Možnosti útoků na současné informační a komunikační prostředky

Aneta Halamíčková

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

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

Jméno a příjmení:	**Aneta Halamíčková**
Osobní číslo:	**L15312**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

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

Zásady pro vypracování:

1. **Analyzujte informační zdroje.**
2. **Vytvořte modely zadaného systému.**
3. **Modelujte struktury a vlastnosti zadaného systému.**
4. **Navrhněte opatření ke zlepšení zadaného systému.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

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

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

[3] SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**prof. Ing. Jiří Dvořák, DrSc.** Ústav krizového řízení
Datum zadání bakalářské práce:	**3. listopadu 2017**
Termín odevzdání bakalářské práce:	**15. května 2018**

V Uherském Hradišti dne 15. listopadu 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

L.S.

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

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1)];
- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se bakalářská práce skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti 27.4.2018

Melanichová
podpis studenta

---

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

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

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

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

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

2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:

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

3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:

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

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

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

ABSTRAKT

Bakalářská práce je v teoretické části zaměřena na kybernetickou kriminalitu a její vývoj. Jsou v ní blíže rozebrány útoky na informační a komunikační prostředky, zejména hacking a vše, co s ním souvisí, a také kybernetické války a kybernetický terorismus. V neposlední řadě jsou analyzovány také podvody všeho druhu a nebezpečí, která hrozí chytrým mobilním telefonům. V praktické části práce je rozebrána ochrana před útoky nejen pro počítače, ale také pro internetové připojení a mobilní telefony. Cílem této části bylo vytvoření dotazníku a sběr statistických dat, které umožnily získat informaci o veřejném povědomí o kybernetické kriminalitě a obezřetnosti před možnými hrozbami. Závěr práce je věnován rozhovoru, který byl uskutečněn se zkušeným programátorem.

Klíčová slova: kybernetická kriminalita, útok, útočník, počítač, ochrana.

ABSTRACT

This bachelor thesis, in its theoretical part, deals with cyber crime and its evolution. In the next chapter, the attacks to information and communication technologies are analyzed with emphasis on the hacking, cyberwars and cyberterrorism. Consequently, the Frans of all kindes and threats to which mobile phones are exposed, are analyzed. In the second part of the thesis, the practical one, the protection against attacks is analyzed in the domain of personal computers, internet connections and mobile phones. The target of the practical part was creation of a quationnaire and gathering of statistical data. Thanks to it, the information about public awareness of cyber crime and about public prudence of existing threats. The conclusion of the thesis is dedicated to a dialog with experienced programmer.

Keywords: cyber crime, attack, attacker, computer, protection.

Chtěla bych projevit dík zejména svým rodičům a svému příteli za pomoc, trpělivost, pochopení a podporu po celou dobu mého studia. Dále bych chtěla poděkovat vedení a programátorům firmy, ve které pracuji, za pomoc a rady při zpracování této práce. A poděkování patří zejména panu prof. Jiřímu Dvořákovi, DrSc. za vedení, rady a věcné připomínky při zpracování této práce.

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

OBSAH

ÚVOD

V současné době plné moderních informačních a komunikačních technologií (dále ICT), ať už v reálné či virtuální, se objevují problémy s bezpečností a kriminalitou čím dál častěji. Z toho vyplývá, že je potřeba předcházet vzniku těchto událostí.

Již název práce napovídá, že se bude zabývat možnostmi útoků na současné informační a komunikační prostředky. Mezi tyto prostředky patří zejména počítač či přenosný počítač, mobilní telefon a hlavní zprostředkovatel, skrze který mohou být tyto útoky páchány. Tímto zprostředkovatelem je především internetové připojení a také samotný internet. Všechny útoky probíhající ve virtuálním světě jsou známy pod pojmem kybernetická kriminalita. Jelikož se s tímto pojmem budeme v práci setkávat častěji, je třeba znát jeho význam. Budu se snažit objasnit jeho podstatu. Kybernetická kriminalita, zkráceně kyberkriminalita nebo kybernalita, je jakýkoliv čin, jehož cílem je zneužít počítač, systém, síť nebo informace v nich obsažené. Tato kriminalita se odehrává v kyberprostoru, který představuje internet a sítě. Ke kybernetické kriminalitě řadíme mnoho útoků, ale mezi ty nejznámější patří hackerství, kybernetické války, kyberterorismus nebo podvody, těmito se budu v práci zabývat podrobněji.

Úvod teoretické části bude zaměřen na vývoj kybernetické kriminality a její pachatele, a v části druhé se bude zabývat již samotnými možnostmi útoků včetně nebezpečí pro mobilní telefony. Právě ty jsou v současné době nejpoužívanějším, hlavně komunikačním prostředkem, a mnoho uživatelů si neuvědomuje, že nebezpečí v podobě útoků hrozí i mobilním telefonům.

Praktická část práce bude v první části zaměřena na ochranu počítače, mobilního telefonu a samozřejmě internetové sítě před hrozícími útoky. Pomocí dotazníku chci zjistit, jaké znalosti o kybernetické kriminalitě mají lidé z mého okolí, a také, do jaké míry jsou na internetu obezřetní. Dále nás praktickou částí provede krátký rozhovor s programátorem, který spravuje nejen e-shop ve kterém pracuji, ale také celý server, na kterém tento e-shop běží. Z praktické stránky nám přiblíží úkony pro bezpečné provozování e-shopu, a také se dozvíme, jak předcházet útokům mířícím proti domácím uživatelům ale také na e-shopy, protože právě ty jsou největším terčem podvodů. Všichni, kteří takto nakupujeme, jsme potencionálními oběťmi hackerů.

I. TEORETICKÁ ČÁST

1 VÝVOJ KYBERNETICKÉ KRIMINALITY

V úvodu práce byl nastíněn pojem kybernetická kriminalita. I když existuje mnoho definicí tohoto pojmu, všechny se shodují na jednom – činnost páchána proti počítači, síti a informacím. Nikde není uvedeno, kdy přesně kyberkriminalita vznikla, ale dle mého názoru její vývoj postupoval s rozvojem počítačů a ostatních informačních a komunikačních prostředků. Jejich největší rozmach probíhal zhruba posledních 20 let minulého století. Do té doby se o kyberkriminalitu úřady ani státní orgány nijak zvlášť nezabývaly, jelikož se neobjevovaly tak často jako v současné době.

Z hlediska rozvoje se kyberkriminalita dělí do tří generací. V první generaci se informační technologie (dále IT) používají ke shromažďování informací nebo jako komunikační prostředky. Ve druhé generaci mluvíme o tzv. hybridní kriminalitě, kdy se IT používají např. k šíření zločineckých dovedností či obchodování s dětskou pornografií. Třetí generací kyberkriminality je automatizovaná kyberkriminalita, která vznikla s rozvojem širokopásmového propojení zařízení např. rozesílání nevyžádané pošty. [1]

První trestné činy související s ICT se týkaly sabotáží[1] zaměřených proti zaměstnavatelům a tzv. dokladové delikty. Mezi nejrozšířenější patřily neoprávněné zásahy do mzdových či účetních dokumentů, kde byla možnost pracovat s penězi. U nás se první počítačový zločin odehrál v 70.letech, kdy nespokojený pracovník nejmenované organizace úmyslně magnetem poškozoval záznamy na magnetických páskách, kterými způsobil vyřazení samočinného počítače z provozu a také kolaps agendy, kterou počítač obsahoval. Další takový útok u nás se odehrál v letech 1985-1987, kdy byl poškozen počítač sovětské výroby, aby se zabránilo jeho nainstalování. [2]

Kyberkriminalitou se koncem osmdesátých let začala zabývat Rada Evropy, která na základě vypracované studie doporučující vytváření nových zákonů zabývajících se činy spáchanými v prostředí počítačových sítí ustavila Komisi expertů na zločin v kyberprostoru, která pracovala na návrhu mezinárodní dohody usnadňující spolupráci při odhalování počítačových zločinů. [3]

---

[1] *„ Počítačová sabotáž je čin spočívající v omezení či znemožnění funkčnosti počítače, jeho části nebo jiného zařízení formou fyzického nebo logického útoku, kdy úmyslem pachatele je poškodit ústavní zřízení nebo obranyschopnost státu.“ [2]*

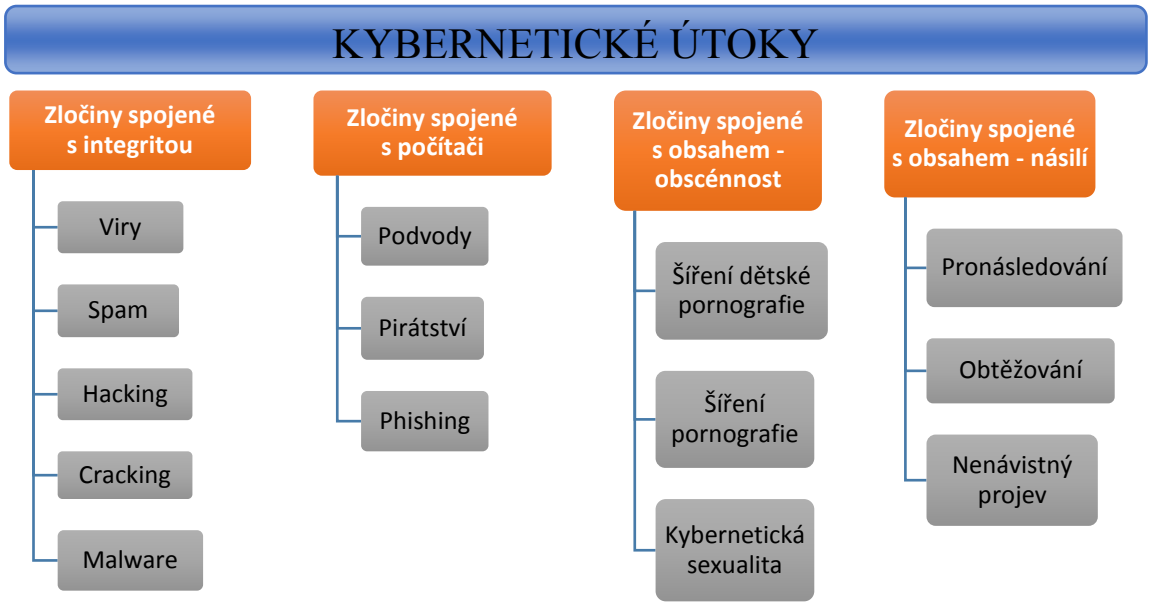
Nejzajímavější je, že se s pojmem kybernetická kriminalita se začalo pracovat, až v roce 2001, kdy vstoupila v platnost Úmluva Rady Evropy o kyberkriminalitě, známá také pod pojmem budapešťská úmluva. [1] Do té doby se pojem kyberkriminalita nepoužíval, tato kriminalita byla nazývána jako počítačová kriminalita, kriminalita spojená s počítači nebo informační kriminalita jelikož k útokům nedocházelo tak často a promyšleně jako dnes. Kybernetická kriminalita je tedy souhrn všech protiprávných činů konaných pomocí počítačových sítí a počítačů a zahrnuje v sobě informační kriminalitu a také sociální kriminalitu.

Úmluva o kyberkriminalitě a dělení zločinů

Úmluva Rady Evropy č. 185 o kybernetické kriminalitě z 23. listopadu 200,1 známá také jako budapešťská úmluva, je ustanovena pro řešení zločinů mířících proti ICT. Vlivem této úmluvy se poprvé prosadil pojem kybernetická kriminalita, se kterým se pracuje dodnes. I když přesná definice neexistuje tak, jak bylo již zmíněno. Budapešťská úmluva také rozdělila zločiny na informační a komunikační prostředky do 4 základních skupin:

1. Zločiny spojené s integritou (nezákonný přístup, nezákonné odposlouchávání, narušení dat, narušování systémů a zneužití prostředků).
2. Zločiny spojené s počítači (počítačové padělání a podvody).
3. Zločiny spojené s obsahem – obscénnost (různé formy trestných činů spojených s dětskou pornografií).
4. Zločiny spojené s obsahem – násilí (nenávistný projev, obtěžování). [1] [3]

Na modelu níže můžete vidět, které útoky patří dle mého názoru do 4 základních skupin definovaných Úmluvou o kyberkriminalitě, které jsou uvedeny výše.



Obr. 1 – Model kybernetických útoků

Zdroj: vlastní

1.1 Pachatelé kybernetické kriminality

Pachatelem jakékoliv kriminality je fyzická osoba, která svým jednáním naplnila všechny znaky trestného činu[2]. Motivy pachatelů se liší věkem, vyspělostí, dovednostmi a také způsoby spáchání. Kriminalitu páchají osoby, které mají problém samy se sebou nebo nejsou spokojeny s daným systémem a pravidly. Dle mého názoru jsou pachatelé ať už klasické kriminality, nebo kybernetické kriminality osoby, které jsou v běžném životě uzavřené a nevýrazné. Samozřejmě pachatelem může být kdokoliv, aniž by o tom věděl.

Klasická kriminalita se vývojem kriminality nijak nezměnila, vražda stále zůstává vraždou, i když se používají zcela jiné nástroje. Ale kybernetická kriminalita přinesla nové druhy kriminality, nejnovější je kyberterorismus a nejrozsáhlejší tvoří podvody všeho druhu. Smejkal [5] ve svém článku, který je uveden v příloze I uvedl nejčastější čtyři skupiny pachatelů:

[2] Trestný čin je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje všechny znaky uvedené v takovém zákoně.

1. Cizí státy
2. Teroristé
3. Zaměstnanci poškozené organizace
4. Organizované skupiny

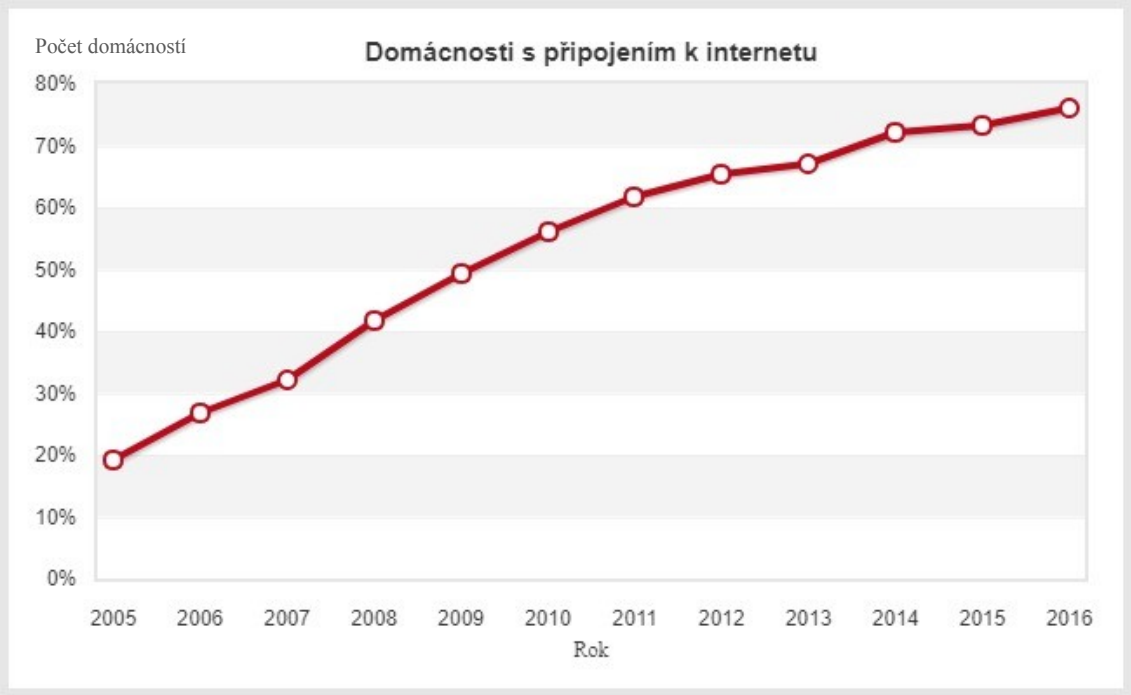
Cizí státy útočí pomocí kybernetických válek. Teroristé mohou velmi účinně zaútočit pomocí počítačových sítí. Nejnebezpečnější skupinou pachatelů jsou zaměstnanci poškozené organizace, kteří mají přístup k informacím a dostatečná oprávnění, aby tyto informace poškodili, odcizili, prodali či upravovali. Organizované skupiny jsou nejčastější pachatelé kybernetické kriminality. [5] Účastníci organizovaného zločinu využívají počítač ke skryté komunikaci, praní špinavých peněz, k výrobě padělků softwarů, platebních karet apod. a také k výrobě a distribuci pornografie. [2]

Každý pachatel kriminality má motiv, pomocí kterého kriminalitu páchá. Pokud je pachatelem zaměstnanec nebo bývalý zaměstnanec poškozené organizace, je nejčastějším motivem pomsta či nespokojenost s prací. Motivem pachatelů kybernetické kriminality bývá převážně možnost osobního obohacení a také zvědavost ,,co by kdyby‘‘.

1.2 Současná kyberkriminalita, komunikační a informační prostředky a možnosti útoků

Současná kyberkriminalita je daleko běžnější než v minulém století. V minulém století nebylo širokopásmové připojení tak rozsáhlé jako dnes, a také nebyly k dispozici tak moderní prostředky zprostředkovávající nejen komunikaci. Mezi informační a komunikační prostředky patří ještě stále stolní počítače, které jsou ale v mnoha případech nahrazovány přenosnými notebooky a tablety, dále televize, mobilní telefony, rozhlasy a v neposlední řadě také tisk. Možná si kladete otázku, proč tisk, ale ten je již od dávných let minulých nejstarším prostředkem, kterým získáváme informace. I v dnešní moderní době je tento informační prostředek stále v kurzu. Ale dnešním nejpoužívanějším informačním a komunikačním prostředkem je internet, jelikož přes internet můžete komunikovat jak slovně, tak písemně a je lhostejné, zda jste připojeni na počítači, notebooku, tabletu, mobilním telefonu nebo jiném zařízení.

Na obrázku níže můžete vidět graf stoupajícího počtu domácností v České republice s připojením k internetu, který zveřejnil Český statistický úřad. Na grafu vidíte, že se během 11 let zvýšil počet domácností s připojením k internetu o více než 50 %.



Obr. 2 – Graf počtu domácností s připojením k internetu

Zdroj: [4]

Hrozbám a útokům jsme vystaveni všichni, kdykoliv jsme připojeni na internet na jakémkoliv zařízení, jelikož v ohrožení jsou hlavně systémy zařízení. S vývojem technologií se také vyvíjejí nové útoky a hrozby, které na nás číhají.

Mezi nejpoužívanější možnosti útoků na informační a komunikační prostředky v dnešní době patří:

- hacking,
- cracking,
- phishing,
- kybernetické války,
- kyberterorismus,
- podvody.

Možností útoků na informační a komunikační prostředky je opravdu mnoho, výše byly jmenovány nejčastější útoky, které se v dnešní době, ale i v minulém století objevovaly a současně objevují nejvíce, a se kterými má společnost nejvíce zkušeností. Tyto útoky budou v práci uvedeny podrobněji.

2 HACKING

Hacking je metoda útoku na informační a komunikační prostředky, která je i v dnešní moderní době stále jednou z nejčastějších. Spočívá v prolomení ochranných prvků cizího systému hackerem, aby mohl získat potřebné informace nejen o samotném jedinci, jehož systém napadl, ale také o veškerých datech, která poté sdílí s ostatními hackery. Jakýkoliv útok, který souvisí s hackingem, je samozřejmě trestným činem. Než se budeme zabývat historií hackingu a vším, co s ním souvisí, je potřeba definovat hacker.

Definovat hackera v dnešní době není jednoduché. Jirovský [3] uvádí, že ,, *hacker je člověk, kterého baví zkoumat detaily programovatelných systému a hledat metody, jak je vylepšit.‘‘* Hackeři jsou také osoby, které s oblibou programují a jsou v programování experty. Používají několik programů pro získání dat v jakémkoliv oboru. Hackeři působí nejčastěji v oblasti porušování autorských práv.

2.1 Historie a vývoj hackingu

Termíny hacking a hacker vznikly přibližně v 50. letech minulého století, kdy si jakási komunita radioamatérů myslela, že hacker je technicky nadaná osoba, která dokáže hledat nové metody pro zlepšení výkonu svého vysílače. ,, *Termín hacking byl převzat z angloamerického jazyka jezdců na koních, který označoval nenucenou vyjížďku do nějakého cíle.‘‘* [3] Později se ,,hackem‘‘ označovalo spáchání nějaké neřesti, kdy byl hříšník nazýván hackerem, a toto označení zůstalo dodnes.

