VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA V ČESKÉ REPUBLICE

Autor práce: František Dubský

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinované

Vedoucí práce: Mgr. František Šnitr

Katedra: Katedra právních oborů a bezpečnostních studií

2017

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 Mgr. Františku Šnitrovi, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

DUBSKÝ, F. *Počítačová kriminalita v České Republice : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2017. 52 s. Vedoucí bakalářské práce : Mgr. František Šnitr.

Klíčová slova: počítač, internet, kriminalita, bezpečnost, pachatel, legislativa, trestný čin

Práce analyzuje současný stav počítačové kriminality, její historický vývoj a vývoj budoucí. Shrne nejčetnější druhy této kriminality, její pachatele a podmínky pro páchání této trestné činnosti v České Republice. Práce poskytne pohled na tento fenomén, jak z pohledu autora, tak z pohledu expertů různých oborů, prognóz, strategií i z pohledu Policie ČR. Po následné komparaci získaných informací, bude odvozen závěr práce. Vše bude zkoumáno za použití důvěryhodných internetových zdrojů, literatury a legislativních dokumentů.

ABSTRACT

DUBSKÝ, F. *Computer crime in the Czech Republic : Bachelor thesis.* České Budějovice : The College of European and Regional Studies, 2017. 52 p. Supervisor : Mgr. František Šnitr.

Key words: computer, internet, crime, security, offender, legislation, crime

The thesis analyzes the current state of cybercrime, its historical development and its future development. It summarizes the most common types of this crime, its perpetrators and the conditions for committing this crime in the Czech Republic. The work will give a look at this phenomenon, both from the point of view of the author and from the point of view of experts of various fields, prognoses, strategies and from the point of view of the Police of the Czech Republic. After the subsequent comparison of the obtained information, the conclusion of the thesis will be derived. Everything will be explored using trusted internet resources, literature, and legislative documents.

Obsah

Úvod

Není to ani tak dávno, co lidé psali na psacích strojích, ve škole se používaly tabule, na které se psalo křídou a v různých povoláních se data uchovávala v obrovských databázích tvořených papírovými archy uchovávanými v papírových či plastových šanonech. Lidé spolu komunikovali buď přímo, telefonicky nebo psaním dopisů. Kriminalita se odehrávala osobně, krádežemi, podvodnými jednáními za osobní účasti pachatele.

Sféra kybernetické bezpečnosti se stává důležitější než kdy dříve a již dnes platí za jeden z určujících faktorů bezpečnostního prostředí České republiky. Kybernetická bezpečnost prezentuje komplex organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá rozpoznávat, posuzovat a řešit hrozby v kyberprostoru, omezovat kybernetická rizika a vylučovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže prostřednictvím posilování důvěrnosti, integrity a dostupnosti dat, systémů a jiných prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka. Zabezpečení kybernetické bezpečnosti státu prezentuje jednu ze zásadních výzev současné doby.[1]

S příchodem počítačů a zejména pak internetu se tedy všechno změnilo. Ať už osobní životy lidí, tak významně také i profesní život, život celé společnosti. Počítače se staly součástí běžného denního života každého z nás, a to jak dětí, dospělých, tak i seniorů. Lidé jsou tzv. „online“ kdekoliv se zrovna nachází, a to zejména díky chytrým mobilním telefonům, kterým disponuje rovněž skoro každý. S tím však bohužel souvisí i proměna, respektive rozšíření kriminality do oblasti internetu. Internet totiž poskytuje pro kriminalitu tolik významnou anonymitu, která je navíc podstatným problémem, ať už v oblasti jejího trestání a potírání.

[1] POLICIE ČR. Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). Praha: Policejní prezidium České republiky. 2017, s. 5.

1 Cíl a metodika bakalářské práce

Cílem práce bude na základě získaných informací analyzovat současný stav počítačové kriminality, její historický vývoj a na základě zjištěných výsledků predikovat vývoj budoucí. Na základě současného stavu ověřit funkčnost přijatých preventivních opatření, případně nová opatření navrhnout. Základním problémem práce jsou případné budoucí hrozby v počítačové kriminalitě a přijatá preventivní opatření.

Z hlediska použitých metod a technik pro zpracování práce lze zmínit především studium odborných pramenů. Pro zpracování bakalářské práce bude využito dostupné literatury, informací získaných z Národní strategie kybernetické bezpečnosti České Republiky na období let 2015 až 2020 (NBÚ), Národního centra kybernetické bezpečnosti (NCKB), údajů Policie ČR, ale i autorů odborných děl či článků zabývajících se oblastí kybernetické bezpečnosti.

Vyhledané zdroje budou nejprve podrobeny analýze, tedy procesu reálného či myšlenkového rozkladu zkoumané oblasti na dílčí části, které se poté stávají předmětem dalšího zkoumání. Půjde o rozbor faktů od celku k částem. Prostřednictvím analýzy informací budou odhalovány odlišné vlastnosti jevů a procesů. Po analýze dat bude navazovat syntéza jakožto myšlenkové propojení informací získaných analytickými metodami v celek, se záměrem pochopit vzájemné souvislosti.

Důležitou metodou bude také komparace získaných informací, neboť bude snaha získat a porovnat informace z různých zdrojů, tedy například statistiky Policie ČR, závěry či myšlenky expertů z oblasti ekonomiky, informačních technologií aj., různé strategie vývoje aj. Při vyvozování závěrů či prognóz vývoje počítačové kriminality bude využito také metody analogie, při níž se vychází ze souboru typových, předtím již (jak zdárně, tak i neúspěšně) řešených případů. Půjde o odvození závěrů dle podobnosti s jinými závěry odborníků, prognóz či predikcí, situací aj.

2 Internet a jeho rizika

Internet prezentuje celosvětovou počítačovou síť, která spojuje vybrané menší sítě, prostřednictvím sady protokolů zvaných IP (Internet Protocol). Název Internet má svůj původ v anglickém jazyce ve slově network (síť), na základě kterého tradičně končily názvy amerických počítačových sítí. Předpona inter (mezi) vyjadřuje, že internet propojil a vstřebal různé starší, dílčí, specializované, proprietální a místní sítě. Význam internetu tkví v přenášení informací a poskytování různých služeb, jako například elektronická pošta, chat, webové stránky, sdílení fotografií, hraní online her, vyhledávání informací do školy či práce aj.[2]

V rámci internetu mohou uživatelé využívat mnoho jeho různých služeb, které zabezpečují počítačové programy komunikující skrze protokoly. K základním službám internetu patří systém webových stránek zobrazovaných na webovém prohlížeči (WWW), dále pak elektronická pošta, online (živá) komunikace mezi uživateli, telefonování přes internet, zasílání různých souborů, sdílení souborů, připojování k vzdáleným počítačům a jiné služby (online hry aj.). Větší část zajímavých obsahů se na internetu nachází právě na WWW. Pro vyhledávání se využívají různé specializované služby – internetové katalogy. K nejznámějším patří Seznam.cz, Centrum.cz, Yahoo aj. Dále lidé mohou informace hledat na automatizovaných systémů pro vyhledávání podle výskytu zadaných slov, např. Google, Bing aj.[3]

Samostatně lze v rámci této práce představit i sociální sítě, které v rámci internetu hrají velmi podstatnou roli. Sociální sítě začaly vznikat až v polovině 90. let minulého století v Americe, a to jako sítě, prostřednictvím kterých mezi sebou komunikovali zejména studenti. Vznik sociálních sítí zahájila sociální síť Facebook, kterou založil právě bývalý student Mark Zuckerberg z důvodu, že chtěl ulehčit studium nově nastupujícím studentům v prvním ročníku Harvadské univerzity. Sociální síť jim umožňovala si zobrazit seznam studentů a ročenek, sdílet své zkušenosti, studijní materiály apod. Časem se Facebook rozšířil i na jiné univerzity a postupně se mohli „připojit" všichni. Nejprve byl Facebook pochopitelně využíván zejména mladými, dnes jsou na něm skoro všichni a sdílejí informace ze všech možných oblastí života.[4] Po Facebooku se pak objevil Twitter a další sociální sítě (LinkedIn, You Tube aj.).

[2] PROCHÁZKA, D. První kroky s internetem. Praha: Grada Publishing a.s., 2010, s. 11.
[3] LALÍK, M. WWW pro každého. Praha: Grada Publishing a.s., 2013, s. 9-10.
[4] KULHÁNKOVÁ, H.; ČAMEK, J. *Fenomén facebook*. Kladno: BigOak, 2010, s. 5–10.

Sociální sítě je možné v současnosti vymezit jako „…*propojenou skupinou lidí, která spolu udržuje on-line komunikaci těmi nejrůznějšími nástroji a prostředky*.“ [5] Pro sociální sítě je typické, že většinu jejich obsahu tvoří samotní uživatelé, což je poněkud odlišné od případu internetu. Na druhou stranu to pochopitelně znamená i zvýšené riziko plynoucí z horší kontroly obsahu sociální sítě, neboť provozovatelé sociální sítě vstupují do jejich fungování jen v nepatrném rozsahu. Východisko sociálních sítí tvoří vztahy mezi uživateli, jejich vzájemné diskuze, odkazy a hodnocení. [6]

Oblíbenost internetu a sociálních sítí je v současné době naprosto obrovská. Například Šebeš[7] cituje některé zahraniční výzkumy, které uvádí, že např. britské děti ve věku 5 – 15 let na internetu tráví průměrně až 6 hodin denně (surfováním na internetu, hraním počítačových her aj.). Děti ve věku 12 – 15 let pak dokonce i 7,5 hodiny za den. Bocan a kol.[8] pak realizovali výzkum, v němž sledovali děti ve věku 10 až 15 let a zjistili, že jen každé desáté dítě by se obešlo bez internetu a televize. Konkrétně bez internetu by se neobešlo dokonce 71 % dětí. Z průzkumu dále vyplynulo, že více než 80 % starších školáků je pravidelně „on-line“. V průběhu týdně na internetu tráví více než jednu hodinu denně (o víkendu je to nad 2 hodiny).

Internet, ačkoliv přináší ať už dětem a dospělým nepřeberné množství informací v téměř aktuálním čase, sebou přináší i mnohá rizika. Těch je pochopitelně velmi mnoho. Tato rizika je v souvislosti s touto prací možné rozlišovat na rizika v rámci a mimo zákona. K rizikům, která nenaplňují žádná kritéria nezákonné aktivity, patří např. vznik závislosti na internetu (např. na počítačových hrách aj.), rizikem může být také přijímání internetu jako náhradního způsobu života (místo, aby lidé chodili do společnosti, raději sedí na internetu aj.).[9] Negativně může internet ovlivňovat i vývoj dětí, což si lze představit skrze používaný jazyk internetu, kde se může vyjadřovat vesměs kdokoliv a jakkoliv, tudíž tak mladí lidé, ale i dospělí mohou přejímat nevhodný jazyk. Navíc tím, že mladí (ale i starší) lidé tráví tolik času na internetu, lze dávat do souvislosti s internetem

[5] KOPECKÝ, L. *Public relations: dějiny - teorie – praxe*. Praha: Grada Publishing a.s., 2013, s. 206.
[6] BEDNÁŘ, V. *Marketing na sociálních sítích*. *Prosaďte se na Facebooku a Twitteru.* Praha: Computer Press, 2011, s. 10.
[7] ŠEBEŠ, M. Děti a mládež v kyberprostoru.[online]. [cit. 08–06–2017]
[8] BOCAN, M.; HOŠKOVÁ, I.; MACHALÍK, T. Děti v ringu dnešního světa. Hodnotové orientace dětí ve věku 6 až 15 let. Praha: Národní institut dětí a mládeže Ministerstva školství, mládeže a tělovýchovy, zařízení pro další vzdělávání, 2012, s. 34–38.
[9] Viz např. MUSIL, J. Elektronická média v informační společnosti. Votobia, 2003, s. 95.

i zvýšení riziko rozvoje nadváhy a obezity či dalších problémů souvisejících s neaktivním trávením volného času.

Lidé, kteří tráví na internetu velké množství svého volného času (a že jich je) pak hrozí určitá forma sociální izolace, která může časem způsobit až deprese. Internet v současné době také umožňuje nepřeberné možnosti nakupování. Na e-shopech si lidé mohou nakoupit v podstatě cokoliv, od oblečení, potravin, elektroniky aj. I takové nakupování na internetu může přerůst v závislost. Z médií dnes také víme, že ne všechny e-shopy či nákupy přes internet jsou bezpečné. I internet je plný podvodníků a ne výjimečně se stává, že si lidé nějaké zboží na internetu objednají, zaplatí předem a zboží nebo služby se již nedočkají.

