Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Počítačová kriminalita

Adam Rokos

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Adam Rokos

Systémové inženýrství a informatika
Informatika

Název práce

Počítačová kriminalita

Název anglicky

Computer crime

Cíle práce

Cílem bakalářské práce je zpracovat téma počítačová kriminalita z pohledu historie a současnosti, vysvětlení základních pojmů vážících se k této problematice a popis jednotlivých typů počítačové kriminality v návaznosti na současnou legislativu a potřebu jejího vývoje, včetně zhodnocení možností ochrany běžného uživatele před jejími dopady.

Metodika

Metodika bakalářské práce bude založena na studiu poznatků z oblasti počítačové kriminality a současných možností ochrany běžného uživatele, které jsou publikovány zejména ve vědecké a odborné literatuře. Výsledky studia budou využity k vypracování teoretické části bakalářské práce. Na základě zpracování teoretické části bude provedeno vyhodnocení získaných poznatků a použito ke zpracování návrhů uživatelských a legislativních opatření na ochranu běžného uživatele.

Doporučený rozsah práce

40 stran

Klíčová slova

Důvěrnost, dostupnost, integrita, internet, kyberkriminalita, malware, počítač, počítačová kriminalita.

Doporučené zdroje informací

KOLOUCH, J., BAŠTA, P. a kol., 2019. CyberSecurity. PRAHA: CZ.NIC, z.s.p.o ISBN 978-80-88168-34-8.

KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

KRÁL, M., 2015. Bezpečný internet: chraňte sebe i svůj počítač. Praha: Grada Publishing. Průvodce (Grada). ISBN 978-80-247-5453-6.

Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti. In: Zakonprolidi.cz [online]. Dostupné z: https://www.zakonprolidi.cz/cs/2014-181.

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

doc. Ing. Edita Šilerová, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 29. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 06. 03. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Počítačová kriminalita" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14. 3. 2021 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Editě Šilerové, Ph.D., za vstřícnost při vypracovávání bakalářské práce a také všem respondentům, kteří se zapojili do vyplňování dotazníku.

Počítačová kriminalita

Abstrakt

Tato bakalářská práce se věnuje pochopení pojmu počítačová kriminalita a možnostem obrany proti ní, a to jak ve formě prevence, tak v rovině trestně právní.

Z uvedeného důvodu jsou v úvodu práce popsány a vysvětleny základní pojmy vážící se k počítačové kriminalitě, počítačům a počítačovým a informačním systémům.

Následující část se pak věnuje počítačové kriminalitě především z pohledu historického vývoje a současnosti. V následujících kapitolách jsou popsány jednotlivé druhy počítačové kriminality, důkazy a specifika vyšetřování počítačové kriminality, a to včetně pachatelů trestných činů. Nástin budoucího vývoje je obsažen v samostatné kapitole. Legislativě, především pak Úmluvě Rady Evropy o kyberkriminalitě, ale i ostatním dokumentům Evropské unie a České republiky je rovněž věnována samostatná kapitola, kde jsou také popsány hmotně právní aspekty kybernetické trestné činnosti.

Praktická část práce se věnuje dotazníkovému šetření za účelem získání aktuálních poznatků o osobních zkušenostech s počítačovou kriminalitou mezi respondenty a možným návrhům na její snížení a předcházení jejímu konání a následkům.

Klíčová slova: Důvěrnost, dostupnost, integrita, internet, kyberkriminalita, malware, počítač, počítačová kriminalita

Computer crime

Abstract

This bachelor thesis deals with the understanding of the concept of computer crime and the possibilities of defense against it, both in the form of prevention and at the level of criminal law.

For this reason, the introduction describes and explains the basic concepts related to computer crime, computers and computer and information systems.

The next part deals with cybercrime, especially from the perspective of historical development and the present. The following chapters describe the various types of cybercrime, the evidence and the specifics of cybercrime investigations, including offenders. An outline of future developments is contained in a separate chapter. A separate chapter is also devoted to legislation, especially the Council of Europe Convention on Cybercrime, but also to other documents of the European Union and the Czech Republic, which also describes the substantive legal aspects of cybercrime.

The practical part of the work is devoted to a questionnaire survey in order to obtain current knowledge about personal experiences with computer crime among respondents and possible proposals to reduce it and prevent its actions and consequences.

Keywords: Confidentiality, availability, integrity, internet, cybercrime, malware, computer, computer crime

Obsah

Seznam tabulek

Seznam grafů

1 Úvod

Počítačová kriminalita je celosvětovým problémem současné doby, který se stále vyvíjí, a který mnozí uživatelé informačních a komunikačních technologií neberou dosud dostatečně vážně. Každoročně jsou napadány stamilióny počítačových, a především pak internetových uživatelů a vzniklé škody jsou dle průzkumu společnosti Microsoft ve výši stovek miliard dolarů. Kybernetická kriminalita se stává stále více výdělečnou činností, a to více než trh s halucinogenními látkami jako jsou konopí (marihuana), heroin či kokain. Z tohoto důvodu je na odhalování a předcházení této nekalé činnosti investováno jednotlivými státy stále více finančních prostředků, ale bohužel i nadále nejsou tyto investice dostatečné.

Tuto problematiku se snaží řešit i státní instituce, které se pokoušejí definovat jasná pravidla, předcházet a postihovat počítačovou nebo moderněji řečenou kybernetickou kriminalitu. Kromě státních a nadnárodních institucí se na vyřešení nebo alespoň popsání problémů podílejí odborníci, kteří se problematice zevrubně věnují ve svých publikacích. Na toto téma probíhají rovněž různé diskuse, ať již na odborné či laické úrovni. Faktem ale zůstává, že provést podrobnou kodifikaci a vymezení v plném a uceleném rozsahu je téměř nemožné. I kdyby se vše podařilo jasně popsat, případně legislativně ošetřit, lze téměř s jistotou tvrdit, že v okamžiku schválení (přijetí) se již bude jednat o překonaný dokument. Počítačové kriminalita je známá svou nestálostí, proměnlivostí a nepředvídatelností.

Pojem počítačová kriminalita vznikl v 90. letech minulého století, tedy v době, kdy trestná činnost byla páchána pomocí informační techniky. V současné době se však k páchání trestné činnosti používají i jiné prostředky nežli počítače či osobní počítače (PC – Personal Computer). Pojem „počítač“ byl tedy nahrazen přesnějším výrazem, a to pojmem „informační a komunikační technologie“ (ICT). Z tohoto důvodu se začal používat i obsáhlejší pojem pro danou trestnou činnost, a to kybernetická kriminalita.

Již jen z výše uvedeného vývoje názvosloví je tedy zřetelný rychlý rozvoj v této oblasti. Cílem této práce však není pouze provést detailní výklad jednotlivých pojmů, které mnozí chápou jako prostá synonyma, ale popsat a vysvětlit podstatu počítačové kriminality a její možný postih na základě platné, případně připravované legislativy.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je zpracovat téma počítačová kriminalita z pohledu historie a současnosti, vysvětlit základní pojmy vážící se k této problematice a popsat jednotlivé typy počítačové kriminality v návaznosti na současnou legislativu a potřebu jejího vývoje, včetně zhodnocení možností ochrany běžného uživatele před jejími dopady.

Cílem praktické části je pak formou dotazníkového šetření získat aktuální poznatky o osobních zkušenostech v oblasti počítačové kriminality mezi respondenty a avizovat možné způsoby, které by pomohly předcházet páchání počítačové kriminality, případně snížily vzniklé škody a odradily pachatele od nezákonného konání.

2.2 Metodika

Metodika bakalářské práce je založena na studiu poznatků z oblasti počítačové kriminality a současných možností ochrany běžného uživatele, které jsou publikovány zejména ve vědecké a odborné literatuře. Výsledky studia jsou využity k vypracování teoretické části bakalářské práce. Na základě zpracování teoretické a praktické části je provedeno vyhodnocení získaných poznatků, které je použito ke zpracování návrhů uživatelských a legislativních opatření na ochranu běžného uživatele.

3 Teoretická část práce

3.1 Základní pojmy

Počítačová kriminalita (známá také jako internetová a kybernetická kriminalita) je termínem pro jakýkoliv trestný čin, který je zaměřen proti počítačům nebo je páchán pomocí počítače. Tedy jde o takové jednání, které je provedeno za pomoci výpočetní techniky, ale je nelegální, nemorální nebo neoprávněné. Nejde o nový typ trestné činnosti, ale pouze o novou technologii, která umožňuje novým způsobem páchat takovou činnost jako je sabotáž, krádež, zneužití, neoprávněné užití věci, vydírání nebo špionáž. [1]

Počítač je souhrn technického a programového vybavení a dat, včetně **počítačového systému**. Tím *„se rozumí jakékoli zařízení nebo skupina vzájemně propojených dat nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Počítačovým systémem je tedy zařízení sestávající z technického (hardware) a programového (software) vybavení, které je určené k automatickému zpracování digitálních dat.“*[2]

Z praktického hlediska je možno považovat za počítač tedy i chytrý mobilní telefon, tablet, prvky chytré domácnosti, navigační přístroje a další přístroje, které jsou schopné datové komunikace, respektive jsou schopny přijímat, zpracovávat nebo sdílet data.

Informační systém je v podstatě *„systém, v němž se vazby mezi prvky chápou jako informace (data), resp. směry jejich toků a jednotlivé prvky jako místa vzniku, sběru, předzpracování, přenosu, uchování, zpracování, distribuce či zániku informací (dat); jeho účelem je tvorba a prezentace informací.“*[3]

Informační systémy využívají k přenosu dat především internet což je *„celosvětové dynamické sjednocení množství síťových zařízení a počítačů. Jako synonym se používají také pojmy datová dálnice, informační infrastruktura, síť sítí apod.“*[4] *„Architektura Internetu je založena na vzájemném propojení milionů počítačů s globálně distribuovaným zpracováním,*

[1] ZAVRŠNIK, Aleš. Kyberkiriminalita. Praha: Wolters Kluwer, 2017. ISBN-978-80-7552-759-2.
[2] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, s. 2307. Velké komentáře. ISBN 9788074004285.
[3] SMEJKAL, Vladimír. Počítačová a internetová kriminalita v České republice. *Právní rozhledy*: C.H. Beck. 1999, roč. 1999, č. 12, s. 1 a násl. ISSN 1210-6410.
[4] MUSIL, Stanislav. Počítačová kriminalita: Dostupné z: http://www.ok.cz/iksp/docs/256.pdf

komunikací a řízením. Tato distribuovaná architektura je klíčová pro stabilitu a odolnost Internetu a pro rychlou obnovu datového přenosu v případě vzniku problému.“[5]

3.2 Počítačová kriminalita a její vývoj v čase

Pokud chceme najít počátek možného zneužití počítače a jeho systému, musíme se vrátit až do období roku 1932, kdy se polskému matematikovi Marianu Rejewskemu podařilo prolomit ochranu šifrovacího stroje Enigma. Odhalením metod šifrování tak umožnil rozluštění německých tajných zpráv.

Jako zajímavost lze uvést, že prolomením bezpečnostních překážek v počítačích a informačních systémech se v padesátých letech minulého století bavila např. komunita studentů americké Massachusetts Institute of Technology.[6] V té době se však ještě nejednalo o závažnou hrozbu.

Rozvoj počítačů, který umožnil jejich hojné využití zejména na akademických pracovištích, v odborných organizacích a obchodních společnostech datujeme do šedesátých a sedmdesátých let minulého století.

Masové rozšíření různých typů výpočetní techniky umožnil další vývoj, díky kterému se uživatelské prostředí stalo jednoduché a snadno ovladatelné pro široký okruh uživatelů. Avšak ani to samo o sobě ještě nemělo na rozvoj počítačové kriminality podstatný vliv[7].