Mezi první hackerské pokusy patřily útoky na nedostatky telefonní sítě AT&T. Jednalo se o uskutečňování nezpoplatněných dálkových hovorů skupinkou technologických nadšenců v USA i ve světě, kdy se této skupince říkalo phreakeři, což je označení pro osoby, které nezákonně využívají telefonní sítě. Skutečný rozvoj nastal až v 80. letech, kdy se objevila technologie BBS[3]. Vznikly první hackerské skupiny, které mezi sebou komunikovaly a vyměňovaly si zjištěné informace o počítačích, jejich systémech a nástrojích. Tyto skupiny se soustředily na zjištění uložených hesel v počítačích nebo o jejich prolomení. V této době se spíše než speciální programy používala vynalézavost hackerů. [3]

[3] BBS byly počítače umožňující vzdálené připojení, které umožňovaly uživateli pomocí standardizovaných dotazů čerpat informace z databáze uložené na počítači. [3]

S nástupem webových technologií se začaly objevovat první hackerské nástroje, které byly označovány „easy-to-use‘‘. S nárůstem informací dostupných na počítačových sítích se rozvíjel také hacking. Vznikaly hackerské weby, kde se daly volně stáhnout programy, které využívaly bezpečnostní díry v systémech, a také utajené vstupy do systémů tzv. back-doors, kterými se systém vzdáleně a skrytě ovládal.

Současní hackeři si počínají daleko problematičtěji než kdy předtím, jelikož využívají nejen technické vybavení, ale i celosvětovou počítačovou síť komerčních subjektů, kde je základem jejich činnosti odhalování nedostatků komerčních projektů, což snižuje dosažitelný zisk napadených firem a projektů. [3] Na jednu stranu je hacking obrovským problémem, protože je to široký pojem pro mnoho druhů útoků na ICT, ale na druhou stranu bychom bez něho neměli tolik bezpečnostních opatření, která máme dnes.

2.2 Osobnosti hackerů

Pojem hacker byl nastíněn již na začátku kapitoly, ale nyní bych se chtěla zaměřit na osobnost hackera a hackerskou komunitu. Ta má také svá pravidla a typické rysy chování. Hacker je osoba, která odmítá nebo se snaží odmítat pravidla a hodnoty dané společnosti a jeho vyznáním je svoboda jedince. Tyto osoby se pohybují převážně v elektronickém světě, protože je zajímají nové výzvy a jsou zvědaví. V normálním ,, živém‘‘ světě jsou nevýrazné, uzavřené a nekomunikativní, ovšem to neznamená, že každý člověk, který se vyznačuje těmito rysy musí být hacker. Hackeři pronikají do cizích systémů, aby zjistili informace, které je zajímají. Jakmile tyto informace zjistí, jsou spokojeni a ze systému „odejdou‘‘. Jirovský [3] ve své knize uvádí, že ,, *morální povinností hackera je sdílení informací a know-how.‘‘* Slovním spojením know-how se v této problematice rozumí dostatek znalostí a potřebných informací. Hackerem nemůže být každý, ne každý je na tyto pozice stavěný.

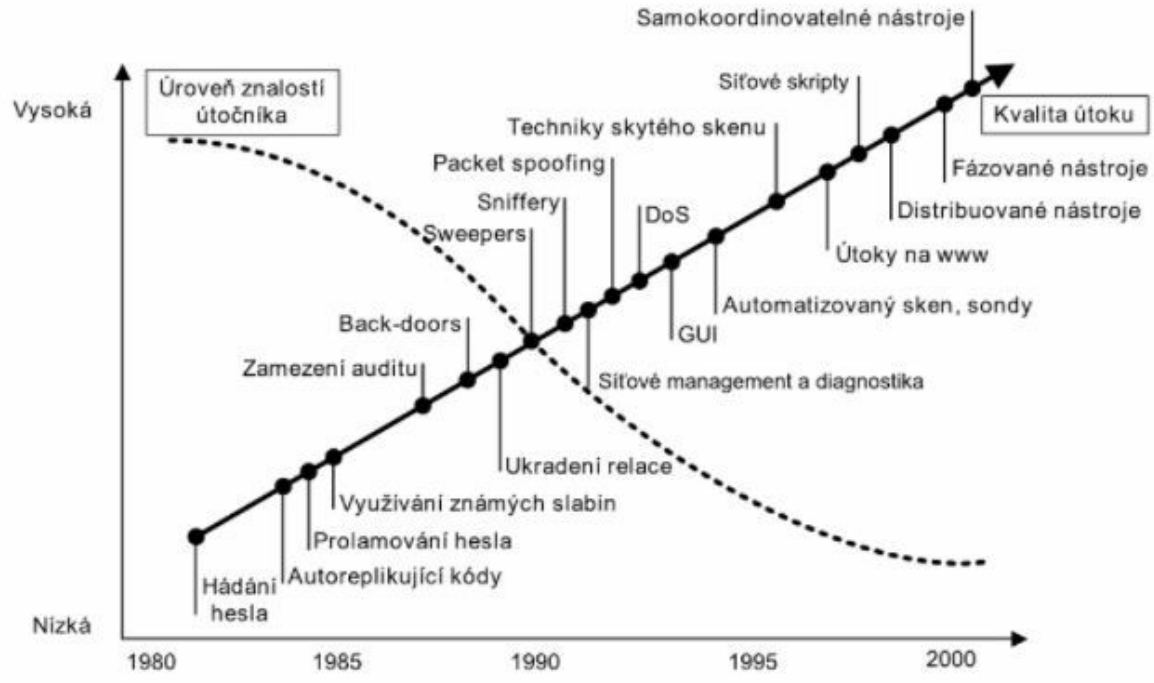
Pro hackery je sdílení informací a přístupy k cizím informacím tím správným pro společnost. Jejich etické hodnoty jsou úplně jiné než hodnoty ostatních občanů. Samozřejmě, že každý zastává jiný názor ale osoby jako jsem já, určitě nezastávají názor, že nabourávání se do systémů cizích a zjišťovat si své potřebné informace je nepřípustné a trestné. Jak uvádí Jirovský [3], v kyberprostoru jsou hackerské komunity ,, *kyberpredátory, kteří se snaží o jeho čistotu a průhlednost‘‘*, a s tímto výrokem mohu plně souhlasit. Samozřejmě aby nebylo jednoduché zjistit hackery, mají také svůj jazyk, kterému rozumí jen oni

sami, a je velmi obtížné zjistit, zdali se jedná opravdu o hackera, který útok provádí, či nikoli.

2.3 Nástroje hackingu

Důležitou součástí hackingu je programové vybavení a nástroje, které jsou potřebné a bez kterých by nebylo možné tyto útoky zprostředkovat. Patří mezi ně hardwarové, softwarové nástroje a také techniky pro zneužití lidí. I když se tyto nástroje stále vyvíjejí a modernizují, nejdůležitějším článkem pro uskutečnění hackerského útoku je samotná osobnost hackera, protože je to on, kdo má nabyté vědomosti, znalosti a dovednosti, které jsou předpokladem pro úspěšný útok.

Na obrázku níže, můžete vidět vývoj hackerských nástrojů od raného hackingu až po nástroje, s kterými se setkáváme dnes.



Obr. 3 – Historie vývoje hackerských nástrojů

Zdroj: [3]

Z obrázku je zřetelné, že úroveň znalostí hackerů se rok od roku zvyšuje a také se stupňují počty útoků. Sami vidíte, že základním a nejjednodušším útokem, kterým hackerství začínalo, bylo hádání a prolomení hesel. V dnešní době musí i hackeři vzhledem k většímu zabezpečení systémů používat a kombinovat více nástrojů a znalostí, aby systém prolomili.

2.4 Cracking

S hackingem úzce souvisí také cracking. Na rozdíl od hackingu škodí systému od začátku prolomení. Jak již bylo zmíněno výše, hackeři data, která jsou v napadeném systému, nemění, u crackingu je tomu přesně naopak. Crackeři jsou osoby, které prolamují jakési bezpečnostní zábrany systémů, převážně zjišťují hesla, aby do nich mohli vniknout. Poté se snaží zjištěná data měnit, odcizovat, nebo dokonce zničit. [2]

Jsou to právě crackeři, kteří do nabouraných systému zavádějí viry, získávají čísla kreditních karet a podobně. Myslím si, že hackeři i crackeři spolu spolupracují. Virů a podobných útoků je nespočet. Chtěla bych tedy dále nastínit nejčastější techniky hackerů a crackerů, se kterými se v průběhu života setkal snad každý z nás.

2.5 Techniky hackingu

Používaných technik v hackingu je mnoho. Zaměřím se na ty nejznámější a nejběžnější. Mezi nejpoužívanější techniky hackingu dle pana majora, doktora a inženýra Stodoly [6] z Univerzity obrany v Brně patří:

- *skenování portů,*
- *prolamování hesel,*
- *zachytávání paketů,*
- *sociální inženýrství,*
- *phishing,*
- *počítačové viry,*
- *trojské koně,*
- *počítačoví červi,*
- *rootkit,*
- *keyloggery.*

Popíši jen některé z těchto technik, které jsou známé u nás v České republice a se kterými se většina z nás setkala.

2.5.1 Prolamování hesel

Prolamování hesel je jedna z metod hackingu, při níž jsou získávána hesla z dat, která jsou buď uložená anebo přenášená systémem v počítačové síti. Může to být například přihlašování na email. Hackeři používají několik způsobů a metod, jakými se snaží hesla prolomit.

Mezi tyto metody patří hádání hesla na základě svých znalostí a dovedností nebo existuje také slovník nejčastěji používaných hesel. Každý jsme se určitě setkali se situací, kdy jsme chtěli v počítači změnit dané nastavení a systém po nás chtěl heslo oprávněného uživatele k těmto změnám, což je administrátor systému. Samozřejmě to není jen jedna z metod hackerů ale funkce systému uživatele. Můžete se ale také setkat s tím, že heslo po vás nežádá váš systém, ale samotný hacker. Ten má možnost prolomit heslo i v případě, kdy je systém nedostatečně chráněn, jelikož si heslo zjistí při jakémkoliv zadávání hesla uživatelem, pokud je na systém ,, nabouraný‘‘. Typickým příkladem této metody je prolomení hesla například na účtu na facebooku[4] a zjišťování informací o napadeném a vydávání se za napadeného. [6]

2.5.2 Phishing

Slovo phishing bylo zmíněno již v kapitole 1.2 při jmenování nejčastějších útoků na současné informační a komunikační prostředky. Nejčastěji se jedná o podvodnou webovou stránku, která vypadá jako pravá, ale ve skutečnosti je vytvořená hackery, jejichž cílem je uživatele oklamat a získat jeho data. Tyto útoky hackeři provádí tak, že rozesílají uživatelům podvodné e-maily s odkazem např. na internetové bankovnictví, aby z uživatele vylákali číslo účtu a heslo, což jsou jedny z nejcitlivějších údajů uživatele a následně mu z účtu ukrást peníze. Phishing se tedy stal značně využívanou formou podvodů. [6]

Např. v loňském roce proběhl phisingový typ útoku přes facebook. Sama mám na facebooku profil, a o tomto útoku jsem slyšela. Nevím, které období to přesně bylo, jestli jaro nebo léto. Každopádně mě samotné od mých přátel přišlo upozornění, že si někdo vytváří stejné profily vašich přátel i s fotkami a údaji, aby profil vypadal věrohodně. Následně vás požádá o přátelství podle vašeho seznamu přátel. Po přijetí žádosti vás žádá o telefonní číslo, aby vám na telefon přišel nějaký kód pomocí zprávy, který mu zpětně napíšete. Uživatelé, kteří bohužel na tento útok narazili, přišli o své peníze.

[4] Facebook je celosvětový server, na kterém lidé mezi sebou komunikují, sdílejí data a zároveň udržují společenské vztahy.

2.5.3 Počítačové viry

Počítačové viry jsou programy, které mají uživatelé v počítačích a neví o nich. Tyto programy jsou samozřejmě škodlivé. Můžete na ně narazit v jakémkoliv souboru na internetu, na který kliknete nebo si jej stáhnete, jelikož je v něm uložený. Jakmile si tento soubor stáhnete nebo na něj kliknete, vir se aktivuje. Viry se objevily již v 80. letech minulého století. ,, *První známé viry napadaly tzv. boot sektory disků.‘‘* [7] První takový virus se jmenoval Brain. Vznikl v roce 1986, byl to první virus, který se přenášel prostřednictvím disket. Princip tohoto viru spočíval v tom, že si ,, *přehrál bootovací sektor diskety na jiné místo, označil jej za vadný a sám se nahrál do místa původního bootovacího sektoru.‘‘* [8] Počítač po napadení virem četl z disket velmi pomalu. Virů je velká spousta a i já osobně mám s virem v počítači zkušenost. Stalo se mi pár let nazpět, že mi ze dne na den začal počítač pracovat pomalu, nereagoval na některé mé požadavky. Existují programy, které vám identifikují, že v systému máte vir, a zároveň jsou schopny vir z počítače odstranit. A právě pomocí jednoho z těchto programů mi kamarád pomohl zjistit, že mám v počítači vir a také se mu podařilo vir z počítače odstranit.

Virus I Love You, který se šířil sítěmi v roce 2000, se kvůli vzniklým škodám a počtu napadených počítačů zapsal na první příčku žebříčku všech virů. Tento virus byl od vzniku virů nejničivější ze všech. Šířil se jako příloha emailu, kterou když příjemce otevřel, virus se dostal do jeho počítače a ,, *vyhledával čísla a hesla kreditních karet.‘‘* [8] Nejenže tato čísla a hesla vyhledával, ale také mazal soubory a data obsažená v počítači od obrázků po dokumenty a dále si vyhledal všechny kontakty v adresáři a tento virus se jim přes email odeslal také. ,, *Virus infikoval 10 % počítačů připojených k internetu, což v roce 2000 činilo 45 milionů a způsobil škody za 5,5 miliardy dolarů‘‘* [8], což je přibližně 20 miliard českých korun.

2.5.4 Trojské koně

Trojské koně patří do virů a řadí se k nejjednodušším druhům škodlivého programu. Trojští koně na první pohled vypadají jako užitečné, ale ve skutečnosti jsou škodlivé. Cílem trojského koně je nasbírat z napadených počítačů veškeré informace a data od uživatele a také o uživateli a tato data poškodit, změnit nebo smazat. V roce 2011 se objevil trojský kůň Duqu, který z napadených počítačů sbíral digitální podpisy a privátní šifrovací klíče. Tento virus byl natolik vyspělý, že používal svůj vlastní programovací jazyk a po 36 dnech se z napadeného systému sám smazal.

V současnosti se také objevují viry a trojské koně útočící na mobilní telefony se systémem Android. Jedním takovým trojským koněm byl v roce 2010 FakePlayer. Vydával se za multimediální přehrávač, ale ve skutečnosti zasílal ,,*SMS na ruská čísla s vysokými poplatky*.‘‘ [8] Naštěstí tento trojský kůň ,, *funguje jen v sítích ruských operátorů.‘‘* [8]

2.5.5 Počítačoví červi

Počítačový červ je dalším druhem viru, který se šíří sítěmi. Červi se mohou spustit jak bez pomoci uživatele, tak jen s jeho pomocí. Prvním počítačovým červem byl červ Morris v roce 1988, který se šířil pomocí internetu. Vytvořil ho student Cornellovy univerzity, aby zjistil počet počítačů připojených k internetu. Tento červ mohl počítač napadnout vícekrát a počítač byl následně zpomalený. Známým červem byl v roce 2010 Stuxnet, který dokázal napadnout systémy, přeprogramovat řídící jednotky a zamést za sebou stopy v průmyslových systémech SCADA[5]. Tento vir byl podle posledních informací vytvořen USA pro boj s Íránem, jelikož 60% z napadených počítačů bylo právě v Íránu. Kaspersky[6] rok 2010 považuje za začátek éry kybernetických válek. [8]

2.5.6 Spyware

Spyware znamenají v překladu ,,špehové v počítači‘‘. Jde o program, který sleduje činnost uživatele napadeného počítače a získané informace odesílá hackerům. O spyware člověk neví, jelikož běží na pozadí a dle mého názoru je nejhorší technikou hackerů jak získat informace. Spyware odesílá vše, co provedete na počítači. Ať už jsou to emailové adresy, uživatelská jména, spuštěné aplikace, otevřené dokumenty, historie internetového prohlížeče a v neposlední řadě hesla. Spyware se do počítače dostane podobně jako viry či trojské koně – nakaženým programem.

Co se týče odstranění spyware ze systému, existují přímo programy, které zjistí veškeré součásti spywaru a celý ho odinstalují, typickým příkladem je Ad-Aware. Tento program

---

[5] ,,*SCADA jsou speciální systémy, které řídí elektrárny, distribuční sítě, dopravní infrastrukturu a další klíčové prvky*.‘‘ [8]

[6] Kaspersky je mezinárodní společnost, která se zabývá ochranou proti počítačovým virům, spamy a jinými kybernetickými útoky.

je nejrozšířenějším programem pro práci se spyware, program zkontroluje celý systém a spyware a všechny jeho součásti vyhledá a odstraní. [9]

2.5.7 Útok DoS a DDoS

Útok DoS (Denial of Service) znamená v překladu odepření služby. Jsou to útoky útočící na firmy a jejich systémy a sítě. Tyto útoky způsobují nedostupnost systémů a ztráty služeb, např. výpadek nějaké internetové stránky. Cílem těchto útoků je narušení nebo úplné znepřístupnění dané služby pro uživatele. K útoku typu DoS není potřeba zvláštních vědomostí, používají se k němu nástroje, které jsou běžně dostupné. Výhodou DoS útoků je to, že narušit systém nebo jeho obvyklou činnost je jednodušší než se do systému „ nabourat‘‘. Útočník může rozeslat tisíce emailů, jimiž zahltí nejen síťové připojení, ale také emailové schránky uživatelů.

Podtypem útoku DoS je DDoS (Distributed Denial of Service). Tento útok může provést jeden člověk, ale také více lidí najednou. Nejčastější DDoS útoky jsou na internetové bankovnictví, kdy si v jednu chvíli stránku prohlíží několik útočníků a také běžní uživatelé a systém internetového bankovnictví přestane reagovat a odpovídat na požadavky uživatelů. Po útoku je potřeba stránky znovu zprovoznit. Tento útok je sice jednou z technik hackerských útoků, ale na rozdíl od jiných neslouží k vniknutí do systémů a získání údajů o uživateli, DDoS útok jen zahltí servery. Tyto útoky jsou vyjádřením nesouhlasu a projevením se. DDoS útoky jsou projevem všech možností útoků na informační a komunikační prostředky, používají je hackeři, teroristé i podvodníci a také jsou projevem kybernetických válek. [10] [11]

Nejznámější hackerskou skupinou, která prováděla DDoS útoky, je skupina Anonymous. Tato skupina je známá vystupováním pod maskou, kterou můžete vidět na obrázku níže.

Obr. 4 – Maska Anonymous

Zdroj: [12]

Tato skupina zaútočila v roce 2016 na Adreje Babiše a další politiky, kteří chtěli schválit zákon o hazardních hrách. Anonymous blokovali weby ministerstva financí a Senátu. Tento útok zahájili z důvodu nesouhlasu se zákonem o hazardních hrách. [13]

Celá tato kapitola se zabývala nejdůležitějšími body, které se hackingu týkají. Hacking je velmi rozsáhlé téma a zahrnuje v sobě mnoho technik útoků, kterými hackeři pronikají do systémů. Část této kapitoly se zabývala osobností hackera, která hraje nejdůležitější roli pro uskutečnění samotného útoku, a dále nejpoužívanějšími technikami, které v dnešní době hackeři používají k přístupu do počítačů a sítí.

3 KYBERNETICKÉ VÁLKY

Kybernetické války jsou spolu s kyberterorismem nejnovějšími útoky na informační a komunikační prostředky. S těmito pojmy se společnost setkala již za studené války, nicméně jejich rozvoj nastal až ke konci minulého století s masivním rozvojem ICT. Kybernetické války známé jako informační války jsou činy států, které napadají nebo škodí počítačům a sítím jiných států. Tyto státy chtějí dosáhnout národních zájmů bez použití tradičních vojenských sil. Tento pojem vlastně představuje politickou válku mezi státy. [3] Nejčastěji se jedná o útoky malware, což jsou škodlivé programy instalované dálkově do počítačů a útoky DDoS, které jsou podtypem útoků DoS. Cílem kybernetických válek ,, *je znemožnit činnost kritické národní informační infrastruktury''* [1] pomocí psychologických operací a jiných aktivit. Mezi tyto infrastruktury patří politická, ekonomická a sociální sféra. [3]

S kybernetickými válkami souvisí také nový název infoware, v překladu informační válka, který v sobě zahrnuje souhrn všech prostředků, jejichž cílem je zničit informační nebo elektronickou infrastrukturu soupeře, a také prostředků, které vedou k informačním bojům. Mezi nejvýraznější vlastnost informačních válek patří dosah, protože útočník může útočit kdekoliv na planetě, kde je možnost připojení k síti. Informační války mohou být zaměřené proti řídícím a velitelským centrům, proti zpravodajským službám, proti elektronickým systémům a také serverům státu.