Kapitolou samou o sobě by pak mohly být třeba internetové seznamky. Jak muži, tak ženy se v současné době hojně seznamují přes internet. Je to logické. Na internetu sami tráví spoustu času, v jejich zaměstnání či ve škole se s nikým, koho by pojali za partnera, zatím nesetkali a jiné možnosti na seznámení třeba z důvodu velkého časového zaneprázdnění, nemají. Internetových seznamek je mnoho, některé jsou dostupné zdarma, jiné jsou zpoplatněné. Podobně se využívá i sociálních sítí. Negativním jevem takových seznamek je anonymita, kterou internet poskytuje. Ne všichni seznamující zde totiž vystupují sami za sebe (zejména pokud už nějaký oficiální vztah mají a na seznamce hledají jen „povyražení“). Navázat „vztah“ je přes internet poměrně jednoduché, rizikem však je, pokud člověk není dostatečně obezřetný a svůj potenciální protějšek si dostatečně neprověří.

Ohrožení ve smyslu trestného činu zde plyne například ze zasílání osobních či citlivých informací a jejich zneužití (ať už rodná čísla, informace o tom, kdy nebudeme doma, někteří lidé jsou schopni se svěřit i se svými hesly, piny aj.). V rámci seznamování může dojít i ke zneužití choulostivých fotografií, což může ve svém důsledku někomu až zničit život (výpověď v práci, znemožnění na veřejnosti při zveřejnění fotografií či videa), lze v tomto ohledu zaznamenat i případy sebevražd skrze zveřejněné citlivé fotografie aj. Takové seznamování pak může dopadnout i znásilněním, okradením či jinými podvody, vše v rámci již skutečného kriminálního chování.

Výše uvedené může vyústit na internetu i v tzv. **kyberšikanu**. Poněvadž jde o fenomén, u něhož lze v poslední době zaznamenat zvýšení intenzity a setkává se s ním pořád více dětí i dospělých, je vhodné se jí na tomto místě věnovat o něco více. Internet

se nachází v současnosti v téměř každé domácnosti a skoro všichni lidé už mají svůj profil na Facebooku a jiných sociálních sítích. Kyberšikanu si lze představuje tak, „…*že se na internetu zveřejňují o oběti pomluvy, nebo i pravdivé, ale choulostivé informace z jejího soukromí, včetně obrazového materiálu (v současné době snadno získatelné mobilním telefonem)*.“[10] Typickým jevem bývá také to, že zneužité fotografie mohou být upravené k co největšímu zkompromitování a ponížení oběti. Kyberšikana navíc může trvat po dlouhou dobu a může být velmi nemilosrdná. U kyberšikanu je typický asymetrický vztah mezi obětí a agresorem. Šikanující při klasické šikaně manifestuje svou moc, ovšem při kyberšikaně může dost často zůstat skrytý. Může jít také o samotnou oběť šikany, která se kyberšikanou mstí. Internet tak může být nástrojem umocňujícím šikanu jako takovou.

Negativní vliv může mít i přílišná otevřenost internetu, kde vesměs není žádné tabu. Běžnou součástí je zobrazování sexuálních obsahů, násilí apod., což se může negativně odrazit na vnímání sexuality, ale i reality obecně. Takový negativní vliv postupně může pochopitelně vést až chování směřujícímu mimo zákon (promiskuita, prostituce, sexuální násilí aj.). Vždy je ovšem důležitý kontext. S otevřeným zobrazováním negativních a odpuzujících obsahů (zprávy o teroristických činech, bojové počítačové hry apod.) mohou souviset dopady jako znechucení nebo ztotožnění a ve svém důsledku to může vést až ke kyberkriminalitě. I to může nakonec podnítit rozvoj kriminálního chování podněcovaného internetem.

Na druhou stranu Giles[11] však uvádí, že problematika nepříznivého vlivu internetu, ale i jiných médií, na zvýšení agresivity je poměrně komplikovaná. Bylo uskutečněno dost velké množství studií, jejichž závěry prokázaly, že internet v rámci médií má prokazatelný vliv na zvýšení agresivity, ovšem někteří odborníci jsou zase toho názoru, že takové výzkumy nejsou přesvědčivé a že jejich závěry nejsou pravdivé.

Jedním ze základních rizik používání internetu jsou počítačové viry. Ty existují vesměs od počátku internetu a každý den vznikají nové a nové typy počítačových virů, které denně útočí na počítače. Ačkoliv má většina lidí ve svém počítači antivirový program, tvůrci počítačových virů jsou natolik kreativní a rychlí, že dokážou zpravidla obelstít i ty nejlepší antiviry. Počítačové viry se nachází různě na internetu. Lidé si je do počítačů stáhnout s nevhodnou přílohou v emailu, návštěvou rizikových internetových stránek apod. Takový počítačový vir dokáže člověku (ale i celým firmám, veřejné správě

[10]ŘÍČAN, P., JANOŠOVÁ, P. 2010. *Jak na šikanu*. Praha: Grada Publishing a.s., s. 24.
[11] GILES, D. Psychologie médií. Praha: Grada Publishing a.s., 2012, s. 35–37.

aj.) značně zkomplikovat život. Umí napadnout počítač tak, že jeho uživateli znemožní jeho používání nebo důmyslným systémem získá od uživatele jeho hesla a další citlivá data. Bránit se, či domáhat se potrestání viníka je zde v podstatě nereálné, neboť je velmi těžké zjistit, kdo stojí za takovým útokem (pokud se sám nepřizná).

Uvedená rizika internetu nejsou rozhodně kompletním souborem všeho, co uživatele v souvislosti s používáním internetu hrozí, avšak alespoň stručně vymezila, z čeho všeho mohou plynout různé problémy. V následující části práce již budou prezentována ta rizika, která spadají do počítačové kriminality.

3 Počítačová kriminalita

Na začátku této kapitoly je nezbytné si vymezit pojem počítačová kriminalita. Různí autoři i různé legislativní normy používají pro označení uvedených aktivit odlišné pojmy. Zmínit lze například informační, informatická, elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost (Computer crime), computer-related-crime, počítačová kriminalita, kybernetická trestná činnost, kyberkriminalita a další. U tohoto pojmu přetrvávají odlišnosti jak v označování uvedeného jevu, ale odlišně bývá chápán i jejich obsahový význam, což často přispívá k chybnému pochopení významu a škodlivosti tohoto typu trestné činnosti.[12]

Kolouch[13] navíc upozorňuje, že je nejprve třeba si také vymezit samotný termín kriminalita. Při provozu informačních technologií totiž dochází k mnohým jednáním, která sice jsou nežádoucí, ovšem nelze je postihnout prostředky trestního práva (i když jsou pro společnost škodlivá. Taková jednání nelze kvalifikovat jako počítačovou kriminalitu, neboť vůbec nejsou kriminalitou vůbec. Kriminalita je totiž souhrnem všech jednání, která lze zahrnout pod určitou skutkovou podstatu, upravenou trestním zákonem. Kriminalitou tak nejsou jednání, která nenaplňují žádnou skutkovou podstatu trestného činu, tedy ani přestupku nebo jiného správního deliktu. Takové vymezení pojmu kriminalita se týká i oblasti informační a komunikační techniky. Páchání trestných činů ve sféře ICT je ovšem typické tím, že často v rámci jejich spáchání používány ty postupy či prostředky, jejichž užití nenaplňuje žádnou skutkovou podstatu trestného činu, ovšem prezentují nedílnou součást nebo podmínku pro jednání další, které již postižitelné prostředky trestního práva je. Současně takové netrestné postupy nebo prostředky

[12] Viz KOLOUCH, J. Cyberkrime. Praha: CZ.NIC, z. s. p. o. 2016, s. 31.
[13] KOLOUCH, J. Cyberkrime. Praha: CZ.NIC, z. s. p. o. 2016, s. 34-35.

prezentují v procesu odhalování a objasňování trestné činnosti podstatné součásti, jejichž identifikace a pochopení je důležité při odhalování pachatelů tohoto typu trestné činnosti. Kybernetická kriminalita, resp. kybernetická trestná činnost, je tak jistou nejširší množinou pro všechnu trestnou činnost, která se realizuje v prostředí informačních a komunikačních technologií.

Na webových stránkách Policie ČR[14] lze nalézt vysvětlení, že pojem kybernetická kriminalita je odvozován od pojmu kybernetický prostor, eventuálně zkráceně kyberprostor. **Kyberprostor** opak vymezován jako „*…virtuální prostředí, které nemá začátek a ani konec, nezná hranice národních států a nelze určit, jak rozsáhlý je*". Kybernetická kriminalita, v dřívějších dobách rovněž vymezována jako informační kriminalita, je Policií ČR následně definována jako *„ …trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí*". Samotná sféra informačních a komunikačních technologií je buď objektem útoku, případně je páchána trestná činnost za evidentního použití informačních a komunikačních technologií jakožto podstatného nástroje k jejímu páchání.

Musil[15] nabízí jednu z obecných definicí počítačové kriminality „*....jako každou nekalou činnost páchanou s pomocí počítačů. Pojem „nekalá činnost" může být specifikována např. společenskou nebezpečností důsledků, které tato aktivita přináší. Což přichází v úvahu zejména v případech přestupků, trestných činů či obecně deliktů ve smyslu porušení platné zákonné úpravy*". Toto vymezení je ovšem na jednu stranu moc široké, zahrnuje např. i triviální machinace mzdové účetní, při nichž mění položky v počítači, podobně jako by je měnila na jiném nosiči, na druhou stranu pak i úzké. Úzké v tom směru, že nezahrnuje např. neautorizovanou distribuci softwarového vybavení počítače. Jde o produkty, k jejichž utváření je zapotřebí počítače, ale k jejich distribuci nikoliv, ačkoliv pochopitelně rovněž použitelný. Podle Jirovského[16] je kyberkriminalita taková činnost, kterou se porušuje zákon, případně je v rozporu s morálními pravidly společnosti. Tento typ kriminality může být namířen proti počítačům, jejich hardwaru, softwaru, datům, sítím aj., případně v ní vystupuje počítač jen jako prostředek pro páchání trestného činu, nebo se odehrává v prostředí počítačové sítě.

[14] POLICIE ČR. Kyberkriminalita. [online]. [cit. 09–06–2017]
[15] MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 6.
[16] JIROVSKÝ, V. Kybernetická kriminalita. Praha: Grada Publishing a.s., 2007, s. 19.

Kolouch[17] uvádí, že při určení obsahu pojmu kybernetická kriminalita je nezbytné zohlednit, že současně s růstem možností využívání informačních a komunikačních prostředků se zvyšuje také možnost jejich užívání (zneužívání) k páchání trestné činnosti. Z toho důvodu tedy neexistuje nějaké univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto termínu plně postihla. Jednu ze současnějších definic počítačové či kybernetické kriminality nabízí například Výkladový slovník kybernetické bezpečnosti[18]. Ten ji vymezuje jako trestnou činnost, *„ ....v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti*."

To, že kyberkriminalita představuje poměrně četný jev, dokládají i některé její statistiky. Například podle údajů společnosti Symantec[19] se každou hodinu stane obětí kyberzločinu více než 50 tisíc lidí, účet kyberkriminality za rok 2011 dosáhl částky 7,5 bilionům Kč (388 miliard USD). Přitom 41 % uživatelů po celém světě si podle tohoto zdroje svoje data nechrání. Potíž je, že bohužel zřejmě zdaleka ne všichni lidé mají alespoň tušení, co se odehrává v kyberprostoru, když svůj počítač nebo Ipad zapíná. Pakliže lidé chtějí něco z kyberprostoru získat, musí mu pochopitelně něco poskytnout, tudíž každý, kdo do kyberprostoru vstoupí, vrávorá na rozhraní soukromí a bezpečnosti. Bohužel, lidé si to stále neuvědomují a nejvíce to je vidět na sociálních sítích (Facebook, Twitter, Linkedin, Líbím se ti, Spolužáci apod.).

