VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA A JEJÍ PŘÍČINY

Autor práce: Filip Kabát

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Prezenční

Vedoucí práce: doc. JUDr. Roman Svatoš, Ph.D.

Katedra: Katedra právních oborů a bezpečnostních studií

2016

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucímu bakalářské práce doc. JUDr. Romanu Svatošovi, Ph.D., za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

KABÁT F. *Počítačová kriminalita a její příčiny: Bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, o. p. s., 2016. 57 s. Vedoucí bakalářské práce: doc. JUDr. Roman Svatoš, Ph.D.

Klíčová slova: počítačová kriminalita, příčiny, internet, počítač, kybernetický útok, pachatel, kyberprostor

Počítače a internet jsou využívány velkou částí populace ke každodenním účelům. Jejich progresivní vývoj je rychlý a spolu s nimi se vyvíjí i počítačová kriminalita, která může ohrožovat každého uživatele využívajícího internet. V práci budou analyzovány nejčastější formy této kriminality, fenomenologie počítačové kriminality, její pachatelé a historický i předpokládaný vývoj. Vše bude analyzováno podle důvěryhodných internetových zdrojů a literatury, které je na toto téma dostatek. Dále bude provedena analýza statistických dat počítačové kriminality.

ABSTRACT

KABÁT, F. *Cybercrime ant its causes: Bachelor thesis.* České Budějovice: The College of European and Regional Studies, 2016. 57 p. Supervisor: doc. JUDr. Roman Svatoš, Ph.D.

Key words: cybercrime, causes, internet, computer, cybber-attack, perpetrator, cyberspace

Computers and internet are used by large part of the population to daily routines. Progression of computers is fast and real problem called cybercrime develops with it. Cybercrime potentially threatens each user of internet. This bachelor thesis contains the analysis of common types of cybercrime, cybercrime phenomenology, its perpetrators and historical and expected development. All objects will be analyzed by trusted internet sources and literature that has been written plenty for this topic. That will be followed by analysis of statistical cybercrime data.

Obsah

Úvod

V dnešní době už jsou počítače a internet používány velkou částí populace, a to pro každodenní účely. Často to jsou např. obchodní služby, získávání informací z nejrůznějších oblastí, hraní počítačových her, používání aplikací nebo komunikace s přáteli atd. Informační technologie jsou dnes už neoddělitelnou součástí dnešního světa a umožňují lidem snadnější vykonávání některých úkonů, a to z pohodlí domova. Počítačový svět spolu se snadnějším životem přináší i novou formu kriminality, která se zdá být v určitém směru také pohodlnější, stejně jako některé každodenní úkony může být i tato nová forma kriminality vykonávána snadněji, anonymně a odkudkoliv.

Počítačová kriminalita, kybernetická kriminalita neboli kybernalita je relativně novým problémem, v simplifikované definici se jedná o protiprávní jednání, které má souvislost s počítači.[1] Tato kriminalita zahrnuje široké spektrum možností, od útoku na určitou osobu nebo krádeže její identity až po ohrožení národní bezpečnosti. Odhadovaná celosvětová škoda, kterou počítačová kriminalita ročně způsobí, je 450 miliard dolarů,[2] což je více než celosvětový roční zisk z drogového obchodu, značné procento této škody je na úkor firem v důsledku porušování duševního vlastnictví.

[1] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 3.
[2] SAUNDLE P. *Cyber crime costs global economy $445 billion a year*. [online]. REUTERS, 2014 [cit. 2015-12-30]. Dostupné z: <http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609>.

1 Cíl a metodika bakalářské práce

Tato bakalářská práce je zaměřena na relativně novou počítačovou kriminalitu. Cílem této práce je objasnit problematiku, kterou tento druh kriminality přináší. Nejdříve se ale zaměřuje na důkladné vymezení základních pojmů jako nezbytně nutných znalostí k pochopení této problematiky. V pozdějších kapitolách budou rozebrány hlouběji některé druhy této kriminality, pachatelé, konkrétně společné znaky pachatelů a rozdělení pachatelů. V poslední části práce bude obsažen historický a předpokládaný vývoj až do roku 2020.

Hlavním cílem bakalářské práce je objasnit základní pojmy jako počítač, kyberprostor, kybernetický útok a zejména pojem počítačová kriminalita. Dále objasnit příčiny této kriminality, analyzovat nejčastější nelegální konání proti počítačům nebo páchané na počítači nebo prostřednictvím počítače a zpracovat fenomenologii počítačové kriminality. Počítačová kriminalita je vzhledem ke svému věku paradoxně rozmanitá a rozebírat podrobně všechny známé podoby této kriminality by bylo náročné a obsahově rozsáhlé, proto vzhledem k této rozmanitosti nebude bakalářská práce obsahovat a analyzovat všechny známé typy, ale bude zaměřena jen na ty, které se aktuálně vyskytují nejčastěji.

Pachatelé této kriminality usilují hlavně o zisk nebo zabezpečená data. Často bývají odborníky v oboru a může být náročné některé pachatele odhalit. Jiní můžou být zase obyčejní lidé, kteří si stáhli autorsky chráněné dílo, případně i nevědomě sdílí jeho obsah přes různé programy. V další části této práce, kde budou rozebíráni pachatelé počítačové kriminality, budou vynechány zdlouhavé metody k jejich odhalení a tato kapitola bude zaměřena spíše na jejich společné znaky a rozdělení.

Fenomenologie počítačové kriminality bude zaměřena na trestné činy § 230 zákona číslo 40/2009 Sb., trestní zákoník ve znění pozdějších právních přepisů (dále jen „trestní zákoník“ nebo „TZ“) – neoprávněný přístup k počítačovému systému a nosiči informací, § 231 TZ – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a § 232 TZ – poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti. Bude zde proveden rozbor jejich skutkových podstat a analýza dat z policejních statistik za posledních pět let.

Vzhledem k prudkému a krátkodobému vývoji výpočetní techniky a s tím i počítačové kriminality nás pravděpodobně ani v budoucnosti nečeká nic příjemného. Počítačové komponenty se stávají menšími a výkonnějšími, internet se zrychluje a uživatelé jsou schopni stahovat a odesílat čím dále větší množství dat v kratších časových intervalech. Bohužel se rychle zdokonaluje i kriminalita v této oblasti. Počítačová kriminalita je moderní a existuje zde relativně krátkou dobu. Napříč tomu už napáchala obrovské škody, a proto je důležitý její historický vývoj jakožto pomocník při předpokládaní budoucích dopadů této kriminality. V poslední části bude práce zaměřena na historický a předpokládaný vývoj počítačové kriminality.

Všechny cíle této bakalářské práce budou analyzovány a vyhodnocovány pomocí odborné literatury, důvěryhodných internetových zdrojů a statistik. Literatura o počítačové kriminalitě je snadno dostupná jak v anglickém tak i v českém jazyce a pro účely této práce budou využity obě uvedené varianty.

2 Počítače a internet – pojem a charakteristika

2.1 Internet

Internet je celosvětová počítačová síť, která se za posledních 15 let mimořádně rozvinula. Rozrůstá se obsahově, geograficky, rychlostně i množstvím uživatelů. V dnešní době je internet tím nejrychlejším a jednoznačně nejobsáhlejším zdrojem informací na celém světě. Každý uživatel, který má přístup k internetu, si může během několika sekund najít různé informace z téměř jakéhokoliv oboru. Počet lidí s přístupem k internetu roku 2000 dosáhl 390 mil. uživatelů. V roce 2015 počet uživatelů internetu vzrostl už na 3 miliardy,[3] tzn., že internet nyní používá zhruba 42% populace a předpokládá se, že počet uživatelů bude značně růst i dále. S ohledem na velký vzrůst počtu lidí s možností připojení k internetu není divu, že se spolu s nimi rozrůstá i velký problém a to je relativně nová forma kriminality páchána ve virtuálním počítačovém světě, který nazýváme kyberprostorem (viz. kapitola 2.3). Internet není nikým vlastněn ani řízen, ale je třeba ho určitým způsobem udržovat a organizovat. K tomuto účelu slouží nadnárodní organizace, např. ICANN a IANA.[4]

2.1.1 Aktivita lidí na internetu v ČR[5]

- Mladí lidé **(16–19 let)** – vyrůstají s internetem a nerozlišují hranici mezi světem online a offline. Často mívají internet v mobilech a mají ho neustále sebou. Internet je pro ně především místem zábavy, komunikace a (postupem času) také důležitou pomocí při studiu.

- Starší uživatelé **(19–29 let)** - považují internet za přirozenou součást svého života. Na rozdíl od mladších uživatelů však ve většině případů internet používají bezpečněji a rozumněji. Na sociálních sítích jsou tito lidé skoro ve stejné míře jako generace předchozí (16-19 let). Někde na pomezí lidí ve věku **30–44 let** už lze najít velké rozdíly ve využívání internetu.

- U starších lidí **(45-65 let)** se často objevuje nedůvěra k internetu.

[3] *Internet Users* [online]. internet live stats, 2015 [cit. 2015-12-30]. Dostupné z: <http://www.internetlivestats.com/internet-users/>.
[4] *Co je to Internet a jak funguje?* [online]. Datacentrum WEDOS, 2010 [cit. 2015-11-10]. Dostupné z: <http://datacentrum.wedos.com/a/17/co-je-internet-jak-funguje.html>.
[5] ECKERTOVÁ, L a DOČEKAL, D. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. 1. vyd. Brno: Computer Press, 2013, s. 25.

2.2 Počítač

Počítač je v nejjednodušším slova smyslu stroj, který zpracovává data. To probíhá podle předem naprogramovaných instrukcí. Počítač se skládá z hardwaru a softwaru. Do hardwarové části patří všechno, co je fyzické. Základní komponenty hardwarové části jsou základní deska, procesor, operační paměť RAM, grafická karta, zdroj a pevný disk. Softwarová část se nazývá programovým vybavením. To je ta část počítače, která je nehmatatelná. Patří sem všechny programy, které určitý počítač používá.

Anglický matematik Charles Babbage (1791 - 1871) je často považován za tvůrce historicky prvního počítače. Už v roce 1834 navrhl programově řízený počítač, nazval ho analytický stroj. Koncepce tohoto stroje je podobná dnešním počítačům.[6]

2.3 Kyberprostor

Jak již bylo v úvodní kapitole naznačeno, dnešní společnost se stává na výpočetní technice často závislá. Tento druh technologií začíná pomalu nahrazovat mnohé činnosti v lidském životě a zároveň je velmi zjednodušuje. Dnes si již lidé mohou pomocí internetu okamžitě pořizovat většinu zboží, zjišťovat veškeré informace, komunikovat s ostatními a to vše přímo z pohodlí domova. Prostor, kde jsou všechny tyto informace uloženy, a úkony prováděny nazýváme kyberprostorem.

Jeho počátek by se dal zařadit do roku 1968, kdy bylo poprvé propojeno několik počítačů. Tím vznikla síť ARPANET,[7] která byla předchůdcem dnešního internetu. Nikdo tehdy nepředpokládal, že v budoucnosti se počítačový svět rozroste tak, jako je tomu dnes. Termín kyberprostor (cyberspace) definoval už v roce 1984 William Gibson ve své knize Neuromancer, a definoval jej následovně:

„Kyberprostor. Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům… grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat.“[8]

[6] *Charles Babbage* [online]. CharlesBabbage.net. 2013 [cit. 2016-01-23]. Dostupné z: <http://www.charlesbabbage.net/>.
[7] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 15.
[8] GIBSON, W. *Neuromancer*. New York: Ace Books, 1984, s. 31.

V současnosti však nejsou definice kyberprostoru úplně jednotné. Existuje mnoho definic a těžko bychom z nich vybírali tu nejvýstižnější. Původní definice kyberprostoru jsou na dnešní poměry neúplné a nepřesné a to z jednoduchého důvodu. Na počátku byl kyberprostor tvořen jen z několika málo propojených počítačů, které tehdy zdaleka neměly takový význam pro lidstvo jako dnes.[9] Dnes už jsou počítače využívány skoro polovinou populace. Kyberprostor se tak stále rozšiřuje a zasahuje do dalších sfér života lidí, proto se definice mění a rozšiřují také.[10]

2.4 Kybernetický útok

Počítačová kriminalita je odlišná od ostatních druhů kriminalit a to tím, že pachatel nemusí být přítomen na místě činu. U ostatních druhů kriminality pachatelé fyzicky napadají vyhlídnuté oběti, lžou nebo zatajují důležité informace, vloupávají se do objektů a často tak riskují snadné odhalení atd. Dnes, hlavně díky závislosti společnosti na výpočetní technice, pachatel tuto kriminalitu může páchat prakticky odkudkoliv a zcela anonymně. Ke spáchání takového útoku stačí pachateli vlastnit počítač s připojením k internetové síti a potřebné znalosti. Takový útok pomocí počítače nazýváme kybernetickým útokem.