4 KYBERTERORISMUS

Jak již bylo zmíněno u kybernetických válek, kyberterorismus společně s kybernetickými válkami patří k nejnovějším globálním hrozbám na informační a komunikační prostředky. Terorismus obecně představuje násilí, které je ideologicky motivováno, což znamená, že může být motivováno nacionálně, nábožensky či politicky. Terorismus také směřuje proti existujícímu systému dané společnosti. Teroristé se zaměřují na představitele státní a ekonomické moci, ale také na anonymní cíle, aby upozornili na svůj cíl a aby ve společnosti vyvolali strach a nejistotu. [14] Kybernetický terorismus je takřka totéž jen s tím rozdílem, že teroristé útočí pomocí ICT, ale se stejným cílem – vyvolat strach. Tak jako u všech výše uvedených typů útoků i kyberterorismem pachatelé získávají, zpracovávají či rozšiřují určité informace a data. Aby ale tyto činy mohly být považovány za kyberterorismus, měl by tento vyústit v násilí proti osobám nebo majetku nebo alespoň navodit strach.

Kyberterorismus se může projevovat těmito metodami:

- vydáváním internetových novin a časopisů z části přebraných od jiných a z části s vlastními příspěvky, kterými budou útočníci směřovat ke změně názorů čtenářů ve svůj prospěch,
- kybertronikou, která využívá podprahové vnímání (využívány jsou např. reklamy cestovních kanceláří, do kterých je zakomponován nějaký obrázek s požadovaným textem)
- haktivismem, což je provozování stránek a serverů s touto problematikou,
- aktivistickým spamem, který je rozesílán různými aktivistickými skupinami s cílem získání podpory pro svůj program,
- útoky vedoucími k omezení bezpečnostních prvků státu z důvodu odstraňování nezákonností,
- útoky na infrastruktury bankovních a finančních institucí, ropného průmyslu,
- útoky na hlasové komunikační služby,
- útoky na zdroje vody. [3]

Pachatelé kyberterorismu

Pachatelem kyberterorismu může být samostatný útočník nebo teroristická skupina. Pokud je útočník sám, je motivem jeho útoku buď uspokojení svého ega a pocit moci nad společností, zvědavost, vzrušení, nebo pomsta. Teroristické skupiny útočí různými druhy útoků

na protivníka. Nejčastější útoky teroristických skupin směřují na webové stránky a na komunikační a bezpečnostní infrastrukturu protivníka, ale také DDoS útoky.

Asi nejznámějším případem kybernetických útoků, které byly později označeny za kyberterorismus, jsou tří týdenní útoky proti Estonsku v roce 2007. Tyto započaly v dubnu 2007, kdy vláda Estonska odstranila památník padlým vojákům Rudé armády ve 2. světové válce, který stál v centru Tallinu. Estonsko se potýkalo s útoky na telefonní a internetové sítě, webové stránky státních institucí, politických stran, bank a také na média. Z těchto útoků Estonsko obvinilo Rusko kvůli pomstě za likvidaci památníku, ale ty Rusko popřelo. Jelikož ministerstvo zahraničních věcí Estonska zveřejnilo seznam IP adres, ze kterých byly útoky vedeny, zjistilo se, že většina adres pochází z Ruska, a jelikož se nepotvrdilo, zda byla v útocích zapojena vláda, či nikoliv, za hlavní útočníky byli poznačeni hackeři z Ruska. Tyto útoky vyvolaly reakce ve vládních řadách a po apelování na veřejné činitele NATO[7] bylo v Tallinu založeno tzv. *NATO Cooperative Cyber Defence Centre of Excellence.* Cílem toho centra byla spolupráce s NATO a rozsáhlá výměna informací. [15]

[7] Severoatlantická aliance.

5 PODVODY

Podvody jsou společně s hackingem v dnešní době nejpoužívanějším druhem útoku na informační a komunikační prostředky. Velmi úzce souvisí s hackerstvím, protože podvodníci musí mít také znalosti a dovednosti ICT na vysoké úrovni, proto se vlastně jedná také hackery. S oblibou internetu přibývá podvedených uživatelů. Pod pojmem podvod si můžeme představit činnost, kterou se podvodník obohatí využitím neznalosti poškozeného nebo

ho uvede v omyl. [16] §209, odst. 1 trestního zákoníku [17] uvádí: ,, *Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.‘‘* Internetové podvody spočívají ve stejné činnosti jako klasické podvody, ale jsou páchány pomocí internetu. Podvodníci si na internetu zjišťují informace o obětech pomocí internetového vyhledávače Google, který o nich nalezne nejen jejich jméno, ale také veškeré informace, které na internetu veřejně sdílely.

5.1 Techniky podvodů na internetu

V současné době se mohou uživatelé internetu setkat s těmito technikami podvodů:

- hoaxem,
- phishingem,
- pharmingem,
- odcizením identity,
- viry, trojským koněm, spywarem. [16]

S phishingem, viry, trojskými koni i spywarem jsme se seznámili již v kapitole 2. zvané Hacking, konkrétně v kapitole 2.5 Techniky hackingu. Nyní se zaměříme na ostatní techniky, používané při podvodech.

5.1.1 Hoax

Hoax je anglické slovo označující podvod, úmyslné klamání nebo žert. Hoax ,, *je nevyžádaná emailová nebo ICQ*[8] *zpráva, která uživatele vatuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod.''* [16] Obsahuje převážně i výzvu, která Vás žádá o rozeslání emailu svým přátelům. Hoax může mít jednu ze tří typických forem.

- **Falešný poplach**

  Tento typ hoaxu zachází s informacemi a snaží se oběť přimět k jejich dalšímu šíření. Tímto typem hoaxu je upozornění o nových radarech Police ČR na dálnicích, které zní: ,,*Všechny Vás informuji o novém typu radarů policie ČR (viz foto), které budou umístěny na dálnicích a rychlostních silnicích. Info je ze zdroje z Policie ČR. Tak dávejte bacha…''* [18] i s připojenou fotografií.

Obr. 5 – Přiložený snímek radaru

Zdroj: [18]

[8] ICQ celým názvem I Seek You je program, pomocí kterého můžete zasílat online SMS zprávy, chatovat a telefonovat. Tento program si instalujete do svého počítače.

- **Zábavná forma**

  Typ hoaxu se vtipnou formou, která oběti vyhrožuje např. 1 rokem neštěstí nebo naopak slibuje. Tyto hoaxy jsou předávány převážně formou řetězových emailů. Příklad známého hoaxu: ,, *Veselé korunky - ať se i k Vám kutálí. Pošli tyto veselé korunky 10ti přátelům a do 4 dnů se Tvoje přání splní..... V opačném případě Tě čekají 4 neúspěšné finanční roky!!!*‘‘ [19]

- **Prosba**

  Tyto typy hoaxů ,, *působí na city a prosí příjemce o darování krve, hledání ztracené osoby, případně přímo vylákává peníze*.‘‘ [16] Známý je případ Alexandra Gála s žádostí o darování krve. Tuto prosbu do sítě vložila přítelkyně manželky pacienta a tento požadavek byl aktuální 2 dny, poté se ho zhostili podvodníci a využívali jej další 4 roky po smrti Alexandra Gála. [20]

5.1.2 Pharming

Pharming je modernější nástupce phishingu, který je ale také nebezpečnější. Cílem pharmingu je překlad jména serveru na odpovídající IP adresu a útok na DNS (Domain Names System), což znamená, že napadá systém doménových jmen. Příkladem může být internetové bankovnictví, pokud se útočníkovi podaří zaměnit DNS záznam například internet banky Moneta Money Bank s adresou https://ibs.internetbanka.cz, přesměruje se komunikace na jiné stránky, které oběť nerozpozná od originálu. Ta zadá své číslo účtu a heslo a přihlásí se, aniž by věděla, že své údaje právě sdělila útočníkovi, který ji chce ukrást její peníze. [16]

5.1.3 Odcizení identity

Tato technika podvodů spočívá ve zjištění hesel do emailu, facebooku nebo na kterýkoliv účet a útočník se začne vydávat za uživatele s cílem získat z účtů peníze anebo šířit pomluvy. ,, *Odborně se tomu říká krádež identity a podle expertů budou tyto útoky stále častější. Krádež identity je nedovolené shromažďování a používání osobních údajů, obvykle za účelem kriminální činnosti.‘‘* [16] Za odcizením identity stojí většinou pomsta útočníka s cílem oběť pomluvit, udělat mu problémy v rodině, v práci, ale i ve společnosti. Nejznámějším případem na facebooku je vydávání se za známou celebritu a přidávání příspěvků pod jejím jménem. Samozřejmě pokud je těchto profilů vytvořeno několik, stávají se podezřelými. Krádež se stává běžnější a největším rizikem pro uživatele jsou dluhy vytvořené

útočníkem, protože ten si díky ukradené identitě vezme například půjčku, aniž by o tom osoba s ukradenou identitou věděla. Na internetu zajímají zloděje identity nejvíce čísla a bezpečnostní kódy kreditních karet, hesla, adresa pobytu, rodné číslo a datum narození apod. [16]

5.2 Útoky na e-shopy

V dnešní době více než polovina společnosti nakupuje přes internetové e-shopy. V rádiu jsem zaslechla, že v loňském roce lidé utratili na českých e-shopech 140 miliard korun a že jen v České republice je zaregistrování přes 40 000 e-shopů a tento počet se stále zvyšuje. E-shop je internetový obchod a je třeba být obezřetný při jeho výběru, protože se můžeme setkat s takovým, který může být falešný, u kterého je požadována pouze možnost zaplacení bankovním převodem. Takový podvodný podnik získá nejen Vaše peníze, ale i informace o Vaší osobě, pomocí kterých mohou útočit na jiné e-shopy a vytvářet tak falešné nákupy.

Pracuji jako administrátorka internetového e-shopu zvaného Svářečky-obchod.cz, který v roce 2007 založil pan Josef Ryšica. Ten je také také ředitelem této firmy a působí na trhu již 11 let. Za tuto dobu se tento e-shop stal jedním z největších dodavatelů svařovací techniky a vybavení dílen v České i Slovenské republice. Již z názvu můžete poznat, že se jedná o obchod zaměřený na svařovací techniku. V posledních letech se nabídka tohoto e-shopu značně rozšířila a nabízí veškeré dílenské vybavení, elektrické, ale i ruční nářadí, stavební stroje, zahradní techniku, nářadí i nábytek, dále kompresory, startovací zdroje a další sortiment tohoto typu. Tento internetový obchod získal mnoho ocenění, mezi které patří certifikát Ověřeno zákazníky na portálu heuréka.cz a také certifikáty Spolehlivá firma. Vzhledem k velkému počtu zákazníků má tento e-shop také již 4 roky v provozu velkou kamennou prodejnu, což také svědčí o tom, že tento e-shop je spolehlivý a ověřený. Ne každý e-shop je v dnešní době spolehlivý a nemůžete spoléhat na to, že je důvěryhodný. Se zvyšujícím se počtem online nákupů se také stupňuje počet útoků nejen na náš e-shop, ale také na všechny existující e-shopy.

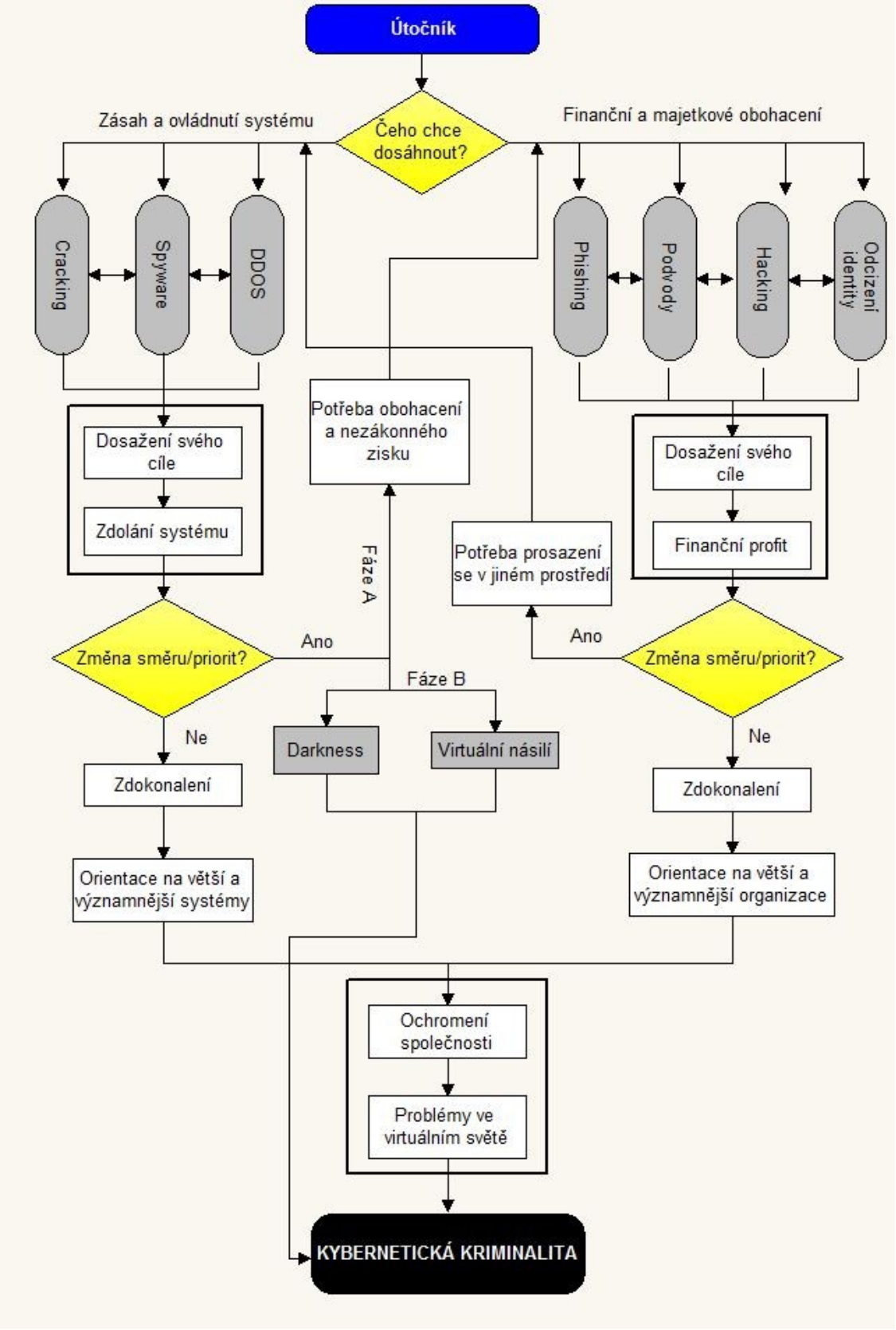
Nejčastějšími útoky na e-shopy jsou podvody. Mezi tato podvodná jednání patří např. falešná identita zákazníka při vytváření objednávky. Jsou zákazníci, kteří mají podvod dobře promyšlený, a prodejce nepozná, zda se jedná o podvodníka, který nezaplatí, jelikož jeho osobní údaje ukradl nějaké oběti. A setkáváme se také s podvodníky, kteří podvod nijak

promyšlený nemají a jako své osobní údaje uvedou nesmysl, přičemž i prodejce pozná, že se nejedná o zákazníka, ale o podvodníka, a objednávkou se dále nezabývá.

Další možností útoku na e-shop je DDoS útok, který byl v práci již také zmíněn. Tento útok spočívá v omezení či vypovězení dané služby, v tomto případě funkčnosti e-shopu. Cílem útočníků je omezení funkčnosti e-shopu. V loňském roce mezi vánočními svátky byl právě na e-shop, ve kterém pracuji, byl zaznamenán DDoS útok. Útočníci opakovaně vkládali položky do košíku a tím zpomalovali celý chod webových stránek obchodu. Naštěstí tento útok nebyl dokončen a našim šikovným programátorem byl odvrácen.

Útočníci mohou na e-shopy útočit také pomocí techniky SQL injection, která spočívá v napadení databáze umístěním ,, *škodlivého kódu do příkazů SQL prostřednictvím vstupu na webové stránce. Vkládání SQL se obvykle vyskytuje, když se uživatele zeptáte na vstup.‘‘* [21] To znamená jeho uživatelské jméno, namísto toho vám dá příkaz SQL a nevědomě tento škodlivý kód spustíte ve své databázi. Hacker získá přístup k vašim účtům a heslům. [21]

V následujícím diagramu můžeme vidět možný postup útočníka při páchání útoku na některý z informačních a komunikačních prostředků a je zřejmé, že tyto útoky mohou být útočníkem promyšlené do nejmenšího detailu, tedy plán A i B. Takto profilovaný útok může být namířen proti počítači, telefonu, internetové síti ale také proti e-shopům.



Obr. 6 – Diagram motivace a průběhu útoku z pohledu útočníka

Zdroj: vlastní

6 MOBILNÍ NEBEZPEČÍ

V této kapitolce se chci zabývat nebezpečím, které hrozí vlastníkům tzv. chytrých telefonů, což jsou dotykové telefony známé také jako smartphony. Na takovém telefonu je několik možností připojení:

- Bluetooth,[9]
- mobilní hotspot,
- WLAN, známé jako WiFi,[10]
- aplikační software.

Ze všech možností připojení je právě Bluetooth tou nejmenší hrozbou pro telefon a je poměrně bezpečný. Přes Bluetooth se dva telefony nebo telefon s počítačem propojí pomocí hesla a dotazem, zda chcete soubor přijmout, nebo ne. Rizikem technologie Bluetooth je tzv. bluejacking, který spočívá v převzetí externího ,, zlého‘‘ programu, díky kterému telefon volá na drahá čísla, a majitel o tom neví. Prostřednictvím Bluetooth se objevily i viry, ale pouze u starších telefonů, v dnešní době se viry přes Bluetooth nevyskytují.

Mobilní hotspot znamená, že se telefonem připojíte na nějaké zařízení, které tento typ připojení umožňuje. Mobilní hotspot je hojně využívaný na cestách a v zahraničí. V nastavení telefonu si aktivujete mobilní hotspot a můžete přes WiFi využívat internetové připojení. Jedinou chybou této technologie je, že se v momentě stáváte WiFi routerem, na který se může napojit jakékoliv zařízení, a pokud si nenastavíte heslo k připojení, může se stát, že se úplně cizí člověk dostane k Vašim osobním údajům a zneužije je.

WiFi je nejpoužívanější připojení nejen telefonů, ale i notebooků, tabletů a dalších zařízení které mají možnost se k internetu připojit. Je to bezdrátové připojení, jehož výhodou je právě bezdrátovost. Bezdrátové připojení je v současnosti hojně využíváno v restauracích, hotelech, barech a dalších veřejných místech. Riziková jsou nezabezpečená připojení, na která se můžete volně připojit. Pokud se připojíte na nezabezpečenou WiFi můžete otevřít svůj přístroj hackerům, a když se podíváte třeba do své emailové schránky, hacker má vaše přístupové údaje a může do vašeho telefonu či notebooku lehce nainstalovat viry. [22]

---

[9] *Bluetooth je technologie umožňující bezdrátové připojení elektronických přístrojů.* [22]
[10] WLAN známé jako WiFi je bezdrátové připojení.

,, Smartphony a moderní tablety jsou k ničemu bez správných programů, jimž se dnes říká aplikační software nebo také ,, apps''.'' [22] Aplikace pro mobilní telefony a tablety poskytují Android a Apple. Vlastním telefon se systémem Android a aplikace a programy do svého telefonu stahuji pomocí Obchod Play. V tomto ,, obchodě'' jsou nabízeny aplikace poskytované zdarma či za poplatek. Samozřejmě si každý raději do svého telefonu nainstaluje aplikaci poskytovanou zdarma než placenou. Obchod Play má integrovanou bezpečnostní funkci, která se aktivuje, když si chcete nainstalovat nějakou aplikaci. Zobrazí se seznam oprávnění, které aplikace vyžaduje, a buď si aplikaci nainstalujete, nebo ne. Je potřeba si všímat, jaká oprávnění jsou požadována. Tato oprávnění mohou být nebezpečná, s menším rizikem ale také bez rizika.