3.1 Historie počítačové kriminality

Při snaze vymezit historii kyberkriminality je pochopitelně zásadní si uvědomit, že o kyberkriminalitě je možné hovořit v podstatě od vzniku internetu. Počátky internetu lze zaznamenávat už ve chvíli, kdy se začalo přemýšlet o vytvoření počítačové sítě, která by spolehlivě propojila strategické, vládní, vojenské a akademické počítače, tak, aby současně zvládla přežít jaderný úder nebo podobné hrozby. Při vytváření internetu byla

[17] KOLOUCH, J. Cyberkrime. Praha: CZ.NIC, z. s. p. o. 2016, s. 33.
[18] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze, 2013, s. 57, 73.
[19] In BUSINESSIT.CZ. Kybernetická kriminalita I: Co se děje v kyberprostoru. [online]. 2012. [cit. 05-06-2017].

důležitým požadavkem jeho nezranitelnost. Byla vytvořena bez hlavního řídicího centra. Skládala se z několika navzájem propojených uzlů rovnocenného významu. Posílaná data se na dobu šíření rozdělila na několik samostatných paketů. Součástí každého paketu byly informace o adresátovi a prezentovaly vesměs autonomní zásilku cestující k adresátovi samostatně nezávisle na zbylých paketech. To byl vlastně základ internetu. K významným milníkům vývoje internetu patří:[20]

- 1969 – vytvoření experimentální sítě ARPANET, prvotní pokusy s přepojováním uzlů.
- 1972 – vyvinuta první emailová aplikace.
- 1980 – experimentální provoz protokolu TCP/IP v síti ARPANET.
- 1984 – vznik DNS (Domain Name System).
- 1987 – poprvé se lze setkat s označením sítě internet.
- 1990 – konec ARPANET.
- 1991 – zapojení WWW (World Wide Net) v evropské laboratoři Cern.
- 1994 – internet se dostává od vědců do komerčního využití.
- 1996 – internet má již více než 55 milionů uživatelů.
- 2000 – internet má více než 250 milionů uživatelů.
- 2006 – nad miliardu uživatelů.

K historii počítačové kriminality Musil[21] uvádí, že programy v současném pojetí se objevily v 60. letech a již od 70. let se začaly objevovat potíže ohledně jejich právní ochrany. V raných etapách rozvoje výpočetní techniky šlo ale problémy poměrně zanedbatelné v porovnání s prostředky a cenou technické části těchto projektů - hardware. Ke změně došlo s prudkým nárůstem výroby personálních počítačů. Od roku 1976 totiž výrazně klesla cena hardware, přičemž výkon personálních počítačů začal být srovnatelný s výkonem tehdejších střediskových počítačů. Existence většího množství izolovaných počítačů byla jedním z motivů směřujících k rozvoji počítačových sítí a k využití výpočetní techniky snad ve všech oblastech lidské činnosti a tím rovněž k nezbytné

[20] PROCHÁZKA, D. První kroky s internetem. Praha: Grada Publishing a.s., 2010, s. 11-12.
[21] MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 22-23.

potřebě legislativní regulace takto vznikajících právních vztahů. Během posledních 40 let došlo k významnému růstu i kvalitativnímu vývoji počítačové kriminality, ve světě i u nás.

Do roku 1968 bylo podchyceno pouhých 13 případů. V roce 1977 dosáhlo množství zaznamenaných případů už 85 a bylo možné hovořit o růstu počítačové kriminality. V té době docházelo například k četným případům magnetického vymazávání a elektronického monitorování. V osmdesátých letech prezentovala počítačová kriminalita mimo podvodů a fyzických škod i krádeže databází, šíření virů, infiltraci logických a časových bomb, rozšiřování a využívání pirátského softwaru. V 90. letech došlo v souvislosti s celosvětovým rozvojem Internetu i jeho zneužití k šíření pornografie, rasismu, šíření výbušnin a drog, k prezentaci extremistů a kriminálních živlů. K útočníkům, jejichž záměrem jsou informace uložené na počítačích, se řadí mimo profesionálních hackerů téiž zpravodajské služby, detektivní kanceláře, média, aktéři organizovaného zločinu i političtí extrémisté.[22]

3.2 Druhy počítačové kriminality

Na dělení počítačové kriminality je možné nahlížet z různých úhlů pohledů. Například Kolouch[23] zmiňuje klasifikaci dle Úmluvy o kyberkriminalitě a dle dodatkového protokolu. Úmluva o kyberkriminalitě rozlišuje kybernetické trestné činy do čtyř kategorií:

1) trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů

2) trestné činy mající souvislost s počítači,

3) trestné činy mající souvislost s obsahem,

4) trestné činy mající souvislost s porušováním autorských práv a práv souvisejících.

Dodatkový protokol pak doplňuje ještě tyto kybernetické trestné činy:[24]

[22] MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 22-23.
[23] KOLOUCH, J. Cyberkrime. Praha: CZ.NIC, z. s. p. o. 2016, s. 38.
[24] KOLOUCH, J. Cyberkrime. Praha: CZ.NIC, z. s. p. o. 2016, s. 38.

1) šíření rasistických a xenofobních materiálů skrze počítačové systémy,

2) rasisticky a xenofobně zaměřené vyhrožování,

3) rasisticky a xenofobně zaměřené útoky,

4) popírání, omezování, schvalování či ospravedlňování genocidy nebo zločinů vůči lidskosti.

Svatoš[25] rozděluje páchání počítačové kriminality na přímou a nepřímou:

Přímá počítačová kriminalita:

- **Útok na počítač, program, údaje komunikačního zařízení (počítačový vandalismus):**
  - fyzické útoky na zařízení výpočetní techniky (rozbití počítače, způsobení zkratu aj.),
  - záměrné vymazání či změna dat, formátování paměťových médií s daty magnetem, použití virů.
- **Neoprávněné použití počítačových programů a nelegální tvorba a rozšiřování kopií programů (počítačové pirátství):**
  - softwarová kriminalita na úrovni koncového uživatele – kopírování softwaru (hudby, filmů atd.) bez povolení,
  - nadužívání licence – v jedné pracovní síti se využívá více přístupů, než bylo zastoupeno,
  - pirátství v počítačových hernách – využívání hry, na kterou výrobce nedal povolení k užití,
  - softwarová kriminalita na internetu – nedovolené stahování softwaru z internetu,
  - prodej počítačů s nelegálním softwarem,
  - plagiátorství – např. prodej softwaru podléhajícímu autorským právům.

[25] SVATOŠ, R. Kriminologie. Plzeň: Aleš Čeněk, s.r.o. 2012, s. 151-158.

- **Nedovolené užívání počítače či komunikačního zařízení (tzv. krádež komunikačních služeb) –** hlavně zneužívání výpočetní techniky, faxů aj. zaměstnanci firmy pro jejich osobní užitek.

- **Nedovolený přístup k utajovaným informacím, dat o jiných osobách (počítačové špionáže) –** vnik do bankovních systémů, systémů státní správy pro získání důležitých informací.

- **Krádeže počítačů, programů, informací, komunikačních zařízení (krádeže materiálních součástí počítačů).**

- **Změny v programech a údajích –** např. zavirováními tzv. počítačové defraudaci.

- **Šíření poplašných zpráv.**

Nepřímá počítačová kriminalita:

- Zneužívání počítačových prostředků pro páchání dalších trestných činů – např. manipulace s elektronickými údaji v rámci účetnictví, falšování technické dokumentace, šíření dětské pornografie aj.

- Počítačové bankovní krádeže, např.:

    - fishing – vyžádání důvěrných informací od uživatelů se záměrem získání hesla a odcizení identity nebo třeba výběr konta;

    - pharming – přesměrování uživatele na stránku záměrně zformovanou pro zneužití (nejčastěji internetové bankovnictví) aj.

Jiní autoři[26] rozdělují počítačovou kriminalitu následovně:

- **Neoprávněné zásahy do vstupních dat –** např. změna vstupního dokladu pro zpracování počítačem; zhotovení dokladus lživými informacemi pro další zpracování dat počítačem,

- **Neoprávněné změny v uložených datech** – machinace s daty, neoprávněný zásah do nich a navazující návrat k normálu,

- **Neoprávněné pokyny k počítačovým operacím –** přímý pokyn k realizaci operace, nebo instalace softwaru uskutečňujícího operace automaticky,

[26] STRAUS, J. a kol. Kriminalistická metodika. Plzeň: Aleš Čeněk, 2006, s. 272–274.

- **Neoprávněné pronikání do počítačů, počítačového systému a jeho databází** – informativní vstup do databáze, bez zneužití dat; neoprávněné užívání dat pro své potřeby; změny, destrukce, nebo nahrazování informací jinými; nelegální „odposlech“ a záznam provozu elektronické komunikace,
- **Napadení počítače, programového vybavení a souborů a dat v databázích** – zhotovení programů sloužících k napadení; zaslání viru do programového vybavení počítače; samotné napadení viry, nebo jinými programy.

3.2.1 Podvodná jednání

Nejčastějším se jedná o přečin Podvod dle ust. § 209 trestního zákoníku, kdy jej může doprovázet i Neoprávněný přístup k počítačovému systému a nosiči informací dle ust. § 230 trestního zákoníku. Konkrétně jde v praxi o podvodné e-shopy, které vznikají se záměrem vylákání peněžních prostředků, ovšem velmi brzy takový e-shop zaniká. Zároveň jdou finance obvykle zasílány mimo území našeho státu kvůli anonymitě finančních toků, eventuálně jsou využívány virtuální měny. Podobné je to při podvodných inzerátech (prodej automobilů, elektroniky, živých zvířat případně i pronájmy bytů), sbírek a zmínit lze také jednání známé jako tzv. nigerijské podvody. Zařadit mezi tyto jednání je možné také podvody prostřednictvím podvržených emailů, eventuálně krádeže peněz z bankovních účtů za pomoci phishingu.[27]

Nejčastěji jde o podvody, při nichž se realizují neoprávněné převody finančních prostředků na zvláštní účet. Pachateli bývají často vlastní zaměstnanci finančních institucí napadající počítačové systémy zabezpečené identifikací a autorizací. Pro zloděje nejsou hlavní jen peníze na účtech, ale zajímají se o cenné informace, jako jsou podnikové strategie, specifikace nových výrobků, detaily o smlouvách, data poté nabízejí konkurenci k prodeji. Zmínit lze zde neoprávněné používání cizí věci podle § 249 trest. zákona, když se pachatel zmocní počítače a neoprávněně jej přechodně užívá nebo jej užívá v rozporu s pokyny vlastníka [28]

[27] POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017].
[28] POŽÁR, J. Vybrané trendy kybernetické kriminality. In Acta Informatica Pragensia, 2015, roč. 4, č. 3, s. 336–348.

3.2.2 Hacking

Hacking je trestným činem (dle ust. § 230 trestního zákoníku) prezentujícím neoprávněný přístup k počítačovému systému a nosiči informací. Do uvedeného paragrafu patří i narušování dat, narušování systému a také zneužívání zařízení. Charakteristicky jde o jednání pachatele, který přemůže zabezpečení počítačového systému a získá přístup k informacím oběti, se kterými pak libovolně nakládá. Součástí takových jednání bývá také šíření škodlivých kódů, implementace tzv. backdoorů do volně přístupných software atp. Mnohem četnější se stávají i útoky do emailových účtů, účtů na sociálních sítích, internetového bankovnictví, díky čemuž pachatelé vniknou do soukromí, získají citlivá data a mohou je poškodit nebo zničit, případně získat finanční prospěch.[29] Neoprávněný přístup k datům lze postihnout podle povahy získaných informací i jako trestný čin vyzvědačství (§ 316 trestního zákoníku).[30]

Na hacking navazuje i další trestná činnost (vydírání, nebezpečné pronásledování, krádeže z účtů, podvody). Součástí tohoto typu trestné činnosti bývají také kybernetické útoky (např. DDoS) či vydírání skrze ransomware. Patří zde také porušení tajemství dopravovaných zpráv dle ust. § 182 trestního zákoníku, jehož nejběžnější projev se označuje jako sniffing (pachatel sleduje reálnou komunikaci v síti a získává tak citlivé informace jak o provozu, tak i obsahu). Odehrává se to mnohdy na nezabezpečených wi-fi připojeních, u zmanipulovaných emailových serverů a aktuálně i útoky na domácí routery. Získaný citlivý obsah (fotky, hesla aj.) je pak využíván k nátlaku na oběť za účelem finančního prospěchu pachatele nebo alespoň poškození pověsti oběti.[31]

3.2.3 Blagging

Jde o různé typy podvodů, které kromě jiného využívají sociálního inženýrství. Ohrožují jak jednotlivce, tak obchodní společnosti. Zmínit lze např. tzv. CEO – Command Executive Order – což je fiktivní příkaz oprávněný k realizaci např. platby na účet. Tyto podvody vznikají díky velmi dobré znalosti trhu, struktury a zákazníků nějaké firmy. Získané informace se zneužívají k případné manipulaci oběti, aby udělala, co pachatelé chtějí. K takovým charakteristickým scénářem je, když si pachatelé pro navázání kontaktu hrají na ředitele podniku (např. prezident, CEO, CFO) či důvěryhodného partnera (např. právníci, notáři, auditoři, účetní atd.) firmy. Pak takto

[29] POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017].
[30] POŽÁR, J. Vybrané trendy kybernetické kriminality. In Acta Informatica Pragensia, 2015, roč. 4, č. 3, s. 336–348.
[31] POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017].

kontaktují zaměstnance např. proto, aby v takové roli vymohli splátku nějaké pohledávky či uzavřeli smlouvy a donutili tak zaměstnance podniku k žádoucí interakci.[32]

3.2.4 Podvodné e-shopy

Nákupy přes internet jsou stále oblíbenější a stoupají jak počty provedených nákupů, tak i objem tržeb internetových obchodů. Nakupování na e-shopu je rychlé, často i levnější a zboží dojde zákazníkovi až domů. Opatrnost je zde ale na místě, a to hlavně při neúměrně nízké ceně zboží a hlavně při požadavku e-shopu na platbu předem (u podvodných obchodů jde obvykle o jedinou možnost platby). Zaznamenat lze i nabídky brigády spočívající v zadávání inzerátů či přeposílání plateb, kde figurují naivní oběti. Takové osoby pak pro pachatele založí bankovní účty, na něž se přeposílají platby z podvodných e-shopů a pak se peníze zašlou nebo jinak předají pachatelům. Takové jednání je však trestným činem legalizace výnosů z trestné činnosti, jehož je možné se dopustit i nedbalostním jednáním dle ust. § 217 trestního zákoníku, nebo také trestného činu podílnictví.