Významným okamžikem, který umožnil rozvoj počítačové kriminality, je vytvoření síťového protokolu, který poprvé v roce 1989 umožnil sdílet informace. Jeho autorem je fyzik Evropské organizace pro jaderný výzkum Tim Berners-Lee[8].

Propojit jednotlivá zařízení a sdílet data umožnila v roce 1993 následná grafická úprava a rozšíření uživatelské dostupnosti protokolu. To byl okamžik, od kterého mohli poskytovatelé internetu nabízet připojení do globálních sítí. [9]

Rozšíření množství potencionálních pachatelů a obětí trestné činnosti umožňuje v současné době skutečnost, že počítačem již nemůžeme rozumět pouze osobní stolní

[5] Stanoviska Evropského hospodářského a sociálního výboru Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.C_.2011.218.01.0130.01.CES
[6] McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009, s. XVI-XVIII. ISBN 0313339740.
[7] BRITZ, Marjie. *Computer forensics and cyber crime: an introduction*. 2nd ed. Upper Saddle River, N.J.: Pearson Prentice Hall, 2009, s. 24. ISBN 0132447495.
[8] McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009, s. XVI-XVIII. ISBN 0313339740.
[9] BRITZ, 2009, op. cit., s. 36.

a přenosné počítače, ale i další zařízení, pomocí nichž se lze připojit do počítačové sítě. To umožňuje nejen rozšíření okruhu potencionálních pachatelů, ale i obětí trestné činnosti, za které můžeme považovat i ty uživatele, kteří se do páchání trestné činnosti zapojují nevědomě.

V posledních letech dochází k velmi rychlému rozvoji informačních a komunikačních technologií v našich domácnostech, ve firmách, ve veřejné správě a v dalších oblastech našeho, ale i veřejného života, což umožnilo, aby počítačová kriminalita nabyla na závažnosti.

3.3 Druhy počítačové kriminality

Dle mezistátní Úmluvy mají být kriminalizovány trestné činy s následujícími znaky:

1) Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
   a. nezákonný přístup,
   b. nezákonný odposlech,
   c. zasahování do dat,
   d. zasahování do systému,
   e. zneužívání zařízení.
2) Trestné činy související s počítači
   a. počítačové padělání,
   b. počítačový podvod,
3) Trestné činy související s obsahem, zejména s dětskou pornografií.
4) Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

3.3.1 Trestné činy proti důvěrnosti, integritě a použitelnosti dat a systémů

Za narušení důvěrnosti se považuje ohrožení bezpečnosti počítače, za narušení integrity a dostupnosti se považuje neoprávněné užívání dat a zásahy, které mohou mít vliv na jejich existenci, kvalitu a správnost. [10]

[10] ŠÁMAL, 2012, op. cit., s. 2305.

Za **nezákonný přístup** (angl. hacking) se považuje snaha pachatele „*o neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části s úmyslem získat počítačová data nebo s jiným nečestným úmyslem.* “[11]

Nezákonný odposlech (zachycení informací) tzv. sniffing je *„úmyslný, neoprávněný, technickými prostředky provedený odposlech neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému přenášejícího taková počítačová data.“*[12]

Za **zasahování do dat** (do vybavení počítače) se považuje manipulace nebo sabotáž mechanického a programového vybavení počítačů, popř. dat uchovávaných jejich prostřednictvím, a to jak v digitální, tak fyzické formě.[13]

Z pohledu českého právního řádu (§ 230 odst. 2 písm. b) TZ) se jedná o trestné činy, které mohou mít podobu vymazání, zničení, poškození, změn, potlačení, snížení kvality nebo učinění dat neupotřebitelnými.

Pro tento druh trestné činnosti se nejčastěji používá škodlivý software známý jako malware. Po instalaci tohoto softwaru mohou probíhat nežádoucí činnosti, které může provádět pachatel sám, nebo na dálku prostřednictvím uživatele s využitím různých klamavých technik.[14]

Způsobů šíření škodlivého softwaru, je celá řada. Metoda tzv. spamu, tedy hromadné nevyžádané elektronické pošty zasílané původně hlavně za účelem přímého marketingu se jeví jako nejefektivnější.

Základní klasifikaci různých škodlivých programů, jejichž funkce a podoba se často liší, je možné vymezit takto:

a) počítačové viry (viruses),

b) počítačoví červi (worms) a

c) tzv. trojští koně (Trojan horses). [15]

Za **zásahy do systému** lze z pohledu trestné činnosti považovat „*neoprávněné závažné omezení funkčnosti počítačového systému vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním nebo potlačením počítačových dat.“*[16]

[11] Úmluva Rady Evropy o počítačové kriminalitě, čl. 2, 2001, op. cit.
[12] Úmluva Rady Evropy o počítačové kriminalitě, čl. 3, 2001, op. cit.
[13] McQUADE, 2009, op. cit., s. 33.
[14] ŠÁMAL, 2012, op. cit., s. 2310.
[15] ŠÁMAL, 2012, op. cit., s. 2310-2311.
[16] Úmluva Rady Evropy o počítačové kriminalitě, čl. 5, 2001, op. cit.

Jedná se o trestné činy, založené na odmítnutí přístupu uživatelům k jejich počítačům či jiným druhům elektronických zařízení, a páchané pomocí útoků typu denial of service (dále jen „DoS“), které přetíží počítačové sítě ve velmi krátké době velmi vysokým množstvím dat. Servery, které zprostředkovávají přenos dat, vysoký nápor nezvládnou a dojde k jejich přetížení. V případě útoků známých jako „SYN Flood“, dochází k obrovskému množství pokusů o připojení ke konkrétní síti. Následkem je vyčerpání volné přihlašovací kapacity napadených serverů.[17]

Nebezpečnější varianta DoS je tzv. *distributed denial of service* (dále jen „DDoS“). Účinnost této varianty je založena na výrazném navýšení počtu škodlivým kódem nakažených počítačů, z nichž je útok prováděn. V podstatě bez vědomí majitele se nakažený počítač napojí do sítě. Pro tuto událost vznikl pojem botnet. Odborná literatura uvádí, že největší botnety měly až 400 000 připojení během 24 hodin.[18]

Za **zneužití zařízení** se považuje dle Úmluvy o počítačové kriminalitě: *„výroba, prodej, opatření za účelem použití „dovoz, distribuci nebo jiné zpřístupňování:*

- *zařízení, včetně počítačového programu, vytvořeného nebo přizpůsobeného zejména za účelem spáchání trestných činů;*
- *počítačového hesla, přístupového kódu nebo podobných dat, pomocí nichž lze získat přístup do celého počítačového systému nebo do jakékoli jeho části s tím úmyslem, že jej bude použito pro účely spáchání trestných činů"*[19]

3.3.2 Trestné činy související s počítači

Podle Úmluvy se jedná o trestné činnosti, které jsou páchány prostřednictvím počítačových systémů.

Počítačové padělání – jedná se o trestné činy: *„vkládání, pozměnění, vymazání nebo potlačení počítačových dat, které povede k nepravosti dat, a to s úmyslem, aby tato data byla považována za pravá nebo aby podle nich bylo pro právní účely jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná či nikoli.“*[20]

[17] McQUADE, 2009, op. cit., s. 63.
[18] Viz bod 3.4 Stanoviska Evropského hospodářského a sociálního výboru, 2011, op. cit.
[19] Úmluva Rady Evropy o počítačové kriminalitě, čl. 6, 2001, op. cit.
[20] Úmluva Rady Evropy o počítačové kriminalitě, čl. 7, 2001, op. cit.

Počítačový podvod – podle Úmluvy se jedná o trestné činy počítačového padělání, nebo počítačového podvodu, které jsou spáchány úmyslně a neoprávněně a mají charakter „*vkládání, pozměnění, vymazání nebo potlačení počítačových dat, či jakýkoliv jiný zásah do fungování počítačového systému s podvodným nebo nečestným úmyslem neoprávněně získat majetkový prospěch pro sebe nebo pro jiného*.“ [21]

3.4 Počítačová kriminalita a její pachatelé

Je obecně známo, že pachatelé počítačové kriminality jsou nadprůměrně inteligentní, mají patřičné know-how a jsou schopni se přizpůsobovat okolnostem pro možné páchání trestné činnosti. Technologický vývoj jim pak jejich konání spíše ulehčuje. Spoléhat se u moderních pachatelů na počítačovou morálku není možné, protože ta u pachatelů již zcela chybí.[22]

Je rovněž běžné, že se pachatelé trestné činnosti spojují a tvoří tak zvané organizované skupiny.[23] Tou se rozumí *„sdružení více osob, v němž je provedena určitá dělba úkolů mezi jednotlivé členy sdružení a jehož činnost se v důsledku toho vyznačuje plánovitostí a koordinovaností, což zvyšuje pravděpodobnost úspěšného provedení trestného činu, a tím i jeho společenskou škodlivost (srov. R 53/1976-II. a R 45/1986).“*[24]

Dochází též k situacím, kdy uživatelé napadených počítačů jsou de *facto* útočníky, nicméně *de iure* se jedná o oběti trestné činnosti. Děje se tak pomocí škodlivého software, kterým je napaden jejich počítač a který se následně stane součástí tzv. botnet sítě, kterou pachatelé využijí k útokům typu odepření služby. Uživatele v tomto případě nelze zpravidla považovat za člena organizované skupiny.[25]

3.5 Počítačové kriminality a její prokazování

K odhalení a usvědčení pachatele je třeba zajistit důkazy, kterými jsou v případě počítačové kriminality tzv. digitální stopy, které za sebou zanechává každá osoba, která pracuje s počítačem. Lze shrnout, že *„digitální stopy vznikají působením (ovládáním, využíváním) člověka (uživatele, pachatele) na aplikační nebo systémový software, funkčností*

[21] Úmluva Rady Evropy o počítačové kriminalitě, čl. 8, 2001, op. cit.
[22] MUSIL, 2000, op. cit., s. 252.
[23] § 129 zákona č. 40/2009 Sb, trestní zákoník, ve znění pozdějších předpisů.
[24] ŠÁMAL, 2012, op. cit., s. 2314.
[25] *Informační systém* [online]. Copyright © [cit. 12.03.2021]. Dostupné z: https://is.muni.cz/th/vyd7c/DP_Pocitacova_kriminalita_FINAL.pdf

digitálního zařízení nebo automatickým (předem naprogramovaným) působením jednoho zařízení, technologie na druhé.“[26]

Cílem každého pachatele je stopy eliminovat, a proto věda, která se se nazývá *počítačová forenzika* (z angl. computer forensics), se zabývá jejich vyhledáváním, obnovením a zachováním.[27]

Pro účel trestního řízení je nezbytné, aby zajištěné důkazy byly relevantní, přípustné a byly schopny napomoci při kvalifikaci trestného činu a odhalení skutečného pachatele. Digitální stopa má, díky svým specifickým vlastnostem, často diskutabilní výpovědní hodnotu. Specifickými vlastnostmi digitální stopy jsou např.:

- latentnost,
- časová dohledatelnost,
- vysoká obsažnost,
- velmi nízká životnost,
- velký datový objem,
- velký geografický rozsah prostoru s digitálními stopami,
- vysoký stupeň ochrany dat a soukromí znemožňuje nebo znesnadňuje práci s digitálními stopami,
- velké množství způsobů zahlazování digitálních stop kvalifikovanými pachateli,
- omezená restaurovatelnost zničených digitálních stop,
- nízká úroveň soudní akceptace digitálních stop v právní praxi.[28]

Elektronický důkaz může v praxi nabývat podobu elektronické dokumentace reálného důkazu, a to například vytvořením počítačového modelu místa trestného činu, a podobu elektronických dat, která jsou samostatným důkazem. Tím jsou myšleny například záznamy telefonních hovorů nebo odposlech elektronické komunikace.[29]