Mezi nebezpečná oprávnění patří:

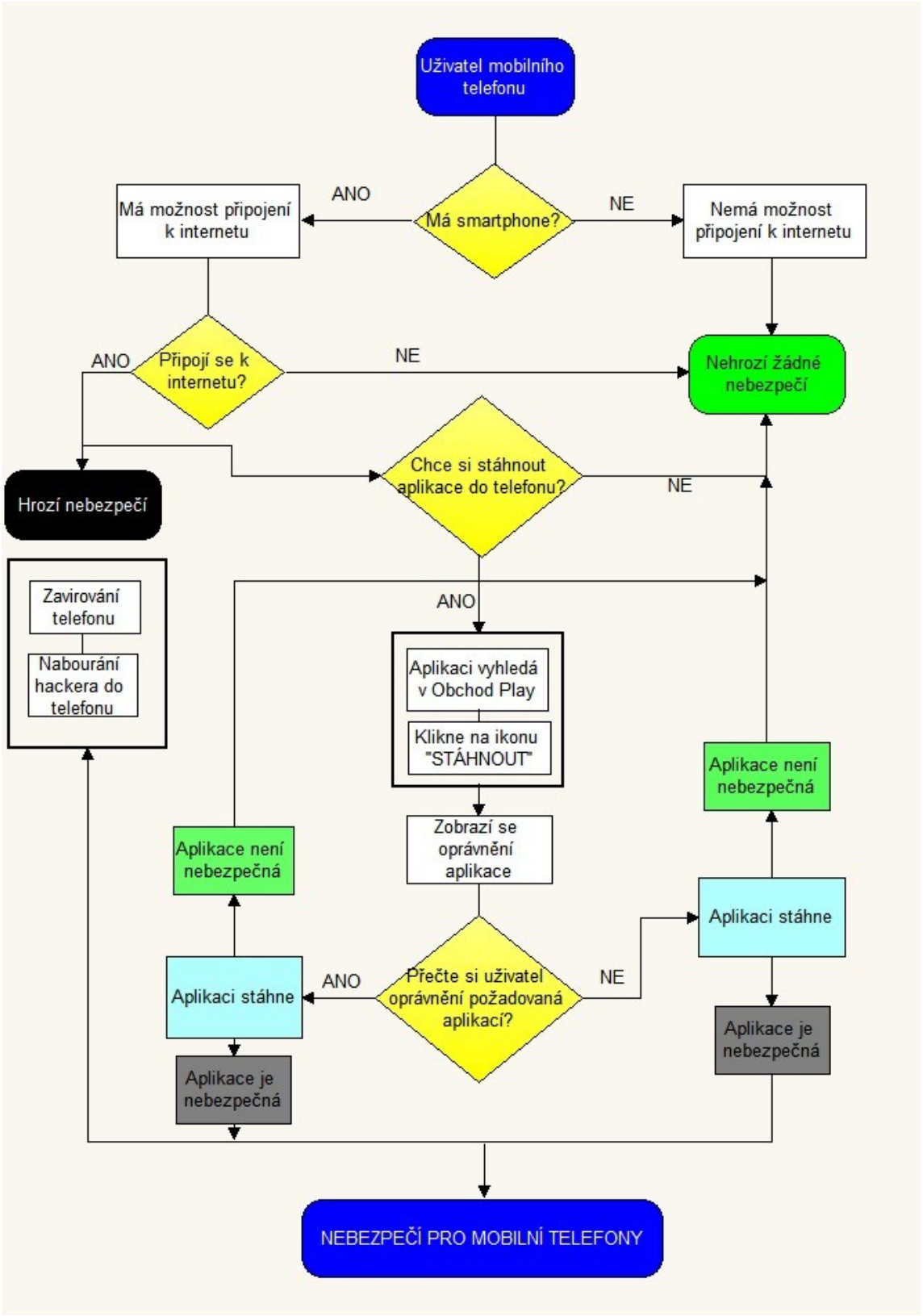
- *Přímá volba telefonních čísel*
  Povolení aplikace vytáčet telefonní čísla, aniž byste o tom věděli.
- *Zasílání SMS*
  Povolení zasílání SMS zpráv i bez vašeho souhlasu (může vás to stát hodně peněz).
- *Čtení a změna kontaktů*
  Povolením tohoto oprávnění riskujete změnu adres a dalších kontaktních údajů.
- *Čtení důvěrných údajů z protokolů*
  Povolením umožníte aplikaci číst vaše veškeré citlivé osobní údaje.
- *Čtení webového protokolu*
  Povolením tohoto oprávnění otevíráte aplikaci cestu k vašim uloženým a navštěvovaným webovým stránkám.
- *Neomezený přístup na internet*
  Jedno z nejnebezpečnějších oprávnění. Povolením by aplikace získala právo na absolutně nekontrolovatelný přenos dat přes internet.
- *Správa seznamu účtů*
  Oprávnění spočívající v zakládání nových účtů a také k úpravě nebo mazání těch starých. Toto oprávnění se doporučuje poskytovat jen aplikacím souvisejících s Facebookem.

Mezi oprávnění s menšími riziky nebo také žádnými riziky patří:

- *Změna nebo mazání uložených obsahů*
  Povolení aplikace k přístupu k obsahům, které jsou v telefonu uloženy.

- *Čtení a identifikace statusu telefonu*
  Povolením tohoto oprávnění může být váš telefon lokalizován kdykoliv a kdekoliv.
- *Stanoviště telefonu*
  Toto oprávnění poskytuje informace o pozici telefonu.
- *Vytvoření připojení Bluetooth*
  Vyžadují aplikace, které mají přenášet data přes Bluetooth.
- *Zobrazení statusu sítě a WLAN*
  Povolením oprávnění povolíte aplikaci přečíst, v které síti je váš mobil zařazen. Jedná se buď o WIFI nebo 3G, což jsou mobilní data poskytovaná operátorem.
- *Vyhledávání známých účtů*
  Oprávnění, které povoluje náhled do všech uživatelských účtů v telefonu. Není nebezpečné, bez rizika.
- *Funkce autentizace účtů*
  Povolení k přístupu uživatelského účtu bez možnosti získat přístup k citlivým údajům.
- *Instalace balíčků*
  Povolením svolíte aplikaci, aby instalovala další aplikace do vašeho telefonu.
- *Ukončení procesů v pozadí*
  Oprávnění, které povolením může ukončit jiné aplikace. Není nebezpečné, relativně bez rizika.
- *Řízení vibrací*
  Použití vibrací k upozornění důležité informace. Není nebezpečné, bez rizika.
- *Pořizování snímků a videa*
  Povolit jen v případě, kdy aplikace pořizovat fotografie a videa musí. V jiných případech nepovolovat kvůli možnému riziku tajného fotografování a dalšího šíření pořízených snímků.

Dalším nebezpečím, které na mobilní telefony číhá, jsou samozřejmě viry. Na viry spoléhají hackeři proto, že systém v telefonu si neaktualizujete každý půl rok, jako to musíte dělat na počítači, a proto se snaží proniknout do hlubších vrstev systémů telefonů a snaží se tam vnořit virus. [22] Následující diagram zobrazuje, jak se do telefonu se systémem Android instaluje aplikace a možná nebezpečí aplikací.



Obr. 7 – Diagram postupu instalace aplikace do mobilního telefonu a hrozící nebezpečí

Zdroj: vlastní

DÍLČÍ ZÁVĚR

Teoretická část byla zaměřena na kybernetickou kriminalitu jako celek, ale také na útoky, kterými lze na současné informační a komunikační prostředky zaútočit. V první části práce je popsán alespoň částečně vývoj kybernality až po její současnost a také pachatelé této kriminality, protože bez nich by tato kriminalita nemohla existovat. Následně se práce zabývala hackingem a vším, co s tímto rozsáhlým tématem souvisí, avšak vymezeny byly jen ty nejpodstatnější body, které je potřeba znát, abychom tuto problematiku alespoň částečně pochopili.

Další nedílnou součástí, která s kybernalitou souvisí, jsou kybernetické války a kyberterorismus. Tyto možnosti útoků na současné informační a komunikační prostředky jsou stále častější a probíhají převážně mezi státy. V práci nechybí také problematika podvodů, které v dnešní době představují nejběžnější typ útoků a zvláště na internetové e-shopy, kterých je velké množství. Lidé více nakupují přes internetové e-shopy než v kamenných prodejnách. V závěru teoretické části byla zmíněna nebezpečí, která hrozí současným mobilním telefonům zvaným smartphony, protože během posledních 5 let jsou nejpoužívanějším komunikačním prostředkem ve společnosti.

II. PRAKTICKÁ ČÁST

7 OCHRANA PŘED ÚTOKY

S vývojem informačních a komunikačních technologií je také daleko častěji ohrožena bezpečnost těchto prostředků a také jsou na ně častěji páchány útoky, které se za poslední léta mnohonásobně prohloubily a zdokonalily, a proto je velmi důležité dodržovat daná pravidla, abychom zamezili rizikům a hrozbám, které na nás číhají především na internetu. Je potřeba chránit nejen sebe a svá data ale především internetové připojení a počítač. Kdo má tzv. chytrý telefon tak také svůj telefon. Struktury a vlastnosti vybraných hrozeb, které nám hrozí, byly rozebrány v teoretické části. Předpokladem pro ochranu před útoky na informační a komunikační prostředky je zdravý lidský rozum a dodržování bezpečnostních pravidel na internetu. Důležitou ochranou počítače i internetových sítí není jen heslo, antivirus a firewall[11], ale především je důležité se o tyto způsoby zabezpečení také starat a hlídat si aktualizace těchto programů, aby běžely na 100%. Doseděl [22] ve své knize definoval tato **bezpečnostní pravidla:**

1. *Všechno důležité zaheslujte,*
2. *s hesly zacházejte opatrně,*
3. *z internetu nic neotvírejte,*
4. *e-maily používejte bezpečně,*
5. *rozesláním e-mailu nikoho nezachráníte,*
6. *chraňte se před viry,*
7. *vyžeňte z počítače špióny,*
8. *pravidelně záplatujte,*
9. *poznejte počítačové kriminálníky,*
10. *důležité věci si zálohujte,*
11. *chraňte data vlastním tělem,*
12. *schovejte se za firewallem,*
13. *se sousedy se domluvte,*
14. *přístupová práva vás nemusí omezovat,*
15. *tajná data šifrujte,*
16. *nikomu úplně nevěřte,*
17. *odlišujte zabezpečené weby,*

[11] ,, *Firewall omezuje riziko, že by někdo zvenčí mohl přes internetové připojení proniknout do PC. ‘‘* [22]

18. víte, s kým se bavíte?,

19. stále jste pod kontrolou,

20. nepropadejte panice,

21. *pozor, kam voláte.*

Všechna tato pravidla spolu úzce souvisejí a je opravdu důležité se na internetu rozhodovat a pohybovat opatrně bez ohledu na to, jestli máme v počítači antivirus, firewall nebo zabezpečené internetové připojení.

7.1 Ochrana počítače

Zabezpečení počítače a hlavně souborů a dat v něm obsažených je pro uživatele velmi důležité a tato ochrana spočívá hlavně v heslech. Mnoho uživatelů ani neví, že lze zabezpečit heslem i základní systém počítače známý jako BIOS[12]. Ten lze zabezpečit heslem a jedná se o základní ochranu před nezvanými hosty. Heslo v BIOSU sice nechrání počítač před viry, spyware nebo jakýmkoliv útokem provedeným prostřednictvím internetových sítí, ale chrání data uložená v počítači, která útočníky lákají. Důvody, kvůli kterým útočníci páchají útoky, jsou uvedeny v teoretické části v kapitole 1.1 Pachatelé kybernetické kriminality. Mezi tyto důvody patří především zjištění informací a následně jejich sdílení, poškození či upravení.

Důležité dokumenty či složky lze také zabezpečit heslem stejně tak jako uživatelský účet. Nicméně tato ochrana zkušeným útočníkům nezabere mnoho času a po několika minutách jsou schopni se dostat jak přes heslo v BIOSu, tak zjistit heslo uživatelského účtu i ostatních dat. [22] K důležité ochraně počítače patří také antivirový program, firewall a zabezpečené internetové připojení. Pokud nemáte chráněné internetové připojení a ani Windows, pro útočníka je Váš počítač jednoduchým cílem. Tímto způsobem dochází k odcizení či ztrátě důležitých dat, nebo dokonce k odcizení identity a tím i k následnému obtěžování a vyhrožování.

[12] *BIOS je základní software, který inicializuje a konfiguruje počítač při startu a poskytuje i některé další funkce během jeho provozu.* [22]

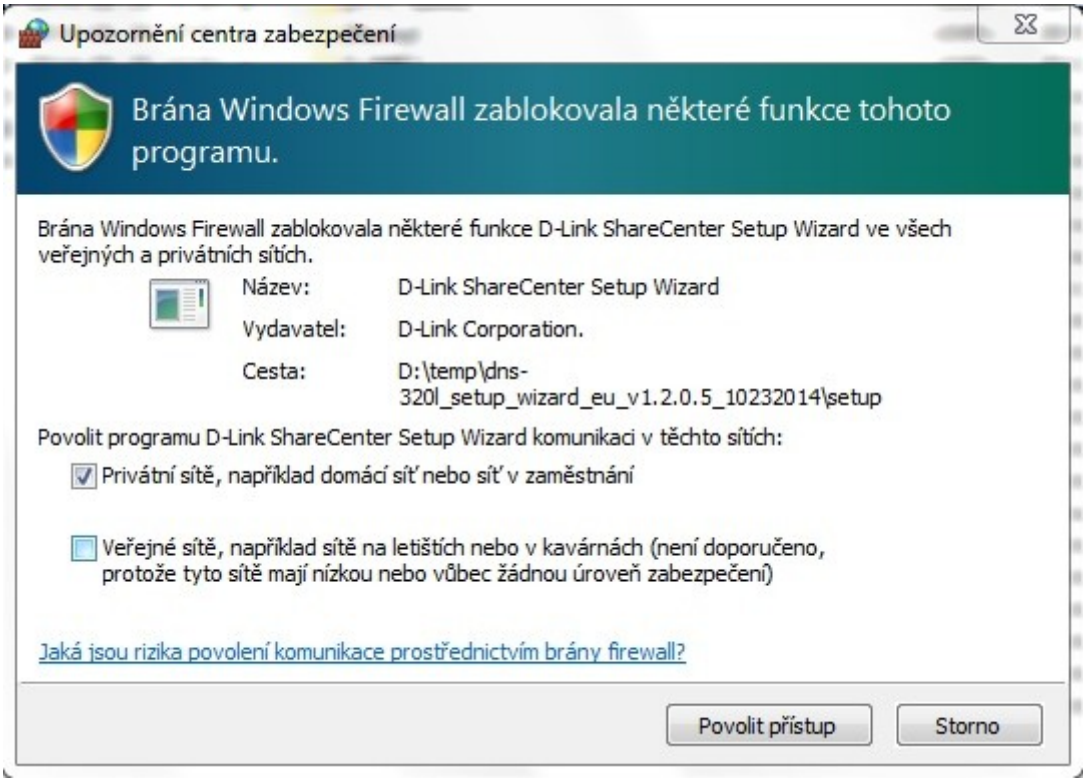
7.1.1 Firewall

Jak již bylo výše zmíněno, firewall může pomoci chránit počítat před tím, aby k němu prostřednictvím internetu nebo sítě získali přístup hackeři nebo nějaký škodlivý software. Integrovaný firewall označován jako ICF (Internet Connection Firewall) v sobě zahrnuje systémy Windows XP a vyšší verze Windows (Vista, 7, 8, 8.1, 10). Starší systémy Windows tuto ochranu v sobě integrovanou neměly, a proto se musela tato ochrana instalovat pomocí aplikačního softwaru, nicméně starší verze Windows, jako je Windows 1, 2, 3, 95, 98 a 2000, se v dnešní době již nepoužívají a Windows XP jen zřídkakdy, současné počítače i notebooky v sobě zahrnují systém Windows 7 a vyšší, které firewall integrovaný mají. Integrovaný firewall počítač spolehlivě ochrání. [24]

A jak poznáte, že máte ochranu integrovanou ochranu firewall aktivní? Ve Windows 7, 8 a 8.1 klepněte na Start / Ovládací panely a vyberte Brána Windows Firewall, již od prvopočátku by tato služba měla být aktivována, pokud ji uživatel osobně nedeaktivoval. Aby byl firewall správně používaný, rozlišuje Windows soukromé neboli domácí sítě a veřejné sítě. Tento fakt je velmi důležitý u bezdrátového připojení, protože tato forma připojení k internetu je dnes nejpoužívanější.

Soukromé neboli domácí sítě jsou takové, u kterých lze předpokládat základní bezpečnost. U veřejných sítí je tomu přesně naopak. Ty bývají využívány především v hotelech, restauracích a ostatních veřejných místech. Pokud se připojíte k nové síti, Windows se automaticky zeptá, zda se jedná o síť soukromou nebo veřejnou, a podle vaší odpovědi použije určitá bezpečnostní pravidla. [22]

Funkci firewallu můžete rozpoznat při instalování nového programu, při kterém se objeví vyskakovací okno s upozorněním, že Brána Windows Firewall zablokovala některé funkce programu, viz obrázek níže.



Obr. 8 – Vyskakovací okno s upozorněním funkce Firewallem

Zdroj: [25]

7.1.2 Antivirový program

Antivirová ochrana patří k dalším prostředkům základní ochrany počítače. Známe ji také pod pojmy také pod pojmy antivir a antivirus. Tento program je důležitý pro ochranu počítače před škodlivými viry. Antivirus dokáže prohledat paměť počítače a všechny soubory na pevném disku a najít přítomné viry a většinou je bezpečně odstraní, aniž by byl napadený soubor poškozen, ale v případě, že to není možné, napadený soubor smaže. [24] Antivirový program se musí do počítače nainstalovat stejně jako jiné programy, které užíváte, a ihned po instalaci je důležité provést kontrolu počítače, která je velmi důležitá.

Antivirový program bývá spuštěn již při startu počítače a chrání ho po celou dobu práce před útoky a viry. V teoretické části bylo zmíněno, že první viry se šířily přes diskety, dnes nejčastěji prostřednictvím internetu, např. škodlivým souborem v příloze příchozího e-mailu. Kvalitní antivir kontroluje všechny spuštěné soubory a také ty, které do počítače přicházejí právě prostřednictvím internetu. Antivirových programů existuje velké množství a jedinou jejich nevýhodou je to, že jsou zpoplatněné a aktuální virovou databázi si musíte hradit. Ale i v dnešní době jsou již k dispozici antivirové programy, které jsou zdarma.

A samozřejmě i zpoplatněné antivirové programy nabízejí vždy zkušební verzi programu, která je bezplatná. Nicméně mnohé zpoplatněné antivirové programy lze používat legálně dlouhodobě, a to po odinstalování a nainstalování nové zkušební 30denní verze.

Mezi programy poskytované zdarma patří známý antivirus Avast! a AVG Anti-virus Free. Za nejspolehlivější antivirus je považován NOD32, který je sice zpoplatněný, ale nabízí zkušební verzi. Antivirus NOD32 jsem používala léta a nikdy jsem neměla problém s virem ani obdobným útokem na svůj počítač. Po zakoupení nového notebooku se systémem Windows 8.1 antivirus instalovat nemusím, protože má v sobě integrovanou antivirovou ochranu i ochranu proti spyware zvanou Windows Defender. Je důležité virovou databázi udržovat stále aktualizovanou, jelikož antivirus bez aktuální virové databáze může napáchat více škody než užitku. Proto je nutné pamatovat na to, že virová databáze antivirového programu musí být stále aktualizována, aby byla funkčnost antiviru 100%.

Windows Defender, který byl zmíněn výše, byl představen s příchodem Windows 7, který v tomto systému bránil počítač proti spyware, nicméně tento program nenabízel skutečnou antivirovou ochranu, jak si mnozí mysleli, tudíž instalace některého z antivirových programů byla nezbytná. S příchozími Windows 8 byl integrovaný program Windows Defender zdokonalen a stal se plně funkční antivirovou ochranou. [24] Můžeme tedy konstatovat, že integrovaná Brána Windows Firewall a antivirus u starších verzí Windows a Windows Defender, u verzí Windows 8 a výše zajišťují spolehlivou ochranu proti virům. Každopádně je také důležité mít zabezpečenou internetovou síť, jejíž ochranou se budeme zabývat v další kapitole.