3.2.5 Mravnostní trestné činy

Trestní zákoník[33] mezi mravnostní trestné činy zařazuje zejména ohrožování výchovy dítěte dle ust. § 201 trestního zákoníku, Šíření pornografie dle ust. § 191 trestního zákoníku, Výroba a jiné nakládání s dětskou pornografií dle ust. § 192 trestního zákoníku, Zneužití dítěte k výrobě pornografie dle ust. § 193 trestního zákoníku, Účast na pornografickém představení dle ust. § 193a trestního zákoníku a v neposlední řadě Navazování nedovolených kontaktů s dítětem dle ust. § 193b trestního zákoníku.

Nejčastěji se jedná o kontaktování dětí mladších 18 let přes internet či sociální sítě za účelem získání jejich intimní fotografie či videa, eventuálně je nalákat na osobní schůzku. Takové fotografii či informace pak pachatel šíří do uzavřených diskusních fór, emailem či P2P sítěmi. Řadí se zde i delikty vůči zletilým osobám, jako např. kuplířství, sexuální nátlak, obchodování s lidmi, atd.[34]

[32] POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017].
[33] Zákon č. 40/2009 Sb., trestní zákoník.
[34] POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017].

3.2.6 Trestné činy proti autorskému právu

Jedná se hlavně o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle ust. § 270 trestního zákoníku[35]. V praxi jde nejčastěji o sdílení hudebních skladeb, filmů a softwaru šířených na webových velkokapacitních úložištích či P2P sítích.[36]

3.2.7 Násilné projevy a hate crime

Zde lze zařadit několik trestných činů, od např. Vydírání dle ust. § 175 trestního zákoníku, Nebezpečné vyhrožování dle ust. § 353 trestního zákoníku, Nebezpečné pronásledování (známý stalking) dle ust. § 354 trestního zákoníku nebo také Šíření poplašné zprávy dle ust. § 357 trestního zákoníku[37]. Těmto činům internet dopřává značnou míru anonymity. Využívají se zde anonymizační servery či služby, např. proxy servery, tor síť, VPN atp. Zařadit zde lze i extremistické projevy povahy trestného činu Hanobení národa, rasy, etnické nebo jiné skupiny osob dle ust. § 355 trestního zákoníku, Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle ust. § 356 trestního zákoníku a další.[38] Na zahraničních serverech se pak lze setkat třeba s webovými stránkami s extrémně pravicovou či levicovou tématikou, které motivují k nenávisti, diskriminaci případně i vybízí k násilí vůči menšinovým skupinám obyvatel nebo politickým uskupením. Patří zde také vymyšlené profily na sociálních sítích a komentáře k různým článkům v médiích.[39]

3.2.8 Trestné činy proti počítačům jako movitým věcem

Skutková podstata je shodná s trestnými činy spáchanými ve spojitosti s jinými movitými věcmi. Jedná se hlavně o trestné činy: § 247 trest. zák. krádež, § 248 zpronevěra, § 250 podvod, §251 a §252 podílnictví a § 254 zatajení věci. Díky určité specifičnosti počítačů lze zmínit zvláštnosti, které prezentují problém skutkových podstat. Trestní zákon mimo uvedených ustanovení chránících jakýkoliv majetek zahrnuje ještě speciální ustanovení zahrnující útoky na počítače jako nosiče informací.

[35] Zákon č. 40/2009 Sb., trestní zákoník, § 270.
[36] POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017].
[37] Zákon č. 40/2009 Sb., trestní zákoník, § 175, 353, 354, 357.
[38] Zákon č. 40/2009 Sb., trestní zákoník, § 355, 356.
[39] POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017].

Jedná se o poškození a zneužití záznamu na nosiči informací podle §257a trest. zákona.[40] [41]

Krádež počítače má ale odlišné vlastnosti na rozdíl od odcizení jiné movité věci. Tato osobitost vyplývá z toho, že počítač obvykle zahrnuje v sobě jak technické zařízení včetně nosiče informací (hardware) a jednak nehmotný obsah, obecně obsahující programy (software) a data (informace). Cena nehmotného obsahu může podstatně ovlivnit celkovou hodnotu ukradené věci. Ta může mnohonásobně převýšit cenu počítače.[42]

3.2.9 Role sociálních sítí v počítačové kriminalitě

Ačkoliv sociální sítě jako Facebook či LinkedIn nemusí samy o sobě prezentovat opravdové původce počítačové kriminality, mohou se stát velmi cenným zdrojem pro počítačový zločin ve smyslu sociálního inženýrství a navazujících efektivních útoků, např. phishing. Příkladem může být schéma, kdy se na sociálních sítích sbírají všechny informace o cílovém jedinci, aby mohlo dojít k přesně zacílenému počítačovému útoku na takovou osobu či k nainstalování škodlivého kódu do jejího počítače.[43]

Pro sociální sítě je pak také typická kybernetická šikana, která je technicky snadná. Odeslání škodlivých zpráv nebo zveřejnění škodlivého textu široké řadě lidí lze provést několika klepnutími myší. Nějaké z forem kyberšikany je u nás vystavena skoro polovina českých dětí (46,8 %).[44] Mimo kyberšikanu mohou být sociální sítě (podobně jako internet obecně) využívány i ke kyberstalkingu, kdy je oběť prostřednictvím sociální sítě pronásledována, což může ve svém důsledku vést až k napadení aj. Přes sociální sítě lze realizovat útoky pedofilů, distribuci dětské pornografie, prodej drog aj.[45]

[40] Zákon č. 40/2009 Sb., trestní zákoník, § 247, 248, 250, 251, 252, 254, 257s.
[41] MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 30.
[42] POŽÁR, J. Vybrané trendy kybernetické kriminality. In Acta Informatica Pragensia, 2015, roč. 4, č. 3, s. 336–348.
[43] PWC. Počítačová kriminalita pod lupou. [online]. 2011. [cit. 22-06-2017].
[44] BUSINESSIT.CZ. Kybernetická kriminalita II: Sociální sítě jako médium budoucnosti i skrytá hrozba. [online]. 2012. [cit. 05-06-2017].
[45] TAVANI, H. T. Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace. In Acm Sigcas Computers and Society. 2000, Vol. 30, No. 3, pp. 3-9.

3.3 Pachatelé počítačové kriminality

I na začátku této kapitoly je vhodné si nejprve vymezit pojem pachatel. O to se stará trestní zákoník[46], který za pachatele označuje subjekt trestného činu, který svým konáním naplnil veškeré znaky trestného činu. Pachatelem bývá označen i spolupachatel, návodce či organizátor, případně ten, kdo se podílí na přípravě trestného činu, či se o něj jen pokusí. Za pachatele označuje zákon jen fyzické osoby (právnické ne), které dosáhly jistého věku a byly v době jeho spáchání příčetné.

Jak uvádí Matoušková[47], není to tak dávno, co se počítačová kriminalita připisovala středním a vyšším vrstvám, spíše podivínům a specialistům. I v současné době se má za to, že počítačová kriminalita vyžaduje vysokou schopnost přizpůsobivosti, odpovídající „know how" a určitou míru inteligence. V počítačové kriminalitě nelze nalézt jeden typ pachatele, ale spíše množství různých, značně specializovaných typů. Z rozboru konkrétních trestných činů počítačové kriminality dosud vyplývá, že většinou jde o typy příležitostné, využívající nastalé situace či dosavadní vlastní sociální zkušenosti. Poté lze takové typy rozdělit na:

- Kořistnicky orientované – nenasytové, hamouni, podvodníci.
- Plánovité – orientované vesměs na překonání překážek ochrany systémů či na vlastní uspokojení z utajované aktivity.
- Situační – využívající vhodných podmínek k realizaci své motivace.

Pachatelé trestné činnosti v oblasti počítačové kriminality je možné rozdělit také do dále uvedených čtyř skupin pachatelů nebo organizátorů trestné činnosti:[48]

1. **Cizí státy –** jedná se o kybernetickou válku (viz např. informační válka Ruska proti Ukrajině).
2. **Teroristé –** teroristé jsou schopni především v rámci tzv. asymetrických konfliktů zaútočit na stát velice efektivně skrze počítačové sítě.
3. **Zaměstnanci** – v mnoha ohledech jsou nejnebezpečnější. Zaměstnanci mají přístup ke všemu, mají většinou i dostatečná oprávnění, dost

[46] In JIROVSKÝ, V. Kybernetická kriminalita. Praha: Grada Publishing a.s., 2007, s. 84-85.
[47] MATOUŠKOVÁ, I. Aplikovaná forenzní psychologie. Praha: Grada Publishing a.s., 2013, s. 159.
[48] STEJSKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017].

možností a informací na to, aby poškodili data, modifikovali, ukradli, prodali nebo použili k vydírání.

4. **Organizované skupiny** – nejčastější „uživatelé“ výnosů páchaní kybernetické kriminality. Organizovaný zločin, který kyberprostor používá pro praní peněz, pro nelegální převody a pro veškeré jiné další činnosti, k nimž je možné počítače využít.

Matoušková[49] pak ještě doplňuje, že pachateli počítačové kriminality obecně bývají podle statistik osoby se středoškolským vzděláním, jiným vyšším nebo vysokoškolských vzděláním, především pak v technických oborech, hlavně v oboru IT. Mnohdy lze u nich zjistit nadprůměrnou inteligenci, vynalézavost, především ve specifické programátorské sféře. Někdy pro ně bývá typické zneužívání svého výsadního postavení v práci a tomu odpovídajících pravomocí. Charakteristické také bývá, že ve svém zaměstnání bývají neuspokojení a jejich protiprávní jednání v oblasti IT nenabývá násilné podoby. Věk osob páchajících počítačovou kriminalitu dosahuje až k hranici 35 let. Používají automatizované postupy přesahující svým časovým trváním i dobu 24 h, pracují v týmech a počítačovou kriminalitu provádí ne pro zábavu, ale finanční prospěch. Jejich pracoviště bývají místa vzbuzující respekt i důvěru společnosti. Pokud kradou počítačovou kriminalitou peníze, tak tak činí spíše po menších částkách. Nemají zájem ublížit někomu konkrétnímu, ale spíše neosobnímu zaměstnavateli, kterého považují za vykořisťovatele. Krádež softwaru či dat je pro ně spíše zapůjčením se záměrem je později vrátit. Z hlediska motivů převažuje v České republice motiv touhy po zisku (dále pak např. získání převahy nad zaměstnavatelem, kompenzace pocitu neuznání, nedostatečného ocenění či touha po riziku). Nejvýnosnější je bankovní kriminalita.

U pachatelů počítačové kriminality se vyskytuje jeden zásadní problém, a to jejich určení, které je velkým problémem. Tím největším je ztotožnění fyzické osoby pachatele s nástrojem trestného činu – počítačem, IP adresou aj. Pakliže jde o útok proti obsahu, pak fenomén nepopiratelnosti provedení trestného činu konkrétní osobou představuje důležitý krok v důkazním řízení před trestním soudem.[50]

[49] MATOUŠKOVÁ, I. Aplikovaná forenzní psychologie. Praha: Grada Publishing a.s., 2013, s. 160.
[50] JIROVSKÝ, V. Kybernetická kriminalita. Praha: Grada Publishing a.s., 2007, s. 85.

