi=fnd&pg=PA118&dq=NATO+and+Cyber+Terrorism,+In+Responses+to+Cyber+Terrorism&ots=KeQQJO3pxz&sig=zmT6qrL1Fs9EiU8jMG3AetNNCmk&redir_esc=y#v=onepage&q=NATO%20and%20Cyber%20Terrorism%2C%20In%20Responses%20to%20Cyber%20Terrorism&f=false

PCTuning (2018). *Jaká jsou nejpoužívanější hesla na internetu?* Retrieved 27. 2. 2020 from World Wide Web: https://pctuning.tyden.cz/index.php?option=com_content&view=article&id=49949&catid=1&Itemid=57

Policie ČR (2020). *Kyberkriminalita*. Retrieved 17. 4. 2020 from the World Wide Web: https://www.policie.cz/clanek/kyberkriminalita.aspx

Petrenko, S. (2018). *Big Data Technologies for Monitoring of Computer Security.* Innopolis: Springer International Publishing

ResearchGate (2001). *What Is Crime? Controversies over the Nature of Crime and What to Do about It.* Retrieved 2. 4. 2020 from the World Wide Web: https://www.researchgate.net/publication/258369244_What_Is_Crime_Controversies_over_the_Nature_of_Crime_and_What_to_Do_about_It

The Jargon File (2016). *Hacker slang and hacker culture.* Retrieved 6. 3. 2020 from the World Wide Web: http://catb.org/jargon/html/distinctions.html

Timehosting.cz (2020). *Nigerijské dopisy.* Retrieved 17. 5. 2020 from the World Wide Web: http://timehosting.cz/nigerijske-dopisy/

Weimann, G. (2008). *The Theater of Terror.* Retrieved 7. 1. 2020 from the World Wide Web: https://www.tandfonline.com/doi/abs/10.1300/J146v09n03_08

Wikipedie (2020). *Silk Road (online market).* Retrieved 25. 3. 2020 from the World Wide Web: https://cs.wikipedia.org/wiki/Silk_Road_(online_market)

Zuna, P. (2011) *Den teroristických útoků na USA (11.září 2001)* Retrieved 5. 3. 2020 from the World Wide Web: https://www.slavne-dny.cz/episode/611507/den-teroristickych-utoku-na-usa-11-zari