7.2 Ochrana internetového připojení

Pokud chcete předejít útokům, nestačí jen zabezpečení systému Windows pomocí brány Firewall a antiviru, ale je také podstatné mít zabezpečenou internetovou síť. Jak již bylo zmíněno v teoretické části hrozbám a útokům jsme vystaveni všichni kdykoliv jsme připojeni na internet na jakémkoliv zařízení, jelikož v ohrožení jsou hlavně systémy těchto zařízení. Připojení k internetu může být drátové probíhající přes DSL modem a bezdrátové probíhající přes router. Router je síťové zařízení, které spojuje sítě a přenáší mezi nimi data. Drátové připojení je známé jako Ethernet a používá se dodnes převážně ve firmách přes DSL modem, ale některé routery pro bezdrátové připojení podporují i ethernetové

připojení. Skrze drátové připojení nehrozí takřka žádné nebezpečí, protože hacker by se musel připojit drátem na stejný modem, a tato pravděpodobnost je minimální.

Jak již bylo zmíněno, bezdrátové připojení funguje pomocí routeru a je známé pod pojmem WiFi. Router ale musí být zabezpečen pomocí uživatelského jména a hesla, aby k němu měla přístup jen určitá osoba, která na tomto routeru nastaví kódování a další zabezpečení. To spočívá ve vytvoření hesla, díky kterému se k dané WiFi dá připojit. Existují také bezdrátové sítě, které nejsou zabezpečené a to jsou převážně sítě na veřejných místech, jako jsou restaurace, hotely apod. Právě přes tyto sítě jsou uživatelé nejčastěji napadáni.

Předtím než své bezdrátové připojení zabezpečíte heslem, je důležité zabezpečit ho také kódováním, které může být WEP, WPA a WPA2. Kódování WEP je starší zabezpečení, které bylo již bohužel prolomeno hackery, a proto se již téměř nepoužívá. Zabezpečení WPA je nástupcem WEP, které bylo zavedeno jen kvůli opoždění nového kódování zvanému WPA2. Všechny dnešní routery ovládají kódování WPA2 a při zabezpečení sítě je stěžejní toto kódování aktivovat. Toto zabezpečení již vyžaduje heslo, které je nejdůležitější částí ochrany internetové sítě. Proto je nejvhodnější kombinovat zvláštní znaky s číslicemi i čísly, aby bylo heslo co nejsložitější a také co nejdelší. Optimální heslo, které lze jen stěží prolomit, by mělo obsahovat minimálně 20 a maximálně 63 znaků.

Po aktivaci kódování WPA2 a nastavení optimálního hesla pro přihlášení k síti je také jedna z možností udělat svou domácí síť neviditelnou pomocí nastavení SSID, což je identifikátor bezdrátové sítě WiFi. Tento identifikátor umožňuje vyhledat Vaši bezdrátovou síť WiFi, ale pokud ji dobře zabezpečíte heslem a kódováním WPA2, nelze se k této síti připojit bez zadání hesla. Každý WiFi router má v sobě obsaženu přesnou adresu, pomocí které jej můžete spravovat a nastavovat právě tato zabezpečení a kroky, a zejména jen vy nikdo jiný. Možností je také zadat, aby síť nebyla ukazována, a nikdo cizí ji nevyhledá.

Po zabezpečení sítě pomocí daného kódování a hesla, daného antivirového programu a firewall máte nejen síť, ale také svůj počítat chráněn před veškerými útoky. Ovšem důležitá je také aktivita při surfování a komunikaci přes sociální sítě. Je také velmi podstatné zformulovat dlouhé a složité heslo i na všech účtech vytvořených na počítači a přes sítě, jako je např. emailová adresa, účet na Facebooku, Twitteru apod. Důležité je také používat pro každý účet jiné heslo a nemít u všech účtů heslo stejné.

7.3 Ochrana mobilních telefonů

Tak jako je důležité mít zabezpečený svůj počítač antivirovým programem a bránou firewall, je také nezbytné mít zabezpečený svůj mobilní telefon. Tato ochrana je se týká dotykových mobilních telefonů známých pod názvem smartphony nebo chytré telefony. Na tuto ochranu se chci zaměřit vzhledem k velkému rozmachu používání mobilních telefonů v současné době. V kapitole 6 Mobilní nebezpečí v teoretické části byly tyto možnosti nebezpečí zmíněny. Je přeci daleko pohodlnější připojit se k WiFi přes mobilní telefon a surfovat a komunikovat přes telefon, než s sebou stále nosit notebook. Na mobilním telefonu je nejvíce využíván e-mail, sociální sítě a v neposlední řadě také platby všeho druhu. Uživatelé si mnohdy neuvědomují, že se jejich telefon může stát terčem útočníků. Přes mobilní telefon se uskutečňují platby bez jakéhokoli potvrzení, a pokud se do chytrého telefonu naboural hacker, může si při nejlepším zjistit osobní data, při nejhorším cokoliv platit, protože při platbách přes mobilní telefony nebývá požadováno potvrzení platby.

Tak jako pro počítače existuje ochrana pomocí brány firewall a pomocí antivirového programu, pro mobilní zařízení lze antivirovou ochranu taky zařídit. Jak již bylo nastíněno v teoretické části práce, aplikace a programy pro telefony poskytují systémy Android a Apple, a zabývala jsem se Androidem a Obchod Play, který poskytuje tyto aplikace. Jako antivirové programy pro počítače byly zmíněny Avast!, AVG antivirus, NOD32 a Kaspersky. Všechny tyto zmíněné programy nabízejí také antivirovou ochranu pro mobilní telefony, které můžete zdarma stáhnout a nainstalovat. Samozřejmě nabízených antivirových programů pro mobilní telefony je daleko více, ale výše zmíněné patří mezi nejspolehlivější. Já osobně mám telefon Huawei Nova, který má nejnovější systém Android a telefony s tímto nejnovějším systémem v sobě mají zabudovanou aplikaci antivirové ochrany se všemi komponenty pod názvem „Správce telefonu‘‘. Pomocí této aplikace můžete provádět kontroly zabudovaného antiviru Avast! na viry, dále sledovat oprávnění, která jste přijali v rámci instalací aplikací, ale také celkovou optimalizaci telefonu, která provede optimalizaci všech funkcí.

Bránit se lze jakémukoliv útoku, ať už jde o vir, malware, spyware nebo jiný. Nezbytné je dodržovat základní pravidla bezpečného chování při práci na internetu nebo se alespoň snažit je dodržovat, ale především mít aktualizovaný systém, firewall a antivirový program nejen v počítači, ale také v telefonu. Jakákoliv mezera v systému nebo zabezpečení je špatně a útočník této mezery může ihned využít.

7.4 Opatření pro zlepšení ochrany před možnostmi útoků na současné informační a komunikační prostředky

Jak již bylo zmíněno výše, je opravdu důležité mít zabezpečený svůj počítač a také internetové připojení tak, abychom mohli předejít útokům, které nám hrozí na internetu. Ne každý má zabezpečený svůj počítač, internetové připojení nebo mobilní telefon. Tito uživatelé jsou vstupní bránou pro útočníky, a proto je ochrana těchto nástrojů skutečně podstatná. **Mezi základní pravidla bezpečného chování na internetu patří:**

- chránit sebe a své komunikační prostředky zabezpečením,
- aktualizovat systémy v počítačích i mobilních telefonech,
- zabezpečit internetové připojení,
- snažit se dodržovat 21 bezpečnostních pravidel,
- nesdílet a neukládat citlivé údaje do prohlížečů i počítačů,
- používat zdravý lidský rozum a myšlení.

Pokud se každý uživatel bude snažit dodržovat pravidla uvedená výše, může předejít hrozícím útokům a chránit tak nejen svá data, ale hlavně také sebe.

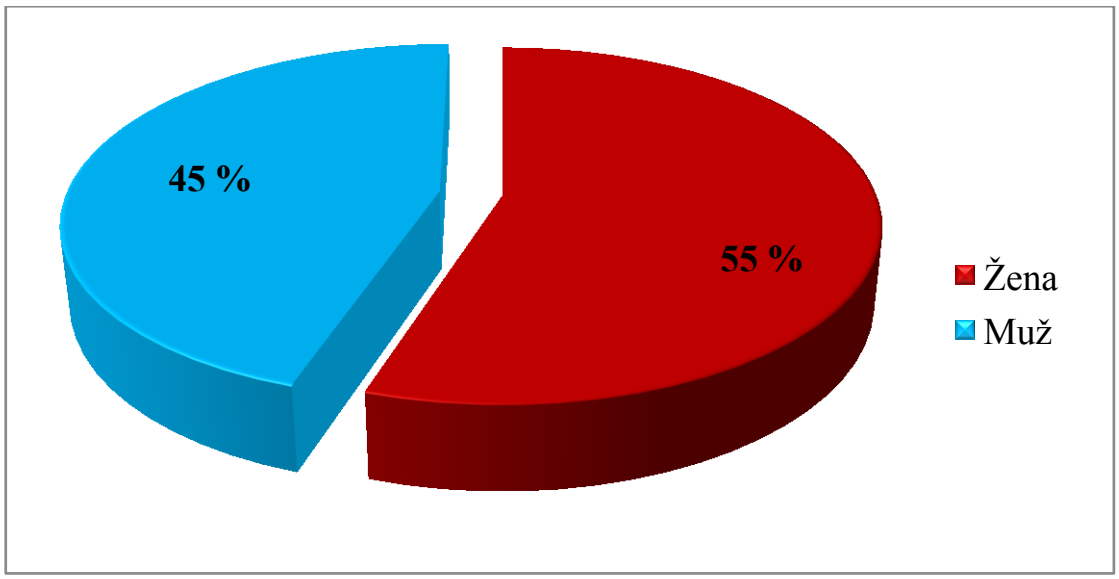
8 DOTAZNÍK

Cílem dotazníku bylo zjistit, jestli dotazovaní vědí, co je to kybernetická kriminalita a zda se sní ve svém životě setkali. A jakým způsobem chrání své osobní údaje a své informační a komunikační prostředky před hrozícími útoky. První část dotazníku je věnována právě kybernetické kriminalitě z obecného hlediska s cílem zjistit, jestli dotázaní tento pojem znají a co si pod ním představují. Druhá část dotazníku se věnuje hrozícím útokům a ochraně informačních a komunikačních prostředků před možnými hrozbami. Cílovou skupinou tohoto výzkumu byli mí přátelé, známí a také rodinní příslušníci. Dotazník byl mezi účastníky rozeslán pomocí sociální sítě Facebook a prostřednictvím e-mailů s odkazem na webovou stránku survio.cz, kde byl dotazník vytvořen. Na otázky odpovědělo100 respondentů. Vzor dotazníku k vyplnění viz Příloha PII.

Vyhodnocení dotazníku

Vyhodnocení dotazníku je provedeno prostorovým výsečovým grafem s procentuálním zobrazením výsledných hodnot a barevným rozlišením.

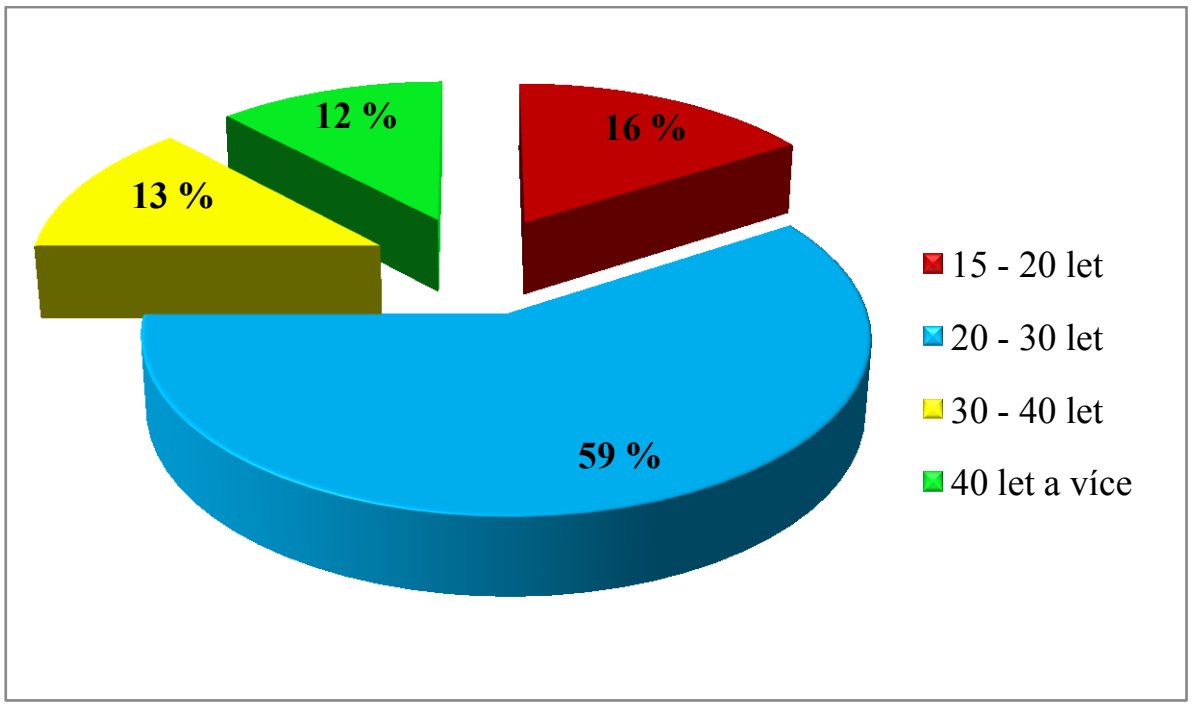
Otázka č. 1 – Jste žena nebo muž?



Obr. 9 – Graf odpovědí k otázce č. 1

Prvním grafem dotazníku otázky *„ Jste žena nebo muž?“* bylo zjištěno, že odpovědělo 55 žen, což činí 55 % a 45 mužů, což činí 45 % z celkového počtu dotázaných. Nadpoloviční většinou jsou ženy, což je v případě cílové skupiny zřejmé, jelikož každá žena má více známých a kamarádů mezi ženami než muži. Zastoupení mužů se od žen liší jen velmi málo, což mě velice překvapilo.

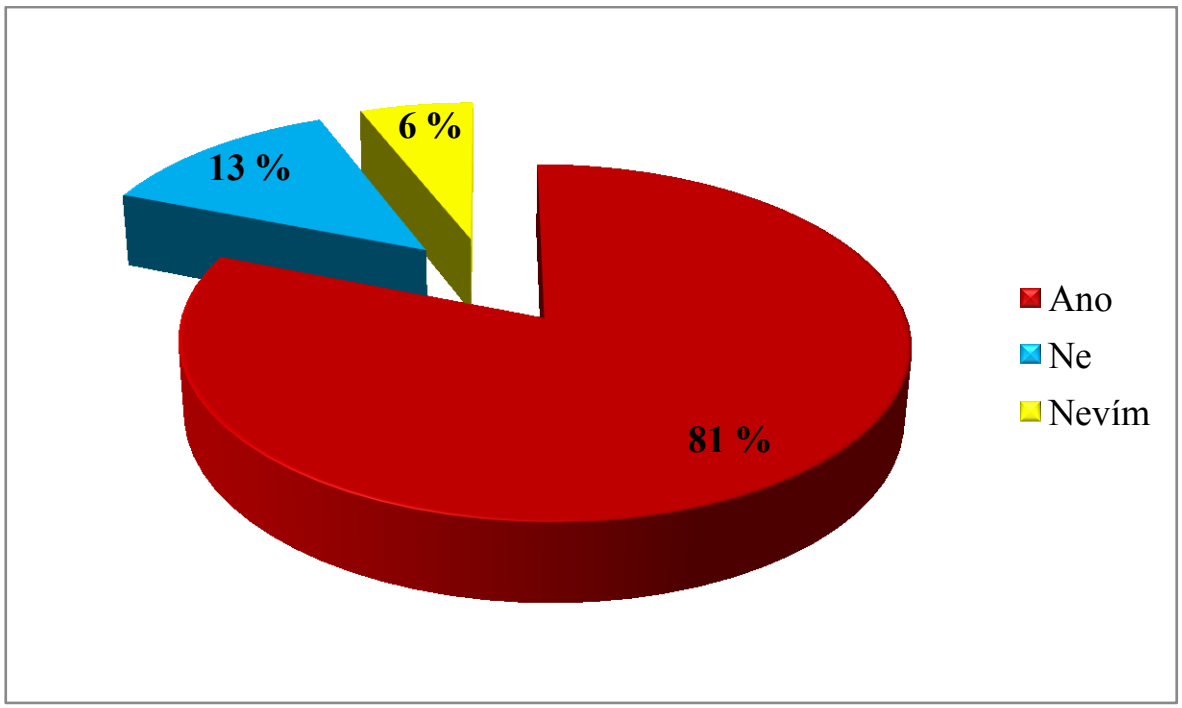
Otázka č. 2 – Do jaké věkové kategorie patříte?



Obr. 10 – Graf odpovědí k otázce č. 2

Z grafu k otázce *,, Do jaké věkové kategorie patříte?'' bylo* zjištěno, které věkové kategorie respondentů na dotazník odpovídaly. Rozdělila jsem je na *15 až 20 let, 20 – 30 let, 30 – 40 let a 40 let a více.* Z grafu je patrné, že největší zastoupení měla kategorie respondentů mezi 20 až 30 lety, která a činí 59 % všech odpovědí, a vzhledem k mému věku jsem také očekávala, že odpovědí v této věkové kategorii bude nejvíce, jelikož převážně v tomto rozmezí věku jsem dotazníkem podrobila přátele, ale také několik osob z řad rodinných příslušníků. Druhou nejčastější odpovědí byla reakce lidí v rozmezí 15 až 20 let, která činí 16 %. Odpověď *30 až 40 let* označilo 13% a odpověď *40 let a více* 12 % respondentů. Dotazovaní v tomto rozmezí byli převážně rodinní příslušníci, mezi které patří hlavně tety, strýcové a v neposlední řadě také rodiče.

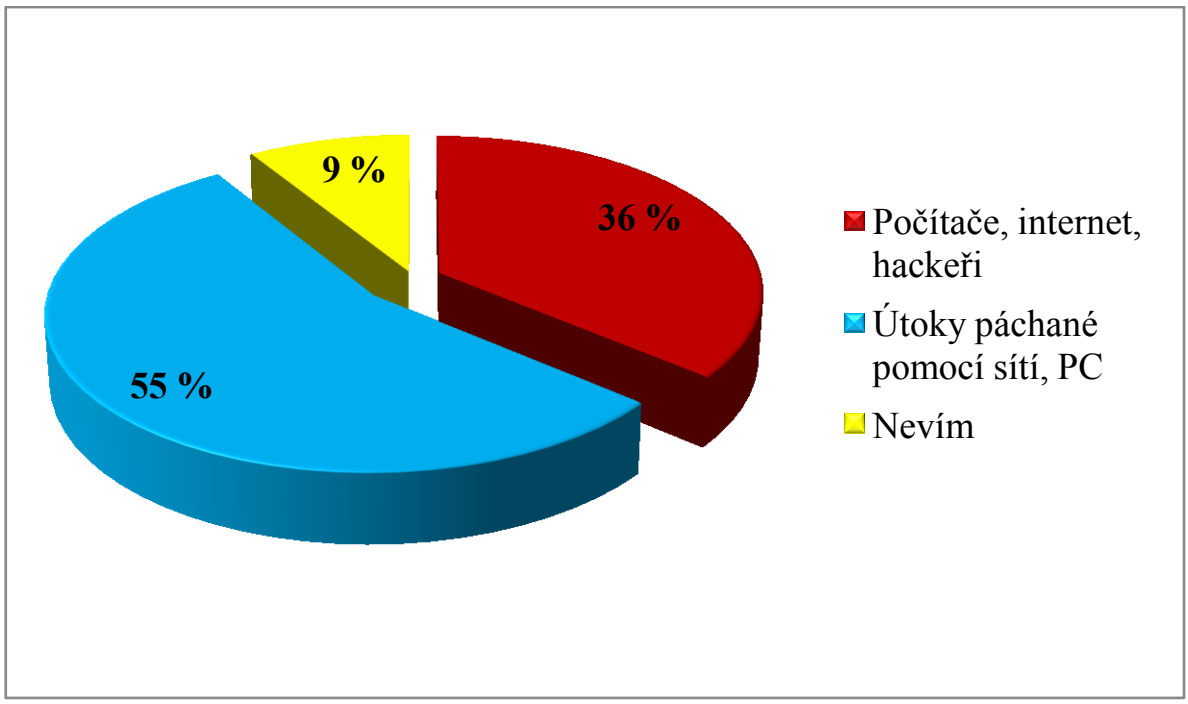
Otázka č. 3 – Slyšeli jste někdy o pojmu kybernetická kriminalita?