Elektronické důkazy jsou těžce přiřaditelné ke konkrétní osobě, a proto úspěšné prokázání, že se elektronický důkaz vztahuje k pachateli, je možné pouze s využitím

[26] RAK, Roman; PORADA, Viktor. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2005, roč. 17, č. 1, s. 16 [cit. 25. 3. 2014]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf
[27] McQUADE, 2009, op. cit., s. 29.
[28] RAK a PORADA, 2005, op. cit., s. 16.
[29] KYNCL, Libor. IP adresa identifikuje místo připojení, nikoli osobu. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy* [online]. Brno: Masarykova universita, 2010, roč. 2, č. 3, s. 6 [cit. 25. 3. 2014]. Dostupné z: https://www.law.muni.cz/dokumenty/12793

elektronického podpisu, použití hesla, čipové karty a jiných autentizačních metod. Bývají tak součástí nepřímých důkazů, které však mohou sehrát důležitou roli v rámci trestního řízení.[30]

3.6 Počítačová kriminalita a její vyšetřování

3.6.1 Právní specifika

I při vyšetřování počítačové kriminality se postupy vyšetřování nemění. Patří mezi ně, stejně jako při vyšetřování jiné kriminality, ohledání místa činu, domovní prohlídky či jiných takových prostor, zajištění a šetření obsahu výpočetní techniky a výslech.[31]

Postup kriminalistů při provádění domovní prohlídky vypadá následně:

1) zajištění nebezpečných osob nebo bezpečnostních rizik,
2) vyhledání a zajištění výpočetní techniky,
3) vykázání neoprávněných osob a personálu,
4) zajištění síťových připojení a k tomu navazující úkony (záleží na okolnostech konkrétního případu, interní správci sítí totiž mohou být pro následné vyšetřování důležití),
5) oddělení všech podezřelých od ostatních osob a jejich přemístění na předem určené místo,
6) analýza důkazních materiálů a následné zaplombování počítačů.[32]

3.6.2 Technologická specifika

Při vyšetřování počítačové kriminality je zapotřebí, aby vyšetřující orgány měly taková technologická vybavení, která zaručí s největší jistotou úplné a správné zajištění důkazů a umožní dále jejich použití pro účely trestního řízení.[33]

Tato technologická zařízení jsou:

- *spouštěcí média,*

[30] *Elektronické důkazy – současnost či budoucnost českého soudnictví?* [online]. Rozhovor s prof. Ing. Vladimírem Smejkalem, CSc., LL.M. Česká advokátní komora: Bulletin Advokacie, publikováno 26. 10. 2012 [cit. 26. 3. 2014]. Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-dukazy-soucasnost-ci-budoucnost-ceskeho-soudnictvi
[31] GŘIVNA a POLČÁK, 2008, op. cit., s. 89.
[32] BRITZ, 2009, op. cit., s. 310.
[33] *Informační systém* [online]. Copyright © [cit. 11.03.2021]. Dostupné z: https://is.muni.cz/th/vyd7c/DP_Pocitacova_kriminalita_FINAL.pdf

- *náhradní hardware a počítačové periferie,*
- *antivirové programy,*
- *zálohovací programy,*
- *forenzní programy.* [34]

3.7 Softwarové projevy počítačové kriminality – malware

3.7.1 Malware

Slovo **malware** vzniklo složením dvou anglických slov, tedy malicious (škodlivý) a software. Jde o škodlivý či obtěžující program, který byl vytvořen za účelem napadání systému a vniknutí do něj. Mezi malware spadají počítačové viry, adware, spyware, phishing, trojské koně, červy, rootkity, ransomware atd. Nejčastěji se malware šíří internetem, e-mailem či flash diskem. Do systému se nejčastěji dostává při navštívení napadených webových stránek nebo stahováním dat. Nejúčinnější obranou před malwarem je mít nainstalovaný antivirový a antimalwarový software, být obezřetný při navštěvování neznámých webových stránek a neotvírání neznámých příloh v emailech.[35]

Spyware – jedná se o typ malwaru, který se využívá jako špionážní program ke špehování vašeho chování na internetu. Zaznamenává celou vaší historii navštívených webových stránek, ve které může sledovat a zaznamenávat vaše osobní údaje jako jsou heslo, přihlašovací údaje či bankovní údaje. Podtyp spywaru je **keylogger**, který umožnuje odposlouchávat vše co napíše uživatel na klávesnici.[36]

Adware je software podporující reklamu – nejčastěji se jedná o reklamy ve formě vyskakovacích oken, reklamy překrývající část obrazovky nebo webové stránky. Ve většině případů adware nepředstavuje významné riziko, ale může odkazovat na nebezpečné stránky, například takové, které šíří malware. Nejčastěji se adware vyskytuje v bezplatných programech. [37]

Phishing (rybaření), patří mezi techniky sociálního inženýrství, kdy se počítačový podvodníci pokoušejí získat citlivé informace jako jsou hesla, údaje o platebních kartách

[34] BRITZ, 2009, op. cit., s. 308.
[35] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-malware
[36] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-spyware
[37] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-adware

apod. Jde o zasílání emailových zpráv či přesměrovávání na falešné webové stránky, které vypadají jako oficiální a věrohodné, kde vás nabádají k vyplnění citlivých dat.[38]

Počítačový virus je program, který se ve většině případů spustí nevědomě v pozadí při spuštění nějakého běžně používaného programu, který byl infikován. Spuštěný vir se začne kopírovat do jiných souborů a bez vědomí uživatele provádí změny v počítači. Viry jsou zejména navrženy tak, aby získávali kontrolu nad napadeným systémem a prováděli destruktivní akce.[39] **Trojský kůň** je typ viru, který se nedokáže sám šířit a ani infikovat jiné soubory, ale dokáže způsobit znatelné škody či krádež dat. Nejčastěji se trojský kůň dostane do zařízení při stáhnutí dobře vypadajícího bezplatného programu či emailovou přílohu.[40] **Počítačoví červi** také patří mezi viry, od počítačového viru se liší způsobem, kterým se šíří. Počítačoví červi se sami dokáží replikovat a také se dokáží šířit prostřednictvím sítě. U infikovaných zařízení většinou dochází ke značnému zpomalení či zařízení dokonce přestávají reagovat celkově.[41]

Rootkit je o program, který je navržen hackery tak, aby útočník mohl maskovat svoji činnost a bez vědomí uživatele tak získat přístupová práva administrátora a na dálku přes vzdálenou plochu ovládat zařízení. Rootkit může být nainstalován do počítače různými způsoby, například zdánlivě bezpečným rozšířením třetích stran, ale sám se šířit nedokáže.[42]

Ransomware je škodlivý kód, který zamezuje uživateli přístup k počítačovému souboru nebo systému. Pro odblokování dat vyžadují útočníci tzv. hackeři zaplacení výkupného s negarantovaným zpřístupněním dat.[43]

3.7.2 Způsob ochrany

Na každý typ malwaru existuje jiné řešení ochrany, ale celkově se od sebe moc neliší. Základem je mít vždy aktualizovaný operační systém, ale i další programy v počítači. Dalším pravidlem je mít funkční a účinný antivirový a antimalwarový software. Při používání internetu by měl mít každý uživatel funkční firewall, který aspoň částečně ochrání uživatele před hrozbami internetu. Firewall ale nemá funkci antivirového či antimalwarového

[38] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-phishing
[39] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus
[40] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-trojan
[41] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-computer-worm
[42] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-rootkit
[43] *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

systému, nejlépe funguje v kombinaci s již zmíněnými programy. I přes využívání všech obraných prvků by se měl uživatel pohybovat na internetu opatrně. Mezi základní pravidla patří neklikání na vyskakovací reklamy, neotvíraní emailových příloh od neznámých odesilatelů, chránit si svá hesla (s nikým je nesdílet ani v případě, že by je vyžadoval administrátor), nesdělovat citlivé informace, kontrolovat správnost URL adres navštěvovaných stránek (například kontrola domény, kdy může být .com místo .cz), kontrola, z jakých zdrojů stahujeme apod. Většina výše zmíněných pravidel ochrání běžného uživatele i před hrozbami jako je sociální inženýrství či proti spamu.

3.8 Nástin budoucího vývoje

Jak se bude vyvíjet počítačová kriminalita už bylo v minulosti mnohokrát řečeno mnohými odborníky. Já si zde dovolím citovat nadčasový výrok pana Schneira, který již v roce 2002 predikoval jakou cestou se bude zločin na internetu vyvíjet. *„Nepůjde o případy virů, trojských koníaDDoS útoků pro zábavu nebo možnost se vychloubat se svými schopnostmi. Půjde o skutečný zločin. Zločinci mají sklon zaostávat za vývojem technologií o pět, deset let, ale nakonec si uvědomí jejich možnosti. Tak jako Willie Sutton začal přepadat banky „protože tam byly peníze“, tak moderní zločinci začnou útočit přes počítačové sítě. Stále více hodnot (finančních prostředků) je online než v penězích reálných.“* [44]

K porovnání běžného „bankovního přepadení“ a phishingového (podvodné stránky či emaily) útoků můžeme použít tabulku statistiky FBI (tabulka níže), kterou představil Jirovský v roce 2007.[45]

Tabulka 1 Porovnání rizika při ozbrojeném přepadení a kybernetického útoku

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje, že bude zraněn či zabit.	Bez rizika fyzické újmy
Zisk	Průměrně 3–5 tisíc USD.	Průměrně 50–500 tisíc USD.
Pravděpodobnost dopadení	Dopadeno 50–60 % útočníků.	Dopadeno cca 10 % útočníků.

[44] Překlad autora. Blíže viz SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing.* [online]. [cit. 6.11.2007]. Dostupné z https://www.schneier.com/crypto-gram/archives/2002/1215.html
[45] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 30. ISBN 978-80-247-1561-2

Pravděpodobnost odsouzení	Odsouzeno 95 % dopadených útočníků.	Z dopadených útočníků dojde k soudnímu projednávání pouze u 15 % útočníků a z nich je odsouzeno jen 50 %.
Trest	Průměrně 5–6 let, pokud pachatel při loupeži nikoho nezranil.	Průměrně 2–4 roky.

Zdroj: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 30. ISBN 978-80-247-1561-2

Bývalý ředitel FBI Robert S. Mueller řekl v roce 2007: „*Jsem přesvědčen o tom, že existují pouze dva druhy společností: takové, do kterých se již hackeři nabourali, a ty, do nichž se teprve nabourají. A i tyto dvě skupiny se velmi rychle spojují v kategorii jedinou: společnosti, do jejichž systémů hackeři pronikli, a společnosti do nichž proniknou znovu.*“[46]

Pachatelé trestné činnosti počítačové kriminality, už nejsou pouhými individualitami, ale jsou to profesionálové, kteří tuto trestnou činnost vykonávají pro své obohacení a mohou pracovat i ve větších organizovaných skupinách.

Kyberkriminalita je velkým problémem, hlavně díky okolnostem jako jsou:

1) závislost společnosti na internetu,
2) skutečnost, že kyberkriminalita se stala výnosným globálním businessem,
3) minimální gramotnost uživatelů.[47]

3.9 Legislativa

3.9.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě

Problematiku počítačové kriminality z pohledu trestních norem zpočátku řešila Organizace pro hospodářskou spolupráci a rozvoj (OECD). Později pak Rada Evropy, která v roce 2001 vytvořila budapešťskou Úmluvu o počítačové kriminalitě, která u nás vstoupila v platnost od 1. prosince 2013 (dále jen „Úmluva“). [48]

[46] MUELLER, Robert. *RSA Cyber Security Conference.* 2012. Dostupné z: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

[47] *Informační systém* [online]. Copyright © [cit. 11.03.2021]. Dostupné z: https://is.muni.cz/el/fss/podzim2020/BSSn4469/um/8_-_kyberneticka_kriminalita/Kolouch_-_cybercrime.pdf

[48] Viz k tomu Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě. In: Sbírka mezinárodních smluv: Česká republika. Praha: Ministerstvo vnitra, 2013, částka 56 [cit. 27. 3. 2014]. Dostupné z: http://www.epravo.cz/ _dataPublic/sbirky/2013/sb0056-2013m.pdf

Česká republika byla jedna z posledních, která Úmluvu ratifikovala. Jako hlavní důvod byla nedostatečná právní úprava, a to především v oblasti procesních opatření.