Kybernetický útok je záměrné zneužívání počítačových systémů. Většinou se jedná o následující činnosti:[11]

- Krádež identity, podvod nebo vydírání pomocí počítače
- Odmítnutí služby (DoS a DDoS útoky)
- Malware, pharming, phishing, spam, spoofing a viry
- Zjišťování hesel
- Kyberšikana
- Pronikání do systémů
- Cyberwarfare

[9] KUŽEL, S. *Kybernetická kriminalita I: Co se děje v kyberprostoru* [online]. BusinessIT. 2015 [cit. 2015-06-04]. Dostupné z: <http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyber prostoru.php>.

[10] BRENNER, Susan W. Cybercrime: criminal threats from cyberspace. Santa Barbara, Calif.: Praeger, 2010, ix, s 9.

[11] *Cyberattack* [online]. techopedia. 2010 [cit. 2015-06-04]. Dostupné z: <http://www.techopedia.com/ definition/24748/cyberattack>.

2.5 Shrnutí a závěr kapitoly

V této kapitole byly objasněny některé základní pojmy. Jsou to pojmy internet, počítač, kyberprostor a kybernetický útok. Některé často se vyskytující formy počítačové kriminality neboli druhy kybernetických útoků budou blíže rozebrány v následující kapitole. Určitě by se sem dala zahrnout celá řada dalších pojmů, ale k pochopení této práce by tyto pojmy měly být dostatečné.

Kyberprostor a internet jsou v této práci uvedeny odděleně, ale vztah mezi nimi není úplně jednoznačný. Zda se jedná o synonyma, nebo o pojmy odlišné se dá určit z různých definic. David Hakken charakterizuje kyberprostor jako sociální arénu, do nichž vstupují sociální aktéři, kteří používají ke vzájemné interakci pokročilé informační technologie.[12] Internet je většinou definován jako celosvětová počítačová síť.

Z definic lze konstatovat, že internetem se myslí fyzická počítačová síť. Kyberprostor je potom místo, které se nachází uvnitř této sítě, avšak se s ním můžeme setkat i mimo internet. Kromě internetu existují různé lokální sítě. Patří sem sítě PAN, LAN, MAN A WAN. Takto jsou rozděleny podle rozlehlosti a účelu. Jsou separované od internetu, ale spojují uživatele dané sítě. Z tohoto důvodu lze podle autorova názoru kyberprostor nalézt i jinde než na internetové síti.

[12] HAKEN, D. *Cyborg @ cyberspace? : an ethnographer : looks to the future.* New York : Routledge, 1999, s. 264.

3 Etiologie počítačové kriminality a její formy

Mezi příčinami počítačové kriminality lze najít takové, které jsou podobné pro jiné druhy kriminalit i příčiny specifické pouze pro tu počítačovou.

První specifickou příčinou je již výše zmiňované **prostředí,**[13] v kterém se snadněji vyhledávají informace, nakupuje zboží, provádí transakce, ale také se v něm snadněji provádí kriminalita. Toto prostředí zajišťuje do jisté míry i anonymitu, což může být pro pachatele trestných činů lákavé. Pokud má pachatel potřebné znalosti, je pro něj jednodušší a lákavější vykrást online banku z domova, než vykrást obchod, dům, banku nebo cokoliv jiného, kde by musel být na místě činu.

Druhou specifickou příčinou jsou **nezkušení uživatelé** internetu a informačních technologií. Internet nyní používá okolo 40% světové populace. Je tedy zřejmé, že ne každý uživatel má znalosti bezpečnostních zásad. Spoustu uživatelů naletí na podvodné zprávy, nerozpoznají podezřelé odkazy a otevírají je, důvěřují osobám, které vlastně ani neznají nebo nemají ani zabezpečený počítač dostupnými programy. Obětí počítačové kriminality se samozřejmě může stát i zkušený uživatel, přičemž nemusí udělat žádnou chybu, ale pravděpodobnost je menší než u nového uživatele.

Poslední specifická příčina je **neznalost činností**, které jsou v rozporu se zákonem. Nezkušený uživatel tak nemusí ani vědět, že on sám porušuje zákon. Např. principem stahování filmů a jiných autorských děl přes tzv. torrenty je sdílení již stažené části ostatním uživatelům, což je porušení zákona. Takto program pracuje, pokud není předem nastaven jinak, torrenty samy o sobě nelegální nejsou, protože obsahují i obyčejná, autorsky nechráněná data, přesto většina z nich obsahuje právě filmy, nelegální software a hry.

[13] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 21-22.

Autorský zákon neporušuje ten, kdo stahuje díla, jejichž užití je autorským zákonem chráněno. V tomto případě zákon porušuje ten, kdo umožní stahování takových děl.[14]

Vzhledem k rychlému a stálému progresu informačních technologií a počítačové kriminality zákon nestíhá pružně reagovat, tudíž neobsahuje vše, co by se mohlo zdát v rozporu s dobrými mravy.

Mezi příčiny společné pro více druhů kriminalit i pro tu počítačovou patří dědičnost, sociální prostředí, média a další.

Všechny vlastnosti člověka, zájmy i postoje jsou alespoň z části dědičné, proto je zřejmé, že to může být příčina jakéhokoliv chování, i toho kriminálního. Už v 19. století začínaly být zkoumány biologické determinanty delikventního chování.[15] **Dědičnost** patří mezi příčiny kriminalit jako jedna z mnoha faktorů. Dále sem patří pohlaví, inteligence a temperament. Muži se dopouštějí kriminálního chování častěji než ženy.

Další příčinou počítačové kriminality je **sociální prostředí**. Zejména rodina, škola, skupiny mládeže a jiné místa, kde se osoba často zdržuje. Dnes už téměř každá domácnost vlastní počítač s internetovým připojením. Děti u počítačů tráví hodně času a jejich znalosti v souvislosti s počítači přesahují znalosti rodičů. Rodina má z nich asi největší vliv, mladší členové rodin napodobují chování rodičů a starších sourozenců. Faktory ovlivňující chování jsou kvalita komunikace mezi členy rodiny, dohled rodičů a způsob výchovy. Ve škole děti stráví část života a setkávají se zde s lidmi, kterými jsou ovlivňovány. Žáci tvoří různé skupiny i mimo školu, v nichž může být napodobováno asociální chování. Dospívající tvoří takové skupiny nejčastěji, navíc jsou v tomto věku náchylnější k delikventnímu chování.

[14] *Stahování z torrentů* [online]. Všebořice.net. 2011-2013 [cit. 2016-02-03]. Dostupné z: <http://www.vseborice.net/navody/torrenty/0>.
[15] RENATO, M. E. *Cesare Lombroso: A Brief Biography* [online]. Cerebromente. 1997 [cit. 2016-02-04]. Dostupné z: <http://www.cerebromente.org.br/n01/frenolog/lombroso.htm>.

V neposlední řadě sem patří také **média**. Ty jsou dnes základním zdrojem informací o mnoha oblastech lidského života. Informace přesahující rámec osobních zkušeností a zkušeností ostatních osob získávají lidé právě prostřednictvím masmédií. Média zobrazují násilí, krádeže, ale i případy počítačové kriminality. Média zásadně ovlivňují to, jak společnost kriminalitu vnímá, jak se o kriminalitě diskutuje a jaká opatření jsou pro občany žádoucí. Zločin je pro média častým objektem, protože tato oblast přitahuje čtenáře. Slavné motto zakladatele britských novin Daily Mail, Lorda Northcliffa hovoří za vše: „Dejte mi jednu vraždu denně“.[16]

3.1 Formy počítačové kriminality

3.1.1 Malware (spyware, adware, viry)

Jedná se o škodlivý softwarový program, který poškozuje nebo vniká do počítačových systémů. Malware jsou viry, trojské koně, spyware a adware.[17] Viry jsou programy, které mohou infikovat jiné programy a šířit se tak v počítači nebo v síti. Mohou např. vymazávat nebo poškozovat složky a data z pevného disku. Spyware odesílá data z uživatelova počítače, aniž by uživatel o něčem věděl. Tyto data mohou zahrnovat cokoliv od historie prohlížení webových stránek až po hesla a čísla kreditních karet. Definice spywaru podle sdružení ASC (jehož členy jsou např. Microsoft, Symantec, LANDesk či Dell) zní takto:

„Nechtěné technologie“, které se instalují bez výslovného povolení uživatelem a/nebo jsou implementovány tak, že nějakým způsobem poškozují uživatele - ovlivňují soukromí uživatele nebo bezpečnost systému, používají jeho systémových zdrojů, včetně již instalovaných programů a/nebo sbírají a odesílají jejich osobní nebo jinak citlivé informace.[18]

[16] VLACH, J. *Média v kriminologické perspektivě* [online]. PREVENCE KRIMINALITY. 2013 [cit. 2016-03-24]. Dostupné z: <http://www.prevencekriminality.cz/evt_file.php?file=169>.
[17] *Malware* [online]. TechTerms.com. 2015 [cit. 2015-10-04]. Dostupné z: <http://techterms.com /definition/malware>.
[18] HLAVÁČ, J. *Spyware konečně definován!?* [online]. diit.cz. 2005 [cit. 2015-10-04]. Dostupné z: <http://diit.cz/clanek/spyware-konecne-definovan>.

Adware je produkt, který komplikuje používání počítače tak, že otevírá různé reklamní aplikace nebo mění domovské stránky.[19] Uživatelé si mohou nainstalovat antivirové a antispywarové programy do počítačů a do určité míry se tak proti nim bránit. Malware je občas pro nezkušené uživatele těžké rozpoznat, může být totiž maskován v nenápadné formě jako je např. email, zpráva na facebooku obsahující odkaz či žádost nebo obyčejný internetový odkaz.

3.1.2 Hacking

Pod pojmem hacking si většina lidí představuje nelegální činnosti. Hacking nemusí být prováděn pouze s protiprávními úmysly. Vedle takového hackingu rozeznáváme také etický hacking, takový hackeři se v angličtině nazývají white hats. Cílem etického hackingu je boj proti hackerům s protiprávními úmysly. Etický hacker musí dobře znát způsoby, kterými hackeři se zlými úmysly útočí, neboli jejich taktiku, dovednosti, nástroje a motivy.[20]

Úkolem takového etického hackera většinou bývá hledání slabých míst určitých systémů pomocí penetračních testů. Etický hacker jimi objeví chyby, které představují největší riziko pro daný systém.

Lidé, kteří hackování používají k činům nelegálním, většinou se infiltrují do systémů kvůli vlastnímu obohacení nebo za účelem poškození systému se nazývají pojmem cracker anglicky black hats. Proti těmto hackerským útočníkům pomáhají etičtí hackeři zabezpečovat systémy. Na rozdíl od etického hackera cracker využívá své schopnosti ke kriminálním účelům. Některé crackovací metody stojí čistě na matematických principech, takže cracker musí mít matematické znalosti. V jiných případech crackerovi stačí, když zná hardwarové registry, to je systém pro ukládání klíčů a hesel v operačním systému windows.[21]

[19] *Adware* [online]. TechTerms.com. 2015 [cit. 2015-10-04]. Dostupné z: <http://techterms.com /definition/adware>.
[20] HARRIS, Shon. *Hacking: manuál hackera*. 1. vyd. Praha: Grada, 2008, s. 32-33.
[21] CRAIG, Paul P a Ron HONICK. *Softwarové pirátství bez záhad*. 1. vyd. Praha: Grada, 2008, s 56.

Mezi black hats a white hats hackery je ještě skupina hackerů, kteří se nedají zařadit ani do jedné z těchto skupin, anglicky jsou nazýváni grey hats. Tito hackeři např. napadají systémy bez povolení a následně informují organizace o největších slabinách.

V praxi to může vypadat tak, že black hat hacker by prolomil systém bez povolení za účelem vlastního obohacení nebo poškození systému, white hat hacker si vyžádá povolení, informuje správce o tom, kdy bude systém testovat a to pouze za účelem vylepšení bezpečnosti. Grey hat hacker napadne systém, aniž by někoho informoval, zjistí jeho slabiny a následně jej sdělí správcům. Grey hats hackeři nepoužívají své znalosti k zlomyslným účelům jako black hats, ale často systém prolomí bez povolení, což je nelegální.[22]

3.1.3 Phishing a pharming

Phishingem jsou označovány emaily, kterými se útočníci snaží zjistit přístupové informace k účtům a jiným systémům, a následně jej zneužít k vlastnímu prospěchu. Nejčastější jsou touto nelegální cestou zjišťovány údaje k bankovním účtům, PINy a přihlašovací údaje k různým účtům např. email, paypal, aukro, amazon.