Obr. 11 – Graf odpovědí k otázce č. 3

Z grafu bylo zjištěno, že na otázku „ *Slyšeli jste někdy o pojmu kybernetická kriminalita?*“ odpovědělo plných 81 % dotázaných možností *Ano,* což činí více než tři čtvrtiny respondentů. Pouze 13 % odpovědělo možností *Ne* a pouhých 6 % respondentů odpovědělo možností *Nevím*. Z daného grafu je zřejmé, že tento pojem je v dnešní době opravdu známý nejen mezi mými blízkými a přáteli, ale jistě také ve světě vzhledem k tomu, že není týdne, kdy by se o kyberkriminalitě nebo samotných útocích na současné informační a komunikační prostředky nemluvilo nebo psalo v televizi, rádiu nebo na internetu. S pojmem kybernetická kriminalita jsme se seznámili již v úvodu práce a s jejím vývojem v teoretické části. O kybernetické kriminalitě a vším, co s ní souvisí, se čím dál častěji konají konference a přednášky pro širokou veřejnost..

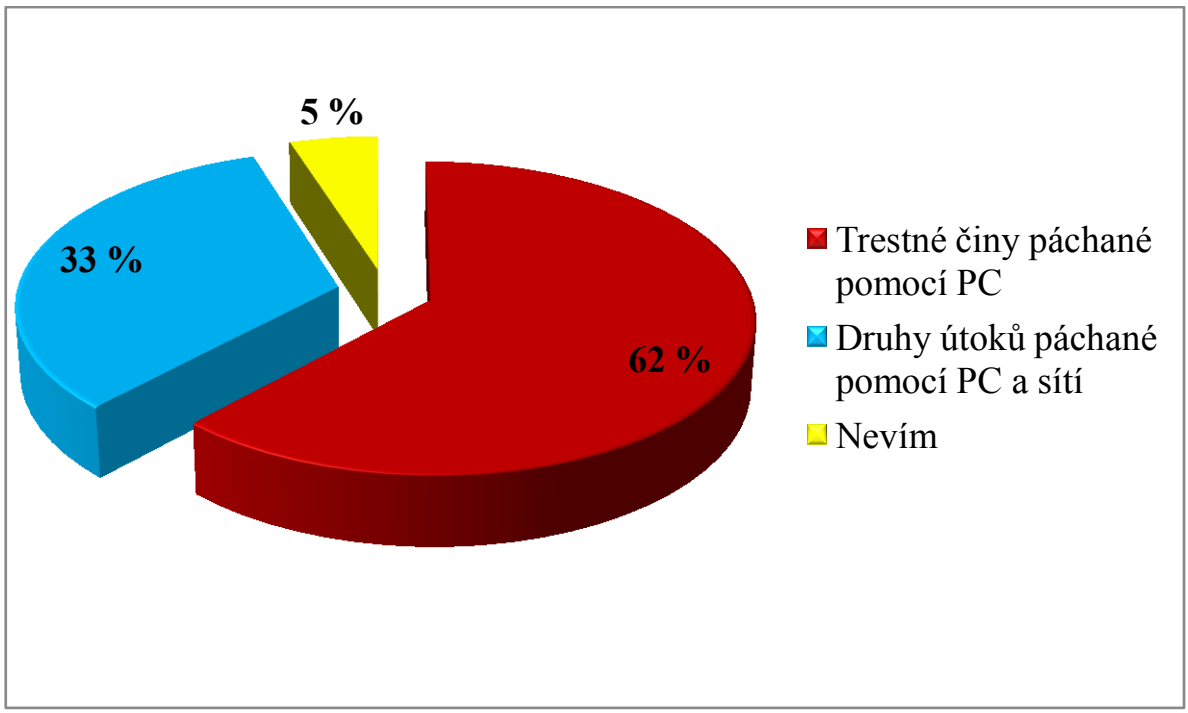
Otázka č. 4 – Co si myslíte, že s kyberkriminalitou souvisí?



Obr. 12 – Graf odpovědí k otázce č. 4

Otázka *,, Co si myslíte, že s kyberkriminalitou souvisí?‘‘* byla otevřená, tudíž mohli dotázaní vyslovit svůj názor. Z grafu výše vidíte ale pouze 3 možnosti, a to proto, že se dotazovaní svými odpověďmi na těchto třech možnostech shodli. Na tvrzení, že s kyberkriminalitou souvisí počítače, internet a hackeři se shodlo 36 % dotázaných. Více než polovina dotazovaných, přesněji 55 % se shodla na tom, že s kyberkriminalitou souvisejí útoky páchané pomocí sítí a počítačů, kde mezi nejčastěji jmenované odpovědi patřily např. kyberšikana, podvody, viry, útoky na sítě, nabourávání se do počítačů a krádeže přes internet. Pouhých 9 % dotázaných neví, co s kyberkriminalitou souvisí nebo o ní nepřemýšlela.

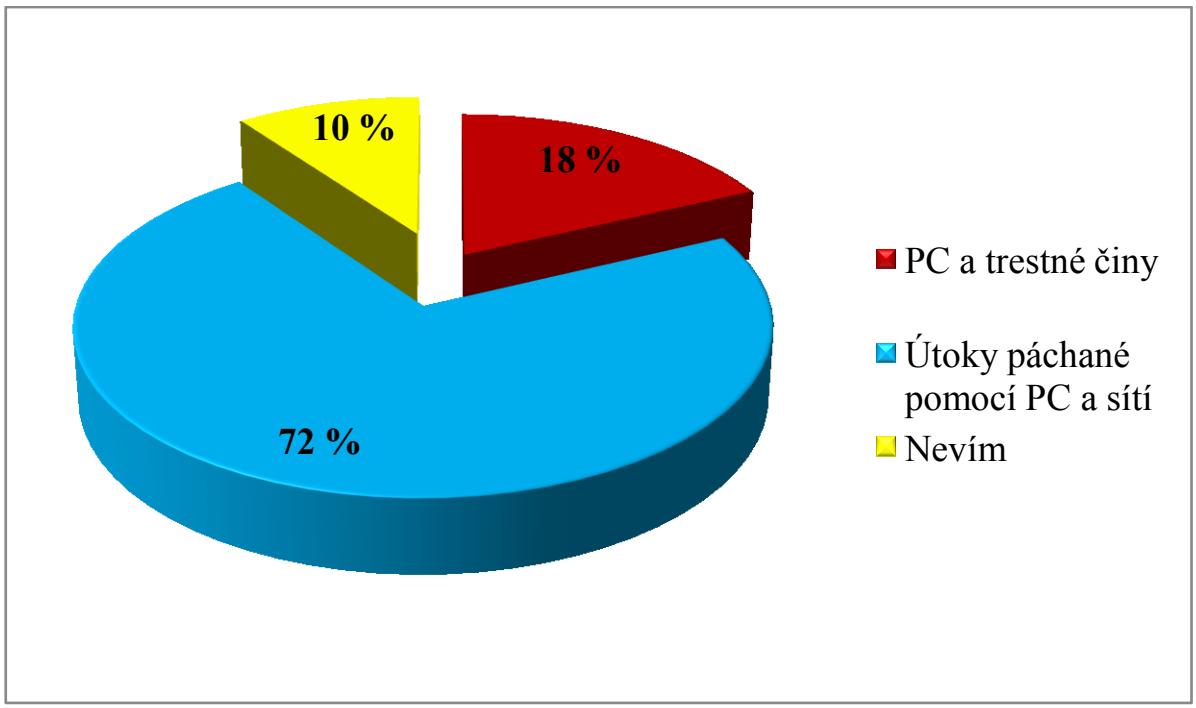
Otázka č. 5 – Co je podle Vás kyberkriminalita?



Obr. 13 – Graf odpovědí k otázce č. 5

Tato otázka ,, *Co je podle Vás kyberkriminalita?*‘‘ byla rovněž otevřená, proto mohli respondenti formulovat svůj názor. Z grafu můžete vidět opět jen 3 možnosti, a to proto, že se dotázaní svými odpověďmi na těchto třech možnostech shodli. Na tvrzení, že kyberkriminalitou jsou trestné činy páchané pomocí počítačů se shodlo 62 % dotázaných, což je více než polovina. Že jsou kyberkriminalitou různé druhy útoků páchané pomocí počítačů a sítí se shodlo 33 % dotázaných. Mezi nejčastěji jmenované druhy útoků patřily podvody, útoky na počítače, neoprávněný přístup k údajům, krádeže přes internet, sledování a pronásledování přes internet a také šikana. Pouhých 5 % dotázaných odpovědělo, že neví, co pojem kyberkriminalita znamená.

Otázka č. 6 – Co si myslíte, že do kyberkriminality patří?

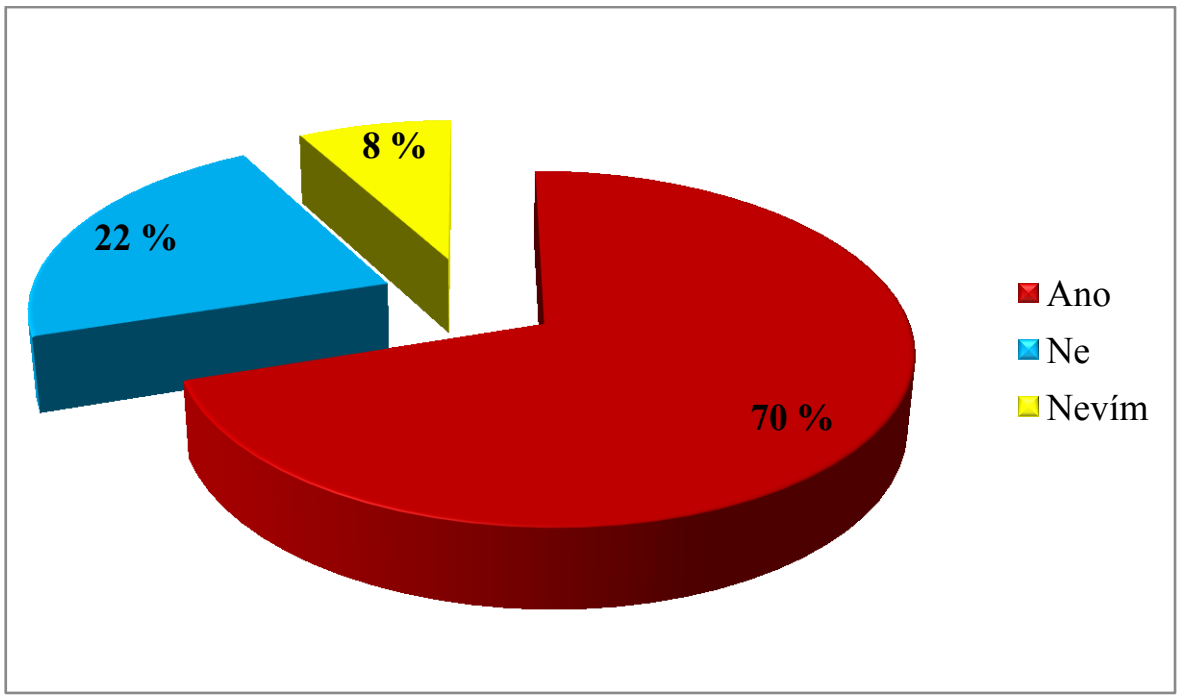


Obr. 14 – Graf odpovědí k otázce č. 6

Otázka *,, Co si myslíte, že do kyberkriminality patří?‘‘* byla poslední otevřenou otázkou, při které mohli dotázaní vyjádřit svůj názor. Z grafu můžeme opět vyčíst pouze 3 možnosti, a to proto, že se dotázaní na těchto třech možnostech svými odpověďmi shodli. Na tvrzení, že do kyberkriminality patří počítače a trestné činy přes ně páchané, se shodlo 18 % dotázaných. Plných 72 % dotázaných se svými odpověďmi shodlo, že do kyberkriminality patří různé útoky páchané pomocí PC a sítí, kde se mezi nejčastěji jmenované útoky řadí kyberšikana, podvody, krádeže, viry, nabourávání se do počítačů a jejich zneužívání. Zbývajících 10% dotázaných odpovědělo, že neví, co ke kyberkriminalitě přiřadit.

Cílem těchto tří otevřených otázek bylo zjistit, zda dotazování vědí, jaký význam má pojem kyberkriminalita a co do ní patří, bez jakékoliv nápovědy odpovědi. Lze tedy říci, že nadpoloviční většina všech dotázaných se s tímto pojmem již setkala a vědí, oč se jedná. Jak již bylo zmíněno ve vyhodnocení otázky č. 3 s pojmem kybernetická kriminalita jsme se seznámili již v úvodu práce a s jejím vývojem v teoretické části.

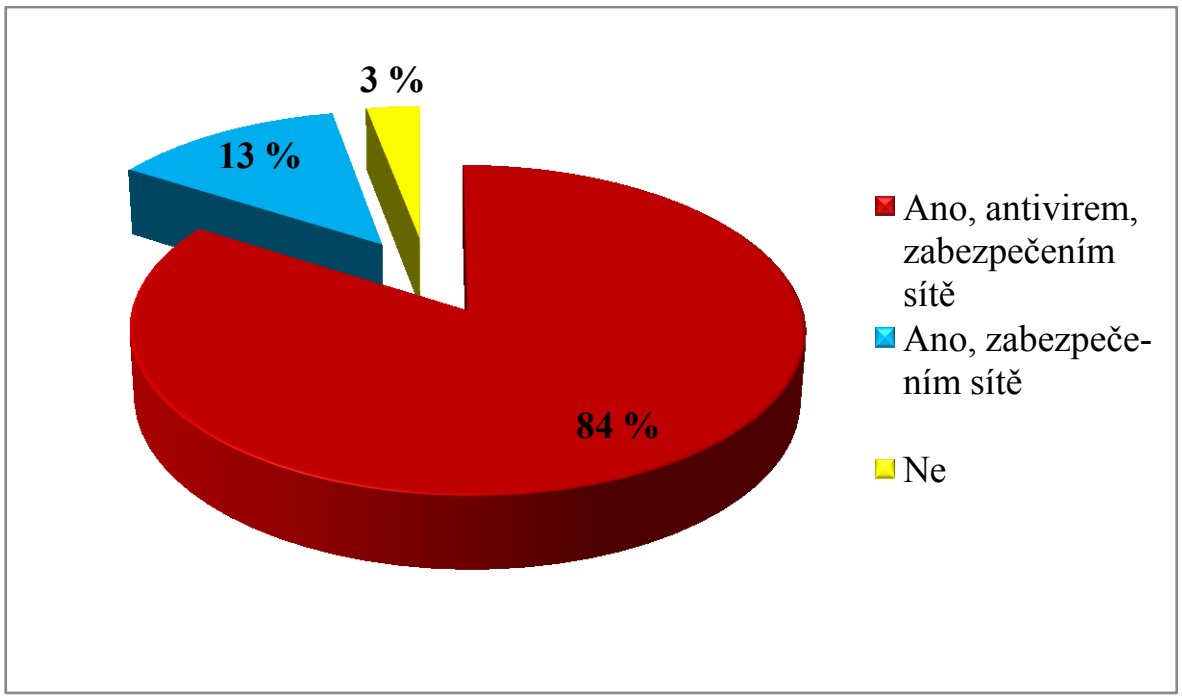
Otázka č. 7 – Měl/a jste někdy v počítači vir, trojského koně nebo něco podobného?



Obr. 15 – Graf odpovědí k otázce č. 7

Na otázku *,, Měl/a jste někdy v počítači vir, trojského koně nebo něco podobného?‘‘* nadpoloviční většina, která činí plných 70 %, odpověděla možností *Ano,* což vidíte také na grafu výše. Možností *Ne* odpovědělo 22 % dotázaných a pouhých 8 % respondentů možností *Nevím.* Těchto 8 osob neví, zda se někdy vir nebo něco podobného v počítači objevil, nebo ne. Z této odpovědi vyplývají 2 předchozí možnosti, které můžeme posoudit. Pokud se rozhodneme pro možnost *Ano*, s virem v počítači by se setkalo 78 % dotázaných osob, a pokud se rozhodneme pro možnost *Ne*, vir v počítači by nemělo 30 % osob. Z této otázky i při uvážení třetí možnosti, kde respondenti odpověděli *Nevím,* je zřejmé, že se ze všech 100 respondentů nadpoloviční většina s virem, trojským koněm nebo s podobným útokem na svůj počítač setkala, což je dle mého názoru poměrně dost. Těmto útokům lze samozřejmě předcházet, a to nejen ochranou počítače a sítí vhodnou ochranou, ale také obezřetností na internetu.

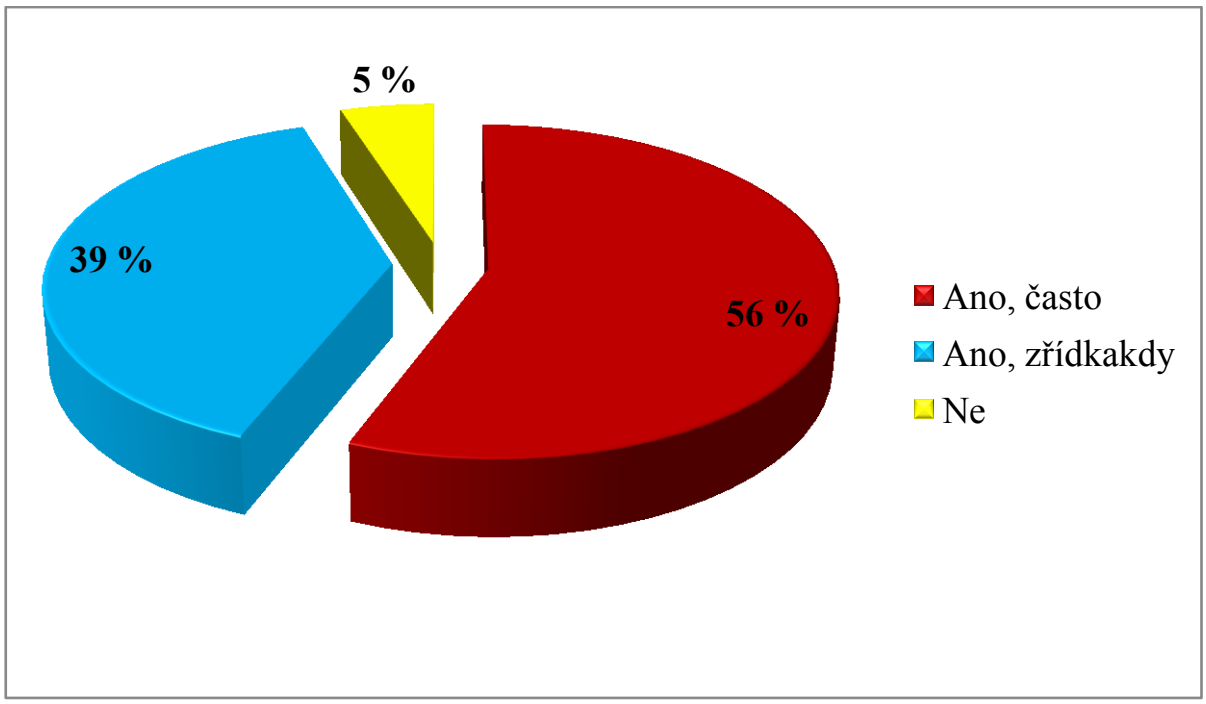
Otázka č. 8 – Máte chráněný počítač a internetové připojení? Jak?



Obr. 16 – Graf odpovědí k otázce č. 8

V otázce ,, *Máte chráněný počítač a internetové připojení? Jak?'' * bylo zjištěno, jestli mají dotázaní chráněný svůj počítač a internetové připojení, či nikoliv. Možností *Ano, antivirem a zabezpečením sítě* odpovědělo 84 % dotázaných. Mohu tedy říci, že mí přátelé a rodina chrání svůj počítač nejen heslem na internetové připojení a tedy i vhodným kódováním, ale také antivirem, který je důležitý ke sledování a upozorňování na potencionální útoky. Možností Ano*, zabezpečením sítě* odpovědělo 13 % dotázaných. Tato ochrana je také důležitá, nicméně s antivirem a bránou firewall je dohromady nejvyšší ochranou, ale to mnoho uživatelů nemusí vědět. Pouze 3 respondenti odpověděli, že počítač a internetové připojení nemají chráněné vůbec, za což jim hrozí obrovské riziko nabourání se hackerů do počítače jednoduchým způsobem, protože tito nemusí překonávat žádnou překážku v internetovém připojení, které by mělo být zabezpečeno příslušným heslem. Ochrana před útoky byla rozebrána v kapitole 7 na začátku praktické části práce.