3.4 Počítačová kriminalita v ČR a její specifika

Společnost PricewaterhouseCoopers[51] Česká republika, s.r.o. vede statistiku o podílu počítačové kriminality na spáchaných podvodech. V České republice prezentuje počítačová kriminalita podle nich 13%podíl, ve střední a východní Evropě je to více, a to 18 %, celosvětově pak 23 %. To dokazuje, že do budoucna lze očekávat v České republice zhoršení. Zaměstnaní lidé v ČR vnímají počítačovou kriminalitu jako hrozbu z vnějšku organizace (37 %). Jako hrozbu zevnitř organizace pociťuje počítačovou kriminalitu 21 % respondentů v ČR. České společnosti se podle všeho v oblasti počítačové kriminality nejvíce obávají krádeže či ztráty osobních údajů (74 %), poškození dobrého jména podniku (72 %), porušení práv duševního vlastnictví včetně krádeže dat (71 %), reálné finanční ztráty (68 %), narušení služeb (63 %), výdajů na vyšetřování a odstranění následků (58 %) a regulatorního rizika (49 %).

Skoro tři čtvrtiny (71 %) zaměstnanců uvádí, že jejich společnosti disponují vlastními prostředky pro prevenci a odhalování počítačové kriminality. Skoro polovina respondentů pak také věří, že jejich zaměstnavatel je schopen počítačovou kriminalitu interně vyšetřit. Tyto schopnosti jsou obvykle přisuzovány právě oddělení IT (to ale také lidé chápou jako nejčastější interní hrozbu v případě počítačové kriminality). Za velmi znepokojivé je možné označit, že 69 % českých firem nespolupracuje se specialisty z oblasti forenzních technologií či o této spolupráci vůbec netuší.[52]

Vývoj počtu případů počítačové kriminality sleduje níže uvedená Tabulka Police ČR.

Tabulka 1 Vývoj nejvíce zastoupenými skupinami trestných činů (roční nápad v řádu stovek případů).[53]

[51] PWC. Počítačová kriminalita pod lupou. [online]. 2011. [cit. 22-06-2017].
[52] PWC. Počítačová kriminalita pod lupou. [online]. 2011. [cit. 22-06-2017].
[53] POLICIE ČR. Kyberkriminalita. [online]. [cit. 09–06–2017]

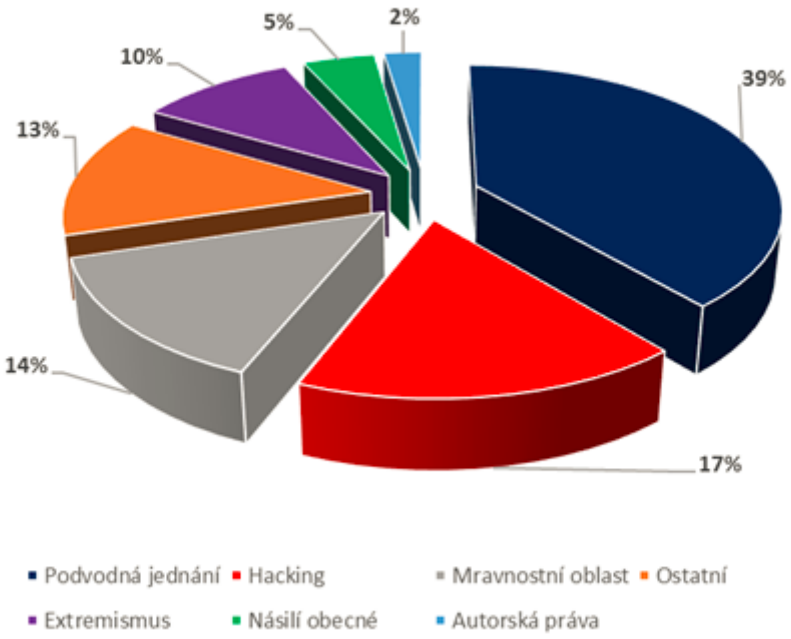
Struktura nápadu	2011	2012	2013	2014	2015	2016
podvodná jednání	917	1303	1863	2478	2932	3235
tj. %	*61,05*	*59,36*	*59,94*	*56,99*	*58,37*	*60,54*
hacking	66	112	220	555	578	534
tj. %	*4,39*	*5,10*	*7,08*	*12,76*	*11,51*	*9,99*
mravnostní delikty	132	161	261	314	351	344
tj. %	*8,79*	*7,33*	*8,40*	*7,22*	*6,99*	*6,44*
autorskoprávní delikty	155	241	181	262	315	237
tj. %	*10,32*	*10,98*	*5,82*	*6,03*	*6,27*	*4,43*
násilné projevy + hate crime	86	111	155	202	230	265
tj. %	*5,73*	*5,06*	*4,99*	*4,65*	*4,58*	*4,96*
ostatní	146	267	428	537	617	729
tj. %	*9,72*	*12,16*	*13,77*	*12,35*	*12,28*	*13,64*

Data v tabulce neznázorňují počet skutků, ale pouze počet TČ, které byly ve vybraných případech kvalifikovány. Běžná kriminální statistika zaznamenává množství skutků[54]. Údaje z této statistiky mají poněkud odlišnou filozofii, i tak z ní je možné vypozorovat trendy a objem nápadu v evidovaných řádech.

V roce 2014 bylo vyšetřováno 2 458 případů podvodů v prostředí informačních technologií a především sítě internet, což prezentuje nárůst o 32 % na rozdíl od roku 2013. Také lze zaznamenat zjevný nárůst detekce trestné činnosti spočívající v neoprávněných manipulacích s daty, kde došlo k nárůstu trestné činnosti o 163 % proti roku 2013. Množství informací o závadovém chování či obsahu na internetu uváděných oznamovateli skrze policejní hotline narůstá každým rokem od zřízení uvedeného komunikačního kanálu (v roce 2014 6 590 podnětů, tedy jde o nárůst o 72 % oproti roku 2013).[55] V roce 2016 bylo skrze formulář pro hlášení závadového obsahu a aktivit v síti internet, přijato už 3 378 oznámení. V roce 2016 byla nejčetnější podvodná jednání. Mezi ně se řadí všechna podvodná jednání i přestupkového charakteru (viz Graf 1).

[54] skutek=trestněprávně relevantní jednání, které může být kvalifikováno jako jeden nebo více trestných činů

[55] In POLICIE ČR. Rozvoj Policie České republiky v letech 2016 – 2020. Praha: Policie ČR. 2015, s. 30-31.



Graf 1 Statistika hlášených počítačových deliktů.[56]

4 Legislativa a prevence počítačové kriminality v ČR

Tato kapitola prezentuje základní legislativní dokumenty, včetně těch dokumentů a aktivit zabývajících se prevencí počítačové kriminality.

4.1 Legislativa počítačové kriminality

Z hlediska legislativy je pochopitelně zjevné, že co se týče kriminality, hlavním zákonem je trestní zákoník, odpovídá to i oblasti počítačové kriminality. Počítačovou kriminalitu je možné postihovat jako širokou škálu trestných činů podle trestního zákoníku, zákona č. 40/2009 Sb., který od 1. ledna 2010 nahradil trestní zákoník č. 140/1961 Sb. Podle údajů Policie České republiky[57] se převážná většina trestných činů proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů nachází v Trestním zákoníku v hlavě V („Trestné činy proti majetku“). Trestné činy, které řeší zákon č.

[56] POLICIE ČR. Kyberkriminalita. [online]. [cit. 09–06–2017]
[57] POLICIE ČR. Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník. [online]. [cit. 05-06-2017].

40/2009 Sb., o trestní zákoník, ve znění pozdějších změn a předpisů, páchané ve vztahu k datům (uloženým informacím) jsou tyto:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230),
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231),
- Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).

Trestné činy řešené zákonem č. 40/2009 Sb., trestní zákoník, ve znění pozdějších změn a předpisů, páchané ve vztahu k datům (uloženým informacím), při kterých je počítač prostředkem k jejich páchání pak spadají pod tyto paragrafy:[58]

- Šíření pornografie (§ 191),
- Výroba a jiné nakládání s dětskou pornografií (§ 192),
- Navazování nedovolených kontaktů s dítětem (§ 193b),
- Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270),
- Hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355),
- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356),
- Šíření poplašné zprávy (§ 357),
- Pomluva (§ 184),
- Vydírání (§ 175), a mnohé další.

Trestní zákoník implementuje ve zmíněných ustanoveních závazky z Úmluvy Rady Evropy o kybernetické kriminalitě a z rámcového rozhodnutí Rady EU 2005/222/SV o útocích proti informačním systémům. Zmínit lze také mezinárodní smlouvy a právní akty EU zavazující ČR k provedení závazků ohledně veřejně přístupné počítačové sítě (např. Úmluva o ochraně dětí před sexuálním vykořisťováním a

[58] POLICIE ČR. Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník. [online]. [cit. 05-06-2017].

zneužíváním, rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu).[59]

Je-li řeč o legislativě, není možné nezmínit také poměrně nový zákon, kterým je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a také Vyhlášku č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

Jedním z úkolů zákona je sjednocení elektronické komunikace, a to jak ve státní správě, tak zčásti i v soukromé sféře. Věnuje se hlavně zvýšení bezpečnosti důležité infrastruktury státu a podniků spravujících osobní údaje většího počtu lidí. Jeho záměrem je prevence závažných bezpečnostních hrozeb a v možnosti jejich řešení v reálném čase. Tento zákon klade na firmy a státní instituce, co se týče kybernetické bezpečnosti, celkem značné nároky. Vybrané státní i soukromé organizace musí hlásit kybernetické útoky a v souladu se zákonem na ně reagovat. Tento zákon se zaměřuje hlavně na státní správu, díky čemuž by se měla stát odolnější vůči potenciálním útokům. Nová úprava se ale týká i mnoha firem. Potíž tkví dosud akorát v tom, že zatím některé firmy neví, že se jich zákon týká. Doplňující vyhlášky jsou totiž poměrně nejednoznačně napsané, což na začátku komplikovalo orientaci jak podniků, tak i státních úředníků.[60]

4.2 Preventivní opatření vůči počítačové kriminalitě

Je obecně známým pravidelně, že kriminalitě, i té počítačové, je lépe předcházet než následně napravovat škody. V současné době je to velmi aktuální. Mnoho států v tomto směru vytváří a uskutečňuje preventivní systémy boje proti počítačové kriminalitě. Typická je pro ně plánovitost a koordinovanost jednotlivých preventivních aktivit. K nim patří i Česká republika. První formou prevence jsou trestní kodexy, jež reflektují hlavně dva základní aspekty. Primárním aspektem je funkce represivní spočívající v ochraně společnosti před zločinem; činí tak skrze systém sankcí (trestů), kterými postihuje jedince či skupiny, které tyto kodifikované normy jistým právně vytyčeným způsobem překročili. Další hlavní funkcí trestního zákona je funkce expresívní, tzn., že vyjadřuje skrze zákazy a zápovědi (interdiktů) jistý systém sociálních a morálních hodnot tak, jak je v té které

[59] POLICIE ČR. Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník. [online]. [cit. 05-06-2017].
[60] DOSTÁL, D. Počítačová kriminalita ve firmách roste. [online]. 2016. [cit. 09–06–2017]

době uznává kolektivní společenské vědomí. Jednou z nejdůležitějších funkcí každého trestně právního systému je jeho generálně preventivní účinek v právním vědomí veřejnosti a hlavně pak v povědomí potenciálních pachatelů trestných činů. Například ve sféře softwarového pirátství je naneštěstí právní povědomí trestnosti u většiny českých občanů poměrně slabé. Je to faktor celkem malé účinnosti českého trestněprávního systému v oblasti počítačové kriminality.[61]

Jedna ze zásadních forem prevence počítačové kriminality je zaměřena na výchovu občanů, formování prostředí náročnosti a odpovědnosti za zacházení s výpočetní technikou i zpracovávanými daty. Zhotovení podmínek pro posílení odpovědnosti by mělo zapříčinit omezování zájmů odborně vzdělaných osob o jednání zapříčiňující narušení řádné činnosti výpočetní techniky. Preventivní opatření tak směřují hlavně k vybudování systému zabezpečujícího přístup k výpočetní technice jen oprávněným osobám při existenci podmínek pro možnou kontrolu výsledků práce takových osob. Dalším východiskem je utváření technických prostředků a vytváření organizačních podmínek pro ochranu počítačů. Podstatný význam však pořád mají ochranné systémy a jejich zdokonalování, protože směřují hlavně k uskutečnění ochrany konkrétní výpočetní techniky i systému automatizovaného zpracování dat.[62]

V České republice se o zvýšení povědomí a vzdělání snaží např. projekt **Bezpečný internet.cz**, nebo třeba projekt **E-Bezpečí**[63] zaměřující se na prevenci, vzdělávání, výzkum, intervenci a osvětu související s rizikovým chováním na internetu a podobnými fenomény. Projekt uskutečňuje Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi.