Emaily často vypadají jako výzva k zaplacení, aktualizaci účtů, výzkumy atd. V emailu je přiložen odkaz, který uživatele přesměruje na falešný web, který se zdá být na první pohled identický s originálním webem, ale při bližším prozkoumání je zjevné, že web vypadá podezřele. Tento falešný odkaz obsahuje formulář, kam by oběť měla napsat a odeslat své přihlašovací údaje. Zkušený uživatel internetu většinou pozná, že se jedná o podvod. Pharmingem se označuje přesměrování uživatele na falešnou stránku.[23]

[22] HOFFMAN, CH. *Hackers Hat Colors Explained* [online]. How To Geek. 2013 [cit. 2016-02-01]. Dostupné z: <http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/>.
[23] *Phishing a pharming* [online]. bezpecnyinternet.cz. 2010 [cit. 2016-02-01]. Dostupné z: <http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx>.

Obrana proti phishingu, pharmingu a zároveň i jiným formám kybernetických útoků se dá shrnout do následujících bodů:[24]

- Neklikat na podezřelé odkazy v emailových zprávách a nikde jinde na internetu
- Pří návštěvě internet. bankovnictví a podobných systémů odkaz napsat ručně
- Používat antivirový software
- Používat bezpečný prohlížeč, mezi nejznámější patří Firefox, Chrome, Explorer, Safari, Opera…
- Používat aktualizovaný operační systém
- Používat antispywarové programy a firewall
- Základní návyky související s bezpečností na internetu
- Zabezpečení bezdrátového připojení
- Nepoužívat jednoduchá hesla

3.1.4 Sniffing

Další formou počítačové kriminality, při které jsou nelegální cestou zjišťovány informace o oběti, je sniffing. V překladu znamená sniffing čmuchat nebo čenichat. Je to technika, která útočníkovi umožňuje neoprávněně monitorovat internetovou komunikaci.[25] Cílem útočníka většinou bývají přístupové údaje, hesla a obsah emailové stránky apod. K takovému účelu je často využíván program keylogger, který monitoruje a následně ukládá každý stisk klávesy.

3.1.5 Warez

Warezem se rozumí neoprávněné nakládání s autorským dílem. Např. zakoupením softwarového programu lidé nekupují právo poskytovat tento program jiným lidem. V praxi se většinou jedná o stahování a sdílení počítačových her, filmů a softwarových programů.

[24] DOČEKAL, D. *Jak se bránit phishingu* [online]. LUPAcz. 2008 [cit. 2016-02-01]. Dostupné z: <http://www.lupa.cz/clanky/jak-se-branit-phishingu/>.
[25] OBR, J. *Sniffing: Odposlech datové komunikace* [online]. ITBIZ. 2009 [cit. 2016-02-02]. Dostupné z: <http://www.itbiz.cz/sniffing-odposlech-datove-komunikace>.

Historie warezu neboli softwarové pirátství je delší než historie samotného internetu, protože už v době audio kazet bylo možno hudbu kopírovat. Jakmile se objevily první CD-ROM a DVD, zařízení k jejich kopírování na sebe nenechala dlouho čekat. Dnes je warez v takovém stavu, že je často možné z internetu stáhnout film nebo počítačovou hru ještě před tím, než je možné si jej koupit na DVD.[26]

3.1.6 Kyberšikana[27]

Kyberšikana je podobná klasické šikaně. Stejně jako u klasické šikany je cílem i u kybernetické šikany ublížení nebo ponížení oběti. Rozdílem je, že v případě kyberšikany jsou k jejímu účelu používány informační technologie. Útočníci tedy nejsou v přímém kontaktu s obětmi. To znamená, že pokud útočník chce, může zůstat do určité míry v anonymitě. Díky velikosti internetu může lidem dnes kyberšikana hodně znepříjemnit život. Stačí sdílet nevhodnou fotku na sociální síti, která může být dále sdílena ostatními uživateli a nekontrolovatelně se šířit dál.

Kyberšikana může být prováděna kdykoliv během celého dne, což může mít nepříznivé psychické následky u oběti. Většinou jde o urážlivé, zastrašující nebo hanlivé zprávy poslané pomocí mobilního telefonu nebo na internetu, obrázky či videa s cílem někoho zesměšnit nebo vydávání se za oběť, přičemž jsou jiným posílány urážlivé zprávy. Prostředky k šíření kyberšikany jsou mobilní telefony, sociální sítě a jiné weby, kde se dají sdílet videa a fotky, emaily a různé chatovací místnosti.[28]

Jsou známy i případy, kdy oběti spáchali sebevraždu. Kanaďanka Rehteah, které bylo 16 let, byla údajně znásilněna na večírku. Po internetu kolovaly fotky z večírku, díky kterým byla Rehteah vystavena výsměchu a urážlivým komentářům. Následkem toho spáchala sebevraždu, rodiče ji našli oběšenou v jejím pokoji. Policie poté obvinila dva muže z šíření dětské pornografie.[29]

---

[26] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 105.
[27] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty*. Vyd. 1. Praha: Portál, 2011, s. 30-38.
[28] *CO JE TO KYBERŠIKANA A JAK SE PROJEVUJE?* [online]. bezpečně-online.cz. 2010 [cit. 2016-02-01]. Dostupné z: <http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html>.
[29] *Kyberšikana zabíjí – sebevraždy dívek hýbou Británií, Kanadou i Itálií* [online]. Česká televize. 2013 [cit. 2016-02-02]. Dostupné z: <http://www.ceskatelevize.cz/ct24/svet/1081921-kybersikana-zabiji-sebevrazdy-divek-hybou-britanii-kanadou-i-italii>.

Specifické znaky kyberšikany, které jsou odlišné od znaků klasické šikany:

- Anonymita – agresor často nevystupuje pod svým jménem
- Publikum – na sociálních sítích je oběť kyberšikany sledována jinými uživateli sociální sítě
- Kyberšikana může být prováděna kdykoliv během celého dne

3.1.7 DoS a DDoS útoky

Útoky Dos (denial of service) patří mezi nejčastější kybernetické útoky. Při těchto útocích jsou různými způsoby zahlcovány napadené servery, čímž se stanou dočasně nefunkční. Z hlediska provedení je DoS útok snadnější než jiné typy.

Jednoduchým příkladem tohoto typu útoku je zahlcení emailové schránky. Emailová schránka má omezenou kapacitu, princip DoS útoku spočívá v tom, že útočník začne na emailovou schránku posílat velké množství emailů, většinou z více emailových schránek, aby byl proud emailových zpráv větší. Pokud se útok nepodaří včas zastavit, server se s takovým množstvím emailů nedokáže vypořádat a emailová schránka je odepsána. Na tomto příkladu je vidět jednoduchost a zároveň i vysoká účinnost DoS a DDoS útoků.

Rozdíl DoS útoku oproti DDoS (distributed denial of service) je, že pokud jde o DoS útok, útočník používá jedno internetové připojení, pokud se jedná o DDoS útok, útočník vede útok většinou z více zařízení připojených k internetu, takže se jedná o typ DoS útoku, který dokáže např. rychleji zahltit emailovou schránku.[30]

V současné době rozeznáváme čtyři základní způsoby DoS útoků, s nimiž se lze v praxi setkat.

První z nich je útok za pomocí obsazení přenosové kapacity, to je metoda, kdy dojde k zablokování přístupu k určité službě. Útočník zkrátka vytvoří takový provoz, který plně vytíží přístupovou cestu, čímž vytěsní ostatní uživatele.

[30] *Denial of Service Attacks* [online]. INCAPSULA. 2015 [cit. 2015-12-14]. Dostupné z: <https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html>.

Dalším typem útoku je přivlastnění systémových zdrojů. „Cílem hry“ v daném případě není zahltit přístupovou linku, ale spotřebovat limitované zdroje oběti. Tedy třeba paměť serveru či volné místo na disku. Útočník v takovém případě vytváří stav, kdy získává podstatnou část systémových zdrojů, takže na uživatele zbyde zanedbatelná kapacita.

Třetím typem DoS útoku je zneužití chyb v programech. Tyto chyby přitom mohou být známé nebo nově objevené. V prvním případě jde zpravidla o servery, jejichž správci zanedbávají záplatování. Vlivem chyby nedokáže program reagovat na neobvyklou situaci a dochází k jeho zhroucení, zacyklení, pádu či jinému nekorektnímu chování. Regulérní uživatel služby k ní nemůže získat přístup

Čtvrtým a zároveň posledním typem DoS útoku je napadení. V podstatě dojde k tomu, že na DNS serverech dojde ke změnám záznamů o IP adresách – tyto jsou změněny tak, že veškerý provoz je měněn ve prospěch útočníka nebo spřízněného subjektu (který ze situace samozřejmě získává nemalý prospěch) nebo že žádosti vedou do „slepé uličky“ (tady sice útočník přímý prospěch nezískává, ale postižený subjekt utrpí škodu). [31]

Dos utok z roku 2000[32]

V roce 2000 se postaral o rozruch mladík z Montrealu s přezdívkou Mafiaboy. Bylo to 7. února, když patnáctiletý hacker spustil sérii DoS útoků proti známým serverům. Byl obviněn z jednoho z největších kybernetických útoků v historii. Mezi napadené servery patřily Amazon, Fifa, CNN, Dell, eBay a Yahoo!. Jméno hackera nemohlo být podle kanadských zákonů zveřejněno, protože byl v té dobé nezletilý. Většina z nap adených serverů byly nepřístupné jen na čtyři hodiny. Dnes už jeho jméno zveřejněno je. Nezletilý hacker jménem Michael Calce byl v tu dobu na svobodě, avšak v souladu s podmínkami kauce směl používat počítač pouze pro školní účely a pod dohledem učitele. Měl zákaz připojení na internet. Policie proto zabavila chlapci jeho domácí počítač.[33]

[31] PŘIBIL, T. *Zákeřný útok jménem DoS* [online]. SystemOnline. 2006 [cit. 2015-12-14]. Dostupné z: <http://www.systemonline.cz/it-security/zakerny-utok-jmenem-dos.htm>.
[32] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez tajemství. 3*. aktualiz. vyd. Brno: Computer Press, 2003, s. 463.
[33] *Nezletilý kanadský hacker Mafiaboy čelí řadě obvinění* [online]. ING. 2001 [cit. 2015-12-14]. Dostupné z: <http://ihned.cz/c1-10329780-nezletily-kanadsky-hacker-mafiaboy-celi-rade-obvineni>.

Michael Calce, několik let odmítal o útocích mluvit, ale později o nich promluvil. Později se stal tzv. etickým hackerem (White hat). Etický hacker je odborník na počítačovou bezpečnost, zaměřuje se na penetrační testy pro zajištění bezpečnosti informačních systémů.

3.1.8 Šíření pornografie

Šíření pornografie patří mezi nejčastěji páchanou ilegální aktivitu na internetu. Propojením počítače s internetem vznikl prostor, kde se tato činnost odehrává často. Lákavá je pro pachatele anonymita na internetu. Z kriminologického hlediska se pornografická díla podle obsahu rozdělují na:

- pornografii tvrdou – dílo, v němž se projevuje násilí či neúcta k člověku nebo které znázorňuje pohlavní styk se zvířetem
- pornografii dětskou – dílo, které zobrazuje, popř. jinak využívá dítě
- pornografii prostou – ostatní pornografická díla[34]

Šíření pornografie je trestným činem § 191 TZ. Tohoto trestného činu se dopustí ten, *kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá, nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje, nebo jinak znázorňuje pohlavní akt se zvířetem. Trestem je odnětí svobody až na jeden rok, zákaz činnosti, propadnutí věci nebo jiné majetkové hodnoty.* [35]

Objektem je ochrana lidské důstojnosti v sexuální oblasti. Tato norma postihuje tzv. tvrdou pornografii. Ta je definována tak, že obsahuje násilí či neúcta k člověku v souvislosti se sexuálními aktivitami, nebo pohlavní styk se zvířetem. **Objektivní stránkou** je jednání ve formě výroby, dovozu, průvozu, nabízení, veřejným zpřístupněním, zprostředkováním, uvedením do oběhu, prodejem nebo jiným opatřením pornografického díla s prvky násilí či neúctě k člověku nebo pohlavním stykem se zvířetem. **Subjektem** je osoba starší patnácti let a příčetná, která takový čin spáchá a **subjektivní stránkou** je zavinění ve formě úmyslu.

[34] ŠÁMAL, P. *Trestní zákoník: komentář.* 2. vyd. V Praze: C.H. Beck, 2012, Velké komentáře. s. 1400.
[35] Zákon č. 40/2009 Sb., trestní zákoník, § 191.