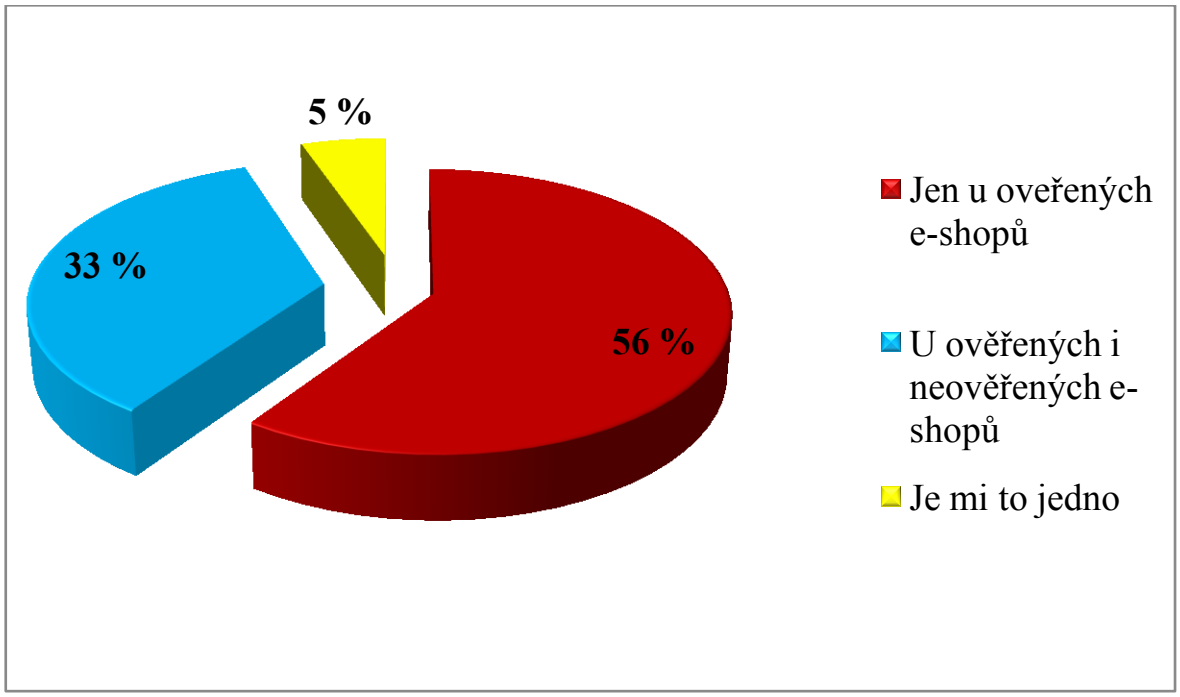
Otázka č. 9 – Nakupujete přes internetové e-shopy?



Obr. 17 – Graf odpovědí k otázce č. 9

Cílem otázky *,, Nakupujete přes internetové e-shopy?‘‘* bylo zjistit, kolik osob z mého okolí nakupuje přes internetové e-shopy, protože těchto e-shopů vzniká rok od roku více, a dle mého názoru přes e-shopy nakupuje v dnešní době více než 50% celé populace, protože mohou nakupovat z pohodlí domova. Jak můžeme vidět na grafu, více než polovina dotázaných, která činí 56 % odpověděla, že nakupuje přes e-shopy často. Odpovědí *Ano, zřídkakdy* odpovědělo 39% dotázaných a 5% osob odpovědělo, že přes e-shopy nenakupují. Následující dotaz *,, Pokud jste odpověděli ,, Ano.‘‘ Nakupujete u ověřených e-shopů, nebo Vám je to jedno?‘‘* s touto otázkou velmi úzce souvisí, jelikož tato otázka nebyla povinná a nemuseli na ni odpovídat všichni respondenti, ale jen ti, kteří odpověděli možnostmi *Ano, často* nebo *Ano, zřídkakdy*.

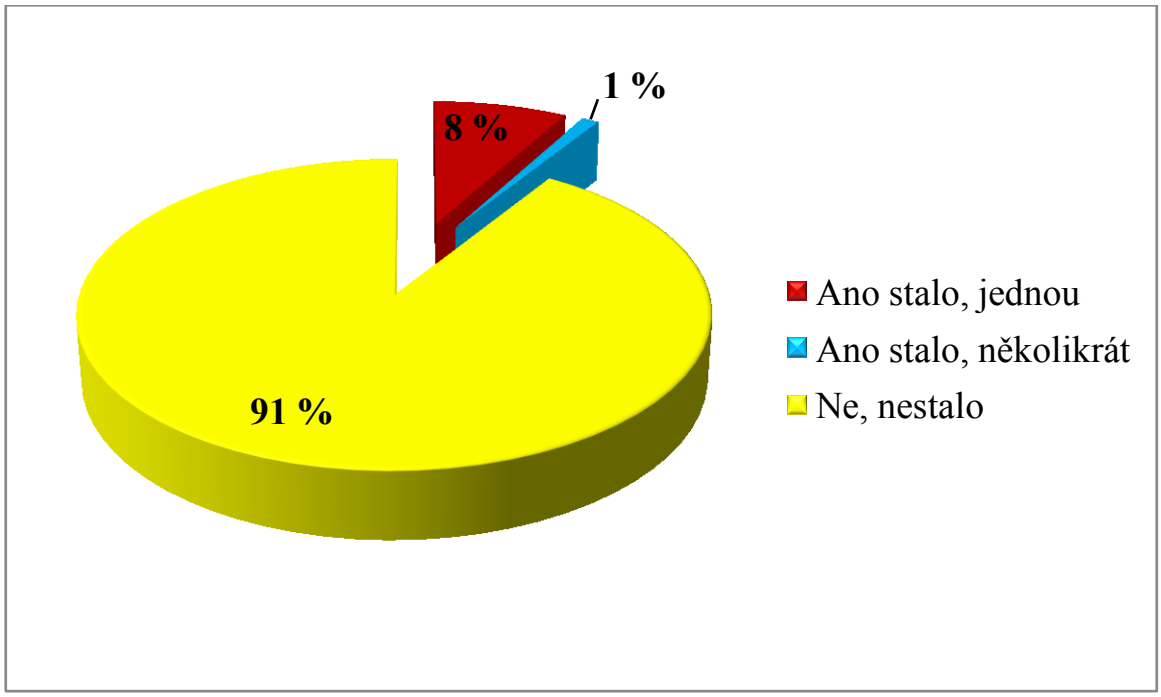
Otázka č. 10 – Pokud jste odpověděli ,, Ano.‘‘ Nakupujete u ověřených e-shopů nebo Vám je to jedno?



Obr. 18 – Graf odpovědí k otázce č. 10

Jak již bylo zmíněno, otázka *,, Pokud jste odpověděli ,, Ano.‘‘ Nakupujete u ověřených e-shopů nebo Vám to je jedno?‘‘* souvisí s předchozí otázkou. Z grafu můžete usoudit, že hodnoty nedosahují plných 100 %, a to proto, že 6 respondentů na tuto otázku neodpovědělo a tvoří tak 6 %, které nám chybí do plných 100 % odpovědí. Těchto 6 osob nezodpovědělo otázku, protože nenakupují přes e-shopy, na což jsme se ptali v předchozí otázce, nemuseli tudíž na tuto otázku odpovídat. Dle předchozí otázky ale přes internetové e-shopy nenakupuje jen 5 osob, šestá osoba na tuto otázku odmítla odpovědět. 56 % respondentů odpovědělo, že nakupuje jen u ověřených e-shopů. 33 % odpovědělo, že nakupuje u ověřených i neověřených e-shopů a 5% odpovědělo možností *Je mi to jedno.*

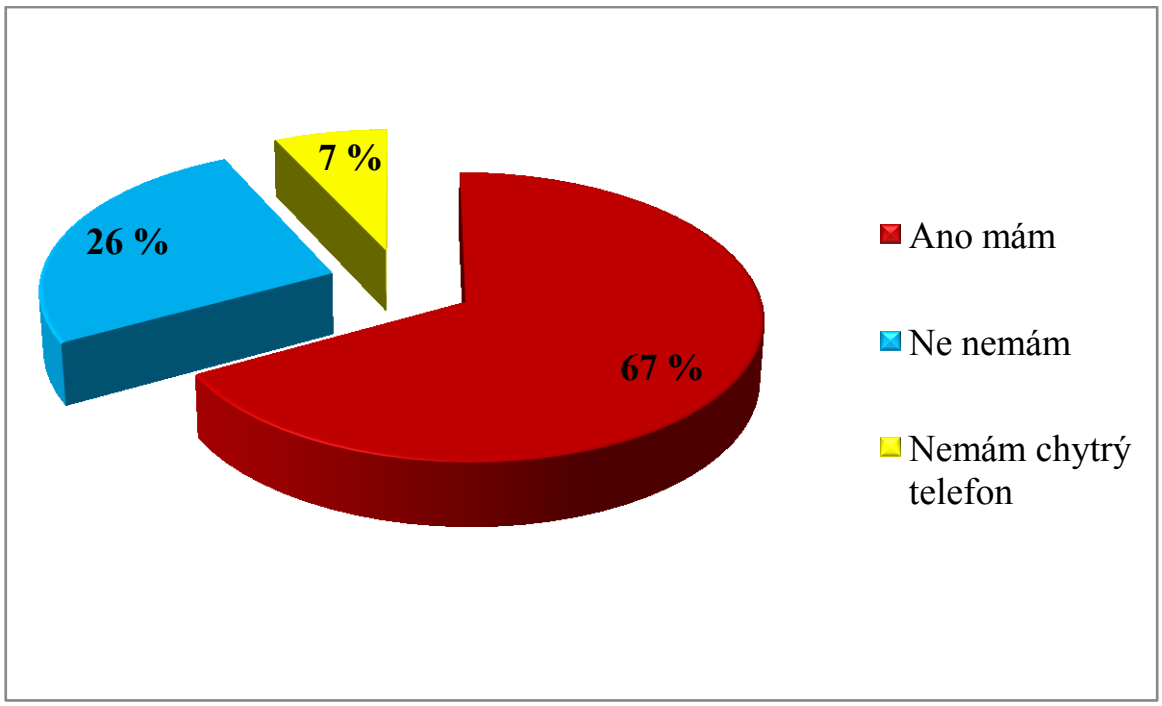
Otázka č. 11 – Stalo se Vám někdy, že jste narazili na podvodný e-shop, tudíž jste byli podvedeni?



Obr. 19 – Graf odpovědí k otázce č. 11

Pouhých 8 % dotázaných odpovědělo na otázku ,, *Stalo se vám někdy, že jste narazili na podvodný e-shop, tudíž jste byli podvedeni?'' možností Ano stalo, jednou.* A jen jedna osoba ze všech dotazovaných odpověděla možností *Ano stalo, několikrát.* To může znamenat, že tato osoba nakupuje převážně u neověřených e-shopů, což značí to, že není vůči sobě a svým údajům obezřetná a nejspíš neví, co hrozí při nakupování na e-shopech tohoto typu. Většina dotázaných, přesněji 91 % odpovědělo možností *Ne, nestalo.* To může znamenat, že nakupují převážně u ověřených e-shopů, kde riziko podvodu majitele e-shopu nehrozí, respektive je minimální. Z celkového výsledku grafu této otázky je zřejmé, že lidé v mém okolí jsou opatrní a při nakupování přes internet si dávají pozor, zda se jedná o ověřený e-shop, nebo neověřený. Problematikou e-shopů a útoky, které proti nim mohou být namířeny se v práci zabývala kapitola 5.2 Útoky na e-shopy.

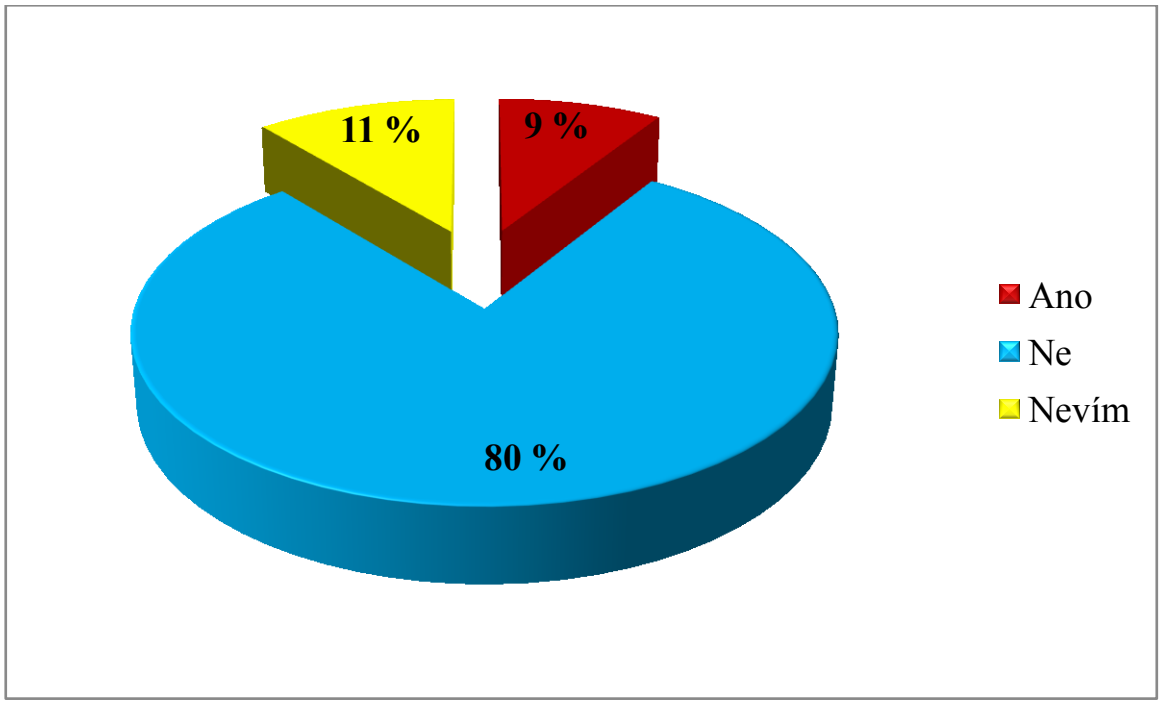
Otázka č. 12 – Máte nějakým způsobem chráněný svůj telefon?



Obr. 20 – Graf odpovědí k otázce č. 12

Tato otázka je směřována na dotykové mobilní telefony, tzv. chytré telefony. Nebezpečí, které těmto mobilním telefonům hrozí je zmíněno v kapitole 6 teoretické části. Z grafu lze vyčíst, že 67 % dotazovaných svůj telefon chráněný má. Většina chytrých telefonů má v systému již bezpečnostní prvek nainstalovaný. Tím si uživatel kontroluje případnou přítomnost viru nebo jiných nežádoucích instalací ve svém telefonu a zároveň tento program chrání při surfování na internetu a stahování různých her. Je také možné si do telefonu pro ještě větší bezpečnost nainstalovat antivirový program. Právě tuto možnost převážně uživatelé chytrých telefonů dělají, protože sami ani neví, že v systému telefonu ochranu již mají, a proto si myslím, že možností *Ne nemám,* odpovídali právě tito uživatelé telefonu, kteří činí 26 %. Zbylých 7 % dotázaných odpovědělo, že chytrý telefon nemají. To je v současné době zvláštní, neboť telefony s tlačítky se prodávají snad už jen v bazarech, ale na druhou stranu by to chtělo více takových lidí z hlediska bezpečnosti, protože u tlačítkových telefonů není tolik možností jako u dotykových. Ano, připojíte se na internet, ale v těchto telefonech nefiguruje Obchod Play jako v chytrých telefonech se systémem Android a ani AppStore v telefonech Apple. Možnost stahování her a různých aplikací do telefonu je tudíž omezená a tím se také snižuje riziko možného útoku na telefon.

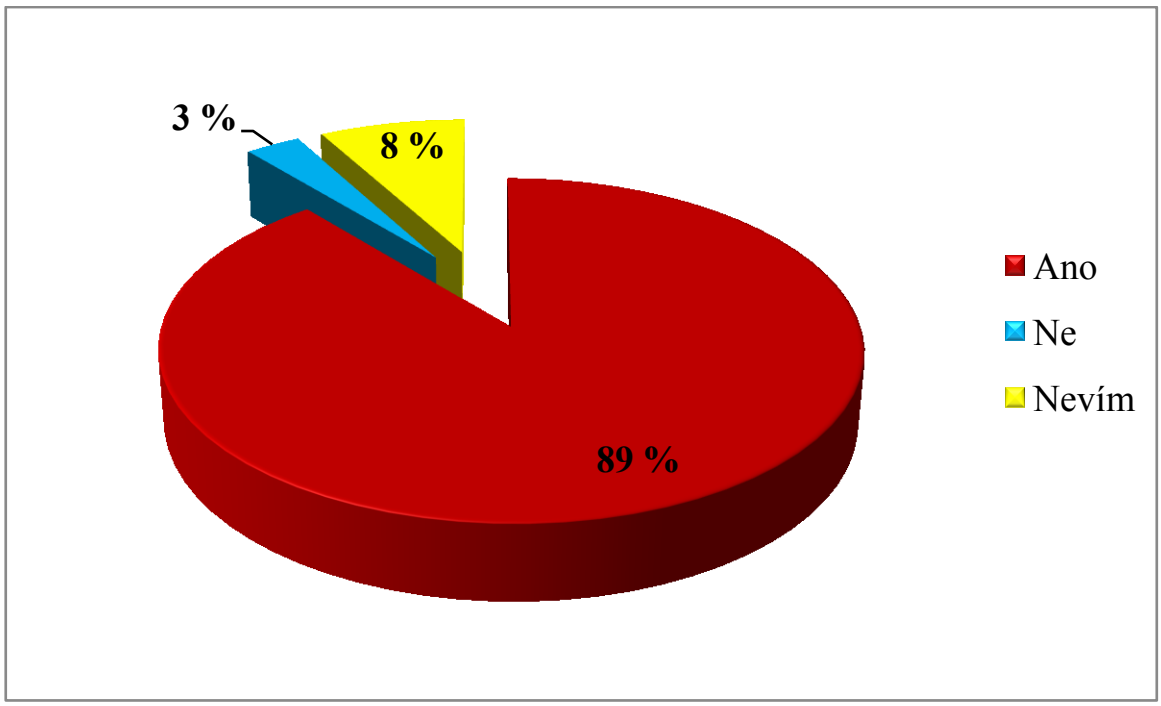
Otázka č. 13 – Stalo se Vám někdy, že jste za měsíční vyúčtování telefonních služeb platili za nějakou službu, o které jste vůbec nevěděli?



Obr. 21 – Graf odpovědí k otázce č. 13

Tato otázka nepřímo navazuje na předchozí otázku *,, Máte nějakým způsobem chráněný svůj telefon?‘‘,* protože z pohledu bezpečnosti je při nechránění svého telefonu možné, že se Vám do telefonu mohou stahovat aplikace zpoplatněné, o kterých nevíte, protože v seznamu aplikací se nezobrazují, ale běží někde v pozadí v systému, a Vy na to přijdete až při příchozím vyúčtování, kdy máte naúčtovány platby, o kterých nevíte. S tímto jevem se setkalo 9 % dotázaných, naštěstí to není mnoho. Plných 80 % odpovědělo možností *Ne,* takže se s tímto jevem nesetkali a také bohudíky. Protože služby, o kterých nevíme a které si můžeme omylem do telefonu stáhnout s nějakou aplikací je mnoho, a proto je důležité číst požadovaná oprávnění aplikací a případně aplikaci do telefonu neinstalovat a také omezovat připojení k internetu, když ho zrovna nepoužíváme. 11 % dotázaných odpovědělo možností *Nevím.* Tito uživatelé nevědí, jestli se s nějakou službou, o které nevěděli a platili za ni, setkali, nebo ne, a může to být tím, že vyúčtování za telefon bývá doručováno převážně SMS zprávou nebo elektronicky, a mnoho lidí to nebere v potaz, zaplatí danou částku a výpisem se dále nezabývá.

Otázka č. 14 – Může být prostřednictvím internetových sítí páchán i terorismus?



Obr. 22 – Graf odpovědí k otázce č. 14

Cílem této otázky bylo zjistit, jaký pohled mají lidé z mého okolí a rodinní příslušníci, kteří byli dotázaní, na dnes velmi aktuální téma terorismus. S tématem terorismu jsme se setkali již v teoretické části, konkrétně v kapitole 4. S mým nadšením plných 89 % odpovědělo možností *Ano,* tudíž si myslím, že vědí, že terorismus může být páchán formou teroristických útoků ve společnosti, kde bývá velká ztráta na životech a zranění, ale také přes internetové sítě a počítače, i když tento útok není namířen přímo proti životům a zdraví osob, ale na technologie a kritickou infrastrukturu státu a mohou také vědět, že takový terorismus se nazývá kyberterorismus. Pouhá 3 % odpověděla možností *Ne* a zbývajících 8 % odpovědělo možností *Nevím*. Mezi tyto osoby patří lidé, kteří se dle mého názoru s pojmem kyberterorismu zatím nesetkali, nebo si nejsou vědomi, že by se s tímto pojmem někdy setkali a že by útoky na technologie a vládní systémy mohly být formou terorismu.