Preventivní úlohu lze připisovat i statistikám v prevenci i represi počítačové kriminality. Objem počítačové kriminality, jejích podob a společenských důsledků prezentuje podstatné vodítko taktiky i strategie jak boje s kriminalitou, tak i podnětem k náležitému zaměření preventivních opatření. Aktuálně je počítačová kriminalita v České republice zahrnována policejními orgány do oblasti hospodářské kriminality, což je nevyhovující, neboť to dostatečně nevystihuje variabilitu i podstatu této sféry trestné činnosti. Policejní orgány mají pro evidenci trestné činnosti a její následné využití k

[61] MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 224-225.
[62] MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 225-226.
[63] E-BEZPEČÍ.CZ. [online]. 2016. [cit. 24–06–2017]

dispozici databázové systémy celostátních policejních evidencí a statistik. Tyto systémy se dělí na dvě oblasti.

Na stránkách Policie ČR[64] lze nalézt statistiky kriminality. Nachází se mezi nimi spoustu různých trestných činů, mezi nimi však žádný se specifikou kyberkriminality. Jsou uvedeny statistiky pro trestné činy, které se řadí i do oblasti kriminality, jako např. sexuální nátlak, vydírání aj., k nimž může docházet i prostřednictvím internetu, ale ve statistikách bohužel není sledováno, jestli k tomu došlo prostřednictvím internetu či jinak. Konkrétní statistiky kyberkriminality v praxi neexistují.

Jedním z významných faktorů prevence i represe počítačové kriminality je spolupráce policie s jinými orgány. Zmínit lze např. mezinárodní organizaci kriminální policie – INTERPOL. Význam má také spolupráce se znalci (pachatelé kyberkriminality jsou odborníky na IT). Významnou prevencí je také bezvadná a poctivá práce všech zaměstnanců zasažené instituce, dodržování předepsaných postupů a provádění nastavených kontrol. Faktem však je, že u nás je praxí spíše to, že ve většině známých případů došlo k odhalení pachatele spíše náhodou než systematickou prací policejních nebo jiných bezpečnostních orgánů. Pro prevenci je také důležité, aby policejní orgány využívaly již vyřešených případů, kazuistik a inspirovaly se pro prevenci.[65]

Strategie prevence kriminality v České republice na léta 2016 až 2020[66] jako hlavní oblast prevence počítačové kriminality vidí nezbytnost především včasné a prakticky zaměřené informovanosti o existujících rizicích a možnostech ochrany před nimi, podobně jako přijímaní různých technických opatření v zabezpečení systémů, aby nemohlo nastávat zneužívání uvedeného virtuálního prostředí a komunikace v něm činěné.

Oblast prevence počítačové kriminality je řešena na různých úrovních a například NATO vytvořilo deset pravidel pro počítačovou bezpečnost:[67]

- **Pravidlo teritoriality** – informační infrastruktura v určitém státu podléhá teritoriální suverenitě daného státu.

[64] POLICIE ČR. Policie ČR. [online]. [cit. 09–06–2017]
[65] MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 225-226.
[66] MV ČR. Strategie prevence kriminality v České republice na léta 2016 až 2020. Praha: Ministerstvo vnitra. [online]. 2016. [cit. 22–06–2017], s. 55.
[67] In MACHÁČEK, M. Počítačová kriminalita a bezpečnost. [online]. 2013. [cit. 22–06–2017]

- **Pravidlo odpovědnosti** – spáchání počítačové kriminality z počítačů či jiných zařízení nacházející se na území jednoho státu se pokládá za důkaz a takový útok může být uvedenému státu připisován.
- **Pravidlo spolupráce** – pakliže byl útok spáchán z počítačových systémů daného státu, je tento stát povinen spolupracovat s obětí formou konzultací, výměny informací, a dalšími způsoby.
- **Pravidlo sebeobrany –** v kyberprostoru má každý nárok na sebeobranu. Reakce silou se v určitých případech připouští.
- **Pravidlo ochrany dat –** data získaná monitorováním internetu se pokládají za osobní. Je možné je ale poskytnout třetí straně, zajistí-li stejnou míru ochrany. Monitorování internetu a výměna informací musí být v rovnováze s ochranou práv jednotlivců.
- **Pravidlo odpovědnosti se starat –** každý by se měl snažit rozumně ochraňovat svá počítačová zařízení.
- **Pravidlo včasného varování –** každý má povinnost informovat případné oběti o připravovaném kyberútoku.
- **Pravidlo přístupu k informacím** – veřejnost má právo na informace o kyberhrozbách vůči životu, bezpečnosti a dobrému žití.
- **Pravidlo zákonnosti –** všechny státy musí do své legislativy zahrnout nejčastější kyberzločiny.
- **Pravidlo mandátu** – schopnost organizace závisí na rozsahu jejího mandátu. Na mezinárodním poli je nezbytné zastavit duplikaci schopností a snah.

4.3 Organizace zabývající se počítačovou kriminalitou v ČR

Počítačová kriminalita prezentuje vážný problém, není tak divu, že k jeho potírání či prevenci vznikají specializované organizace, týmy aj., a to jak na národní, tak i mezinárodní úrovni, jak vládní, tak neziskové. Jde zejména o tyto:

Národní bezpečnostní úřad (NBÚ)

Jde o orgán moci výkonné zřízený zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, a to k 1. srpnu 1998. Od roku 2011

je gestorem kybernetické bezpečnosti a současně národní autoritou v této sféře. NBÚ tuto činnost zajišťuje skrze Národní centrum kybernetické bezpečnosti (NCKB). Je ústředním správním úřadem v oblasti kybernetické bezpečnosti.[68]

Národní centrum kybernetické bezpečnosti (NCKB)

Činnosti centra se zaměřují na koordinaci spolupráce na národní i mezinárodní úrovni při prevenci kybernetických útoků i při návrhu a přijímání nařízení při řešení incidentů i proti uskutečňovaným útokům. Mezi nejdůležitější činnosti centra patří:[69]

- provozování Vládní CERT České republiky (GovCERT.CZ),
- spolupráce s dalšími národními CERT® týmy a CSIRT týmy,
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy,
- příprava bezpečnostních standardů pro vybrané skupiny organizací v ČR,
- osvěta a podpora vzdělávání ve sféře kybernetické bezpečnosti,
- výzkum a vývoj v rámci kybernetické bezpečnosti.

Rada pro kybernetickou bezpečnost (RKB)

Tato organizace vznikla v roce 2011 a prezentuje poradní orgán předsedy vlády pro oblast kybernetické bezpečnosti. Má za úkol také podporu výkonu gesční a koordinační role NBÚ v rámci kybernetické bezpečnosti s potřebou součinnosti státních institucí a subjektů kritické infrastruktury. K jejím hlavním úkolům patří: [70]

- slaďování činnosti státních organizací ohledně kybernetické bezpečnosti a přispívání k zabezpečení plnění závazků meziresortního charakteru,
- slaďování státních institucí při plnění závazků v rámci kybernetické bezpečnosti, které plynou z členství České republiky v mezinárodních organizacích a koordinace zastupování České republiky v mezinárodních organizacích a v dalších zahraničních činnostech majících souvislost s kybernetickou bezpečností,

[68] NBÚ. Národní bezpečnostní úřad. [online]. 2013. [cit. 22–06–2017]
[69] NCKB. Národní centrum kybernetické bezpečnosti. [online]. 2013. [cit. 22–06–2017]
[70] NCKB. Národní centrum kybernetické bezpečnosti. [online]. 2013. [cit. 22–06–2017]

- aktivní formování okolností pro hladké fungování spolupráce mezi členy Rady,
- řešení současných záležitostí kybernetické bezpečnosti a předkládání odborných návrhů a doporučení vládě,
- monitorování plnění závěrů z jednání Rady jejími členy,
- shromažďování, analýza a vyhodnocení informací o situaci zabezpečení kybernetické bezpečnosti poskytovaných členy Rady,
- příprava návrhu zprávy ohledně zabezpečení kybernetické bezpečnosti České republiky, která je pravidelně zasílána předsedou vlády vládě jako hlavní dokument, který určuje priority a z nich plynoucí úkoly ve sféře kybernetické bezpečnosti pro nadcházející období,
- spolupráce s externími odbornými subjekty a využívání jejich výstupů v zájmu zabezpečení kybernetické bezpečnosti České republiky.

CSIRT a CERT

CSIRT a CERT jsou týmy bezpečnostních expertů, které se zabývají řešením incidentů (a jejich předcházením), které mohou vzniknout na internetu. Funkce týmu závisí na poli jeho působnosti. Ve větších firmách fungují interní týmy, které se zabývají prevencí bezpečnostních hrozeb, vzděláváním zaměstnanců. Další skupinou jsou bezpečnostní týmy na národní úrovni. Jejich pole působnosti tvoří celý stát. U nás působí dva bezpečnostní týmy – národní a vládní.[71]

First a Trusted Introducer

Jde o mezinárodní instituce, jejich záměrem je vytvořit pro všechny aktéry důvěryhodné prostředí, jednodušší systém pro vyhledávání informací ve světě a zabezpečené fórum pro vzájemnou výměnu zkušeností mezi bezpečnostními týmy.[72]

Policie ČR

Policie České republiky představuje jednotný ozbrojený bezpečnostní sbor, jehož úkolem je „*…chránit bezpečnost osob a majetku, chránit veřejný pořádek a předcházet trestné činnosti. Plní rovněž úkoly podle trestního řádu a další úkoly na úseku vnitřního*

[71] KRÁL, M. Bezpečný internet: Chraňte sebe i svůj počítač. Praha: Grada Publishing a.s., 2015, s. 134.
[72] KRÁL, M. Bezpečný internet: Chraňte sebe i svůj počítač. Praha: Grada Publishing a.s., 2015, s. 134.

pořádku a bezpečnosti svěřené jí zákony, předpisy Evropských společenství a mezinárodními smlouvami, které jsou součástí právního řádu České republiky“.[73]

Co se týče kyberkriminality, tak od poloviny roku 2016 funguje v rámci Policie ČR policejní superúřad pro boj s organizovaným zločinem – Národní centrála proti organizovanému zločinu (NCOZ). Jedním z jejich útvarů je sekce kybernetické kriminality. Policie ČR od roku 2011 monitoruje množství trestných činů spáchaných v kyberprostoru (zejm. v síti Internet). Od roku 2012 provozuje na internetových stránkách www.pcr.cz policejní internetovou HotLine, která slouží pro hlášení závadového obsahu a aktivit v síti Internet.

Česká protipirátská unie (ČPU)

ČPU vznikla pro ochranu autorského práva a práv souvisejících s právem autorským k audiovizuálním dílům a potírání všech podob pirátství ve sféře výroby, dovozu a šíření audiovizuálních děl. ČPU zastupuje na základě plných mocí a pověření členské společnosti a další poškozené, kteří mají práva k audiovizuálním dílům, zvukověobrazovým záznamům a televiznímu vysílání (na našem území i na Slovensku).[74]

Business Software Alliance (BSA)

BSA funguje ve více než 80 zemích světa, v nichž brání zájmy komerčního softwarového průmyslu a jeho hardwarových partnerů. Posláním BSA je podpora aktivit a iniciativy, které zapříčiňují technologické inovace, investice do informačních technologií a důvěru ve výpočetní techniku.[75]

Národní centrum bezpečnějšího Internetu (NCBI)

O obranu či prevenci před počítačovou kriminalitou se u nás starají i některé neziskové organizace a NCBI je jedna z nich. Cílem centra je podílet se na zvýšení bezpečnosti užívání internetu, moderních informačních a komunikačních technologií, zvýšení povědomí uživatelů o jejich pozitivech a případných nebezpečích, podílet se na osvojování etických norem v online prostředí, napomáhat prevenci a omezování případných sociálních rizik souvisejících s jejich užíváním. Hlavním záměrem je utvoření

[73] POLICIE ČR. Policie ČR. [online]. [cit. 09–06–2017]
[74] ČPU. Česká protipirátská unie. [online]. [cit. 26-06-2017].
[75] BSA. [online]. [cit. 26-06-2017].

a provoz odborného pracoviště pro osvětu, vzdělávání a ochranu uživatelů před nelegálním a nebezpečným obsahem na internetu.[76]

Bezpečný internet.cz

Neziskový projekt, jehož záměrem je prezentovat četná rizika související s používáním internetu a rovněž na způsoby, jak se jim efektivně bránit. Projekt se zaměřuje jak na děti, tak specificky na rodiče, začátečníky uživatele internetu aj. Hlavním cílem projektu jsou aktivity pro posílení celkového povědomí o rizicích a vzdělávat české uživatele internetu v tomto směru.[77]

4.4 Zhodnocení dosavadních opatření pro potírání počítačové kriminality v ČR

Jak již vyplynulo z předešlých kapitol, počítačová kriminalita se potýká obecně s významnými problémy zejména souvisejícími s komplikací při identifikaci pachatele, jeho rozpoznání, ale třeba i místa vzniku trestného činu a jeho vyšetření.