Druhý odstavec postihuje tzv. pornografii prostou, což je trestné pouze v případě, že je *nabídnuta, přenechána nebo zpřístupněna dítěti nebo když je vystavena nebo jinak zpřístupněna na místě, které je dětem přístupné. Trest je v tomto případě odnětí svobody až na dva roky, zákaz činnosti či propadnutí věci nebo jiné majetkové hodnoty.*

Ve třetím a čtvrtém odstavci je obsažena kvalifikovaná skutková podstata. To znamená vyšší trest, spáchá-li pachatel čin uvedený v odstavci 1 a 2:

- *tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobným způsobem*
- *jako člen organizované skupiny*
- *v úmyslu získat pro sebe nebo pro jiného značný prospěch*
- *jako člen organizované skupiny působící ve více státech*
- *v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu*[36]

3.2 Shrnutí kapitoly

V první části této kapitoly byly uvedeny některé příčiny počítačové kriminality. Mezi příčiny specifické byly uvedeny tyto: počítačové prostředí, nezkušení uživatelé a neznalost činností, které jsou v rozporu se zákonem. Uvedeny jsou zde i některé společné příčiny pro více druhů kriminalit a to dědičnost, sociální prostředí a média.

V druhé části kapitoly jsou uvedeny některé často se vyskytující formy počítačové kriminality. Jsou zde rozebrány činnosti nazývané malware, hacking, phishing a pharming, sniffing, warez, kyberšikana, DoS útoky a šíření pornografie. V části o DoS útocích je popsán jeden z největších kybernetických DoS útoků z roku 2000, při němž byly napadeny známé servery Fifa, Amazon, eBay a CNN. Na závěr je rozebrána skutková podstata trestného činu šíření pornografie.

[36] Zákon č. 40/2009 Sb., trestní zákoník, § 191.

4 Fenomenologie počítačové kriminality

V této kapitole jsou zmíněny tři trestné činy související s počítačovou kriminalitou v ČR. Jsou zde podrobně rozebrány jejich skutkové podstaty a provedena analýza statistických dat.

4.1 Trestné činy související s počítačovou kriminalitou a jejich skutkové podstaty

4.1.1 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)[37]

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části,

bude potrestán:

- *odnětím svobody až na jeden rok,*
- *zákazem činnosti nebo*
- *propadnutím věci nebo jiné majetkové hodnoty.*

(2) Kdo získá přístup k počítačovému systému nebo nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

[37] Zákon č. 40/2009 Sb., trestní zákoník, § 230.

bude potrestán:

- *odnětím svobody až na dva roky,*
- *zákazem činnosti nebo*
- *propadnutí věci nebo jiné majetkové hodnoty.*

(3) Spáchá-li pachatel čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo

b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat,

bude potrestán:

- *odnětím svobody na šest měsíců až tři roky,*
- *zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*

(4) Pokud pachatel

a) spáchá čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí takovým činem značnou škodu,

c) způsobí takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,

d) získá takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem,[38]

bude potrestán:

- *odnětím svobody na jeden rok až pět let nebo*

peněžitým trestem.

[38] Zákon č. 40/2009 Sb., trestní zákoník, § 230.

(5) Pokud pachatel

a) způsobí činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) získá takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu,

bude potrestán:

- *odnětím svobody na tři roky až osm let.*[39]

Skutková podstata

Tato norma je zaměřena na ochranu informací v počítačových systémech. **Objektem** tohoto trestného činu je tedy ochrana počítačových systémů a jejich dat a to je právě zájem, který je chráněn státem. **Objektivní stránku** definuje jednání a následek, mezi nimiž musí být příčinná souvislost neboli kauzální nexus. Jednání je v tomto případě překonávání bezpečnostního opatření, a tím neoprávněné získání přístupu k počítačovému systému nebo jeho části. **Následkem** je porušení objektu neboli práva na ochranu počítačových systému a jejich dat. **Předmětem** útoku je nosič informací, respektive jeho obsahové a technické vybavení. **Subjektem** je osoba starší patnácti let a příčetná, která takový čin spáchá a **subjektivní stránkou** je zavinění ve formě úmyslu.

Tento trestný čin je závažnější pokud pachatel data v počítači zneužije, vymaže, pozmění, vloží, páchá-li tento čin s úmyslem způsobit někomu škodu, sobě nebo jinému neoprávněný prospěch nebo s úmyslem omezit funkčnost počítačového systému.

V prvním odstavci je zmíněno překonání bezpečnostního opatření a zároveň neoprávněné získání přístupu k počítačovému systému. V tomto případě nezáleží na tom, že pachatel se získanými informacemi již nějakým způsobem nemanipuloval. Dostačující je, že pachatel obešel bezpečnostní systém a to je trestným činem.

K naplnění skutkové podstaty v druhém odstavci pachatel musí učinit navíc další kroky, než jen získat přístup. V tomto případě nemusí být tento přístup neoprávněný, jako v prvním odstavci, ale tato osoba může mít k těmto datům legální přístup. Dalšími kroky je myšleno neoprávněné užívání dalších dat, vymazání, poškození, změnění, padělání vložení dat. Trest je v tomto případě také vyšší.

[39] Zákon č. 40/2009 Sb., trestní zákoník, § 230.

V dalších odstavcích se objevují už jen kvalifikované skutkové podstaty. V třetím odstavci je obsažen čin v odstavci 1 nebo 2, ale pachatel musí tímto činem navíc jinému **úmyslně** způsobit škodu, získat sobě či někomu jinému prospěch nebo omezit funkčnost systému. Zde jde o motiv, je rozdíl, když někdo získává data nebo s nimi manipuluje, a když to samé dělá s úmyslem někomu způsobit újmu.

Čtvrtý odstavec opět zmiňuje čin v odstavci 1 nebo 2, ale trest je také vyšší, protože pachatel musí čin spáchat jako člen organizované skupiny, musí činem spáchat **značnou škodu** nebo získat **značný prospěch.** To je v obou případech **minimálně 500 tis. Kč**.

Pátý odstavec je obdobný, ale pachatel musí způsobit **škodu velkého rozsahu**, nebo získat **prospěch velkého rozsahu**. To je v obou případech **minimálně 5 mil. Kč**.

4.1.2 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ)[40]

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

bude potrestán:

- *odnětím svobody až na jeden rok,*
- *zákazem činnosti nebo propadnutí věci nebo jiné majetkové hodnoty.*

[40] Zákon č. 40/2009 Sb., trestní zákoník, § 231.

(2) Pokud pachatel

a) spáchá čin uvedený v odstavci 1 jako člen organizovaná skupiny, nebo

b) získá takovým činem pro sebe nebo pro jiného značný prospěch,

bude potrestán:

- *odnětím svobody až na tři roky,*
- *zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*

(3) Pokud pachatel získá činem uvedeným v odstavci 1 pro sebe nebo pro někoho jiného prospěch velkého rozsahu, bude potrestán odnětím svobody na šest měsíců až pět let[41]

Skutková podstata

K splnění skutkové podstaty tohoto činu není třeba získat přístup k počítačovým systémům jako v § 231, ale stačí, když si někdo opatří nebo přechovává zařízení s programovým vybavením, počítačové heslo nebo podobný prostředek, pomocí kterého lze získat přístup k počítačovému systému a to vše s úmyslem spáchat trestný čin neoprávněného přístupu k počítačovému systému. V téhle situace jde vlastně o formu přípravy, pachatel si obstarává nástroj k neoprávněnému přístupu do počítačového systému a už tato forma přípravy je definována jako trestný čin. **Objektem** tohoto trestného činu je ochrana počítačových systémů a jejich dat. **Jednáním** je výroba, přechovávání, prodávání nebo opatřování prostředku, kterým se lze neoprávněně dostat to počítačového systému a **následkem** je porušení práva na ochranu počítačových systému a jejich dat. **Předmětem** útoku je nosič informací, respektive jeho obsahové a technické vybavení. **Subjektem** je osoba starší patnácti let a příčetná, která tento čin spáchá a **subjektivní stránkou** je zavinění ve formě úmyslu. Odstavce 2 a 3 už obsahují pouze kvalifikovanou skutkovou podstatu, tedy i vyšší trest, pokud pachatel spáchá čin v odstavci 1 jako člen organizované skupiny nebo získá takovým činem pro sebe či pro jiného značný prospěch nebo prospěch velkého rozsahu.

[41] Zákon č. 40/2009 Sb., trestní zákoník, § 231.

4.1.3 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ)[42]

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu,

bude potrestán

- *odnětí svobody až na šest měsíců*
- *zákaz činnosti nebo propadnutí věci nebo jiné majetkové hodnoty.*

2) Pokud pachatel způsobí činem uvedeným v odstavci 1 škodu velkého rozsahu, bude potrestán odnětím svobody až na dva roky, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Skutková podstata

Objektem toho trestného činu je ochrana počítačových systémů a jejich dat. **Jednáním** je porušení povinnosti, a tím znehodnocení dat v počítačovém systému nebo učinění zásahu do technického nebo programového vybavení počítače nebo jiného technického zařízení, a tím způsobení značné škody na cizím majetku. N**ásledkem** je porušení práva na ochranu počítačových systémů a jejich dat. **Předmětem útoku** je nosič informací, respektive jeho obsahové a technické vybavení, v tomto konkrétním případě znehodnocení dat v počítačovém systému nebo učinění zásahu do technického nebo programového vybavení počítače nebo jiného technického zařízení a tím způsobení značné škody na cizím majetku. **Subjektem** je osoba starší patnácti let a příčetná, která tento trestný čin spáchala a **subjektivní stránkou je zavinění** ve formě hrubé nedbalosti. Definice hrubé nedbalosti z trestního zákoníku zní takto: přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.[43]

[42] Zákon č. 40/2009 Sb., trestní zákoník, § 232.
[43] Zákon č. 40/2009 Sb., trestní zákoník, § 16.

4.2 Analýza statistických dat počítačové kriminality

V této části práce jsou analyzovány policejní statistiky, konkrétně poškozování a zneužívání záznamu na nosiči informací za posledních pět let. Tyto statistické záznamy obsahují zjištěné trestné činy od 1. 1. do 31. 12. daného roku. Statistický záznam poškozování a zneužívání záznamu na nosiči informací obsahuje všechny tři trestné činy, které byly rozebrány v předešlé kapitole (§ 230-232 TZ).

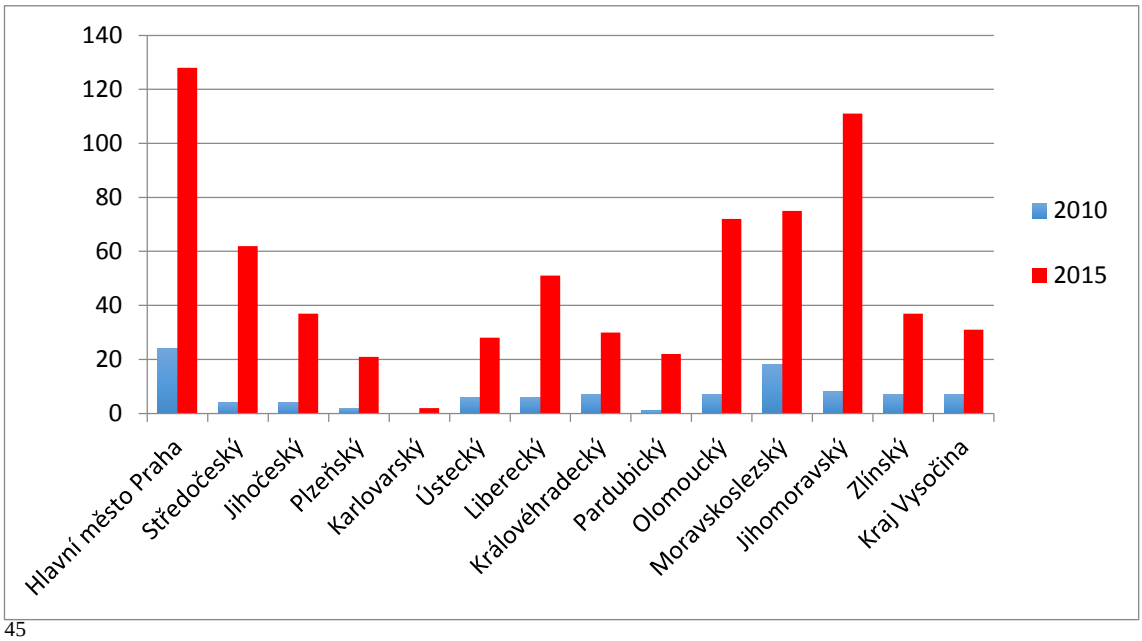
Tabulka č.1 - Poměr zjištěných a objasněných trestných činů v kategorii poškozování a zneužívání záznamu na nosiči informací (§ 230-232 TZ)[44]

Poš. a zneuž. záz. na nos. informací	Zjištěno	Objasněno	Objasněnost v procentech
2010	101	30	29,7%
2011	134	54	40,3%
2012	178	45	25,3%
2013	301	76	25,2%
2014	669	192	28,7%
2015	707	144	20,4 %

Z tabulky je patrné, jak se počítačové systémy a počítačová kriminalita rychle rozrůstá. Za rok 2010 bylo zjištěno pouhých 101 trestných činů v kategorii poškozování a zneužívání záznamu na nosiči informací. V dalších letech postupně přibýval jejich počet a za rok 2015 je jich zjištěno 707, to je sedmkrát více, než za rok 2010. Objasněnost těchto činů naproti tomu nestoupá, ale spíše klesá. Podle těchto zjištěných statistických výsledků se průměrně pohybuje okolo 30%. To je zapříčiněno zřejmě vysoce anonymním prostředím v počítačovém světě.