Úmluvu ratifikovalo již mnoho států (státy Evropy, USA, Austrálie, Japonsko, ale i Argentina, Israel aj.), a i když některé státy tuto smlouvu ještě neratifikovali, neznamená to, že její principy neuplatňují.

Úmluva o kyberkriminalitě je základním kamenem pro sjednocení právní legislativy a k ochraně společnosti před kyberkriminalitou. Úmluva stanoví smluvním stranám povinnost implementovat do národních právních řádů takové nástroje, které umožní postih definovaných trestných činů.[49] Úmluva o kyberkriminalitě[50] se skládá z preambule a 48 článků, které jsou rozděleny do 4 kapitol.

3.9.2 **Dokumenty Evropské unie**

Z důvodu potřeby harmonizací právních úprav při potírání kybernetické trestné činnosti mezi jednotlivými státy EU vzniklo několik dalších dokumentů.

Z pohledu boje s kyberkriminalitou jsou nejvýznamnějšími následující dokumenty:

- Směrnice Rady 91/250/EHS o právní ochraně počítačových programů.
- Rozhodnutí Rady 92/242/EHS o bezpečnosti informačních systémů.
- Směrnice Evropského parlamentu a Rady č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice č. 98/48/ES.
- Směrnice č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“).
- Rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu.
- Rámcové rozhodnutí Rady 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků.

[49] *Informační systém* [online]. Copyright © [cit. 11.03.2021]. Dostupné z: https://is.muni.cz/el/fss/podzim2020/BSSn4469/um/8_-_kyberneticka_kriminalita/Kolouch_-_cybercrime.pdf

[50] Kompletní znění Úmluvy v českém překladu je možné nalézt [online]. [cit. 20. 8. 2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

- Směrnice Evropského parlamentu a Rady č. 2002/21/EC o společném regulačním rámci pro sítě a služby elektronických komunikací (rámcová směrnice).
- Směrnice Evropského parlamentu a Rady č. 2002/19/EC o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice).
- Směrnice Evropského parlamentu a Rady č. 2002/20/EC o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice).
- Směrnice Evropského parlamentu a Rady č. 2002/22/EC o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací (směrnice o universální službě).
- Směrnice Evropského parlamentu a Rady 2002/58/EC týkající se zpracovávání osobních údajů a ochrany soukromí v oblasti elektronických komunikací (směrnice o ochraně údajů v elektronických komunikacích).
- Směrnice Komise č. 2002/77/ES o hospodářské soutěži na trzích s elektronickými komunikačními sítěmi a službami (soutěžní směrnice).
- Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy.
- Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům.
- Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) ze dne 15. 11. 2006.
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007.
- Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti ze dne 27. listopadu 2008.

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“ ze dne 30. 3. 2009[51].
- Sdělení komise Radě a Evropskému parlamentu, Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě 2012.
- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013, o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004, ze dne 21. května 2013.
- Směrnice Evropského parlamentu a Rady 2013/40/EU, o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, ze dne 12. srpna 2013.
- Nařízení Evropského parlamentu a Rady (EU) č. 513/2014, kterým se jako součást Fondu pro vnitřní bezpečnost zřizuje nástroj pro finanční podporu policejní spolupráce, předcházení trestné činnosti, boje proti trestné činnosti a řešení krizí a zrušuje rozhodnutí Rady 2007/125/SVV, ze dne 16. dubna 2014.
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ze dne 23. července 2014.
- Nařízení Evropského parlamentu a Rady (EU) 2016/794, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. května 2016.
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[51] : KOLOUCH, Jan a Petr VOLEVECKÝ. Trestněprávní ochrana před kybernetickou kriminalitou. Praha: Policejní akademie České republiky v Praze, 2013, s. 76

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, ze dne 6. července 2016 (NIS Directive). [52]

3.9.3 Dokumenty České republiky

V České republice (dále jen „ČR“) je gestorem kybernetické bezpečnosti Národní bezpečností úřad (dále jen „NBÚ“), jehož aktivity spočívají v oblasti budování Národního centra kybernetické bezpečnosti (dále jen „NCKB“), tedy pro přípravu a tvorbu legislativy, jakožto implementace zákona č.181/2014 Sb., ve znění pozdějších předpisů, o kybernetické bezpečnosti. Ten také určuje kritickou informační strukturu mezinárodní spolupráce, národní spolupráce a zvyšuje povědomí a osvětu v oblasti kybernetické bezpečnosti.[53] NBÚ za přispění dalších ministerstev, úřadů a jiných subjektů připravil „*Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále jen „NSKB“)*“, která byla přijata usnesením vlády České republiky č. 105 ze dne 16. února 2015 a „*Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále jen „AP“)*, který byl přijat usnesením vlády České republiky č. 382 ze dne 25. května 2015. [54]

3.10 Právní normy ČR

3.10.1 Právní normy bezprostředně související s kybernetickou činností:

- zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,
- zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů,
- zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů,
- zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže,
- zákon č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů,
- zákon č. 127/2005 Sb., o elektronických komunikacích,

[52] KOLOUCH, JAN. *CyberCrime.* Praha: CZ NIC, 2016, s. 335–337
[53] Vyhledávání ASPI | epravo.cz. *EPRAVO.CZ – Váš průvodce právem – Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 11.03.2021]. Dostupné z: https://www.epravo.cz/vyhledavani-aspi/?Id=87470&Section=1&IdPara=1&ParaC=2
[54] Částka 13/2018 a 8/2018 Sb.m.s.- RA1173 NB 16/2016 – kybernetická bezpečnost

- zákon č. 480/2004 Sb., o některých službách informační společnosti,
- zákon č. 273/2008 Sb., o Policii České republiky,
- zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů,
- zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů,
- zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví,
- zákon č. 441/2003 Sb., o ochranných známkách, ve znění pozdějších předpisů,
- zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích, ve znění pozdějších předpisů,
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů,
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- zákon č. 160/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti, ve znění pozdějších předpisů. [55]

3.10.2 **Skutková podstata trestných činů v oblasti kybernetiky**

Trestní zákoník, který nabyl účinnosti v roce 2010, již obsahuje nová znění skutkových podstat trestných činů, které mohou být páchány i v rámci počítačové kriminality. Mezi ně je možno zařadit:

- *§ 180 neoprávněné nakládání s osobními údaji,*
- *§ 181 poškození cizích práv,*
- *§ 182 porušení tajemství dopravovaných zpráv,*
- *§ 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,*
- *§ 184 pomluva,*
- *§ 191 šíření pornografie,*
- *§ 192 výroba a jiné nakládání s dětskou pornografií,*

[55] KOLOUCH, JAN. *CyberCrime.* Praha: CZ NIC, 2016, s. 338

- *§ 193 zneužití dítěte k výrobě pornografie,*
- *§ 193b navazování nedovolených kontaktů s dítětem,*
- *§ 205 krádež,*
- *§ 207 neoprávněné užívání cizí věci,*
- *§ 209 podvod,*
- *§ 213 provozování nepoctivých her a sázek,*
- *§ 216 legalizace výnosů z trestné činnosti,*
- *§ 228 poškození cizí věci,*
- *§ 230 neoprávněný přístup k počítačovému systému a nosiči informací,*
- *§ 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,*
- *§ 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti,*
- *§ 234 neoprávněné opatření, padělání a pozměnění platebního prostředku,*
- *§ 236 výroba a držení padělatelského náčiní,*
- *§ 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití,*
- *§ 268 porušení práv k ochranné známce a jiným označením,*
- *§ 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem,*
- *§ 269 porušení chráněných průmyslových práv,*
- *§ 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi,*
- *§ 272 obecné ohrožení*
- *§ 276 poškození a ohrožení provozu obecně prospěšného zařízení,*
- *§ 287 šíření toxikomanie,*
- *§ 290 získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou,*
- *§ 291 ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla,*
- *§ 311 teroristický útok,*
- *§ 316 vyzvědačství,*

- *§ 317 ohrožení utajované informace,*
- *§ 345 křivé obvinění,*
- *§ 348 padělání a pozměnění veřejné listiny,*
- *§ 353 nebezpečné vyhrožování,*
- *§ 354 nebezpečné pronásledování*
- *§ 355 hanobení národa, rasy, etnické nebo jiné skupiny osob,*
- *§ 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod,*
- *§ 357 šíření poplašné zprávy,*
- *§ 361 účast na organizované zločinecké skupině,*
- *§ 364 podněcování k trestnému činu,*
- *§ 365 schvalování trestného činu,*
- *§ 400 genocidum,*
- *§ 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka,*
- *§ 404 projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka,*
- *§ 405 popírání, zpochybňování, schvalování a ospravedlňování genocidia,*
- *§ 407 podněcování útočné války.*[56]

4 Praktická část práce

V teoretické části práce jsem se věnoval počítačové kriminalitě především z pohledu historie a současnosti, dále dle druhů počítačové kriminality, dle typu pachatelů a specifik při jejím vyšetřování. Rovněž jsem se pak zabýval legislativou a způsoby možné ochrany před tímto druhem kriminality.

V praktické části jsem se formou výzkumného šetření zaměřil na běžného uživatele výpočetní techniky pohybující se v internetovém prostředí a na jeho povědomí o počítačové kriminalitě a jeho postoji k rizikům a možným škodám.

Obecným cílem výzkumného šetření byla snaha zjistit, jak běžný uživatel chápe pojmy spojené s počítačovou kriminalitou, jaké má vlastní zkušenosti, případně zda mu byly

[56] KOLOUCH, JAN. *CyberCrime.* Praha: CZ NIC, 2016, s. 339–340

způsobeny nějaké škody, zda se chrání, případně jakým způsobem a jakou oblast počítačové kriminality považuje za nejvíce osobně a společensky nebezpečnou. Cílem šetření bylo také zjistit, co by nejvíce přispělo z pohledu běžného uživatele ke snížení počítačové kriminality, a zda by se i stát měl v této oblasti angažovat případně jakým způsobem.

Výzkum jsem provedl strategií kvantitativního šetření, kdy se data získávají pomocí dotazníků vyplňovaných respondenty.

Dotazník jsem zveřejnil na internetu na adrese www.vyplnto.cz.

Šetření probíhalo v období: 18. 02. 2021 - 04. 03. 2021

Počet respondentů: 155

Počet otázek: 17

Zobrazení otázek na internetu: celý dotazník najednou

Návratnost dotazníků: 68,62%

Průměrná doba vyplňování: 00.02:53

4.1 Úvodní informace zveřejněné respondentům

Dobrý den, jsem studentem 3. ročníku vysoké školy, oboru Informatika a obracím se na Vás s prosbou o vyplnění níže uvedeného dotazníku, který je zaměřen na problematiku počítačové kriminality. Výsledek tohoto dotazníkového šetření bude součástí bakalářské práce, jejímž cílem je přispět k potlačení počítačové kriminality podnětnými návrhy. Dotazník je anonymní, nezjišťuje správné či chybné odpovědi, ale slouží pouze ke zjištění Vašich názorů.