Závěrem dotazníku mohu říci, že vytyčený cíl, kterým bylo zjistit, zda lidé v mém okolí a také rodina vědí, co je z obecného hlediska kybernetická kriminalita a jestli se s tímto jevem ve svém životě setkali. Dále také jakým způsobem chrání svá data a své informační a komunikační prostředky před hrozícími útoky. Mohu říci, že dotázaní z většiny vědí, co znamená pojem kybernetická kriminalita, respektive vědí, co si pod tímto pojmem představit a které komponenty do ní mohou patřit. I přes dnešní moderní útoky a možnosti jsou dotázaní na internetu nejen při nakupování ale také při surfování opatrní a chrání si jak své počítače tak také telefony, což jsou dva nejrozsáhlejší informační a komunikační prostředky současné doby.

9 ROZHOVOR

Závěrem práce nás provede krátký rozhovor se zkušeným programátorem, který spravuje e-shop svářečky-obchod.cz a také se stará o celý server, na kterém tento e-shop běží. Bohužel jsem neměla možnost se s programátorem setkat osobně, protože firma, v níž pracuje a která spravuje tento e-shop, sídlí na Slovensku, a proto je rozhovor také částečně ve slovenském jazyce. Nicméně jsem měla možnost tento rozhovor provést alespoň přes komunikační program Skype. Rozhovor probíhal tedy v písemné formě, ale online. Nedílnou součástí práce tohoto programátora je správa e-shopu, ve kterém pracuji, a nejen toho, ale i mnoha dalších a také péče o bezpečné provozování e-shopů a serverů, na kterých běží. Pro mě jsou tyto informace velmi zajímavé, protože mě tato problematika zajímá kvůli práci v tomto oboru, a protože pracuji jako externí pracovník, o mnoho těchto informací přicházím.

Od kolegů jsem zjistila, že spravujete náš e-shop a hlavně server, na kterém tento e-shop běží, je to tak?

,, Ano přesně tak.‘‘

Spravujete tento server od založení tohoto e-shopu?

,, Nie.‘‘

A od kterého roku tedy, když byl založen v roce 2007?

,, Myslím, že v roku 2016 sme robili 1. programátorské práce, stránky sa přesunuli na nový server v roku 2017, kedy sme začali spravovat aj server.‘‘

V čem vlastně spočívá Vaše práce, smím-li se zeptat?

,, Aktuálně vykonáváme na stránkách programátorské práce - keď treba na stránkách niečo zmeniť, upravit cokoliv, nebo třeba jinak nastavit, všetko co nemože spravit administrátor… Například tento rok budeme robit celý nový dizajn. Staráme sa aj o server ako bolo spomenuté, keď je výpadok alebo spomalenie alebo nějaký problém, sme schopní to vyriešit.‘‘

Práce tedy máte více než dost. Setkal jste se někdy za dobu spravování tohoto e-shopu s nějakým útokem mířícím proti tomuto e-shopu?

,, Ano setkal jsem se s útokem, pravděpodobně robot cíleně vkládal každé 2-3 sekundy produkty do košíku, vždy pod inou ip adresou v určitom rozsahu, keď sa mu takto podarilo

vytvoriť 10 tisíce záznamov v databázi, začalo to spomalovat server… Momentálně su dané ip adresy zabanované a proces vkládaní do košíku předělaný, odolný voči útokům. Útok byl směřován pravděpodobně z USA.‘‘

Až z takové dálky? Tomu se nedá ani věřit. To je opravdu možné, aby na český a slovenský e-shop byl mířený útok až z USA?

,, Jj proto říkám, že pravděpodobně to byl robot, ktorý automaticky našiel stránky na internetě a automaticky našiel citlivé miesto a začal ho využívat, každopádně veřejné ip adresy z ktorých útočil sú registrované v USA.‘‘

Je pravda, že na domácího uživatele taky může zaútočit člověk z úplně cizí země, takže to dává smysl. Jak jste vlastně zjistil, že útok probíhá nebo se o něj někdo pokouší?

,, Od administrátorů eshopu byly sťažnosti na pomalý server a když jsem dělal optimalizace stránek, aby tak nezaťažovali server a byly rychlejší, všimol som si, že treba i o 1 v noci přibývá každé 2-3 sekundy záznam do databáze do tabulky košíka... Z toho som zistil, že tam exstuje už obrovské množstvo dat, vzhľadom k tomu, že původně to bylo ještě zle naprogramované, tak to celé začalo spomaľovať server. Přesně tak už som viděl pár útokov na stránky, vždy to bylo z azie/ruska/usa, nikdy som neviděl útok přímo z česka alebo slovenska. Z toho usudzuju, že útoky prebiehajú většinou pro zábavu, alebo pro vyskušání technologií, nikdy ne kvôli konkurenci.‘‘

Jakým způsobem jste dokázal tento útok odvrátit, nebo i jiné útoky, použil jste nějaké zvláštní prostředky?

,, Ohladom tohoto útoku ako som pisal, zabanovali sme rozsah ip adries z ktorých prebiehal na stránky útok + byl předělán spôsob ukládání košíku odolný voči útoku... Co sa týká ostatních útoků, to byly stránky postavené například na systémoch Joomla alebo Wordpress, tam stačilo aktualizovat systém na najnovšiu verzi, pretože sa útočníci dostávali na stránky cez chyby, ktoré byly v aktualizacích opraveny. Inak viem, že kolegyňa sa stretla z nahrávánim nebezpečných súborov cez formulář na stránkach - například miesto přílohy obrázku niekto nahrál nebezpečný súbor. Ošetrila to tým, že zablokovala nahravanie všetkych typov súborů okrem obrázkov.‘‘

Já myslela, že server našeho e-shopu spravujete jen vy, je vás tedy více, když píšete, že kolegyňka?

,, Ano píšu za našu firmu. Sme 2 programátoři + 1 kolegyňa programátorka, ktorá je ale mimo našu firmu, ale pomáhá s pracemi. Pak je eště jeden kolega, ktorý spravuje niektoré marketingové kanále ako mailing.‘‘

Už je mi to jasnější. Je pravda, že takové množství práce byste sám asi těžko zvládal. Nebo zvládal, ale nedělal byste nic jiného. Jestli se smím zeptat, jak dlouho se nejen v tomto oboru, ale celkově v oboru ICT pohybujete?

,, Jj přesně tak. Sám by som to asi zvládal, ale svářečky sú len jedna z mnohých stránek, ktoré naša firma spravuje... Tak niečo som programoval a riešil už ako 15 ročný, to je asi rok 2005, ale reálně za peniaze som začal programovat asi v roku 2011 popri škole.‘‘

Jak si myslíte, že lze předcházet těmto útokům nejen na tento e-shop ale i celkově na uživatele? V knihách se píše, že nejlepší ochrana je mít v počítači firewall a antivirus a internetové připojení mít také zabezpečené. Máte podobný názor? Respektive, co byste jako zkušený uživatel doporučil domácím uživatelům používajících informační a komunikační prostředky?

,, Co sa týká eshopov, existuje séria bodov a opatření ktoré je nutné dodržať aby sa předešlo mnohým typom útokov - tu je to len o tom si vyhľadat najnovšie typy útokov a najnovšie sposoby ochrany...‘‘

,, Co sa týká obyčajného uživatela a například ochrany počítača, tak ano přesně tak, mať naistalovaný firewall a antivirus a hlavně aj aktualizovaný, taktiež vždy aktualizovaný aj operačný systém, většinou sú vydávané aktualizace kv ôli objaveným zranitelným miestám v systéme. Samozřejme pak neotvárat podozrivé súbory.‘‘

DÍLČÍ ZÁVĚR

Praktická část práce je zaměřena na ochranu počítače, internetového připojení, ale také chytrých mobilních telefonů před potenciálními útoky a hrozbami. Nedílnou součástí této části práce byl dotazník, který byl zaměřen na kybernetickou kriminalitu jako celek a dále na ochranu osoby samotné a také informačních a komunikačních prostředků před útoky. Dotazník byl směřován na osoby z mého okolí a bylo zjištěno, že pojem kybernetické kriminality znají a vědí, co si pod tímto pojmem představit. Následně bylo zjištěno, že na internetu jsou opatrní a mají také zabezpečeny své informační a komunikační prostředky.

Závěrem praktické části nás provedl rozhovor se zkušeným programátorem z firmy, ve které pracuji. Popsal úkony pro bezpečné provozování e-shopu, jakým způsobem se dá odvrátit hrozící nebo již probíhající útok. Vysvětlil také, jak předcházet útokům mířícím nejen na e-shopy ale také proti domácím uživatelům.

ZÁVĚR

Vybrané téma bakalářské práce má velmi široký záběr a mnoho oblastí, kterými se dá zabývat. Nicméně mým cílem bylo vymezit jen to nejdůležitější, co s tímto tématem souvisí. Cílem teoretické části bylo zaměřit se na kybernetickou kriminalitu jako celek, ale hlavně na útoky, kterými lze na současné informační a komunikační prostředky zaútočit.

V první části práce je popsán alespoň částečně vývoj kybernality až po její současnost a také pachatelé této kriminality, protože bez nich by tato kriminalita nemohla existovat. Následně jsou v práci popsány nejčastější druhy útoků na informační a komunikační prostředky. V závěru teoretické části jsou zmíněna nebezpečí, která hrozí současným mobilním telefonům zvaným smartphony, protože během posledních 5 let jsou nejpoužívanějším komunikačním prostředkem ve společnosti.

Praktická část práce je zaměřena na ochranu počítače, internetového připojení ale také chytrých mobilních telefonů před potenciálními útoky a hrozbami. Cílem této části práce byl dotazník směřován mezi mé přátele a blízké. Byl zaměřen na kybernetickou kriminalitu jako celek a také na ochranu osoby samotné a také informačních a komunikačních prostředků před útoky. Závěr praktické části patřil rozhovoru se zkušeným programátorem z firmy, ve které pracuji, který mimo jiné popsal úkony pro bezpečné provozování e-shopu a jakým způsobem se dá odvrátit hrozící nebo již probíhající útok. Následně také jak předcházet útokům mířícím nejen na e-shopy ale také proti domácím uživatelům.

SEZNAM POUŽITÉ LITERATURY

[1] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

[2] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 8073805014.

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

[4] Domácnosti s připojením k internetu. In: *Český statistický ústav* [online]. [cit. 2017-12-12]. Dostupné z: https://www.czso.cz/csu/czso/informacni_technologie_pm

[5] SMEJKAL, Vladimír. Kybernetická kriminalita - fenomén dneška. In: *Právní prostor* [online]. 20.7.2015 [cit. 2018-01-02]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

[6] STODOLA, Petr. *Kybernetická a informační válka: Téma č. 4 Způsoby a nástroje hackingu* [online]. In: . [cit. 2017-12-14]. Dostupné z: https://moodle.unob.cz/pluginfile.php/20720/mod_resource/content/1/KIV%20T-4.pdf

[7] SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. Brno: Zoner Press, 2006. Encyklopedie Zoner Press. ISBN 80-86815-04-8.

[8] *Technet.cz* [online]. In: . [cit. 2017-12-21]. Dostupné z: https://technet.idnes.cz/15-nej-viru-světa 0ja/software.aspx?c=A120716_110329_software_nyv

[9] ČERNÝ, Jaroslav. *Domácí internet: 150 programů pro maximální využití a zabezpečení*. Brno: CP Books, 2005. ISBN 80-251-0452-4.

[10] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez tajemství*. 3. aktualiz. vyd. Brno: Computer Press, 2003. ISBN 80-7226-948-8.

[11] Co to je DDoS útok a jak se dělá? In: *Diit.cz* [online]. [cit. 2017-12-23]. Dostupné z: https://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

[12] *Google: Anonymous* [online]. In: . [cit. 2017-12-23]. Dostupné z: https://www.google.cz/search?q=anonymous&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiTsqqM1aDYAhUE2qQKHeDrB3AQ_AUICigB&biw=1366&bih=637#imgrc=4xQY6wtCaQ2YsM

[13] *Wikipedie: otevřená encyklopedie* [online]. In: . [cit. 2017-12-23]. Dostupné z: https://cs.wikipedia.org/wiki/Anonymous_(skupina)

[14] ZOUBKOVÁ, Ivana. *Kriminologický slovník*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. ISBN 978-80-7380-312-4.

[15] Estonsko-ruský incident v kontextu kyberterorismu. In: *Global Politics: Časopis pro politiku a mezinárodní vztahy* [online]. 19.1.2014 [cit. 2018-01-03]. Dostupné z: http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu

[16] ONDREJKA, Viliam. *Podvody na internetu*. České Budějovice: Nová Forma, 2010. ISBN 978-80-87313-82-4.

[17] ČESKO. Zákon č. 40/2009 Sb. In: Zákony pro lidi.cz [online]. © AION CS 2010-2018 [cit. 7. 1. 2018]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[18] Nové radary ve svodidlech. In: *Hoax: Hoax* [online]. [cit. 2018-01-07]. Dostupné z: http://www.hoax.cz/hoax/nove-radary-ve-svodidlech/

[19] Veselé korunky. In: *Hoax.cz: Řetězové e-maily* [online]. [cit. 2018-01-07]. Dostupné z: http://www.hoax.cz/retezove-emaily/vesele-korunky/

[20] Daruj krev - Alexander Gál. In: *Hoax.cz: Hoax* [online]. [cit. 2018-01-07]. Dostupné z: http://www.hoax.cz/hoax/daruj-krev---alexander-gal/

[21] SQL Injection. In: *W3schools .com* [online]. [cit. 2018-01-07]. Dostupné z: https://www.w3schools.com/sql/sql_injection.asp (přeloženo)

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

[23] DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti*. Brno: CP Books, 2005. ISBN 80-251-0574-1.

[24] KOCMAN, Rostislav a Jakub LOHNISKÝ. *Jak se bránit virům, spamu, dialerům a spyware*. Brno: CP Books, 2005. ISBN 80-251-0793-0.

[25] Funkce firewall. In: *Google* [online]. [cit. 2018-03-13]. Dostupné z: https://www.google.cz/search?biw=1366&bih=588&tbm=isch&sa=1&ei=MAOoWqfKMpD3gQbsz76IBA&q=funkce+firewall&oq=funkce+firewall&gs_l=psy-ab.3..0i24k1.149706.151491.0.151639.15.11.0.4.4.0.157.1227.5j6.11.0....0...1c.1.64.psy-ab..0.15.1238...0.0.snxf5IoIeh4#imgrc=ZOLJnHvYvrtpHM:

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT	Informační a komunikační technologie
IT	Informační technologie
AT&T	Americká telekomunikační společnost
USA	Spojené státy americké
BBS	Technologie umožňující vzdálené připojení
SMS	Krátká textová zpráva
SCADA	Speciální systémy řídící elektrárny, distribuční sítě a další klíčové prvky
DoS	Denial of Service (odepření služby)
DDoS	Distributed Denial of Service (distribuční odepření služby)
IP	Internet Protokol (používá se ve spojení s adresou tzv. IP adresa)
NATO	Severoatlantická aliance
ICQ	I Seek You (program pro online komunikaci)
ČR	Česká republika
DNS	Domain Names System (systém doménových jmen)
WLAN, WiFi	Bezdrátové internetové připojení
3G	Mobilní data poskytována operátorem
ICF	Internet Connection Firewall (internetový firewall)
DSL	Digital Subscriber Line (technologie umožňující vysokorychlostní přenos dat)
BIOS	Basic Input-Output Systém (základní software počítače)
WEP	Wired Equivalent Privacy (soukromí ekvivalentní drátovým sítím)
WPA, WPA2	Wifi Protected Access (chráněný přístup k WiFi)
SSID	Service Set Identifier (identifikátor bezdrátové sítě WiFi)

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA PI: INFORMAČNÍ ZDROJE ZABÝVAJÍCÍ SE KYBERNETICKOU KRIMINALITOU NA INFORMAČNÍ A KOMUNIKAČNÍ PROSTŘEDKY

Vybrané informační zdroje zabývající se kybernetickou kriminalitou:

- ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.
- SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 8073805014.
- JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
- Článek Kybernetická kriminalita – fenomén dneška

  SMEJKAL, Vladimír. Kybernetická kriminalita - fenomén dneška. In: *Právní prostor* [online]. 20.7.2015 [cit. 2018-01-02]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska
- Konference „Kyberkriminalita a ochrana soukromí“ konající se dne 16. 7. 2017 uspořádána Senátem Parlamentu ČR
- Konference o kybernetické bezpečnosti konající se dne 1. 3. 2018 v Clarion Congress hotelu v Praze
- Kybernetika - Home. *Kybernetika - Home* [online]. Dostupné z: http://www.kybernetika.cz/

Vybrané informační zdroje zabývající se útoky na informační a komunikační prostředky:

- STODOLA, Petr. *Kybernetická a informační válka: Téma č. 4 Způsoby a nástroje hackingu* [online]. In: . [cit. 2017-12-14]. Dostupné z: https://moodle.unob.cz/pluginfile.php/20720/mod_resource/content/1/KIV%20T-4.pdf
- SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. Brno: Zoner Press, 2006. Encyklopedie Zoner Press. ISBN 80-86815-04-8.

- MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez tajemství*. 3. aktualiz. vyd. Brno: Computer Press, 2003. ISBN 80-7226-948-8.
- Estonsko-ruský incident v kontextu kyberterorismu. In: *Global Politics: Časopis pro politiku a mezinárodní vztahy* [online]. 19.1.2014 [cit. 2018-01-03]. Dostupné z: http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu
- ONDREJKA, Viliam. *Podvody na internetu*. České Budějovice: Nová Forma, 2010. ISBN 978-80-87313-82-4.

PŘÍLOHA P II: DOTAZNÍK

Kybernetická kriminalita

Dobrý den,

Chtěla bych Vás poprosit o několik minut svého času k vyplnění následujícího dotazníku. Dotazník je anonymní a pomůžete mi tím ke zpracování mé bakalářské práce. :)

Předem děkuji za Váš čas.

1. Jste žena nebo muž?

- Žena.
- Muž.

2. Do jaké věkové kategorie patříte?

- 15-20 let.
- 20-30 let.
- 30-40 let.
- 40 let a více.

3. Slyšeli jste někdy o pojmu kyberkriminalita?

Tento pojem je známý také pod názvy kyberkriminalita, kybernalita, počítačová kriminalita nebo kriminalita spojená s počítači.

- Ano.
- Ne.
- Nevím.

4. Co si myslíte, že s kyberkriminalitou souvisí?

Do pole níže napište svou odpověď.

5. Co je podle Vás kyberkriminalita?

Do pole níže napište svou odpověď.

6. Co si myslíte, že do kyberkriminality patří?

Do pole níže napište svou odpověď.

7. Měl/a jste někdy v počítači vir, trojského koně nebo něco podobného?

- Ano.
- Ne.
- Nevím.

8. Máte chráněný počítač a internetové připojení? Jak?

- Ano, antivirem, zabezpečením sítě.
- Ano, zabezpečením sítě.
- Ne.

9. Nakupujete přes internetové e-shopy?

- Ano, často.
- Ano, zřídkakdy.
- Ne.

10. Pokud jste odpověděli „ Ano“. Nakupujete u oveřených e-shopů nebo Vám to je jedno?

- Jen u ověřených e-shopů.
- U ověřených i neověřených e-shopů.

- Je mi to jedno.

11. Stalo se Vám někdy, že jste narazili na podvodný e-shop?

Podvodný e-shop znamená e-shop, který provozují podvodníci, kde je jediná možnost platby platba předem na účet a e-shop není ověřený. Zboží samozřejmě nedostanete a peníze zpět také ne.

- Ano stalo, jednou.
- Ano stalo, několikrát.
- Ne nestalo.

12. Máte nějakým způsobem chráněný svůj telefon?

Tato otázka je myšlena na chytré telefony.

- Ano mám.
- Ne nemám.
- Nemám chytrý telefon.

13. Stalo se Vám někdy, že jste za měsíční vyúčtování telefonních služeb platili za nějakou službu, o které jste vůbec nevěděli?

Např. telefonovalo Vám určité číslo a při přijmutí hovoru se nikdo neozýval a na konci měsíce jste na vyúčtování zjistili nemilé částky. Tyto hovory jsou zprostředkovávány hackery, kteří tímto vydělávají. Nebo např. do telefonu se Vám samy od sebe stahovaly aplikace a na vyúčtování jste zjistili, že jsou za poplatek.

- Ano.
- Ne.
- Nevím.

14. Může být prostřednictvím internetových sítí páchán i terorismus?

- Ano.
- Ne.
- Nevím.