[44] *Statistiky* [online]. POLICIE ČESKÉ REPUBLIKY. 2016 [cit. 2016-03-01]. Dostupné z: <http://www.policie.cz/statistiky-kriminalita.aspx>.

Graf č.1 – Rozdělení zjištěných trestných činů v kategorii poškozování a zneužívání záznamu na nosiči informací (§ 230-232 TZ) z roků 2010 a 2015 podle krajů



[45]

Nejvíce trestných činů (§ 230-232 TZ) bylo spácháno v Praze a nejméně v Karlovarském kraji. To je pochopitelně ovlivněno počtem obyvatel a jinými faktory jako např. tím, kolik obyvatel v daném kraji vlastní počítač s přístupem k internetu. Praha měla na začátku roku 2015 kolem 1 259 079 obyvatel a v Karlovarském kraji jich bylo pouze 299 293. Z tohoto důvodu se na první pohled nedá porovnat stav kriminality krajů. Je logické, že v kraji s vyšším počtem obyvatelstva bude větší pravděpodobnost větší intenzity kriminality. Pro takové účely je zaveden ukazatel kriminality. Úroveň kriminality je vyjadřována v indexech na 10 000 nebo 100 000 obyvatel.

$$\text{Index} = \frac{\text{počet TČ}}{\text{počet obyvatel na vymezeném území}} \times 100\,000\ (10\,000)$$ [46]

[45] *Statistiky* [online]. POLICIE ČESKÉ REPUBLIKY. 2016 [cit. 2016-03-01]. Dostupné z: <http://www.policie.cz/statistiky-kriminalita.aspx>.

[46] KUCHTA, J. a VÁLKOVÁ, H. *Základy kriminologie a trestní politiky*. Vyd. 1. Praha: C.H. Beck, 2005, Beckovy mezioborové učebnice, s. 124.

Tabulka č.2 – Index kriminality (§ 230-232) v jednotlivých krajích ČR v roce 2015

Kraj	Zjištěné TČ[47] (§ 230-232 TZ)	Počet obyvatel[48]	Index 100 000
Hlavní město Praha	128	1 259 079	10,2
Středočeský	62	1 315 299	4,7
Jihočeský	37	637 300	5,9
Plzeňský	21	575 123	3,7
Karlovarský	2	299 293	0,7
Ústecký	28	823 972	3,4
Liberecký	51	438 851	11,6
Královehradecký	30	551 590	5,4
Pardubický	22	516 372	4,3
Olomoucký	72	635 711	11,3
Moravskoslezský	75	1 217 676	6,2
Jihomoravský	111	1 172 853	9,5
Zlínský	37	585 261	6,3
Kraj Vysočina	31	509 895	6,1

[47] *Statistiky* [online]. POLICIE ČESKÉ REPUBLIKY. 2016 [cit. 2016-03-01]. Dostupné z: <http://www.policie.cz/statistiky-kriminalita.aspx>.
[48] Český statistický úřad – stav ke dni 31.12.2014.

Nejvíce trestných činů (§ 230-232 TZ) bylo spácháno v Praze. To ale neznamená, že v Praze je míra těchto trestných činů nejvyšší. V tabulce č. 2 index ukazuje, že míra této kriminality je nejfrekventovanější v Libereckém a Olomouckém kraji. Praha je až na třetím místě. Z indexu vychází 11,6 trestných činů (§ 230-232 TZ) na 100 000 obyvatel v Libereckém kraji. Nejméně trestných činů (§ 230-232 TZ) bylo spácháno v kraji Karlovarském. Zde také vychází nejmenší míra této kriminality. Podle indexu na 100 000 obyvatelů vychází necelý jeden trestný čin (§ 230-232 TZ), přesněji pouhých 0,7. Malá míra této kriminality vychází také v kraji Ústeckém a Plzeňském.

4.3 Shrnutí kapitoly

V této kapitole je obsažena praktická část práce. Tato kapitola obsahuje trestné činy, které mají souvislost s počítačovou kriminalitou. Jsou to § 230 TZ – neoprávněný přístup k počítačovému systému a nosiči informací, § 231 TZ – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a § 232 TZ – poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti. Nejdříve jsou zde rozebrány skutkové podstaty těchto trestných činů. Dále tato kapitola obsahuje analýzu policejních statistik za roky 2010 - 2015, konkrétně těchto trestných činů. Z tabulky č. 1 je patrné, že těchto trestných činů rychle přibývá, ale jejich objasněnost nestoupá, spíše kolísá mezi 20 – 40%. V grafu č. 1 je rozdělení těchto trestných činů za roky 2010 a 2015 podle krajů a následně proveden výpočet indexu kriminality. Podle indexu je míra této kriminality nejfrekventovanější v Libereckém a Olomouckém kraji a nejméně frekventovaná v kraji Karlovarském.

5 Pachatelé počítačové kriminality

Pachatelé počítačové kriminality bývají nejčastěji mladší lidé, s odborným vzděláním souvisejícím s tímto tématem. Dalším znakem pachatele je problematičnost v oblasti začleňování se do společnosti, ale není to pravidlem. Motivem bývá nejčastěji osobní obohacení, ale jsou známy i další časté motivy, patří k nim zejména pocit převahy nad zaměstnavatelem či veřejnými orgány, pocit beztrestnosti, snaha kompenzace nespokojenosti s prací, názor, že firmě nemohou uškodit malé ztráty a touha po riziku.[49] Dnes už je těžké vypracovat obecný profil pachatele počítačové kriminality, protože se znaky profilů rozrůstají spolu s vývojem počítačové kriminality, která stále zasahuje do nových sfér života. V některých oblastech počítačové kriminality pachatelé ani nepotřebují odborné vědomosti. Např. v oblasti počítačového pirátství stačí, pokud pachatel nějakým způsobem sdílí chráněný obsah. Z tohoto důvodu není už dnes možné profily pachatelů příliš zobecňovat jako dříve, když byly počítače a internet využívány malým počtem lidí.

Rozdělení skupin pachatelů podle Doc. Ing. Ivo Látal, CSc. z Policejní akademie ČR z hlediska vztahu pachatelů k informacím:[50]

5.1 Amatéři

Jsou osoby, které se náhodně nebo cílevědomě infiltrují do systémů a vyhledávají jejich slabiny. Ve většině případů si takový pachatel plně uvědomuje své počínání. Amatéři bývají osoby s vysokou inteligencí, snadno ovládají počítače a umí rychle reagovat na změněné situace.

Amatéry jde dále rozdělit na tyto kategorie:[51]

5.1.1 Hackery (grey hats)

Osoby, které pronikají do chráněných systémů bez zájmu poškození tohoto systému, snaží se prokázat své schopnosti. (viz. kapitola 3.1.2)

[49] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, Pro praxi. s. 135.
[50] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení*, materiál z přílohy časopisu Policista č. 3/1998, Policejní akademie České republiky Praha, 1998.
[51] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení*, materiál z přílohy časopisu Policista č. 3/1998, Policejní akademie České republiky Praha, 1998.

5.1.1 Neúspěšné kritiky

Tyto osoby chtějí narušením systému upozornit na závady a nedostatky v jejich ochraně. Jejich cílem není osobní obohacení, chtějí pouze donutit správce k zásahu.

5.1.2 Mstitelé

Motivace mstitelů je evidentně msta, většinou vyplývá ze vztahu k nespravedlivému zaměstnavateli, který ho nějakým způsobem poškodil.

5.1.3 Crackeři

To jsou osoby, jejichž motivy nebývají zcela „racionální“. Neoprávněně získávají data, aniž by je nějakým způsobem zneužívaly. Jejich cílem je většinou pouze poškození systému.

5.2 Profesionálové

Do této skupiny patří pracovníci tajných služeb, podnikatelé všeho druhu (manažeři), detektivové, teroristé a žurnalisté. Informace většinou nezískávají pro sebe, ale pro své zaměstnavatele. Z kriminálního hlediska je skupina profesionálů pachatelem, až když se dopustí protiprávního činu, což většinou nepřichází v úvahu u profesionálů ve státní sféře nebo bezpečnostní službě. Dále se do této skupiny řadí softwaroví piráti, kteří prodávají nelegální software.

Teroristé jsou zvláštní skupinou organizovaného zločinu. Mají vlastní zpravodajské sítě, kterými získávají informace a chrání své gangy. Od ostatních skupin se pochopitelné liší zaměřením a cílem.[52]

Pachatelé počítačové kriminality se v posledním období také začínají organizovat do skupin. Často je snahou těchto skupin zapojit do činnosti mladé lidi, kteří takové zločiny poté páchají. Tito lidé však nejsou kvůli nízkému věku trestně odpovědní.[53]

[52] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení*, materiál z přílohy časopisu Policista č. 3/1998, Policejní akademie České republiky Praha, 1998.
[53] POŽÁR, J. *Kybernetická kriminalita v organizaci.* Teorie IB. 2014 [cit. 2015-06-04]. Dostupné z: <http://www.teorieib.cz/pbi/files/51-31-Pozar_01-2.pdf >.

Skupina Anonymous

Anonymous je hackerská mezinárodní skupina. Je označována jako volné společenství hackerů. Ve skupině není žádné vedení ani hierarchické uspořádání. Tato skupina začala působit v roce 2003. Anonymous se nejvíce prezentuje svými hackerskými útoky, různými žerty a varovnými nebo sdělovacími zprávy.[54] Tyto projevy jsou často reakcí na činnost politiků, soudů a policie. Symbolem této skupiny je maska Guye Fawkese. To byl voják, který chtěl v 17. století vyhodit Britský parlament do povětří. Skupina často používá kybernetické útoky typu DDoS (viz. kapitola 3.1.7). Členové skupiny komunikují skrz e-maily a sociální sítě. Jsou rozptýleni po celém světě do malých skupin, takže i když bude určitá skupina dopadena, celkovou činnost Anonymous to nějak nenaruší. Terčem jejich útoků se staly např. společnost Visa, Mastercard a Universal Music, TV Fox nebo Pentagon.[55] V ČR se staly terčem útoku např. stránky protipirátské unie, české vlády nebo databáze ODS.

V poslední době (2016) se členové této skupiny proslavili bojem proti radikálům z hnutí Islámský stát. Vyřadili jim velké množství webových stránek a účtů na sociálních sítích. Po teroristickém útoku v Bruselu 23. 3. 2016 Anonymous vyhlašuje Islámskému státu válku.[56] Skupina na internetu zveřejnila den po útocích video, ve kterém muž v masce Guye Fawkese upozorňuje, že opět došlo k útoku na svobodu. "Znepřístupnili jsme tisíce účtů na Twitteru, které byly přímo spojené s ISIS. Budeme je tvrdě trestat, zničíme jejich elektronické portfolio a odřízneme je od přísunu peněz," uvedl mluvčí hnutí ve videu.[57]

---

[54] *Anonymous* [online]. Novinky.cz. 2016 [cit. 2016-03-26]. Dostupné z: <http://tema.novinky.cz/anonymous>.

[55] *Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and Paypal* [online]. INDEPENDENT. 2016 [cit. 2016-03-26]. Dostupné z: <http://www.independent.co.uk/news/uk/crime/anonymous-hackers-jailed-for-ddos-attacks-on-visa-mastercard-and-paypal-8465791.html>.

[56] *Dohra útoků v Bruselu: Anonymous jdou do války. Chtějí zničit Islámský stát* [online]. Eurozprávy.cz. 2016 [cit. 2016-03-26]. Dostupné z: <http://zahranicni.eurozpravy.cz/eu/149749-dohra-utoku-v-bruselu-anonymous-jdou-do-valky-chteji-znicit-islamsky-stat/>.

[57] *ANONYMOUS VARUJE: ISIS zaplatí za útoky v Bruselu! Čím se chtějí teroristům pomstít?* [online]. PRÁSK! 2016 [cit. 2016-03-26]. Dostupné z: <http://prask.nova.cz/clanek/novinky/anonymous-varuje-isis-zaplati-za-utoky-v-bruselu-cim-se-chteji-teroristum-pomstit.html>.