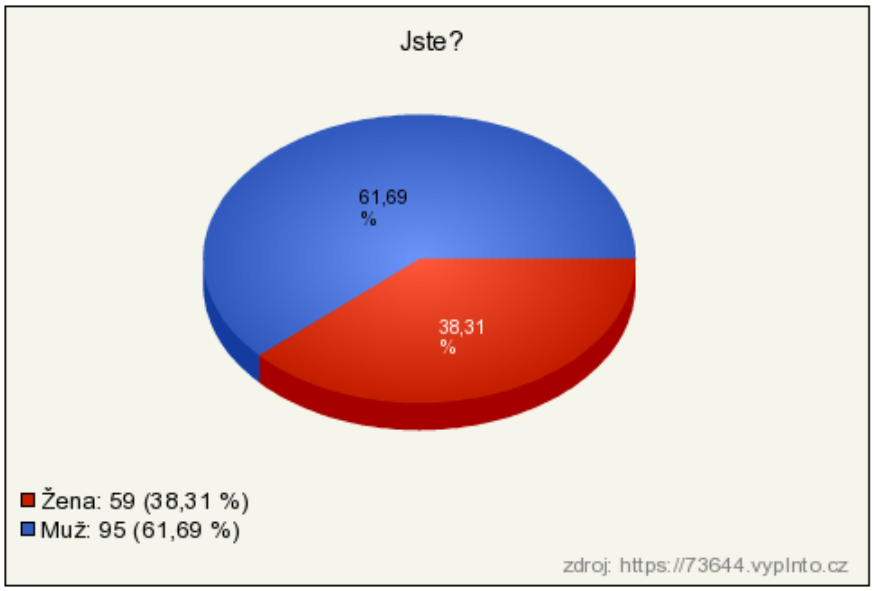
4.2 Vyhodnocení dotazníkového šetření

Otázka č. 1

Jste muž/žena? (Povinná otázka)

Většinu respondentů tvořili muži, tedy 95 (61,69 %) z celkových 154 dotázaných. Zbylých 59 respondentů byly ženy (38,31 %).

Graf 1 Pohlaví



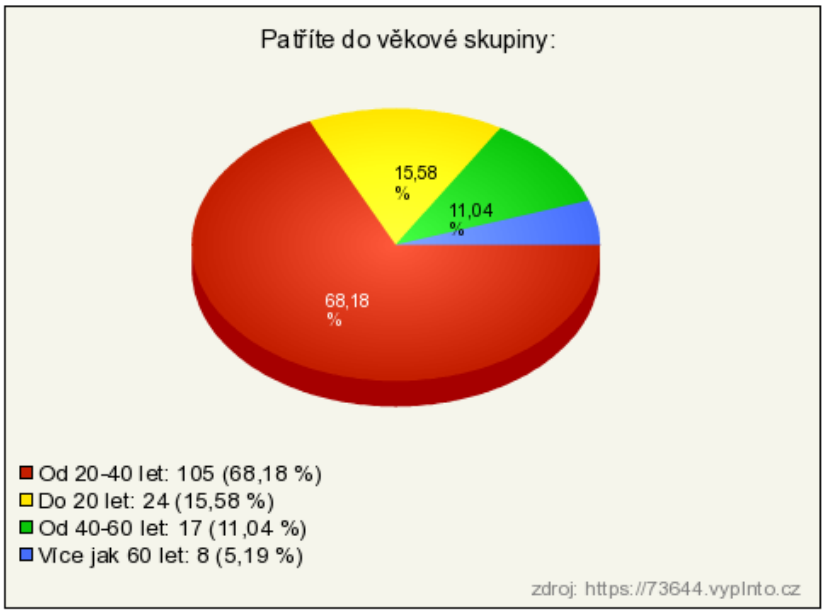
Otázka č. 2

Patříte do věkové skupiny: (Povinná otázka)

Byly vytvořeny 4 věkové skupiny – do 20 let, od 20-40 let, od 40-60 let a více jak 60 let.

Nejpočetnější skupinou vyplňujících tento dotazník byla skupina 20-40 let s počtem 105 dotázaných (68,18 %), další početnou skupinou byla skupina do 20 let s 15,58 %, méně početnou byla skupina 40-60 let s 11,04 % a nejmenší počet respondentů byl ve skupině více jak 60 let, kterou vytvořilo pouze 5,19 % dotázaných. Z těchto výsledků je zřejmé, že majoritní skupinu dotázaných tvořily skupiny od 20-40 let a do 20 let, které společně vytvořily 83,76 %.

Graf 2 Věková skupina

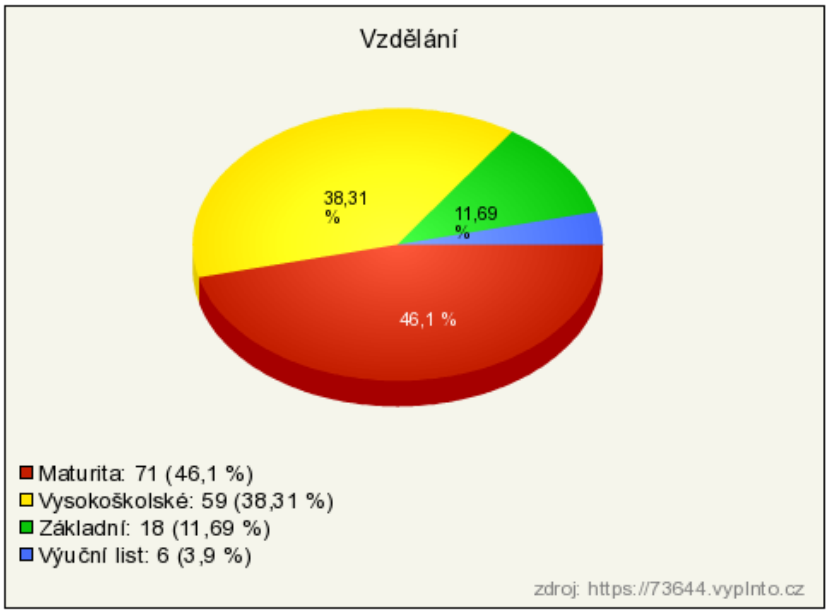


Otázka č. 3

Vzdělání (Povinná otázka)

Necelou polovinu respondentů (46,1 %) tvořila skupina, ve které nejvyšší dosažené vzdělání je ukončené maturitou. Více jak třetina respondentů uvedla vysokoškolské vzdělání (38,31 %). Respondentů se základním vzděláním bylo 11,69 % a minoritní počet respondentů tvořila skupina, jejichž nejvyšší vzdělání bylo ukončeno výučním listem - 3,9 %. Z těchto výsledků je patrné, že většina respondentů ukončila své vzdělání maturitou.

Graf 3 Vzdělání

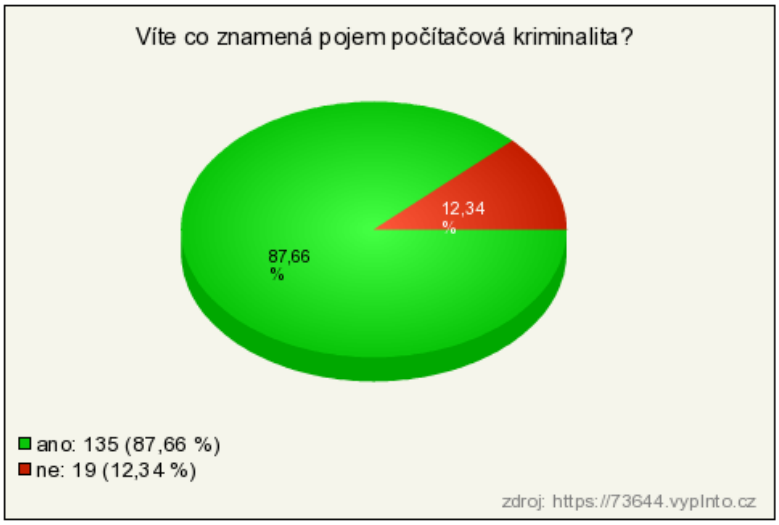


Otázka č. 4

Víte, co znamená pojem počítačová kriminalita?

Naprostá většina respondentů (87,66 %) odpověděla "ano", teda že tento pojem zná a ví co znamená, pouze menšina s 12,34 % tento pojem nezná.

Graf 4 Víte, co znamená pojem počítačová kriminalita?

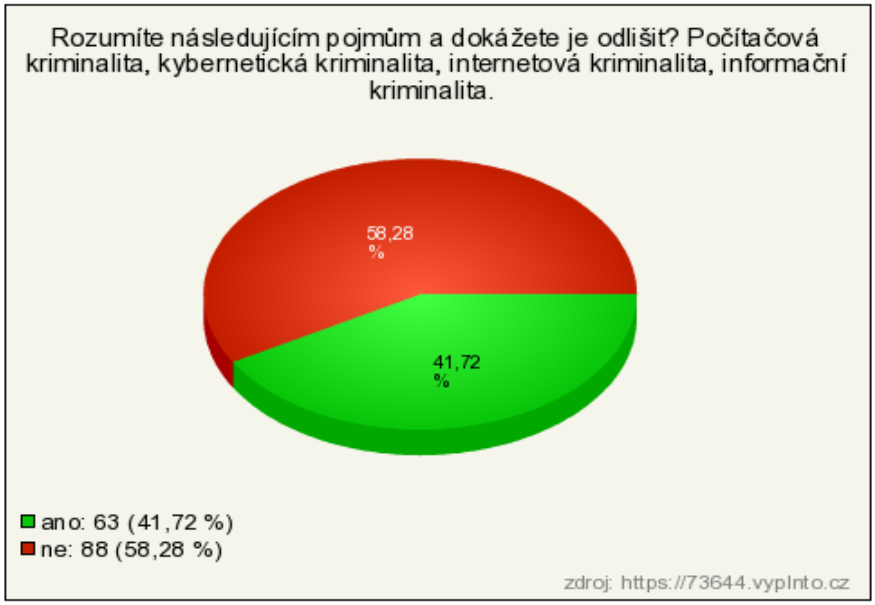


Otázka č. 5

Rozumíte následujícím pojmům a dokážete je odlišit? Počítačová kriminalita, kybernetická kriminalita, internetová kriminalita, informační kriminalita.

Nad poloviční většina respondentů (58,28 %) na tuto otázku odpověděla "ne", tzn. že tyto pojmy buď neznají, nerozumí jim či je nedokáží rozlišit. Zbylých 41,72 % dotázaných odpovědělo "ano", tedy ví, co tyto pojmy znamenají a dokáží je rozlišit.

Graf 5 Rozumíte pojmům: počítačová kriminalita, kybernetická kriminalita, internetová kriminalita, informační kriminalita.

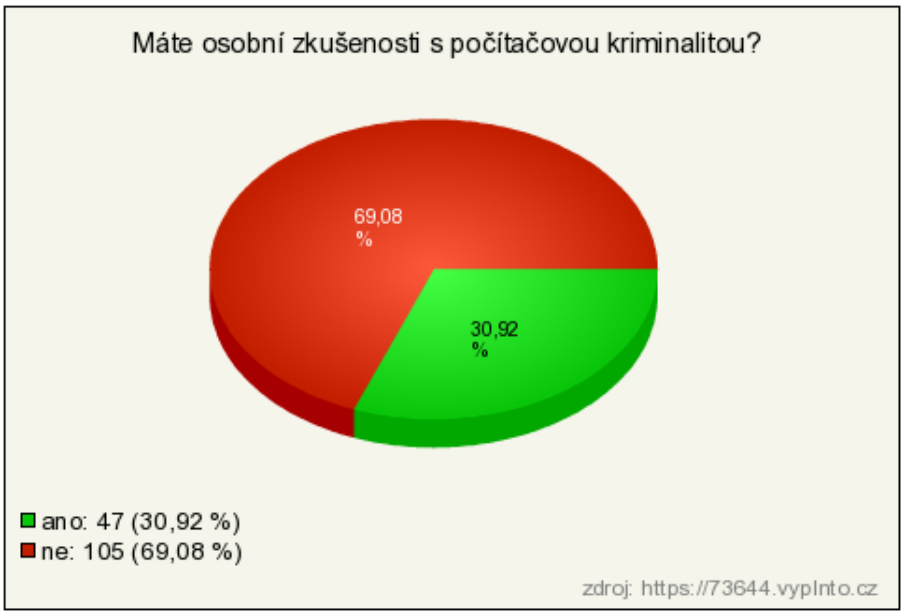


Otázka č. 6

Máte osobní zkušenosti s počítačovou kriminalitou?

Většina respondentů (69,08 %) odpověděla "ne", tedy nemají osobní zkušenost s počítačovou kriminalitou zaměřenou proti nim, pouze menšina (30,92 %) odpověděla, že tuto zkušenost mají.

Graf 6 Osobní zkušenost s počítačovou kriminalitou

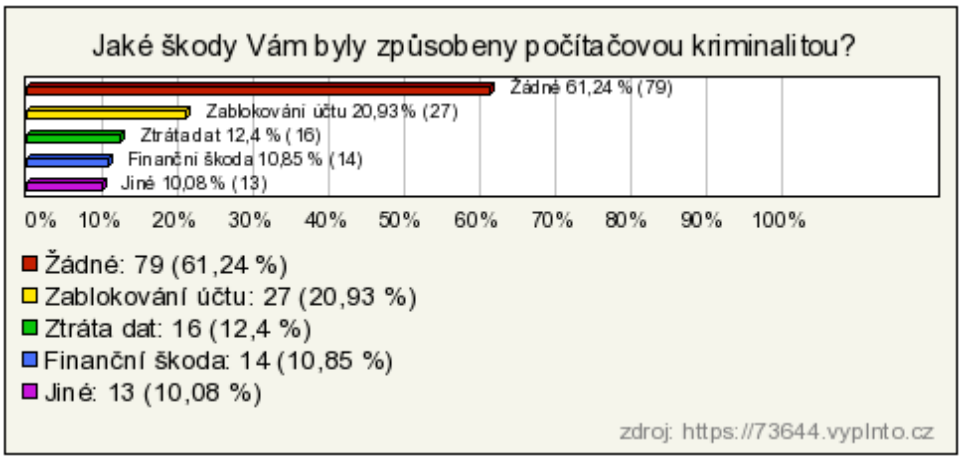


Otázka č. 7

Jaké škody Vám byly způsobeny počítačovou kriminalitou? (Respondenti mohli zvolit více z nabízených odpovědí.)

Počítačovou kriminalitou nebyly způsobeny žádné škody nad poloviční většině (61,24 %) dotazovaných. Dalším 38,76 % respondentům byly způsobeny škody jako zablokování účtu (20,93 %), ztráty dat (12,4 %), finanční škody (10,85 %) nebo jiné škody (10,08 %).

Graf 7 Jaké škody Vám byly způsobeny počítačovou kriminalitou

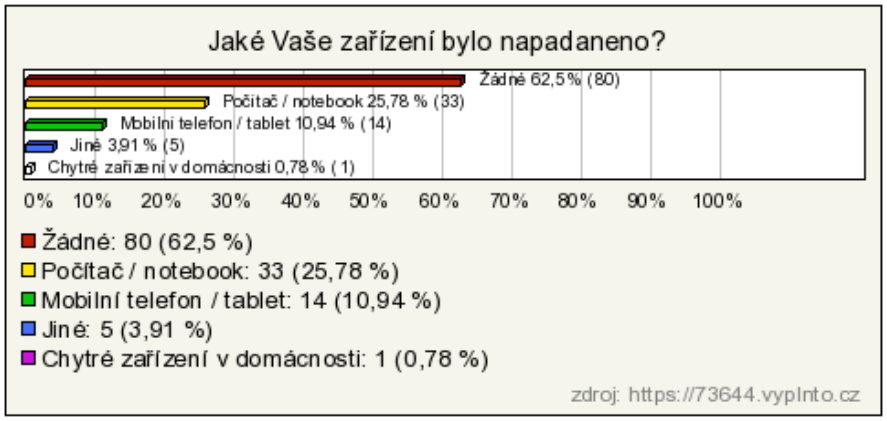


Otázka č. 8

Jaké Vaše zařízení bylo napadeno? (Respondenti mohli zvolit více z nabízených odpovědí.)

Většině respondentů (62,5 %) nebylo napadeno žádné zařízení. Ve zbylých 37,5 % případů byly napadeny počítač / notebook (25,78 %) a mobilní telefon / tablet (10,94 %), chytré zařízení v domácnosti bylo napadeno v 0,78 % a jiné zařízení v 3,91 %).

Graf 8 Jaké Vaše zařízení bylo napadeno

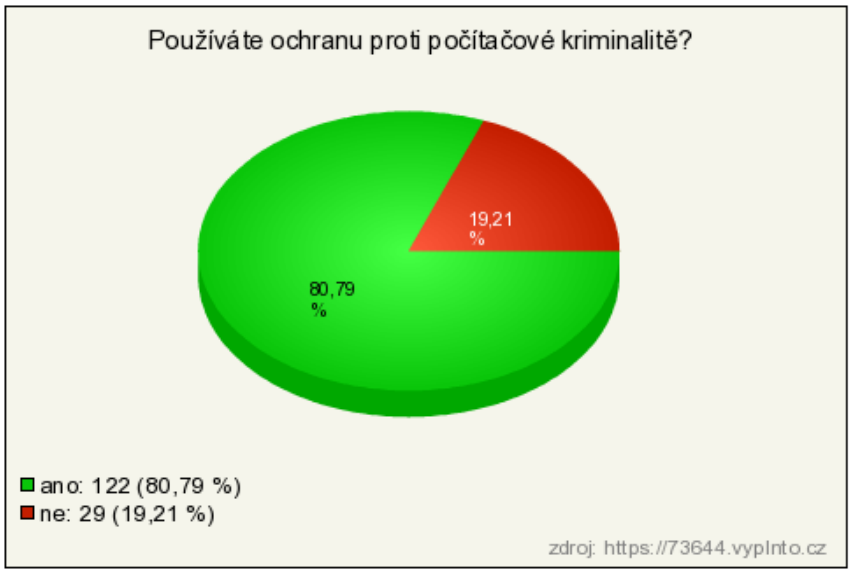


Otázka č. 9

Používáte ochranu proti počítačové kriminalitě?

Na otázku, zda dotázaní používají nějakou ochranu proti počítačové kriminalitě, uvedla majoritní skupina (80,79 %) "ano", pouze 19,21 % respondentů uvedlo, že "ne", tedy že žádnou ochranu nepoužívají.

Graf 9 Použití ochrany proti počítačové kriminalitě

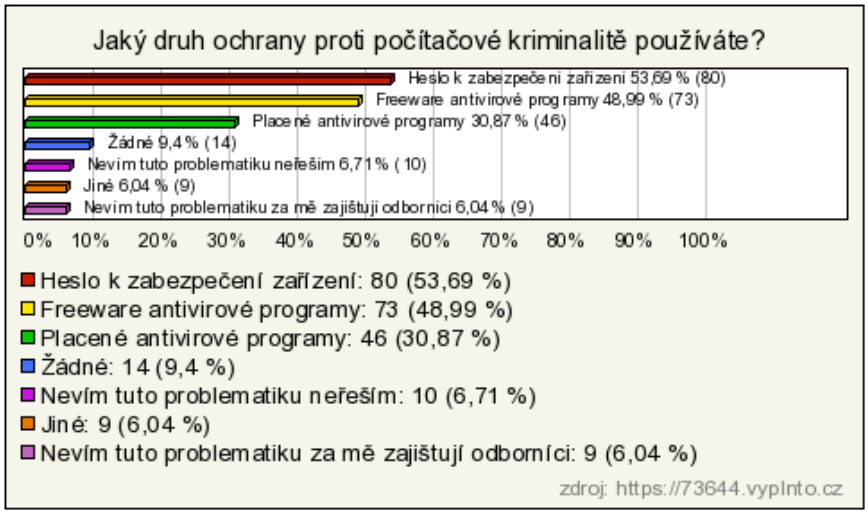


Otázka č. 10

Jaký druh ochrany proti počítačové kriminalitě používáte? (Respondenti mohli zvolit více z nabízených odpovědí.)

Jako druh zabezpečení respondenti nejvíce uváděli heslo k zabezpečení zařízení (53,69 %), freeware antivirové programy (49,99 %) a placené antivirové programy (30,87 %). Někteří respondenti (12,75 %) také uvedli, že neví a že tuto problematiku neřeší (6,71 %) nebo ji někdo řeší za ně (6,04 %). Zbylých 15,44 % odpovědí uvádí, že používají jiný druh ochrany (6,04 %) nebo žádný (9,4 %).

Graf 10 Druhy ochrany proti počítačové kriminalitě

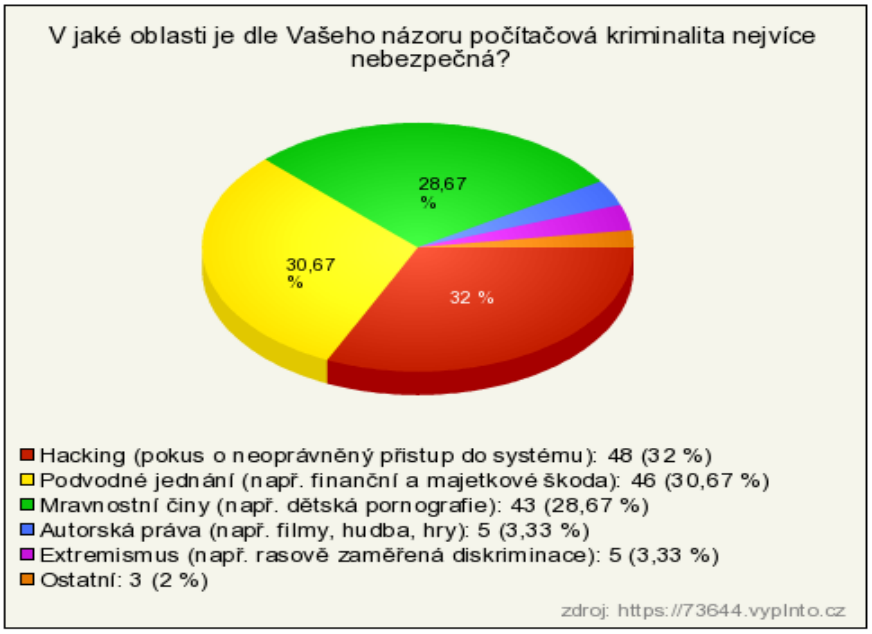


Otázka č. 11

V jaké oblasti je dle Vašeho názoru počítačová kriminalita nejvíce nebezpečná?

Jako nejvíce nebezpečnou počítačovou kriminalitu respondenti uváděli hacking (32 %), podvodné jednání (30,67 %) a mravnostní činy (28,67 %). Naopak jako nejméně nebezpečná uvedli autorská práva (3,33 %), extremismus (3,33 %) a ostatní (2 %).

Graf 11 Nejnebezpečnější oblasti počítačové kriminality



Otázka č. 12

Jaký je podle Vašeho názoru nejškodlivější malware (škodlivý program)?

Respondenti uvedli jako nejškodlivější malware viry (32,14 %) a phishing (25,71 %). Méně častěji uváděli jako nejškodlivější malware rootkit (15,71 %), spyware (12,14 %) a ransomware (11,43 %). Nejméně krát označili adware (2,86 %).

Graf 12 Nejškodlivější malware

Otázka č. 13

Měl by stát více aktivněji přispívat k potírání počítačové kriminality?

Celkem 78,47 % respondentů uvedlo, že by měl stát být aktivnější a více přispívat k potírání počítačové kriminality. Pouze zbylých 21,53 % respondentů si myslí, že momentální stav je dostačující.

Graf 13 Požadovaná aktivita státu na potírání počítačové kriminality

Otázka č. 14

Které z níže uvedených návrhů by přispěly nejvíce k snížení počítačové kriminality?

Na tuto otázku odpovědělo 43,45 % respondentů, že k snížení počítačové kriminality by nejvíce přispěla lepší spolupráce na mezistátní a celosvětové úrovni při objasňování počítačové kriminality za účelem dopadení pachatelů, 23,45 % dotázaných uvedlo vyšší tresty pro pachatele a 16,55 % lepší zákony na ochranu uživatelů internetu. Zbylých 16,55 % uvádí, že by pomohla lepší činnost policie (4,83 %) anebo jiné (11,72 %) návrhy.

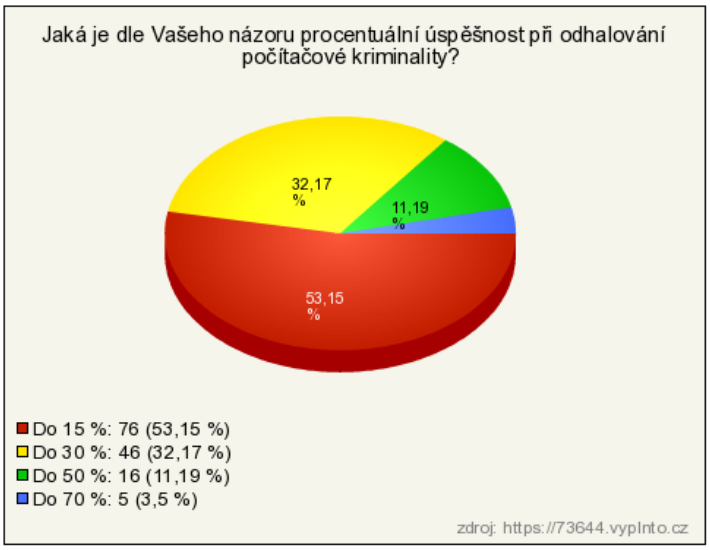
Graf 14 Návrhy k snížení počítačové kriminality

Otázka č. 15

Jaká je dle Vašeho názoru procentuální úspěšnost při odhalování počítačové kriminality?

Nejčastěji respondenti uváděli, že úspěšnost odhalování počítačové kriminality je do 15 %. Tuto odpověď uvedlo 53,15 % dotázaných, 32,17 % dotázaných se domnívá, že jich je odhaleno 30 %. Naopak nejméně respondentů se domnívá, že objasněnost je maximálně do 50 % (11,19 %) a nejméně pak, že objasněnost je do 70 % (3,5 %).

Graf 15 Úspěšnost při odhalování počítačové kriminality



Otázka č. 16

Měli byste zájem získávat pravidelné informace o nových hrozbách počítačové kriminality a možných způsobů ochrany ze stránek spravovaných státem?

Na otázku, zda by respondenti měli zájem získávat pravidelné informace o hrozbách počítačové kriminality ze stránek spravovaným státem, se respondenti rozdělili na dvě stejně početné skupiny – pro "ano" i pro "ne" se vyjádřilo 50 % respondentů.

Graf 16 Zájem o pravidelné informace od státu

Otázka č. 17

Měl by stát poskytovat ochranu proti počítačové kriminalitě formou bezplatného softwaru?

Zda by měl stát poskytovat bezplatnou ochranu proti počítačové kriminalitě, respondenti většinou odpověděli „ano zcela zdarma“ (59,59 %) a zbytek respondentů (40,41 %) uvedlo „ne, stát by se neměl angažovat“.

Graf 17 Poskytování bezplatného softwaru státem

4.3 Shrnutí výzkumného šetření

Dotazníkového šetření se zúčastnilo 155 respondentů, z toho 83 % byli respondenti do čtyřiceti let věku, v 84 % případů se jednalo o respondenty jejichž vzdělání bylo ukončeno maturitou nebo měli vysokoškolské vzdělání. Muži byli zastoupeni v 62 % a ženy v 38 %.

Pojem počítačová kriminalita znalo 88 % respondentů, ale v pojmech jako je kybernetická, internetová či informační kriminalita se přesně orientuje pouze 41 % respondentů. Osobní zkušenost s počítačovou kriminalitou mělo 31 % respondentů. Škody, které vznikly respondentům, měly především podobu zablokování účtu a to u 21 % respondentů, ztrátou dat bylo postiženo 12 % respondentů, finanční škoda vznikla 11 % respondentů, jiné škody pak zaznamenalo 10 % respondentů. Kromě počítačů a notebooků, které byly napadeny u 26 % respondentů, byly napadeny u 11 % i mobilní telefony a tablety. Je zajímavé, že téměř 5 % respondentů uvedlo napadení jiných, respektive chytrých zařízení

v domácnosti. Dále bylo zjištěno, že relativně málo respondentů svá zařízení chrání přístupovým heslem, konkrétně se jednalo o 53 % respondentů. Za uspokojivější pak lze uvést použití antivirových programů (freeware nebo placený), které používá celkem 80 % respondentů. Bohužel 16 % respondentů problematiku ochrany proti počítačové kriminalitě neřeší žádným způsobem. Jako nejvíce nebezpečnou oblast počítačové kriminality respondenti vnímají neoprávněné přístupy do systému a to v 32 %, podvodné jednání v 30 % a mravnostní činy v 28 %. Pouze 3 % respondentů uvedlo, že vnímají nebezpečí v porušování autorských práv a 3 % vnímá nebezpečí v extremismu. Za nejškodlivější programy považují respondenti viry a to v 32 %, následovaly podvodné stránky (phishing) s 26 %, neoprávněné získávání přístupových práv (rootkit) v 16 %, shromažďování informací (spyware) v 12 %, ransomware v 11 % a softwary pro šíření reklamy a ostatní pak tvoří 3 % z odpovědí dotázaných.

Respondenti se rovněž domnívají, že by se stát měl aktivněji podílet na potírání počítačové kriminality. Jedná se o názor 78 % respondentů. Ke snížení kriminality by dle 43 % respondentů nejvíce přispěla lepší spolupráce na mezinárodní a celosvětové úrovni při objasňování případů za účelem dopadení pachatelů. Vyšší tresty by pomohly v boji s počítačovou kriminalitou podle názoru 23 % respondentů, 16 % respondentů si myslí, že by pomohla kvalitnější legislativa, 5 % respondentů by ocenilo lepší činnost policie, jiné blíže nespecifikované návrhy pak uvedlo 13 % respondentů.

Respondenti si uvědomují v 53 %, že procentuální úspěšnost odhalení páchání počítačové kriminality je velmi nízká.

Respondenti avizovali 50 % zájem o pravidelné informace o nových hrozbách a možných způsobech ochrany, které by byly dostupné na bezplatných stránkách spravovaných státem. Přičemž 59 % respondentů se domnívá, že softwarová podpora by měla být státem poskytována bezplatně všem zájemcům.

5 Závěr

Pomocí této práce, která měla za cíl zpracovat téma počítačové kriminality z pohledu historie a současnosti a dále pak vysvětlit pojmy vážící se k této problematice, popsat jednotlivé typy počítačové kriminality v návaznosti na současnou legislativu a představit možné způsoby ochrany, jsem došel k následujícím závěrům.

Počítačovou kriminalitou je trestná činnost, která je páchána prostředky výpočetní techniky. K celosvětovému rychlému rozvoji počítačové kriminality pak přispěly dvě zásadní okolnosti, a to masivní rozvoj (dostupnost) osobních počítačů a vznik počítačových sítí, tedy vzdálený přístup k počítačům. V České republice se poprvé objevila v 70. letech minulého století, ale až v letech 1991–1992 dochází v ČR k nezbytným právním úpravám především trestního zákona.

Z kriminalistického pohledu je informační a počítačová kriminalita relativně novým oborem. Její rychlý rozvoj umožňují především tři okolnosti, a to malá počítačová gramotnost uživatelů, obrovský nárůst uživatelů různých informační a komunikační technologie a jejich závislost na internetu, a také skutečnost, že kyberkriminalita se stala výnosným globálním businessem s nízkou mírou odhalení pachatelů.

Z charakteru počítačové kriminality pak vyplývá, že bojovat s ní nemohou jednotlivé státy pouze osamoceně. Problematiku počítačové kriminality z pohledu trestních norem začala řešit Organizace pro hospodářskou spolupráci a rozvoj (OECD). Později pak Rada Evropy, která v roce 2001 vytvořila budapešťskou Úmluvu o počítačové kriminalitě, která u nás vstoupila v platnost od 1. prosince 2013 (dále jen „Úmluva“). Úmluva jakožto mezinárodní smlouva je univerzálním předpisem, který zakotvuje pro signatářské státy závazky nejen hmotného, ale i procesního charakteru.

Členské státy Úmluvy se v této souvislosti domluvily na definičním členění trestných činů, které mají být členskými státy kriminalizovány. Jedná se o trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů (neoprávněný přístup, neoprávněné zachycení informací, zásah do dat, zásah do systému, zneužití zařízení), trestné činy související s počítači (falšování údajů souvisejících s počítači, podvod související s počítači), trestné činy související s obsahem, zejména s dětskou pornografií a trestné činy související s porušením autorského práva.

Pachatelé počítačové kriminality jsou většinou středoškolsky nebo vysokoškolsky vzdělaní jedinci se zaměřením na informační technologie, bývají nadprůměrně inteligentní, vynalézaví, a v programátorské oblasti velice zdatní, což jejich dopadení a usvědčení činí velice obtížným.

Pro jejich usvědčení je důležité zachycení a důkladné analyzování tzv. digitální stopy. Tuto stopu teoreticky zanechává každá osoba, která je aktivní na počítači nebo na obdobném zařízení. Jedná se o jakýsi virtuální podpis. Věda, která se zabývá vyhledáváním, obnovením

a zachováním digitálních stop a důkazů, se nazývá *počítačová forenzika* (z angl. computer forensic).

V souvislosti s pácháním počítačové kriminality jsou využívány i standartní vyšetřovací metody, mezi které patří domovní prohlídky, prohlídky jiných prostor, ohledání místa činu, zajištění a šetření obsahu výpočetní techniky a výslech obviněného.

Rozvoj a dostupnost informačních a komunikačních technologií vede k masivnímu propojování různých počítačových systému do kyberprostoru. Lze tvrdit, že čím více je připojených zařízení, tím větší je jejich zranitelnost a tím roste i počet útoků a závažnost trestných činů.

Z teoretické části práce vyplývá, že k potírání kyberkriminality je třeba nejen zajistit, aby právní dokumenty, které přispívají k ochraně společnosti před kyberkriminalitou, mezi které patří bezesporu Úmluva o kyberkriminalitě a další dokumenty EU, a které vznikají z důvodu potřeby harmonizace právních úprav členských států, držely svými novelizacemi krok s rozvojem kyberkriminality, ale zejména předcházely vzniku podmínek pro páchání této činnosti a to nejen rozvojem nových ochranných systémů, ale rovněž, a to zejména, i zvyšováním gramotnosti uživatelů počítačových systémů.

Praktickou část práce, ve které jsem se snažil využít teoretických poznatků, jsem formou dotazníkového šetření zacílil na získání aktuální poznatků o gramotnosti uživatelů v oblasti počítačové kriminality. Dotazníkové šetření, které jsem provedl, a kterého se zúčastnilo 155 respondentů převážně se středoškolským a vysokoškolským vzděláním a věkem do čtyřiceti let, avizovalo několik podnětných postřehů a statistických zjištění. Jedná se především o 31 % respondentů, kteří mají osobní zkušenost s počítačovou kriminalitou, a to zejména v podobě zablokování účtu v 21 %. Ztrátou dat bylo dále postiženo 12 % respondentů, finanční škoda vznikla 11 % respondentů, jiné škody pak zaznamenalo 10 % respondentů. Kromě počítačů, notebooků, mobilních telefonů a tabletů se začínají objevovat i případy počítačové kriminality páchané na chytrých zařízeních v domácnostech, což uvedlo 5 % respondentů. Z mého pohledu je však opravdu alarmující nízký počet respondentů, kteří chrání svá zařízení přístupovým heslem. Jednalo se o pouhých 53 % respondentů. Antivirový program (freeware nebo placený) používá celkem 80 % respondentů, ale bohužel 16 % respondentů problematiku ochrany proti počítačové kriminalitě neřeší žádným způsobem. Jako nejvíce nebezpečnou oblast počítačové kriminality respondenti vnímají neoprávněné přístupy do systému a to v 32 %, podvodné

jednání v 30 % a mravnostní činy v 28 %. Za nejméně nebezpečnou považují respondenti počítačovou kriminalitu páchanou v oblasti porušování autorských práv (3 %) či extremismu (3 %). Za nejškodlivější programy považují respondenti viry a to v 32 %, následovaly podvodné stránky (phishing) v 26 %, neoprávněné získávání přístupových práv (rootkit) v 16 %, shromažďování informací (spyware) v 12 %, ransomware v 11 % a softwary pro šíření reklamy a ostatní pak tvoří 3 % z odpovědí respondentů. Podle názorů respondentů, by se na potírání počítačové kriminality měl aktivněji podílet stát. Jedná se o názor 78 % respondentů. Ke snížení kriminality by dle 43 % respondentů nejvíce přispěla lepší spolupráce na mezinárodní a celosvětové úrovni. Vyšší tresty by pomohly v boji s počítačovou kriminalitou podle názoru 23 % respondentů, 16 % respondentů si myslí, že by pomohla lepší legislativa, 5 % respondentů by ocenila lepší činnost policie, jiné blíže nespecifikované návrhy pak uvedlo 13 % respondentů. Respondenti si uvědomují v 53 %, že procentuální úspěšnost odhalení páchání počítačové kriminality je velmi nízká. Zajímavé je i zjištění, že 50 % respondentů avizovalo zájem o pravidelné informace o nových hrozbách a možných způsobech ochrany, které by byly dostupné na bezplatných stránkách spravovaných státem. Přičemž 59 % respondentů se domnívá, že softwarová podpora by měla být státem poskytována bezplatně všem zájemcům. S tímto názorem se pak v samém závěru ztotožňuji i já osobně.

6 Seznam použitých zdrojů

6.1 Seznam použité literatury

1. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 30. ISBN 978-80-247-1561-2
2. BRITZ, Marjie. *Computer forensics and cyber crime: an introduction*. 3. vyd. Boston: Pearson, 2013, ISBN 978-0-13-267771-4
3. GŘIVNA, Tomáš a POLČÁK, Radim. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008. ISBN 9788090378674.
4. GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana a kol. *Kriminologie*. 5. aktualizované vydání. Praha: Wolters Kluwer, 2019, ISBN 978-80-7598-554-5.
5. HOLT, Thomas J.; BOSSLER, Adam M.; SEIGFRIED-SPELLAR, Kathryn C. *Cybercrime and digital forensics: an introduction*. 2. vydání. London: Routledge, 2018, ISBN 978-1-138-23873-2.
6. JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 3. aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, 242 s. ISBN 978-80-7251-436-6.
7. KREMLING, Janine; PARKER, Amanda M. Sharp. *Cyberspace, cybersecurity, and cybercrime.* Thousand Oaks: SAGE Publications, 2017, ISBN 978-15-063-4725-7.
8. LEŠČINSKÝ, Jan. K trestněprávnímu postihu počítačové sabotáže. *Trestněprávní revue*: C.H. Beck, 2002, roč. 2002, č. 04, ISSN 1213-5313.
9. McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. ISBN 0313339740.
10. POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, ISBN 978-80-7598-045-8.
11. POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, Právnická fakulta, 2016.
12. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, ISBN 978-80-7380-720-7.
13. SMEJKAL, Vladimír; SOKOL, *Tomáš. K možnostem postihu útoků DoS/DDoS v rámci českého právního řádu.* Data security management. 2013, ISSN 1211-8737.

14. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012. ISBN 9788074004285.
15. ŠÁMAL, Pavel a kol. *Trestní právo hmotné*. 8. přepracované vydání. Praha: Wolters Kluwer, 2016, ISBN 978-80-7552-358-7.
16. Trestní zákoník č.40/2009 Sb., ve znění pozdějších předpisů
17. VÁLKOVÁ, Helena; KUCHTA, Josef; HULMÁKOVÁ, Jana a kol. *Základy kriminologie a trestní politiky.* 3. vydání. Praha: C.H. Beck, 2019, ISBN 978-80-7400-732-3.
18. ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, ISBN 978-80-7552-758-5.

6.2 Seznam použitých internetových zdrojů

1. *Elektronické důkazy – současnost či budoucnost českého soudnictví?* Rozhovor s prof. Ing. Vladimírem Smejkalem, CSc., LL.M. Česká advokátní komora: Bulletin Advokacie, publikováno 26. 10. 2012. Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-dukazy-soucasnost-ci-budoucnost-ceskeho-soudnictvi
2. GŘIVNA, Tomáš. *Soulad české právní úpravy s Úmluvou o kybernetické kriminalitě*. Dostupné z: http://www.europen.cz/Proceedings/32/Umluva%20o%20kybernetickе%20kriminalite.pdf
3. KOLOUCH, JAN. *CyberCrime*. Praha: CZ NIC, 2016. Dostupné z: https://news.microsoft.com/stories/cybercrime/
4. KOLOUCH, Jan; BAŠTA, Pavel a kol. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019, 560 s. ISBN 978-80-88168-34-8 Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf
5. Kompletní znění Úmluvy v českém překladu. Dostupnost: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0
6. KYNCL, Libor. IP adresa identifikuje místo připojení, nikoli osobu. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova universita, 2010. Dostupné z: https://www.law.muni.cz/dokumenty/12793

7. MUELLER, Robert. *RSA Cyber Security Conference.* 2012. Dostupné z: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
8. MUSIL, Stanislav. *Počítačová kriminalita*: Dostupné z: http://www.ok.cz/iksp/docs/256.pdf
9. *Ochrana před hrozbami na Internetu* [online]. Dostupné z: https://www.avast.com/
10. Dobiáš, Martin. *Počítačová kriminalita*. 2014. Dostupnost z: https://is.muni.cz/th/348441/pravf_m/DP_Pocitacova_kriminalita_FINAL.pdf
11. Předkládací zpráva vládního návrhu, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluvy o počítačové kriminalitě. Dostupné z: http://www.senat.cz/xqw/webdav/pssenat/original/66810/56264
12. RAK, Roman; PORADA, Viktor. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství*. 2005, roč. 17. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf
13. SCHNEIER, Bruce. Crime: *The Internet's Next Big Thing*. Dostupné z https://www.schneier.com/crypto-gram/archives/2002/1215.html
14. Stanoviska Evropského hospodářského a sociálního výboru. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.C_.2011.218.01.0130.01.CES
15. Úmluva Rady Evropy ze dne 23. listopadu 2001 o počítačové kriminalitě, čl. 2. Český překlad – Sbírka mezinárodních smluv: Dostupné z: https://www.epravo.cz/_dataPublic/sbirky/2013/sb0056-2013m.pdf

7 Příloha – dotazník

Dotazník

Dobrý den, jsem studentem 3. ročníku vysoké školy, oboru Informatika a obracím se na Vás s prosbou o vyplnění níže uvedeného dotazníku, který je zaměřen na problematiku počítačové kriminality. Výsledek tohoto dotazníkového šetření bude součástí bakalářské práce, jejímž cílem přispět k potlačení počítačové kriminality podnětnými návrhy. Dotazník je anonymní, nezjišťuje správné či chybné odpovědi, ale slouží pouze ke zjištění Vašich názorů. Předem děkuji za vyplnění dotazníku.

Otázky 1,2,3 jsou povinné. U otázek 7, 8, 10 je možnost odpovědět na jednu či více odpovědí.

1. Jste?

- ☐ Muž
- ☐ Žena

2. Patříte do věkové skupiny:

- ☐ Do 20 let
- ☐ Od 20-40 let
- ☐ Od 40-60 let

3. Vzdělání

- ☐ Maturita
- ☐ Vysokoškolské
- ☐ Základní

4. Víte, co znamená pojem počítačová kriminalita?

- ☐ ano
- ☐ ne

5. Rozumíte následujícím pojmům a dokážete je odlišit? Počítačová kriminalita, kybernetická kriminalita, internetová kriminalita, informační kriminalita.

- ☐ ano
- ☐ ne

6. Máte osobní zkušenosti s počítačovou kriminalitou?

- ☐ ano
- ☐ ne

7. Jaké škody Vám byly způsobeny počítačovou kriminalitou?

- ☐ Finanční škoda
- ☐ Jiné
- ☐ Zablokování účtu
- ☐ Ztráta dat
- ☐ Žádné

8. Jaké Vaše zařízení bylo napadeno?

- ☐ Mobilní telefon / tablet
- ☐ Počítač / notebook
- ☐ Žádné

9. Používáte ochranu proti počítačové kriminalitě?

- ☐ ano
- ☐ ne

10. Jaký druh ochrany proti počítačové kriminalitě používáte?

- ☐ Freeware antivirové programy
- ☐ Heslo k zabezpečení zařízení
- ☐ Nevím tuto problematiku neřeším
- ☐ Placené antivirové programy
- ☐ Žádné

11. V jaké oblasti je dle Vašeho názoru počítačová kriminalita nejvíce nebezpečná?

- ☐ Hacking (pokus o neoprávněný přistup do systému)
- ☐ Mravnostní činy (např. dětská pornografie)
- ☐ Podvodné jednání (např. finanční a majetkové škoda)

12. Jaký je podle Vašeho názoru nejškodlivější malware (škodlivý program).

- ☐ Phishing (podvodné stránky či emaily, které se pokoušejí zjistit vaše citlivé informace)
- ☐ Ransomware (omezuje uživateli přistup k systému či souborům)
- ☐ Rootkit (k získávání přístupových práv administrátora bez vašeho vědomí)
- ☐ Spyware (shromažďuje informace o vašem chování na internetu)
- ☐ Viry (pokoušejí se získat kontrolu nad systémem a následně spáchat co největší škody)

13. Měl by stát více aktivněji přispívat k potírání počítačové kriminality?

- ☐ ano
- ☐ ne

14. Které z níže uvedených návrhů by přispěly nejvíce k snížení počítačové kriminality?

- ☐ Jiné
- ☐ Lepší spolupráce na mezistátní a celosvětové úrovni při objasňování počítačové kriminality za účelem dopadení pachatelů
- ☐ Lepší zákony na ochranu uživatelů internetu
- ☐ Vyšší tresty pro pachatele (např. propadnutí majetku)

15. Jaká je dle Vašeho názoru procentuální úspěšnost při odhalování počítačové kriminality?

- ☐ Do 15 %
- ☐ Do 30 %
- ☐ Do 50 %

16. Měli byste zájem získávat pravidelné informace o nových hrozbách počítačové kriminality a možných způsobů ochrany ze stránek spravovaných státem?

- ☐ ano
- ☐ ne

17. Měl by stát poskytovat ochranu proti počítačové kriminalitě formou bezplatného softwaru?

- ☐ Ano (zcela zdarma)
- ☐ Ne, stát by se neměl angažovat