Počítačová kriminalita v České republice se potýká hlavně s některými problémy při jejím odhalování a dokazování. Zmínit lze problém jurisdikce, komplikaci, kterou je vůbec možnost odhalení trestné činnosti, aby bylo možné dokázat, kdo je pachatelem a dokázat pachateli, že jde o jeho trestnou činnost. Potíží jsou rovněž chybějící nebo špatně definované skutkové podstaty nového trestního zákoníku, ačkoliv ten je pochopitelně mnohem sofistikovanější, než byl trestní zákoník předchozí.[78]

Aktualizovaná Koncepce rozvoje Policie České republiky do roku 2020[79] (z roku 2017) uvádí, že jedním z problémů je, že v současné době není policie schopna reagovat na sofistikovanější a technologicky komplikované způsoby páchání kyberkriminality a zvyšování množství jejich případů. Nepostradatelnými podmínkami pro boj policie s kyberkriminalitou jsou zdroje technicko-technologické, připravení a kvalitní odborníci s průběžným vzděláváním a odpovídajícím platovým ohodnocením a zabezpečení odpovídající mezinárodní spolupráce.

[76] NCKI. Národní centrum bezpečnějšího internetu. [online]. [cit. 22–06–2017]
[77] BEZPEČNÝ INTERNET.CZ. [online]. [cit. 26-06-2017].
[78] SMEJKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017].
[79] POLICIE ČR. Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). Praha: Policejní prezidium České republiky. 2017, s. 45.

Smejkal[80] v souvislosti s legislativou hovoří o vybraných problémech. Jako první zmiňuje, že zatímco při fyzickém útoku na nějaké technické zařízení jde celkem dobře zjistit, kde došlo ke spáchání trestného činu, u dálkového přístupu a používání virtuálních počítačů, cloudů apod. v oblasti IT existuje problém. Servery mohou být kdekoli na světě, v jakémkoli výpočetním centru nadnárodní společnosti. To se pochopitelně negativně odráží jak v oblasti civilního práva (např. ohledně odpovědnosti za škodu), tak z hlediska trestního procesu, kdy vlastně nelze vědět, kde se ten trestný čin stal a jak postupovat.

Dále je zde problém odhalování kyberkriminality. Existuje několik fází, které trestný čin provázejí od jeho vzniku až do eventuálního potrestání pachatele. Může dojít k tomu, že vůbec nebude zjištěno, že k něčemu došlo. Ve sféře počítačů je to celkem časté, míra latence je značná. Problémem je i to, že skutky, u nichž se zjistí, že se staly, pak nejsou vyhodnoceny jako činy trestné. Navíc jsou zde skutky, u nichž se zjistí, co se stalo, vyhodnotí se jako trestné činy, ale jejich případný oznamovatel je chce utajit (např. banky, které se bojí o svou důvěryhodnost). Nebo jsou skutky, které se odhalí, oznámí, ovšem policie pachatele nenajde (buď neexistuje vůbec žádný podezřelý, anebo existuje, ale nepodařilo se vyšetřování ukončit sdělením obvinění). V praxi se lze setkat s případy, kdy bylo zahájeno trestní stíhání, ovšem obžaloba nebyla podána, či byl obžalovaný zproštěn. Bývá to mnohdy častý problém s nezvládnutím procesu dokazování, kdy nebyly zabezpečeny stopy, nebo byly zajištěny chybné stopy, nebyly zpracovány kvalitní znalecké posudky aj. Žádoucí z pohledu boje proti kybernetické kriminalitě je, když je obžalovaný uznán vinným a rozsudek nabude právní moci poté, co jej potvrdily všechny soudní instance.[81]

Zásadní je prokazatelnost, že se stopa k odhalení počítačové kriminality nacházela na nějakém místě, a že od jejího zabezpečení až do ukončení zkoumání či dokonce ukončení celého trestního procesu nebyla nijak pozměněna. To bývá dost často opomínáno. Navíc je zde potíž s fyzickou přítomností pachatele, který se může nacházet kdekoliv, problém času, který lze v počítačovém systému měnit, problém čitelnosti dat (ne všechna data lze s časovým odstupem přečíst), problém identifikace a autentizace. Velkým problémem bývá také průkaznost důkazů, hlavně na úrovni Policie České republiky a jí přibíraných znalců – nekvalifikované postupy, eventuálně postupy

[80] SMEJKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017].
[81] SMEJKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017].

nejednotné. S tím souvisí navíc i neadekvátní metodika pro zabezpečování stop v kyberprostoru.[82]

Současným problémem je také to, že pachatelé kyberkriminality jsou obvykle rychlejší, než vývojáři antivirových programů či jiných bezpečnostních opatření. Policie ČR stále nedisponuje dostatečným počtem kvalifikovaných a vzdělaných odborníků na tuto oblast. Spolupráce se zahraničními odborníky na toto téma rovněž není úplně dostatečná.

5 Budoucnost počítačové kriminality v ČR

Do budoucnosti hledí také Koncepce rozvoje Policie České republiky do roku 2020[83]. V ní zaznívá, že v rámci informační kriminality lze v nejbližší budoucnosti očekávat monitorování technologických trendů pachateli. Tak, jako se zvyšuje poměr množství mobilních zařízení a význam zpracovávaných dat v těchto mobilních zařízeních (v ČR vzrostl od roku 2010 počet uživatelů mobilního internetu ze 700 tis. na 2,5 mil.), bude se tedy rozšiřovat i šíření mobilního malware a budou se množit útoky na tato zařízení více než doteď. Zcela určitě je možné očekávat projevy nesouhlasu s politickými či jinými veřejnými názory, na které vzniknou reakce prostřednictvím hackerských útoků. Míra profesionalizace pachatelů informační kriminality bude vzrůstat a bude ji provázet dělba konkrétních rolí.

Masivněji lze očekávat zapojení tzv. botnetových sítí, jejichž úkolem je anonymizovat aktivitu původce nelegálního jednání a zároveň zvyšovat masivnost či technologickou koordinaci útoku. S ohledem na nedávný vývoj v oblasti tzv. cloudových řešení je možné předpokládat zvýšení množství útoků na takto centralizovaná data a masivnější únik informací. Nové technologie nabízejí a pořád častěji budou nabízet i větší možnosti pachatelů různé trestné činnosti zakrývat vzájemnou komunikaci nebo výměnu dat s využitím právě nových služeb v informačních technologiích. Více do budoucna dojde k digitalizaci většiny nepřímé komunikace včetně citlivých, osobních nebo jinak chráněných informací. V tomto směru se bude exponenciálně zvyšovat míra důležitosti

[82] SMEJKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017].
[83] Viz POLICIE ČR. Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). Praha: Policejní prezidium České republiky. 2017, s. 31.

ochrany a nezbytnosti žádoucího opatření při narušování takové ochrany, která obvykle bude mít kriminální povahu.[84]

Rozvoj počítačové kriminality se bude zajisté podílet i na celkovém zrychlení jakýchkoliv kriminálních jevů. Počítač a internet již teď využívají teroristé k tomu, aby se jim dařilo získávat příznivce po celém světě. Na internetu se tito lidé sdružují prostřednictvím „zájmových skupin" a vše je celkově zrychlené. Nábory teroristů probíhají téměř online a to lze očekávat i do budoucna, nejen v oblasti kyberterorismu, ale v podstatě jakékoliv skupiny hackerů aj. se takto budou více kontaktovat a plánovat útoky. Posílení tohoto trendu bude doprovázet i to, že lze také očekávat sofistikovanější způsoby ochrany anonymity konverzací aj.

Značnou hrozbou je zajisté to, že skoro všechny lidské činnosti se začínají organizovat a řídit prostřednictvím internetu. Existují bezpečnostní systémy napojené na internet, úřednické systémy, celá veřejná správa, bankovnictví aj. je odkázáno na internetové připojení. Se zvyšováním informovanosti a vzdělanosti pachatelů počítačové kriminality lze očekávat stále dokonalejší a agresivnější útoky. Kdyby například došlo k úplnému zrušení hotovostních plateb (zatím sice daleká budoucnost), objevuje se prostor pro útoky na celé systémy bezhotovostních platebních styků. SW vývojem bezpilotních letadel či vývojem automobilů, které nepotřebují řidiče lze také očekávat riziko jejich napadané kyberzločinci. Stejně tak je zde do budoucna riziko „lidského malware", které souvisí s lékařskými implantáty, které budou v budoucnu ovládány skrze wi-fi připojení.[85]

Jak již bylo uvedeno[86], současné řešení internetové kriminality naráží zatím u nás na některé problémy, například problém, že skutečně mnohdy nevíme, kde se ten trestný čin stal, kde byl pachatel, kde je poškozený a tak dále. Do budoucna by to mohlo vyřešit zformování nového konceptu, nových kritérií pro aplikaci principů místní působnosti. K tomu již svým způsobem dochází, a to prostřednictvím rozhodovací praxe různých soudů, ale nelze hovořit o jednotnosti. Řešením by také mohlo být konstatování, že existuje jistá informační vrstva bez místní jurisdikce státu. Něco jako je eurozatykač, který by fungoval na základě Evropské unie, na základě Úmluvy Rady Evropy o

[84] Viz POLICIE ČR. Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). Praha: Policejní prezidium České republiky. 2017, s. 31.
[85] Viz GLASSBERG, J. The Future of Crime: 8 Cybercrimes to Expect in Next 20 Years. [online]. 2014. [cit. 22–06–2017]
[86] SMEJKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017].

kyberkriminalitě. Spíše by ale lepším řešením mělo být něco, co by působilo celosvětově, neboť lze disponovat jistým ujednáním v rámci EU, pokud se ale pachatel odstěhuje mimo EU, je mimo oblast působnosti. Bylo by tak vhodné zvážit vznik instituce mezinárodního soudu pro kyberkriminalitu.

Smejkal[87] také odhaduje, že je třeba počítat s tím, že nadále porostou útoky prostřednictvím sociálních sítí. A to nejen útoky na čest a duševní zdraví, jak to dosud ze sociálních sítí bylo známo. Je třeba počítat s útoky sofistikovanějšími. Bude se jednat o útoky takové, aby si lidé virus, který bude monitorovat, co píšou na klávesnici, nainstalovali skrze Facebook. To už je dnes poměrně běžné, když z lidí někdo vyláká nějaké finance na Facebooku, neboť se vydává za uživatelova tzv. „kamaráda nebo přítele".

Samostatnou kapitolou do budoucna jsou podniky a organizace, které jsou jedněmi z významných obětí počítačové kriminality. Do budoucna lze stále očekávat nárůst jejich napadání. Podporuje to skutečnost, že firmy často tyto útoky ani nehlásí, neboť netuší, odkud přišly. Případně se stydí za to, že si svá data neochránily (případy bank aj.) a nechtějí to na veřejnosti prezentovat. Případně mají negativní zkušenosti s pátráním policie, které nepřineslo žádné výsledky.

Pochopitelným dopadem počítačové kriminality do budoucna jsou další a další finanční ztráty. Podle výzkumné a poradenské společnosti v oblasti informačních technologií dojde ke zvýšení počítačové kriminality každoročně o 10 %. V roce 2014[88] počítačová kriminalita způsobila finanční ztráty někde mezi 375 miliardami a 575 miliardami dolarů. Do konce roku 2016 mělo jít o ztráty z počítačové kriminality mezi 450 až 690 miliardami dolarů.[89] Stejně tak lze očekávat zvýšení finančních výdajů na potírání a prevenci počítačové kriminality policí ČR.

Lonegran[90] hovoří o zvyšování podílu nákupů prostřednictvím tabletů a mobilních telefonů (v roce 2017 už 87 %). To do budoucna bude prezentovat zvýšení nebezpečí z malwarových aplikací, které obvykle směřují na operační systém Android. S rychlým

[87] SMEJKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017].
[88] KIRK, J. Cybercrime Losses Tops $400 Billion Worldwide. [online]. 2014. [cit. 22–06–2017]
[89] GARTNER. Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond. [online]. 2011. [cit. 22–06–2017]
[90] LONEGRAN, K. The future of cybercrime. [online]. 2014. [cit. 22–06–2017]

šířením smartphonů je však nevyhnutelné, že začnou vznikat více specializované malware na Android, IOS a Windows.

Ze zprávy společnosti AVG z roku 2011[91] vyplývá, že zvýšené riziko kyberkriminality tkví nejen v technologiích (softwaru a hardwaru), ale častěji z aktivit uživatelů (wetware). Uživatelé totiž přestávají být tak opatrní při zabezpečování svých on-line přístrojů, což vede ke katastrofálním scénářům počítačové kriminality. Kyberzločinci se začínají více zaměřovat na lidský faktor, než na stroje – chtějí přimět uživatele ke stahování a instalování vadného softwaru, vydávají se za poskytovatele antivirových programů či za jiný důvěryhodný zdroj.

Výhledem do budoucna je zřejmé, že pro kybernetickou bezpečnost České republiky bude zapotřebí podpory vývoje v oblasti potírání a prevence kybernetické bezpečnosti. Jak bylo uvedeno, setkáváme se aktuálně v České republice s mnohými problémy, ať už v oblasti legislativy, tak činnost policie ohledně prošetřování a zjišťování kyberzložinů. V reakci na hrozbu počítačové kriminality existuje naléhavá potřeba reformovat metody policie a rozvíjet nadnárodní policejní dovednosti a spolupráci. To platí obecně nejen pro ČR, ale po celém světě[92].

Koncepce rozvoje Policie České republiky do roku 2020[93] z hlediska cílů do budoucnosti uvádí mimo jiného např. potřebu aktivnějšího vyhledávání závadového obsahu v prostředí internetu, aktivnějšího působení v prostředí skrytého internetu, zlepšení spolupráce a vzájemné koordinace se zahraničními policejními a justičními orgány; dalšími partnery, zachovávání adekvátní úrovně technologického vybavení pracovišť kybernetické kriminality, preventivní aktivity při vzdělávání obyvatelstva ohledně bezpečného chování na internetu a kybernetické kriminality obecně, ve spolupráci s Ministerstvem vnitra, neziskovými organizacemi, Asociací krajů České republiky národním a vládním CERT týmem aj.

[91] CHIP. Budoucnost kyberzločinu. [online]. 2011. [cit. 27–06–2017]
[92] Viz např. BROADHURST, R. Developments in the global law enforcement of cyber- crime. Policing: An International Journal of Police Strategies & Management. 2006. Vol. 29 Iss. 3, pp. 408-433
[93] POLICIE ČR. Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). Praha: Policejní prezidium České republiky. 2017, s. 68.

Závěr

Předložená závěrečná práce se věnovala problematice počítačové kriminality se zaměřením na situaci v České republice. Práce vycházela ze skutečnosti, že počítačová nebo také kyberkriminalita prezentuje současný trend kriminality, který představuje velmi významné ohrožení bezpečnosti a práv jednotlivců, firem, veřejné správy, ale v podstatě celé lidské společnosti. Ochrana před tímto typem kriminality však není vůbec snadná a v praxi se ukazuje, že se nejsme schopni adekvátně bránit.

Cílem práce bylo na základě získaných informací analyzovat současný stav počítačové kriminality, její historický vývoj a na základě zjištěných výsledků predikovat vývoj budoucí. Dílčím cílem bylo na základě současného stavu ověřit funkčnost přijatých preventivních opatření, případně nová opatření navrhnout. Základním problémem práce byly eventuální budoucí hrozby v počítačové kriminalitě a přijatá preventivní opatření.

Pro naplnění stanovených cílů a problémů bylo využito dostupné literatury, informací získaných z Národní strategie kybernetické bezpečnosti České Republiky na období let 2015 až 2020 (NBÚ), Národního centra kybernetické bezpečnosti (NCKB), údajů Policie ČR, ale i autorů odborných děl či článků zabývajících se oblastí kybernetické bezpečnosti.

Z práce mimo jiného vyplynulo, že v České republice existuje hned několik problematických oblastí týkajících se počítačové kriminality. Patří k nim záležitost náročnosti až nemožnosti identifikovat a usvědčit pachatele kyberkriminality, nedostatečná vzdělanost uživatelů internetu, špatné zabezpečení firemních počítačových sítí a je zde také problém, že Policie ČR vůbec nevede dosud statistiky počítačové kriminality, tudíž jen těžko takto může vyhodnocovat dosavadní trendy počítačové kriminality a co hůře, nemůže se ani dostatečně zaměřit na žádoucí úroveň prevence počítačové kriminality. Do budoucna lze navíc očekávat stále intenzivnější, sofistikovanější a nebezpečnější útoky kyberzločinců.

Seznam použitých zdrojů

Literární zdroje

1. BEDNÁŘ, V. *Marketing na sociálních sítích*. *Prosaďte se na Facebooku a Twitteru.* Praha: Computer Press, 2011b. 200 s. ISBN 978–80–251–3320–0.
2. BOCAN, M.; HOŠKOVÁ, I.; MACHALÍK, T. Děti v ringu dnešního světa. Hodnotové orientace dětí ve věku 6 až 15 let. Praha: Národní institut dětí a mládeže Ministerstva školství, mládeže a tělovýchovy, zařízení pro další vzdělávání, 2012. ISBN 978-80-87449-24-0.
3. BROADHURST, R. Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management. 2006. Vol. 29 Iss. 3, pp. 408-433.
4. DRMOLA, J. Konceptualizace kyberterorismu. In Vojenské rozhledy, 2013, roč. 22, č. 54, č. 2, s. 94–102, ISSN 1210-3292.
5. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.
6. JIROVSKÝ, V. Kybernetická kriminalita. Praha: Grada Publishing a.s., 2007. 284 s. ISBN 9788024715612.
7. KOPECKÝ, L. *Public relations: dějiny - teorie – praxe*. Praha: Grada Publishing a.s., 2013. 238 s. ISBN 978–80–247–4229–8.
8. KOLOUCH, J. Cyberkrime. Praha: CZ.NIC, z. s. p. o. 2016. ISBN 978-80-88168-18-8.
9. KRÁL, M. Bezpečný internet: Chraňte sebe i svůj počítač. Praha: Grada Publishing a.s., 2015. 184 s. ISBN 9788024798219.
10. KULHÁNKOVÁ, H.; ČAMEK, J. *Fenomén facebook*. Kladno: BigOak, 2010. 128 s. ISBN 978–80–904764–0–0.
11. LALÍK, M. WWW pro každého. Praha: Grada Publishing a.s., 2013. 168 s. ISBN 9788024784076.
12. MATOUŠKOVÁ, I. Aplikovaná forenzní psychologie. Praha: Grada Publishing a.s., 2013. 304 s. ISBN 9788024784229.
13. MIHÁL, V. Dopad televize na vývoj dítěte. In Pediatrie praxi 2012; 13(4): 281–282.

14. MUSIL, S. Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000. ISBN 80-86008-80-0.
15. NBS. Národní strategie kybernetické bezpečnosti ČR 2015-2020. 2015.
16. POLICIE ČR. Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). Praha: Policejní prezidium České republiky. 2017. 146 s.
17. POLICIE ČR. Rozvoj Policie České republiky v letech 2016 – 2020. Praha: Policie ČR. 2015. 58 s.
18. POŽÁR, J. Vybrané trendy kybernetické kriminality. In Acta Informatica Pragensia, 2015, roč. 4, č. 3, s. 336–348.
19. PROCHÁZKA, D. První kroky s internetem. Praha: Grada Publishing a.s., 2010. 108 s. ISBN 9788024732558.
20. SVATOŠ, R. Kriminologie. Plzeň: Aleš Čeněk, s.r.o. 2012, 290 s. ISBN 978-80-7380-389-6.
21. ŠEVČÍKOVÁ, A. a kol. Děti a dospívající online: Vybraná rizika používání internetu. Praha: Grada Publishing a.s., 2015. 184 s. ISBN 9788024796451.
22. ŠTRAUS, J. a kol. Kriminalistická metodika. Plzeň: Aleš Čeněk, 2006.
23. TAVANI, H. T. Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace. In Acm Sigcas Computers and Society. 2000, Vol. 30, No. 3, pp. 3-9.

Elektronické zdroje

1. BSA. [online]. [cit. 26-06-2017]. Dostupný z http://ww2.bsa.org/country/BSA%20and%20Members.aspx.
2. BEZPEČNÝ INTERNET.CZ. [online]. [cit. 26-06-2017]. Dostupný z http://www.bezpecnyinternet.cz/.
3. BUSINESSIT.CZ. Kybernetická kriminalita I: Co se děje v kyberprostoru. [online]. 2012. [cit. 05-06-2017]. Dostupný z http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php.
4. BUSINESSIT.CZ. Kybernetická kriminalita II: Sociální sítě jako médium budoucnosti i skrytá hrozba. [online]. 2012. [cit. 05-06-2017]. Dostupný z http://www.businessit.cz/cz/kyberneticka-kriminalita-ii-socialni-site-medium-hrozba-facebook.php.
5. ČPU. Česká protipirátská unie. [online]. [cit. 26-06-2017]. Dostupný z http://www.cpufilm.cz/.
6. DOSTÁL, D. Počítačová kriminalita ve firmách roste. [online]. 2016. [cit. 09–06–2017] Dostupný z http://www.businessinfo.cz/cs/clanky/pocitacova-kriminalita-ve-firmach-roste-83291.html.

7. E-BEZPEČÍ.CZ. [online]. 2016. [cit. 24–06–2017] Dostupný z https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu.

8. GARTNER. *Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond*. [online]. 2011. [cit. 22–06–2017] Dostupný z http://www.gartner.com/newsroom/id/1862714.

9. GLASSBERG, J. The Future of Crime: 8 Cybercrimes to Expect in Next 20 Years. [online]. 2014. [cit. 22–06–2017] Dostupný z http://www.foxbusiness.com/personal-finance/2014/05/14/future-crime-8-cyber-crimes-to-expect-in-next-20-years/.

10. CHIP. Budoucnost kyberzločinu. [online]. 2011. [cit. 27–06–2017] Dostupný z http://www.chip.cz/novinky/budoucnost-kyberzlocinu/.

11. KIRK, J. Cybercrime Losses Tops $400 Billion Worldwide. [online]. 2014. [cit. 22–06–2017] Dostupný z http://www.computerworld.com/article/2490566/security0/cybercrime-losses-top--400-billion-worldwide.html.

12. LONEGRAN, K. The future of cybercrime. [online]. 2014. [cit. 22–06–2017] Dostupný z http://www.information-age.com/future-cybercrime-123458380/.

13. MACHÁČEK, M. Počítačová kriminalita a bezpečnost. [online]. 2013. [cit. 22–06–2017] Dostupný z http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/.

14. MV ČR. Strategie prevence kriminality v České republice na léta 2016 až 2020. Praha: Ministerstvo vnitra. [online]. 2016. [cit. 22–06–2017] Dostupný z http://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2016-az-2020.aspx.

15. NBÚ. Národní bezpečnostní úřad. [online]. 2013. [cit. 22–06–2017] Dostupný z https://www.nbu.cz/cs/o-nas/.

16. NCKI. Národní centrum bezpečnějšího internetu. [online]. [cit. 22–06–2017] Dostupný z http://www.ncbi.cz/.

17. NCKB. Národní centrum kybernetické bezpečnosti. [online].[cit. 22–06–2017] Dostupný z https://www.govcert.cz/.

18. POLICIE ČR. Policie ČR. [online]. [cit. 09–06–2017] Dostupný z http://www.policie.cz/clanek/o-nas-policie-ceske-republiky-policie-ceske-republiky.aspx.

19. POLICIE ČR. Kyberkriminalita. [online]. [cit. 09–06–2017] Dostupný z http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09NA%3D%3D.

20. POLICIE ČR. Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník. [online]. [cit. 05-06-2017]. Dostupný z http://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx.

21. POLICIE ČR. Jednotlivé druhy kyberkriminality. [online]. [cit. 05-06-2017]. Dostupný z http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

22. PWC. Počítačová kriminalita pod lupou. [online]. 2011. [cit. 22-06-2017]. Dostupný z http://www.pwc.com/cz/en/hospodarska-kriminalita/assets/Crime_survey_CR_czech_ele.pdf.

23. SMEJKAL, V. Kybernetická kriminalita - fenomén dneška. [online]. 2015. [cit. 05-06-2017]. Dostupný z http://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska.

24. ŠEBEŠ, M. Děti a mládež v kyberprostoru. [online]. [cit. 08–06–2017] Dostupný z http://www.mediapodlupou.cz/lekce/deti-a-mladez-v-kyberprostoru.

Legislativní dokumenty

1. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In *Sbírka zákonů České republiky*. 2014, částka 75, s. 1926-1936. Dostupné z http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231
2. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů České republiky*. 2009, čáska 11, s. 354-464. Dostupné z http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405
3. ČESKO. Zákon č. 273/2008 Sb., o Policii České republiky. In *Sbírka zákonů České republiky*. 2008, částka 91, s. 4086-4156. Dostupné z http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5332

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- databáze Automatizovaného rozpočtového informačního systému MF ČR,

Seznam zkratek

Seznam tabulek a grafů

Přílohy