Skupina LulzSec

Další známou hackerskou skupinou je Lulzsec. Podobně jako skupina Anonymous je LulzSec označována jako volné společenství hackerů. Členové této skupiny provedli mnoho útoků na velké firmy po celém světě. Nejvíce se proslavili v roce 2011, když se jim úspěšně podařilo dokončit několik útoků na firmu Sony. Na internet unikly útržky z komunikace členů této skupiny. O tento únik se pravděpodobně postaral jeden z členů skupiny s přezdívkou m_nevra. Následně mu bylo vyhrožováno ze strany ostatních členů. Z těchto uniknutých informací vyplynulo, že se nejedná o velkou organizaci a přezdívka leadera skupiny. LulzSec začala působit v květnu 2011 a 25. 6. 2011 oznámili, že ukončují svou činnost. Přesto však někteří členové skupiny nadále v činnosti pokračovali. V březnu 2012 byly zveřejněny dokumenty obsahující informace o spolupráci lídra této skupiny s FBI.[58]

5.3 Shrnutí kapitoly

Pátá kapitola je zaměřena na pachatele kybernetické kriminality. Mezi společné znaky pachatelů patří mladší věk, odborné vzdělaní související s informačními technologiemi a problematičnost v oblasti začleňování se do společnosti. Dále kapitola obsahuje rozdělení pachatelů na amatéry a profesionály. Poslední část je věnována známým hackerským skupinám Anonymous a LulzSec. Anonymous je aktuálně zajímavé téma kvůli boji proti radikálům z hnutí Islámský stát.

[58] MOOS, J. *hackeři z LulzSec jdou za mříže, lídr je zradil (1)* [online]. *CDR.* 2012 [cit. 2016-03-26]. Dostupné z: <http://cdr.cz/clanek/lulzsec-vznik-a-pad-tymova-zrada>.

6 Historický a předpokládaný vývoj počítačové kriminality

6.1 Historie počítačové kriminality ve světě

S vývojem výpočetní technologie se vyvíjela i počítačová kriminalita. Dne 12. 8. 1981[59] byl na trh uveden první počítač. V 80. letech 20. století se osobní počítače začínaly pomalu rozšiřovat mezi domácnosti. Propojení počítačů pomocí modemů do sítí netrvalo dlouho a stalo se předchůdcem dnešního internetu. Nejdříve to byli počítačoví fandové, kteří zkoušeli pronikat do systému, představovalo to pro ně intelektuální výzvu. Poté se však objevili lidé, kteří pronikali do systému za účelem poškození systému nebo obohacení se.[60] První vir byl nazvaný Brain byl vytvořen roku 1986.[61] V roce 1988 byl do počítačového světa vypuštěn první internetový červ.[62] Poté zažívá svůj zrod oblast kybernetické kriminality - počítačové pirátství neboli warez. V roce 1994 v případě Citibank[63] pronikla hackerská skupina z Ruska do počítačů Citibank a odcizila částku kolem 10 mil. dolarů. Počítačové nadšence střídají profesionálové, sledují jen dosažení zisku, objevují se nové viry a jejich nebezpečnost rapidně stoupá. Může za to i nový přístup sdílení dat, dříve byl internet založen na principu klient-server, tzn., že data musela existovat na konkrétním serveru, nově se objevil způsob peer-to-peer, tedy připojení přímo k uživateli, který nabízí svůj daný obsah. Devadesátá léta tedy s celosvětovým rozvojem internetu přináší i jeho zneužití k šíření rasismu, pornografie a propagaci zakázaného zboží.

---

[59] STACH, J. *PC slaví 33 let – IBM PC model 5150 se objevil 12.8.1981 – po 33 je PC stále na vzestupu!* [online]. DDWORLD.cz 2014 [cit. 2015-06-04]. Dostupné z: <http://www.ddworld.cz/aktuality/aktuality/pc-slavi-33-let-ibm-pc-model-5150-se-objevil-12.8.1981-po-33-je-pc-stale-na-vzestupu-2.html>.

[60] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 18.

[61] *Počítačové viry* [online]. ivt.wz.cz. 2014 [cit. 2015-06-04]. Dostupné z: <http://ivt.wz.cz/strnad/viry.htm>.

[62] *The First Internet Worm & Internet Worm Virus* [online]. streetdirectory. 2015 [cit. 2015-06-04]. Dostupné z: <http://www.streetdirectory.com/travel_guide/113972/computers_and_the_internet/the_first_internet_worm__internet_worm_virus.html>.

[63] *Hacking Theft of $10 Million From Citibank* [online]. Revealed. latimes. 2015 [cit. 2015-06-04]. Dostupné z: <http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system>.

V knize Počítačová kriminalita od Michala Matějky je uvedeno následující rozčlenění historie počítačové kriminality:[64]

1. pravěk – období od vynálezu telefonu do uvedení prvního PC na trh v roce 1981
2. středověk – období od roku 1981 do případu Citibank v roce 1994
3. novověk – od případu Citibank až do současné doby

6.1.1 Počítačový pravěk

Není úplně jasné, do kterého období zařadit zrod oboru počítačová kriminalita. Počítačový pravěk spadá do období, kdy informační technologie nebyla ještě příliš obvyklá. Přesto se v tomto období staly činy, které by se daly považovat za první činy se znaky počítačové kriminality.

V roce 1801 se stal první takový čin.[65] V této době vynalezl francouzský tkadlec Jacquard stroj, který automatizoval jednotlivé úkony při tkaní speciálních látek. Jeho zaměstnanci dostali strach z toho, že by je tento vynález mohl časem nahradit. Z tohoto důvodu tento vynález nepřijmuli a započala série sabotáží. To donutilo Jacquarda zastavit další vývoj tohoto stroje.

Počátek počítačového věku je datován až k roku 1946. 2. února tohoto roku byl dokončen vývoj historicky prvního počítače ENIAC. Jeho vývoj byl zahájen roku 1943 v Pensylvánii. Tento druh počítačů zabíral celou místnost a vlastnily je jen velké korporace.[66]

V tomto období se odehrály dvě skutečnosti, které mají souvislost s počítačovou kriminalitou. V ČR je znám v tomto období pouze jeden případ. Tento případ bude zmíněn v kapitole *Historie počítačové kriminality v ČR*.

První skutečností má souvislost s upravováním programů. Programátoři těchto velkých sálových počítačů tehdy pracovali s programy, které nebyly dokonalé, proto tyto programy začali všemožně upravovat. Tyto zásahy do programů za účelem vylepšení se označovaly pojmem hack. Programátorům upravujícím tyto programy se logicky říkalo hackeři. Časem tento termín však získal i jiný význam a dnes si již pod pojmem hacking většina lidí vybaví nelegální činnosti.

[64] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 17.
[65] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 18.
[66] *Programming the ENIAC*. COLUMBIA UNIVERSITY. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.columbia.edu/cu/computinghistory/eniac.html>.

Druhou skutečností je myšlen případ známý pod pojemam Cap 'n Crunch. Cap 'n Crunch byly cereálie určené pro děti. Do těchto cereálií se přidávaly píšťalky, které vydávaly zvuk o stejné frekvenci (2 600 HZ) jako používala telefonní společnost AT&T. Toho si všiml veterán vietnamské války John Draper a pomocí píšťalky a zařízení Blue box dokázal uskutečnit hovory zdarma. Zveřejněním těchto závad se zrodila oblast phreaking, to znamená nelegální telefonie.[67] [68]

6.1.2 Počítačový středověk

Počítačový středověk začíná rokem 1981, kdy byl na trh uveden první IBM (osobní) počítač. Velikost tohoto nového typu počítačů zajistila brzké rozšíření do domácností a brzy došlo ke spojení počítačů pomocí modemů. V počítačovém středověku je důležité období, kdy počítačové nadšence, kteří pronikali systémem ze zvědavosti a bez negativních úmyslů, vystřídali lidé, kteří proniknutím do systému chtěli způsobit škodu.

Další důležitou událostí v počítačovém středověku je nástup virů. Prvním z nich byl vir, který se nazývá trojský kůň. Tyto viry byly maskované tím, že nejdříve vypadaly jako neškodný nebo užitečný program (např. hra nebo spořič obrazovky) ve skutečnosti ale uživatelům způsobovaly škodu. Roku 1986 se objevil první vir, nazvaný Brain. Vytvořili ho bratři Basit a Amjads Farooq Alvi z Pakistánu. Dávali ho jako bonus lidem, kteří si u nich obstarávali nelegální software. V roce 1988 se zrodil první internetový červ, který vytvořil student Robert Morris.

Tento vir byl údajně vypuštěn omylem. Internetový červ se šířil velkou rychlostí a nakonec napadl asi 2000 počítačů. Morris byl odsouzen k tříletému podmíněnému trestu.[69]

Dále je v tomto období důležitý vznik CD-ROM a CD-R. CD-R mechaniky. Díky těmto technologiím vznikla oblast nazvaná počítačové pirátství. [70]

[67] *WHO IS JOHN DRAPER AKA CAPTAIN CRUNCH* [online]. John Draper. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.webcrunchers.com/who-is-john-draper-aka-captain-crunch>.
[68] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 18.
[69] *How The \'Computer Wizard\' Who Created The First Internet Virus Got Off Without A Day Of Jail* [online]. BUSINESS INSIDER. 2015 [cit. 2016-03-16]. Dostupné z: <http://www.businessinsider.com/why-robert-morris-didnt-go-to-jail-2013-1>.
[70] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 21.

6.1.3 Počítačový novověk

V počítačovém středověku byla počítačová kriminalita prudce rozšířena, ale v novověku je hlavně díky rozšíření internetu a počítačů rozšířena ještě daleko více. Zakončuje ho případ Citibank,[71] kdy ruská hackerská skupina pronikla do počítačů banky Citibank a odcizila částku 10 mil. dolarů. Velkou roli v novověku hraje nový přístup sdílení dat nazvaný peer to peer (P2P), nebo klient-klient. To znamená, že mezi sebou komunikují jednotliví uživatelé a nabízejí si svůj obsah, který může být škodlivý. Počítačové viry se v tomto období stávají čím dál dokonalejšími a tím nebezpečnějšími. Mezi nejznámější patři vir nazvaný Melissa[72] z roku 1999, který se sám rozesílal pomocí emailových schránek.

V roce 1999 byla také v provozu hudební služba Napster,[73] vytvořena Shawnem Fannigem. Tato služba fungovala právě na principu peer to peer. To uživatelům této služby umožňovalo sdílení a kopírování hudby mezi sebou. Po tomto programu se objevily řady dalších podobných programů a jejich kontrola nebyla dostatečná.

6.2 Historie počítačové kriminality v ČR

Protože počítače byly u nás veřejnosti déle nedostupné, počítačová kriminalita je u nás relativně novým oborem. První počítače dostupné pro veřejnost se objevily až po roce 1989. Přesto se dá tvrdit, že první případy[74] naplňující znaky trestných činů se staly na přelomu 70. a 80. let. V této době byly používány pouze velké sálové počítače.

První známý počítačový trestní čin v České republice se stal na Úřadu důchodového zabezpečení. Nespokojený zaměstnanec úmyslně znehodnotil záznamy na magnetických páskách, použil k tomu obyčejný magnet. Za tento trestní čin byl odsouzen k více než 10. letům odnětí svobody.

Další případ počítačové trestné činnosti se stal na konci 80. Let. Několik zaměstnanců výpočetního střediska úmyslně znehodnotilo počítačové zařízení. Chtěli tím dosáhnout jeho výměny za kvalitnější zařízení. Tito zaměstnanci byli tehdy původně stíháni za sabotáž. Později bylo stíhání několikrát změněno a nakonec zastaveno z důvodu amnestie prezidenta ČSSR.

---

[71] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 28.
[72] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 32.
[73] NĚMEC, R. *Napster – je to krádež?* [online]. Chrisnet.cz. 2000 [cit. 2016-03-16]. Dostupné z: <http://www.christnet.cz/clanky/1375/napster_je_to_kradez.url>.
[74] Smejkal, Vl., *Informační a počítačová kriminalita v České republice*, MV ČR, 1999.

Největší vliv na rozvoj informačních technologií a tím i počítačové kriminality v ČR mají dva důležité faktory. Prvním je otevření trhu zahraničním účastníkům po roce 1989 a s ním i masivní dovoz počítačové technologie na naše území. Druhým největším důvodem je oficiální připojení k internetu. ČSFR byla oficiálně připojena 13. února 1992.[75]

6.3 Předpokládaný vývoj počítačové kriminality

Předpoklady pro internet v roce 2020 podle networkworld:[76]

- Více uživatelů na internetu
- Internet bude více rozptýlen i z hlediska geografie
- Menší spotřeba energie pro provoz internetu
- Správa internetové sítě bude více automatická
- Více hackerských útoků na internetu

Předpoklady pro internet podle businessinsider[77]

Za pět let od roku 2015 bude mít každý člověk možnost připojení k internetu. V Americe bylo v roce 2005 připojeno 66% populace, v roce 2015 už 87% a předpokládá se, že do roku 2020 bude připojeno i zbylých 13% pomocí neziskových organizací např. Connect2Compete. Více zařízení bude mít možnost připojení - od praček až k zámkům u dveří.

Do patnácti let od roku 2015 budou existovat virtuální školy. V publikaci Thinking forward to 2030[78] se píše, že učitelé budou využívat internetový přístup k efektivnějšímu učení žáků.

[75] KRČMAŘOVÁ, G. *20 let Internetu v České republice* [online]. IKAROS. 2012 [cit. 2015-12-13]. Dostupné z: <http://ikaros.cz/20-let-internetu-v-ceske-republice>.
[76] *10 fool-proof predictions for the Internet in 2020* [online]. NETWORKWORLD. 2010 [cit. 2016-02-04]. Dostupné z: <http://www.networkworld.com/article/2238913/wireless/10-fool-proof-predictions-for-the-internet-in-2020.html>.
[77] *Here\'s what the internet will look like in 5, 10, and 15 years* [online]. BUSINESS INSIDER. 2015 [cit. 2016-02-04]. Dostupné z: <http://www.businessinsider.com/sc/future-of-the-internet-in-5-years-2015-2>.
[78] *GrantThornton* [online]. Thinking forward to 2030. 2013 [cit. 2016-02-04]. Dostupné z: <http://www.grant-thornton.co.uk/Global/Publication_pdf/Thinking-Newsletter-Dec-2013.pdf>.

Internet bude pravděpodobně zasahovat ještě do více sfér, bude se na něj možno připojit z více zařízení a bude více uživatelů. Je otázkou, zdali je dobře, že bude internet pravděpodobně rozšířen i do věcí jako jsou bezpečnostní zámky.

V roce 2015 vláda ČR schválila národní strategii kybernetické bezpečnosti na pět let dopředu.[79]

Hlavní úkoly této strategie jsou:[80]

- vytvoření efektivního modelu spolupráce mezi subjekty kybernetické bezpečnosti na národní úrovni
- vytvořit koordinovaný postup pro zvládání incidentů a metodologii pro hodnocení rizik
- zohledňovat odpovídajícím způsobem neustále se vyvíjející problematiku kybernetických hrozeb
- aktivní mezinárodní spolupráce a navazovat vztahy s dalšími státy
- účastnit se a organizovat mezinárodní školení
- podporovat vznik dalších pracovišť typu CERT a CSIRT v ČR

McAfee je americká globální firma zabývající se bezpečnostním softwarem. Firma se zabývá i výzkumem, v kterém odhaduje budoucnost kybernetických útoků na pět let dopředu, to znamená až do roku 2020. Výzkum klade důraz na 14 klíčových oblastí[81] počítačové kriminality a zabývá se jejich prevencí. Do těchto oblastí patří např. hardware, tzv. ransomware což je druh malwaru, který zabraňuje přístup k počítači, online platební systémy, kyber-špionáž, přenosná elektronika, automobily, integrita a hackerství.

[79] *Vláda schválila novou strategii kybernetické bezpečnosti na příštích pět let* [online]. Právní rádce. 2015 [cit. 2016-02-04]. Dostupné z: <http://pravniradce.ihned.cz/c1-63549360-vlada-schvalila-novou-strategii-kyberneticke-bezpecnosti-na-pristich-pet-let>.

[80] nckb. *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020*. 2015.

[81] DIMITROVA, M. *How Will Cyber Crime Change by 2020? McAfee's Report* [online]. SENSORSTECHFORUM. 2015 [cit. 2016-02-05]. Dostupné z: <http://sensorstechforum.com/how-will-cyber-crime-change-by-2020-mcafees-report/>.

Předpoklady počítačové kriminality podle ESET pro rok 2016[82]

Eset je slovenská forma zabývající se bezpečnostním softwarem. Byla založena roku 1992 a je oceňována jako nejúspěšnější slovenská firma.[83]

- Více SCAM programů a malwaru (hlavně ransomwaru) fungujících společně
- Cílem ransomwaru se stane více zařízení než počítač
- Více uživatelů počítačových technologií a více kybernetických útoků
- Adobe flash a Oracle Java se stanou častým cílem útoků (udržujte je aktualizované)
- DDoS útoků na různé oblasti webových stránek také přibyde
- Útoky na kreditní karty budou stále pokračovat
- SCADA (monitorování tech. zařízení a procesů) zajistí práci více lidem
- Společnosti budou nadále prodávat zařízení a různé aplikace, které vyžadují osobní údaje
- (Doufejme) více výrobců bude vydávat oznámení o odhalení slabých stránek jejich produktů
- Více zařízení a účtů bude novelizováno metodami, které zvýší bezpečnost
- Po celém světě se budou vlády zabývat kybernetickou bezpečností a počítačovou kriminalitou

[82] *ESET predictions and trends for cybercrime in 2016* [online]. welivesecurity. 2015 [cit. 2016-03-16]. Dostupné z: <http://www.welivesecurity.com/2015/12/23/eset-predictions-for-cybercrime-trends-in-2016/>.
[83] *Firma roka je Eset a najúspešnejšia banka VÚB* [online]. SME Ekonomika. 2009 [cit. 2016-03-16]. Dostupné z: <http://ekonomika.sme.sk/c/5103938/firma-roka-je-eset-a-najuspesnejsia-banka-vub.html>.

Předpoklady z ostatních zdrojů pro budoucnost počítačové kriminality[84] [85] [86] [87] [88]

- Uživatelé budou mít více internetových účtů a digitálních zařízení
- Mobilní platby budou tvořit více než 50% všech finančních transakcí
- Kybernetická bezpečnost bude cílem politických
- Více online účtů
- Více digitálních zařízení v roku 2016 než kdy jindy
- Pachatelé kybernetické kriminality najdou více způsobu, pomocí kterých budou napadat internetové platby, online účty apod.
- Kybernetická bezpečnost bude globálně prioritní otázkou
- Rekordní počet kybernetických útoků v roce 2016
- V roce 2019 dosáhnou škody napáchané kybernetickou kriminalitou přes 2 triliony dolarů
- Čím dál menší přístroje budou mít přístup k internetu
- V roce 2020 bude kybernetická kriminalita rozdělena na dvě skupiny pachatelů, první skupina bude útočit na velké korporace a druhá skupina bude útočit na jednotlivé lidi
- Hackeři budou dále krást osobní informace a data o zákaznících a jejcich online aktivitách

[84] BAUMHOF, A. *6 cybercrime predictions for 2016* [online]. The Business Journals. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.bizjournals.com/bizjournals/how-to/growth-strategies/2016/01/6-cybercrime-predictions-for-2016.html?page=all>.

[85] *ThreatMetrix 2016 internet predictions* [online]. ThreatMetrix. 2015 [cit. 2016-03-16]. Dostupné z: <https://www.threatmetrix.com/threatmetrix-2016-cybercrime-predictions/>.

[86] *Cybercrime will Cost Businesses $2 Trillion by 2019* [online]. SECURITY. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.securitymagazine.com/articles/86352-cybercrime-will-cost-businesses-2-trillion-by-2019>.

[87] RIGOLI, E. *Cybercrime Outlook 2020: The Good, Bad, and Ugly for Your Online Privacy* [online]. PrivateWifi. 2011 [cit. 2016-03-16]. Dostupné z: <http://blog.privatewifi.com/cybercrime-outlook-2020-the-good-bad-and-ugly-for-your-online-privacy/>.

[88] JOURNITZ, J. *Top 5 Cybercrime predictions for 2016* [online]. IT Security. 2016 [cit. 2016-03-16]. Dostupné z: <http://research.pomona.edu/itsecurity/2016/01/05/top-5-cybercrime-predictions-for-2016/>.

6.4 Shrnutí kapitoly

V této kapitole jsou obsaženy předpoklady pro internet, počítače a jejich bezpečnost a kybernetickou kriminalitu z různých zdrojů až do roku 2020. Mezi zdroji jsou i firmy ESET a McAfee, které se zabývají antivirovými programy. Na základě prudkého vývoje informačních technologií a počítačové kriminality za posledních patnáct let se předpokládá, že úroveň počítačové kriminality bude nadále stoupat spolu s růstem internetu. Kybernetických útoků bude přibývat v každém roce a jejich nebezpečnost bude také stoupat.

Mezi některé předpoklady, které se objevují nejčastěji, patří: více uživatelů informačních technologií a internetu, více kybernetických útoků, více internetových účtů, rozptýlení internetu z hlediska geografie, informační technologie, internet i počítačová kriminalita bude zasahovat do více oblastí života.

Závěr

Hlavním cílem této bakalářské práce je objasnění pojmu počítačové kriminality. V druhé kapitole *počítače a internet – pojem a charakteristika* jsou uvedeny základní pojmy nezbytné k pochopení problematiky počítačové kriminality a této práce. Jsou zde uvedeny a objasněny pojmy internet a kyberprostor, protože to je „prostředí“, v kterém se počítačová kriminalita vyskytuje. Protože počítač je předmětem počítačové kriminality, je v této kapitole stručně popsán. Posledním základním pojmem je kybernetický útok. Otázka ohledně pojmu počítačová kriminalita je řešena v průběhu celé práce.

Dalším cílem této práce je objasnění příčin počítačové kriminality a analýza často se vyskytujících forem počítačové kriminality. V třetí kapitole *Etiologie počítačové kriminality a její formy* jsou tyto otázky vyřešeny. V této kapitole jsou příčiny rozděleny podle toho, jestli jsou specifické pro počítačovou kriminalitu nebo společné pro více druhů kriminalit. Mezi příčiny specifické jsou uvedeny tyto: počítačové prostředí, nezkušení uživatelé a neznalost činností, které jsou v rozporu se zákonem. Příčiny společné pro více druhu kriminalit jsou dědičnost, sociální prostředí a média.

V druhé části třetí kapitoly jsou rozebrány často se vyskytující formy počítačové kriminality. Jsou to: malware, hacking, phishing a pharming, sniffing, warez, kyberšikana a DoS útoky. V závěru kapitoly je pro zajímavost popsán kybernetický DoS útok z roku 2000, při němž byly napadeny známé servery Fifa, Amazon, eBay a CNN.

Ve čtvrté kapitole nazvané *Fenomenologie počítačové kriminality* jsou rozebrány trestné činy § 230 - 232 TZ a jejich skutková podstata. V další části čtvrté kapitoly je provedena analýza dat z policejních statistik, konkrétně je porovnáván poměr objasněných a zjištěných trestných činů za posledních pět let (2010-2015). Z tabulky, která obsahuje počet trestných činů § 230 – 232 TZ je viditelné, že se počítačová kriminalita rychle rozrůstá, ale objasněnost těchto činů nestoupá. Dále je zde graf ukazující tyto trestné činy v jednotlivých krajích ČR za rok 2010 a 2015 a v poslední části této kapitoly je vypočítán index pro každý kraj, z kterého lze určit, kde je míra těchto trestných činů největší. Podle indexu vyšlo, že míra je nejvyšší v kraji Libereckém a Olomouckém.

Pátá kapitola je nazvána *Pachatelé počítačové kriminality*. Cílem této části práce je rozbor pachatelů. Jsou zde uvedeny společné znaky pachatelů a to: mladost, odborné vzdělání a problémy v oblasti začleňování se do společnosti. Dále je zde řešen motiv pachatelů, jímž nejčastěji bývá osobní obohacení. V poslední části kapitoly je uvedeno stručné rozdělení pachatelů a jejich popis.

Posledním cílem práce je podat ucelený pohled na historický a předpokládaný vývoj počítačové kriminality. Kapitola *Historický a předpokládaný vývoj počítačové kriminality* začíná historií počítačové kriminality ve světě, je zde rozdělení podle Matějkovy knihy[89] na počítačový pravěk, středověk a novověk. Dále je v kapitole popsán historický vývoj v ČR. Jsou zde uvedeny první trestné činy souvislé s počítači, které byly provedeny na území ČR. Třetí část kapitoly je věnována předpokládanému vývoji počítačové kriminality. Zde jsou uvedeny některé předpoklady až do roku 2020.

Cíle této práce jsou objasnit základní pojmy, zejména pojem počítačová kriminalita, objasnit její příčiny, analyzovat nejčastější nelegální konání proti počítačům nebo páchané na počítači nebo prostřednictvím počítače, zpracovat fenomenologii počítačové kriminality a odhalit společné znaky pachatelů počítačové kriminality. Všechny cíle byly splněny.

[89] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002.

Seznam použitých zdrojů

Literární zdroje

1. BRENNER, Susan W. *Cybercrime: criminal threats from cyberspace*. Santa Barbara, Calif.: Praeger, 2010, 281 s. ISBN 9780313365478.
2. CRAIG, Paul P a Ron HONICK. *Softwarové pirátství bez záhad. 1. vyd*. Praha: Grada, 2008, 224 s. ISBN 978-80-247-1765-4.
3. ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče.* 1. vyd. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.
4. GIBSON, William. *Neuromancer*. New York: Ace Books, 1984, 271 s. ISBN 0441569595.
5. HARRIS, Shon. *Hacking: manuál hackera.* 1. vyd. Praha: Grada, 2008, 399 s. ISBN 978-80-247-1346-5.
6. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.
7. KUCHTA, Josef a Helena VÁLKOVÁ. *Základy kriminologie a trestní politiky*. Vyd. 1. Praha: C.H. Beck, 2005, 544 s. Beckovy mezioborové učebnice. ISBN 80-7179-813-4.
8. MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, 106 s. ISBN 80-7226-419-2.
9. MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez tajemství.* 3. aktualiz. vyd. Brno: Computer Press, 2003, 660 s. ISBN 80-7226-948-8.
10. ROGERS, Vanessa. Kyberšikana: *pracovní materiály pro učitele a žáky i studenty.* Vyd. 1. Praha: Portál, 2011, 97 s. ISBN 978-80-7367-984-2.
11. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2.
12. HAKEN, D. *Cyborg @ cyberspace? : an ethnographer : looks to the future.* New York: Routledge, 1999, 264 s. ISBN 0415915589.

Elektronické zdroje

1. *10 fool-proof predictions for the Internet in 2020* [online]. NETWORKWORLD. 2010 [cit. 2016-02-04]. Dostupné z: <http://www.networkworld.com/article/2238913/wireless/10-fool-proof-predictions-for-the-internet-in-2020.html>.
2. *Adware* [online]. TechTerms.com. 2015 [cit. 2015-10-04]. Dostupné z: <http://techterms.com/definition/adware>.
3. *Anonymous* [online]. Novinky.cz. 2016 [cit. 2016-03-26]. Dostupné z: <http://tema.novinky.cz/anonymous>.
4. *Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and Paypal* [online]. INDEPENDENT. 2016 [cit. 2016-03-26]. Dostupné z: <http://www.independent.co.uk/news/uk/crime/anonymous-hackers-jailed-for-ddos-attacks-on-visa-mastercard-and-paypal-8465791.html>.
5. BAUMHOF, A. *6 cybercrime predictions for 2016* [online]. The Business Journals. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.bizjournals.com/bizjournals/how-to/growth-strategies/2016/01/6-cybercrime-predictions-for-2016.html?page=all>.
6. *Co je to Internet a jak funguje?* [online]. Datacentrum WEDOS, 2010 [cit. 2015-11-10]. Dostupné z: <http://datacentrum.wedos.com/a/17/co-je-internet-jak-funguje.html>.
7. *CO JE TO KYBERŠIKANA A JAK SE PROJEVUJE?* [online]. bezpečně-online.cz. 2010 [cit. 2016-02-01]. Dostupné z: <http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html>.
8. *Cyberattack* [online]. techopedia. 2010 [cit. 2015-06-04]. Dostupné z: <http://www.techopedia.com/definition/24748/cyberattack>.
9. *Cybercrime will Cost Businesses $2 Trillion by 2019* [online]. SECURITY. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.securitymagazine.com/articles/86352-cybercrime-will-cost-businesses-2-trillion-by-2019>.
10. *Denial of Service Attacks* [online]. INCAPSULA. 2015 [cit. 2015-12-14]. Dostupné z: <https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html>.

11. DIMITROVA, M. *How Will Cyber Crime Change by 2020? McAfee's Report* [online]. SENSORSTECHFORUM. 2015 [cit. 2016-02-05]. Dostupné z: <http://sensorstechforum.com/how-will-cyber-crime-change-by-2020-mcafees-report/>.
12. DOČEKAL, D. *Jak se bránit phishingu* [online]. LUPAcz. 2008 [cit. 2016-02-01]. Dostupné z: <http://www.lupa.cz/clanky/jak-se-branit-phishingu/>.
13. *ESET predictions and trends for cybercrime in 2016* [online]. welivesecurity. 2015 [cit. 2016-03-16]. Dostupné z: <http://www.welivesecurity.com/2015/12/23/eset-predictions-for-cybercrime-trends-in-2016/>.
14. *Firma roka je Eset a najúspešnejšia banka VÚB* [online]. SME Ekonomika. 2009 [cit. 2016-03-16]. Dostupné z: <http://ekonomika.sme.sk/c/5103938/firma-roka-je-eset-a-najuspesnejsia-banka-vub.html>.
15. *GrantThornton* [online]. Thinking forward to 2030. 2013 [cit. 2016-02-04]. Dostupné z: <http://www.grant-thornton.co.uk/Global/Publication_pdf/Thinking-Newsletter-Dec-2013.pdf>.
16. *Hacking Theft of $10 Million From Citibank* [online]. Revealed. latimes. 2015 [cit. 2015-06-04]. Dostupné z: <http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system>.
17. *Here\'s what the internet will look like in 5, 10, and 15 years* [online]. BUSINESS INSIDER. 2015 [cit. 2016-02-04]. Dostupné z: <http://www.businessinsider.com/sc/future-of-the-internet-in-5-years-2015-2>.
18. HLAVÁČ, J. *Spyware konečně definován!?* [online]. diit.cz. 2005 [cit. 2015-10-04]. Dostupné z: <http://diit.cz/clanek/spyware-konecne-definovan>.
19. HOFFMAN, CH. *Hackers Hat Colors Explained* [online]. How To Geek. 2013 [cit. 2016-02-01]. Dostupné z: <http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/>.
20. *How The \'Computer Wizard\' Who Created The First Internet Virus Got Off Without A Day Of Jail* [online]. BUSINESS INSIDER. 2015 [cit. 2016-03-16]. Dostupné z: <http://www.businessinsider.com/why-robert-morris-didnt-go-to-jail-2013-1>.
21. *Charles Babbage* [online]. CharlesBabbage.net. 2013 [cit. 2016-01-23]. Dostupné z: <http://www.charlesbabbage.net/>.

22. *Internet Users* [online]. internet live stats, 2015 [cit. 2015-12-30]. Dostupné z: <http://www.internetlivestats.com/internet-users/>.
23. JOURNITZ, J. *Top 5 Cybercrime predictions for 2016* [online]. IT Security. 2016 [cit. 2016-03-16]. Dostupné z: <http://research.pomona.edu/itsecurity/2016/01/05/top-5-cybercrime-predictions-for-2016/>.
24. KRČMAŘOVÁ, G. *20 let Internetu v České republice* [online]. IKAROS. 2012 [cit. 2015-12-13]. Dostupné z: <http://ikaros.cz/20-let-internetu-v-ceske-republice>.
25. KUŽEL, S. *Kybernetická kriminalita I: Co se děje v kyberprostoru* [online]. BusinessIT. 2015 [cit. 2015-06-04]. Dostupné z: <http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyber prostoru.php>.
26. *Kyberšikana zabíjí – sebevraždy dívek hýbou Británií, Kanadou i Itálií* [online]. Česká televize. 2013 [cit. 2016-02-02]. Dostupné z: <http://www.ceskatelevize.cz/ct24/svet/1081921-kybersikana-zabiji-sebevrazdy-divek-hybou-britanii-kanadou-i-italii>.
27. *Malware* [online]. TechTerms.com. 2015 [cit. 2015-10-04]. Dostupné z: <http://techterms.com/definition/malware>.
28. MOOS, J. *hackeři z LulzSec jdou za mříže, lídr je zradil (1)* [online]. *CDR*. 2012 [cit. 2016-03-26]. Dostupné z: <http://cdr.cz/clanek/lulzsec-vznik-a-pad-tymova-zrada>.
29. NĚMEC, R. *Napster – je to krádež?* [online]. Chrisnet.cz. 2000 [cit. 2016-03-16]. Dostupné z: <http://www.christnet.cz/clanky/1375/napster_je_to_kradez.url>.
30. *Nezletilý kanadský hacker Mafiaboy čelí řadě obvinění* [online]. ING. 2001 [cit. 2015-12-14]. Dostupné z: <http://ihned.cz/c1-10329780-nezletily-kanadsky-hacker-mafiaboy-celi-rade-obvineni>.
31. OBR, J. *Sniffing: Odposlech datové komunikace* [online]. ITBIZ. 2009 [cit. 2016-02-02]. Dostupné z: <http://www.itbiz.cz/sniffing-odposlech-datove-komunikace>.
32. *Phishing a pharming* [online]. bezpecnyinternet.cz. 2010 [cit. 2016-02-01]. Dostupné z: <http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx>.

33. *Počítačové viry* [online]. ivt.wz.cz. 2014 [cit. 2015-06-04]. Dostupné z: <http://ivt.wz.cz/strnad/viry.htm>.
34. *Programming the ENIAC*. COLUMBIA UNIVERSITY. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.columbia.edu/cu/computinghistory/eniac.html>.
35. PŘIBIL, T. *Zákeřný útok jménem DoS* [online]. SystemOnline. 2006 [cit. 2015-12-14]. Dostupné z: <http://www.systemonline.cz/it-security/zakerny-utok-jmenem-dos.htm>.
36. RENATO, M. E. *Cesare Lombroso: A Brief Biography* [online]. Cerebromente. 1997 [cit. 2016-02-04]. Dostupné z: <http://www.cerebromente.org.br/n01/frenolog/lombroso.htm>.
37. RIGOLI, E. *Cybercrime Outlook 2020: The Good, Bad, and Ugly for Your Online Privacy* [online]. PrivateWifi. 2011 [cit. 2016-03-16]. Dostupné z: <http://blog.privatewifi.com/cybercrime-outlook-2020-the-good-bad-and-ugly-for-your-online-privacy/>.
38. SAUNDLE P. *Cyber crime costs global economy $445 billion a year*. [online]. REUTERS, 2014 [cit. 2015-12-30]. Dostupné z: <http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609>.
39. *Stahování z torrentů* [online]. Všebořice.net. 2011-2013 [cit. 2016-02-03]. Dostupné z: <http://www.vseborice.net/navody/torrenty/0>.
40. STACH, J. *PC slaví 33 let – IBM PC model 5150 se objevil 12.8.1981 – po 33 je PC stále na vzestupu!* [online]. DDWORLD.cz 2014 [cit. 2015-06-04]. Dostupné z: <http://www.ddworld.cz/aktuality/aktuality/pc-slavi-33-let-ibm-pc-model-5150-se-objevil-12.8.1981-po-33-je-pc-stale-na-vzestupu-2.html>.
41. *The First Internet Worm & Internet Worm Virus* [online]. streetdirectory. 2015 [cit. 2015-06-04]. Dostupnéz: <http://www.streetdirectory.com/travel_guide/113972/computers_and_the_internet/the_first_internet_worm__internet_worm_virus.html>.
42. *ThreatMetrix 2016 internet predictions* [online]. ThreatMetrix. 2015 [cit. 2016-03-16]. Dostupné z: <https://www.threatmetrix.com/threatmetrix-2016-cybercrime-predictions/>.
43. *Vláda schválila novou strategii kybernetické bezpečnosti na příštích pět let* [online]. Právní rádce. 2015 [cit. 2016-02-04]. Dostupné z: <http://pravniradce.ihned.cz/c1-63549360-vlada-schvalila-novou-strategii-kyberneticke-bezpecnosti-na-pristich-pet-let>.

44. VLACH, J. *Média v kriminologické perspektivě* [online]. PREVENCE KRIMINALITY. 2013 [cit. 2016-03-24]. Dostupné z: <http://www.prevencekriminality.cz/evt_file.php?file=169>.
45. *WHO IS JOHN DRAPER AKA CAPTAIN CRUNCH* [online]. John Draper. 2016 [cit. 2016-03-16]. Dostupné z: <http://www.webcrunchers.com/who-is-john-draper-aka-captain-crunch>.

Legislativní dokumenty

1. ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5.
2. Zákon č. 40/2009 Sb., trestní zákoník.

Ostatní zdroje

1. Český statistický úřad – statistiky.
2. LÁTAL, I., Počítačová (informační) kriminalita a úloha policisty při jejím řešení, materiál z přílohy časopisu Policista č. 3/1998, Policejní akademie České republiky Praha,1998.
3. Policie ČR – statistiky.

Seznam tabulek a grafů

Tabulky:

Graf: