VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Jiří Němec

Studijní program: Bezpečnostně právní činnost

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Prezenční

Místo studia: České Budějovice

**Název bakalářské práce: Počítačová kriminalita a její příčiny.**

**Název bakalářské práce v anglickém jazyce: Cybercrime and its causes.**

Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce (jméno a příjmení, titul): doc. JUDr. Roman Svatoš, Ph.D

Datum zadání bakalářské práce (měsíc, rok): duben 2019

Cíl bakalářské práce: Cílem bakalářské práce je zjistit, jaká je dynamika počítačové kriminality, dále zjistit jaké jsou její příčiny a navrhnout opatření, která by mohla pozitivně ovlivnit především počítačovou kriminalitu páchanou formou Darknet.

| | | |
|---|---|---|
| Student: Jiří Němec | 30.4.2019 | Němec |
| Vedoucí práce: doc. JUDr. Roman Svatoš, Ph.D. | 6.5.2019 | |

Schvaluji zadání bakalářské práce:

| | | |
|---|---|---|
| Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D. | 6.5.2019 | |
| Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová | 7.5.19 | Ferebauerová |
| Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D. | 13.5.2019 | J. Dušek |

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

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

# BAKALÁŘSKÁ PRÁCE

# POČÍTAČOVÁ KRIMINALITA A JEJÍ PŘÍČINY

**Autor práce: Jiří Němec**

**Studijní obor: Bezpečnostně právní činnost ve veřejné správě**

**Forma studia: Prezenční**

**Vedoucí práce: doc. JUDr. Roman Svatoš, Ph.D**
**Katedra: Katedra právních oborů a bezpečnostních studií**

**2020**

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce – v elektronické podobě ve veřejně přístupné části infodisku VŠERS a v tištěné podobě knihovnou VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

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

# ABSTRAKT

NĚMEC, J. *Počítačová kriminalita a její příčiny: bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2020. 60 s. Vedoucí bakalářské práce : doc. JUDr. Roman Svatoš, Ph.D.

**Klíčová slova:** počítačová kriminalita, kyberkriminalita, počítač, internet, kybernetický, kyberprostor, informační technologie

Bakalářská práce se zaměřuje na počítačovou kriminalitu jako jednu ze závažnějších kriminalit dnešní doby vůbec, a to ve smyslu využívání internetu jako prostředku k jejímu páchání. Progresivní vývoj počítačů a informačních systémů je rychlý a spolu s nimi se vyvíjí i počítačová kriminalita, která může ohrožovat každého uživatele využívajícího internet. V práci jsou analyzovány nejčastější formy této kriminality, fenomenologie počítačové kriminality, její pachatelé a historický vývoj.

# ABSTRACT

NĚMĚC, J. *Cybercrime and its causes: Bachelor Thesis.* České Budějovice : The College of European and Regional Studies, 2020. 60 p. Supervisor : doc. JUDr. Roman Svatoš, Ph.D

**Key words:** computer crime, cybercrime, computer, internet, cybernetic, cyberspace, information technology

Bachelors thesis focuses on computer crime, as one of the most serious crimes today, in terms of the use of the Internet as a means to commit it. The progressive development of computers and information systems is rapid, and with them the development of computer crime, which can endanger any user using the Internet. The work analyzes the most common forms of this crime, the phenomenology of computer crime, its perpetrators and historical development.

# Obsah

# Úvod

Počítačová kriminalita patří k novějším odvětvím kriminality, přišla až s rozvojem informačních technologií. V dnešní době, kdy dochází stále ke zdokonalování a rozšiřování technologií v oblastech obchodu, zábavy, výroby, komunikace a přechází to až v závislost na těchto technologiích. Hlavní spojnicí je internet, bez kterého by nebylo možné tyto technologie využívat, bez jejich propojení by nedocházelo k tak důležité věci, jako je přenos dat.

Počítačová kriminalita, kybernetická kriminalita neboli kybernalita je relativně novým problémem, v simplifikované definici se jedná o protiprávní jednání, které má souvislost s počítači.[1] Jak už bylo řečeno, v dnešní době dochází ke stálému zdokonalování sítí ať už pro veřejnost, tak i pro státní orgány pro ulehčení jejich práce a propojení úřadů. Dále pak zdokonalování dnes už předmětů denní potřeby, zmíněných, chytrých telefonů, chytrých hodinek, chytrých domácích spotřebičů, které nám usnadňují život, ale mohou být pro nás i rizikem ve chvíli, kdy toho bude někdo chtít využít a uškodit nám. Proto nejdůležitější téma je i zabezpečení sítí a celkově "počítačů", proto jsem také začlenil rozhovor s bezpečnostním analytikem Martinem Kuncem, který se této problematice dlouhodobě věnuje a pracuje jako specialista síťových technologií, vývojář a analytik.

[1] MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. s. 3

# 1 Cíl a metodika bakalářské práce

Tato bakalářská práce je zaměřena na počítačovou kriminalitu, která je poměrně novým pojmem. Cílem této práce je objasnit problematiku, kterou tento druh kriminality přináší. Nejdříve se zaměřuje na vymezení základních pojmů jako nezbytně nutných znalostí k pochopení této problematiky. V pozdějších kapitolách budou rozebrány hlouběji některé druhy této kriminality a jejich pachatelé. V poslední části práce bude obsažen historický vývoj za posledních deset let.

Hlavním cílem bakalářské práce je objasnit základní pojmy jako počítač, kyberprostor, kybernetický útok a zejména pojem počítačová kriminalita. Dále objasnit příčiny této kriminality, analyzovat nejčastější nelegální konání proti počítačům nebo páchané na počítači nebo prostřednictvím počítače a zpracovat fenomenologii počítačové kriminality. Počítačová kriminalita je vzhledem ke svému stáří velmi rozmanitá a rozebírat podrobně všechny známé podoby této kriminality by bylo náročné a obsahově rozsáhlé. Vzhledem k této rozmanitosti nebude bakalářská práce obsahovat a analyzovat všechny známé typy, ale bude zaměřena jen na ty, které se aktuálně vyskytují nejčastěji. Pachatelé této kriminality usilují hlavně o zisk nebo zabezpečená data. Často bývají odborníky v oboru a může být náročné některé pachatele odhalit. Jiní můžou být zase obyčejní lidé, dokonce i děti, kteří si stáhli autorsky chráněné dílo, případně i nevědomě sdílí jeho obsah přes různé programy. V další části této práce, bude tedy obsažena analýza počítačové kriminality, která bude vycházet ze statistik Policie ČR.

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

Cílů této bakalářské práce bude dosaženo analýzou a vyhodnocením odborné literatury a důvěryhodných internetových zdrojů a statistik kriminality. Literatura o počítačové kriminalitě je snadno dostupná jak v anglickém, tak v českém jazyce a pro

účely této práce budou využity obě uvedené varianty. Dále bude proveden řízený rozhovor a vyhodnoceny informace tímto získané.

# 2 Počítačová kriminalita

Pod pojmem počítač lze rozumět souhrn technického (hardware) a programového (software) vybavení včetně dat, popřípadě jeho určitých komponentů, pokud je sama o sobě schopna jakýmkoli způsobem zpracovávat a sdílet informace. Definice podle Jirkovského: „*Počítačovou kriminalitou rozumíme takovou činnost, kterou je porušován zákon, nebo je v rozporu s morálními pravidly společnosti*“[2] Nebo si také lze počítačovou kriminalitu vyložit: „*Pod pojmem počítačová kriminalita chápeme nelegální nebo nemorální činnost zahrnující užití dat získaných prostřednictvím výpočetní techniky nebo změnu těchto dat*“ [3] Počítačová kriminalita je tedy mířena proti širokému spektru počítačů, nejen ve slova smyslu jak známe počítač, ale v dnešní době v důsledku technologického rozvoje se dnes počítač vyskytuje v mnoha podobách. Jedná se v podstatě o každé zařízení, které je schopno přijmout, zpracovat nebo sdílet data. Za počítač tak považujeme i chytré mobilní telefony, tablety, interaktivní elektronické doplňky, spotřební elektroniku, domácí vybavení, navigační přístroje a ostatní mobilní zařízení, která dokáží mezi sebou vzájemně datově komunikovat. Dochází k napadání jejich hardwaru, softwaru, ale také sítí, sociálním sítím, sítím bankovní sféry a webovým stránkám. V těchto činech tedy figuruje počítač jako nástroj pro páchání trestné činnosti.

Počítačovou kriminalitu můžeme chápat i jako prostředek pro kriminalitu obecnou, kdy počítače a sítě slouží jako nástroj pro páchání jiné trestné činnosti, např. šíření dětské pornografie. Vyšetřováním počítačové kriminality se v České republice zabývá Služba kriminální policie a vyšetřování (dále jen „SKPV“), odbory hospodářské kriminality.[4]

[2] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.*Praha, Grada Publishing, a.s., 2007. s. 19.
[3] SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku*. VŠERS, 2010. s. 123.
[4] ŠÁMAL, Pavel.Trestní zákoník: komentář.2. vyd. Praha: C.H. Beck, 2012., Velké komentáře. s. 9

Můžeme se setkat i s pojmem kybernetická kriminalita, nebo kyberkriminalita což vesměs je jedno, a je to samé jako počítačová kriminalita. Tato slovní spojení mají tedy stejný význam a není třeba v nich hledat rozdíl.

Definice kybernetické kriminality podle Václava Jirovského ve stejnojmenné publikaci definuje takto:*„Kybernetická kriminalita, označovaná v anglické literatuře mnohdy jako „IT crime" nebo „cybercrime" může velmi zjednodušeně řečeno, znamenat jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených. Oficiálních definicí počítačové kriminality existuje celá řada, avšak většina z nich vychází z podstaty uvedené výše. Podle materiálu OSN, který se zabývá počítačovou kriminalitou jsou jejím obsahem „Tradiční zločinné aktivity jako krádež, podvod nebo padělám, tedy činy trestné ve většině zemí na světě. Počítač rovněž tvoří prostředí pro nové činy spočívající ve zneužití počítačů, které jsou nebo by měly být ve své podstatě trestné. ". Ve stejném materiálu se UN snaží odlišit dva základní" případy - náhodné a neúmyslné použití počítače, které vede ke vzniku škody, a úmyslné použití počítače jako nástroje nebo předmětu kriminálního deliktu.“*[5]

Jeden z nejvyšších evropských orgánů, Rada Evropy, začala projevovat zájem o řešení problematiky počítačové kriminality již koncem osmdesátých let. Na základě studie vypracované v roce 1989 byla publikována doporučení pro úpravy a vytváření nových zákonů, které by měly kriminalizovat činy spáchané prostřednictvím počítačových sítí v doporučení RE (Rady Evropy) č. 9 z roku 1989 nebo informačními technologiemi v doporučení RE č. 13 z roku 1995. V roce 1997 byla ustavena Komise expertů na zločin v kyberprostoru (Commi-tee of Experts on Crime in Cyber-Space), která pracovala na návrhu mezinárodní dohody usnadňující mezinárodní spolupráci při odhalování počítačových zločinů.[6]

## 2.1 Společný znak počítačové kriminality

Obecně počítačovou kriminalitu tvoří velké množství trestných činů, které mají jeden společný znak, jak uvádí Šámal: „*Je jím nové sociálně interaktivní prostředí, jehož specifikum spočívá především v neexistenci časových a prostorových bariér,*

[5] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007., s.91
[6] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007., s.91

*mnohonásobné konektivitě, anonymitě a možnostech změny online-identity, což vytváří nové normy a zákonitosti závadného jednání, které jsou kvalitativně odlišitelné od jiných druhý kriminality.“*[7] Lze tedy počítačovou kriminalitu vymezit jako veškerou trestnou činnost, která v daném rozsahu souvisí s počítačovým a informačním systémem. Hlavním a společným znakem je online-identita, tedy pachatelé si myslí, že jednají anonymně a jejich pravou identitu nelze zjistit.

## 2.2 Počítačová kriminalita – jak a proč vznikla?

Co bylo důvodem vzniku počítačové kriminality?

Důvody vzniku přímo vyplývají z historického vývoje. Například prapůvod průniku do systému je ve zcela legitimní snaze odstranit jeho chyby a optimalizovat ho pro co možná nejefektivnější využití později, s masovým využitím počítačů, ale především s rozvojem jejich propojováni do rozsáhlých síti typu Internet, spolu se vzrůstající potřebou komerčních subjektů se k takovým sítím připojovat, začalo být pro pachatele zajímavé používat k nelegálním průnikům do systému za účelem krádeže dat nebo elektronických loupeži na bankovních účtech počítače. Literatura většinou uvádí jako základní kriminogenní faktory, které mají vztah k počítačové kriminalitě, případně ji usnadňují následující:

**1. Složitost informačních technologií** a jejich provozu je pro značnou část uživatelů neproniknutelná. Z toho pramení vnímání světa počítačů jako čehosi neuchopitelného a již od základu podezřelého.

**2. Důvěra** uživatelů ve výstupy z informačních technologií; klasicky se zde uvádí skutečnost, že málokoho napadne kontrolovat například účet připravený počítačovým systémem v supermarketu, či ověřovat správnost výpočtů provedených počítačem v rámci firemního účetnictví. V důsledku toho může zůstat dlouho neodhalen pachatel počítačového podvodu či zpronevěry, který si z finančních toků procházejících systémem pravidelně odečítá mikroskopické částky pro vlastní obohacení apod.

**3. Objem dat** v prostředí, kde se pachatelé pohybují je často enormní. Je technicky neproveditelné efektivně kontrolovat veškerá data procházející třeba sítí Internet.

[7] ŠÁMAL, Pavel. *Trestní zákoník: komentář.2*. vyd. Praha: C.H. Beck, 2012., Velké komentáře. s. 10

**4.** Páchání trestné činnosti **od obrazovky počítače** je neporovnatelně **snazší** než je tomu v reálném životě. Řečeno s nadsázkou, vyloupit banku několika stisky klávesy Enter je mnohem jednodušší než si obléknout neprůstřelnou vestu, kuklu, opatřit zbraň a vydat se do akce. Zřejmě by bylo možné namítnout, že elektronická cesta je náročnější na znalosti, nicméně i pro klasickou loupež je třeba znát prostředí v bance, bezpečnostní systém objektu, vědět, jaký čas je třeba pro loupež zvolit apod., Čili lze říci, že se požadované znalosti liší pouze svým obsahem, ale ve všech ostatních aspektech je elektronická cesta snazší.

**5.** Obecně **nízké právní vědomí** populace, které se projevuje v jiných oblastech práva, je v případě informačních technologií ještě nižší. Tento stav je nicméně zcela pochopitelný, normy, a to jak z oblasti veřejného, tak soukromého práva, které se týkají oblasti IT, jsou často velmi složité. Navíc pro mnoho běžných občanů je obtížné si pod slovy například takového zákona o elektronickém podpisu cokoli představit, natož si utvořit ucelenou představu o tom, co a jak je v něm upraveno.

**6**. **Nedokonalost legislativy**. Právní normy upravující oblast IT jsou mnohdy obtížně vyložitelné a jejich mezerovitost je značná. Samozřejmě, vzhledem k dynamickému vývoji v dané oblasti tomu jinak ani být nemůže, protože ucelená soustava právních norem se nemůže vytvořit, dokud nedojde ke konsolidaci dotyčného odvětví, což v případě IT zatím nenastává.[8]

Dále existují ještě specifické kriminogenní faktory pro jednotlivé typy počítačové kriminality:

**Protiprávní jednání proti počítači**

Co se týče činů zde uvedených pod bodem 2, a to zejména tam, kde jsou nebo byly páchány tzv. novými pachateli, je nutno vzít v úvahu jednu podstatnou skutečnost. Vznik počítačové kriminality v těchto případech má úzkou *spojitost s undergroundem*, alternativní kulturou. Tak tedy podle filozofie hackerů, tak jak ji zachytil ve své knize Zátah na hackery - Řád a chaos v elektronickém pohraničí americký publicista Bruce Sterling, například: *„Technická moc a speciální vědomosti jakéhokoli získatelného druhu patří plným právem do rukou těch lidi, jež jsou natolik odvážní a odhodlaní, aby si je opatřili – všemi dostupnými prostředky. Nástroje, zákony nebo systémy, které brání*

[8] MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. s. 8-9

*volnému přístupu a šíření vědomostí, jsou provokacemi. jež by měl každý svobodný a sebevědomý hacker neúnavně ničit. „Soukromí" vlád, obchodních společností a jiných bezduchých technokratických organizaci nesmí být chráněno ke škodě svobody a neomezené iniciativy individuální techno-krysy. Jenže v našem současném prozaickém světě si jak vlády, tak obchodní společnosti dávají velice záležet na restrikci informací, které jsou tajné, obchodním tajemství pro vnitřní potřebu, důvěrné, copyrightované, patentované, nebezpečné, nelegální, neetické, poškozující pověst či jinak citlivé."*[9]

Sterling se ve své knize dostává k velmi zajímavým závěrům a vznik počítačové kriminality probírá z mnoha různých úhlů. Pro hackery je podle něj často prvotním motivem touha po informacích, které jsou jim vládnoucím establishmentem, jenž je pouhou loutkou mamutích korporací, upírány, a to zcela bezdůvodně, nesprávně, a snad dokonce zločinně.

# 3 Kyberprostor

‚Když v roce 1968 došlo k prvnímu síťovému propojení mezi čtyřmi univerzitními počítači a ke vzniku zárodku sítě ARPANET.[10]**ARPANET Advanced Research Projects Agency NETwork** byla počítačová síť spuštěná v roce 1969, která byla zárodkem toho, co dnes chápeme jako Internet. Nikdo nepředpokládal obrovský rozvoj síťových technologií propojujících miliony uzlů. V době návrhu dnes nejrozšířenějšího protokolu TCP / IP nepředpokládali jeho tvůrci tak obrovský rozmach internetu, a tak na bezpečnostní charakteristiky sítí a protokolů nebyl kladen takový důraz jako dnes. Nicméně technologie pokročily dopředu rychleji, než bylo očekáváno a slabiny těchto technologií se staly cílem nelegálních aktivit čekajících v počítačových sítích.

Abychom pochopili současný vztah společnosti a technologií, je třeba si uvědomit, že rychlost, se kterou se rozvíjely počítačové a komunikační technologie, byla mimo veškeré běžné praktiky a společnost, zvyklá na relativně pomalý technický rozvoj, reagovala se zpožděním. Výpočetní technika a telekomunikace absolvovaly devadesát

[9] MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002., s. 9
[10] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007., s.15

procent své historie během druhé poloviny minulého století, a tak při tomto překotném vývoji není divu, že lidská společnost, která představovala zvyky, morálku a etiku do podoby zákonů a pravidel po staletí, začala za postupem technologií zaostávat.[11]

## 3.1 Internet

Internet je celosvětová počítačová síť navzájem propojených počítačů, lze ho také definovat jako *„síť sítí“*, kde mezi sebou počítače komunikují. Slouží také jako komunikační a informační médium, umožňující miliónům lidí na celém světě být v neustálém kontaktu v reálném čase. Každý den zde najdeme nejaktuálnější informace a množství různých služeb.

Nikdo nemůže zpochybnit, že Internet se stal jedním z nejvýraznějších fenoménů přelomu druhého a třetího tisíciletí a že jeho role v dějinách lidstva bude s největší pravděpodobností stejně významná jako role Guttenbergova knihtisku nebo Wattova parního stroje. Významnou je ale i skutečnost, že Internetu - na rozdíl od většiny významných technologických milníků lidstva- již nemůžeme přiřadit jeho autora (vynálezce, majitele práv) v podobě konkrétní osoby XY nebo definovatelné skupiny osob. Aniž bych chtěl zabíhat do detailů ohledně vzniku, budování a současného stavu Internetu, je třeba konstatovat, že Internet můžeme a musíme chápat skutečně jako „Síť“ neboli „síť sítí". Technicky je to tedy soustava serverů, komunikací a k nim připojených počítačů, organizačně jsou to provozovatelé jednotlivých sítí a podsítí, směrovačů a páteřních propojek, zprostředkovatelé připojení (provideři), uživatelé apod. Tento prostředek jako celek nemá svého majitele; majitele bychom pravděpodobně dokázali nejednoduchou cestou najít pro jednotlivé kousky sítí a servery, ovšem nenajdeme žádnou právnickou ani fyzickou osobu, která by byla naším partnerem za Internet jakožto takový; z toho vyplývá jeho neuchopitelnost jako celku a obtížnost „vejít se" do obvyklého právního řádu. Prvotně byla Internetu věnována pozornost především z

[11] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007., s.15

hlediska jeho technické a programátorské stránky nebo jako uživatelsky atraktivnímu, multi-informačnímu, zcela volně přístupnému médiu.[12]

Pozdější úvahy byly směřovány futurologicky a filozoficky. Podstatnou náležitostí, aby Internet překročil práh mezi trávením volného času směrem k profesionalitě a masovějšímu komerčnímu využívání, je vyřešení dvou základních problémů:

**l. právních otázek;**

**2. otázek bezpečnosti a spolehlivosti.**

Právní stránka byla doposud zmiňována spíše okrajově, obvykle v souvislosti s některou vysoce medializovanou otázkou, jakou bývá v pravidelných intervalech výroba výbušnin nebo dětská pornografie. Přitom z hlediska celkového objemu a globálního dosahu Internetu jde o zcela okrajové, byť z hlediska kriminální prevence důležité, otázky. V souvislosti s provozováním Internetu vzniká ovšem řada dalších, podstatnějších právních problémů, dotýkajících se přímo jeho podstaty a existence.[13]

Řekněme si tedy z předchozího vyplývající kacířskou či provokativní myšlenku, že Internet jako takový právně neexistuje. Přesně řečeno, nemůže nabývat práv ani se zavazovat. Internet jako takový není subjektem práva nemá právní subjektivitu. Tuto subjektivitu mohou mít v mezích stanovených právním systémem lidé, právnické osoby (sdružení fyzických nebo právnických osob, účelová sdružení majetku jednotky územní samosprávy, jiné subjekty, o kterých to stanoví zákon). I když částí Internetu je kromě věcí také mnoho osob (Internet Society a další uživatelé), jako celek není a - jak z předchozího vyplývá - ani nemůže být subjektem práva. Internet není ani ryze hmotným předmětem, tedy věcí, jak je chápána v základních právních normách. Není ani čistě nehmotným statkem, tj. právem nebo jinou majetkovou hodnotou - např. informací. A konečně není ani objektivní právní skutečností, nezávislou na lidském chování.

Jedná se o složitý iformační systém, který se skládá ze všech výše uvedených komponent, tj. z různých subjektů práva: lidí a organizovaných sdružení lidí (právnických osob) včetně států, dále z majetku, tj. věcí práv a jiných majetkových hodnot. Problém je, že na rozdíl od běžných automatizovaných informačních systémů netvoří technické a

[12] SMEJKAL, Vladimír. *Internet a §§§*. Praha: Grada, 2001. s. 16-17
[13] SMEJKAL, Vladimír. *Internet a §§§*. Praha: Grada, 2001. s. 17

programové prvky a určitou společenskou celistvost, tj. instituci, která může být subjektem práva. Pokud se tedy na internet díváme očima práva, musí být náš pohled krajně nedůvěřivý. Existuje TO (nepochybně), funguje TO (jak kdy, ale občas ano), točí se okolo TOHO obrovský peníze (a hlavně všichni doufají, že se točit budou) a přitom TO jako celek nikomu nepatří.[14]

Jak již bylo uvedeno, tak kyberprostor či internet neznají hranic. Tedy, co se týká hranic mezi státy, jak je chápeme jako občané toho či onoho státu. Samozřejmě, že i internet své hranice má, neboť jen těžko může být dostupný na izolovaném počítači, tedy tam, kde není připojen síťový kabel, nebo není v dosahu žádná Wi-Fi, mobilní či jiná síť a ani žádný satelit do daného zařízení internet nepřenáší. Proto je novým druhem interkulturní komunikace, kde geografická lokace nemá prakticky žádný význam. Přesto se však stává, že i tato lokace má na přístup k datům vliv. Některé stránky či provozovatelé webů filtrují veřejné IP adresy, tedy adresy, které jsou počítačům propůjčeny, aby se mohly k internetu připojit, a určité uživatele nežádoucích států na své stránky nepouští. Avšak toto je zřejmě zásah do principu internetu, tedy toho, že internet nemá hranice a jednou publikovaný materiál by měl být dosažitelný odkudkoli bez výjimky. V některých zemích by tato „filtrace“ či vlastně diskriminace mohla narážet na národní právní předpisy, které v těchto zemích IP adresu považují za „osobní údaj“, na který se vztahují příslušné zákony o ochraně osobních údajů, a proto by neměla být daná omezení aplikována na základě takto nezákonně získaných informacích. Jiná věc je případná cenzura státu, který může obsah internetu pro své občany a na svém území filtrovat.[15]

**IP adresa** je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol. IP adresa slouží k rozlišení síťových rozhraní připojených k počítačové síti. Zkratka IP znamená Internet Protocol, což je protokol, pomocí kterého spolu komunikují všechna zařízení v Internetu. V současné době je nejrozšířenější IPv4, která používá 32bitové IP adresy, které jsou zapisovány dekadicky po jednotlivých oktetech (tj. po osmicích bitů), například 192.168.0.2. Z důvodu

[14] SMEJKAL, Vladimír. *Internet a §§§*. Praha: Grada, 2001. s. 17-18
[15] ROSENZWEIG, Paul. *Cyber warfare: how conflicts in cyberspace are challenging America and changing the world*. Santa Barbara, Calif.: Praeger, c2013. s. 201-210

nedostatku adres je IPv4 postupně nahrazován protokolem IPv6, který používá 128bitové IP adresy zapsané hexadecimálně, například 2001:db8:0:1234:0:567:8:1.16

### 3.1.1 Internet v ČR

V Československu se internet objevuje po pádu komunismu v roce 1989. V květnu roku 1990 se k nám dostává síť EUNET. V říjnu téhož roku se k nám dostává také evropská síť EARN, která je odnoží evropské sítě Bitnet. K oficiálnímu připojení Československa k internetu došlo v listopadu roku 1991. Formální připojení ČSFR k internetu se uskutečnilo slavnostně 13. února 1992. Internet byl tehdy dostupný v Praze na ČVUT, ale o připojení měly zájem i ostatní vysoké školy ČSFR.[17]

Před rokem 1995 měl v naší zemi ponětí o existenci internetu jen málokdo. Na přelomu let 1995 a 1996 se však tato situace mění, protože na trh vstupuje celá řada subjektů, které poskytují připojení k internetu. Do této doby zabraňoval rozvoji komerčních poskytovatelů monopol společnosti Eurotel (Český Telecom, dnešní O2), který se vztahoval mimo jiné i na veřejné služby přenosu dat. Tím, že tento monopol na sklonku roku 1995 skončil, otevřel se prostor pro komerční využití internetu a s tím spojený jeho rozmach.[18]

# 4 Formy počítačové kriminality

Používání informačních technologií a jejich adaptace do běžného života společnosti odhaluje velké množství způsobů, jakými mohou počítače a jiná elektronická zařízení figurovat v páchání trestné činnosti. Proto je mimo prostého dělení dle konkrétních skutkových podstat trestných činů zapotřebí počítač jako prostředek zařadit do několika kategorií, které se vzájemně odlišují objekty a subjekty, na něž konkrétní závadné jednání dopadá. Nejvýznamnější místo v tomto směru prozatím zaujímá Úmluva.

[16] IP adresa – Wikipedie. [online]. Copyright © 2020 [5.4.2020]. Dostupné z: https://cs.wikipedia.org/wiki/IP_adresa
[17] PEKÁREK, O., ČÍŽEK, V. Práce s agenturními a elektronickými informacemi. České Budějovice, 2007., s. 8.
[18] HULANOVÁ, L. Internetová kriminalita páchaná na dětech. Praha, 2012. s. 17.

Ta je ve svém přístupu k problematice nejkomplexnější. Pokud jde o definiční členění trestných činů, které mají být členskými státy Úmluvy kriminalizovány, pak tato stanoví následující znaky:

Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů

a. neoprávněný přístup
b. neoprávněné zachycení informací
c. zásah do dat
d. zásah do systému
e. zneužití zařízení

2) Trestné činy související s počítači

a. falšování údajů souvisejících s počítači
b. podvod související s počítači

3) Trestné činy související s obsahem, zejména s dětskou pornografií

4) Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.[19]

Je nutné poznamenat, že tento výčet v sobě zahrnuje pouze ta jednání, v nichž počítač vystupuje jako přímý či nepřímý prostředek páchání trestné činnosti. Zcela logicky sem nespadají jednání, při kterých sice bylo využito počítače nebo jemu podobných zařízení, avšak tato nebyla pro dokonání trestného činu nezbytná, nicméně přispěla určitou měrou k zefektivnění a ulehčení postupu pachatelů. V této souvislosti se autor Samuel C. McQuade pokusil o jiné dělení:

1) Zločin s využitím počítače–jedná se o protiprávní jednání, pro jehož spáchání byl užitečný jeden nebo více počítačů, avšak tyto počítače nebyly pro dokonání nezbytné (např. porušení obchodního tajemství pracovníkem veřejné správy, při kterém se zmocnil elektronických kopií chráněných dokumentů).

[19] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. V Praze: C.H. Beck, 2012., s. 2305

2) Počítačový zločin –pod tímto pojmem si lze představit protiprávní jednání, pro jehož spáchání a dokonání bylo zapotřebí použít jednoho nebo více počítačů (např. prolomení bezpečnostních kódů k přístupu do prostor vládního zařízení).

3) Zneužití počítače –použití počítače takovým způsobem, který je schopen přivodit újmu jednotlivci, skupině či organizaci, a který může současně narušovat zavedená pravidla nebo procedury. Při zneužití počítače nicméně nemusí nastat taková míra společenské škodlivosti, která by vedla k porušení trestních předpisů (např. porušení interních počítačových směrnic společnosti zaměstnancem nebo kopírování know-how).

4) Počítač jako nástroj deviace–tím je myšleno takové chování, které využívá počítačová nebo telekomunikační zařízení jako nástroj k porušování sociálních norem, mnohdy až s trestněprávním přesahem (např. šíření dětské pornografie, on-line stalking apod.).[20]

Tyto kategorie jsou následně konkretizovány do skupin, které mají zásadně negativní dopad na společnost a které jsou si typově podobné. Těmito skupinami jsou (1) neopatrné užívání informačních systémů, (2) běžné zločiny spáchané s pomocí počítačů a jiných elektronických zařízení, (3) on-line podvody, (4) získávání neoprávněného přístupu, (5) tvorba a distribuce škodlivého počítačového kódu, (6) digitální pirátství (7) on-line šikana, (8) on-line stalking a obtěžování, (9) podvody na akademické a vědecké půdě, (10) organizovaný zločin, (11) vládní a průmyslová špionáž a (12) kyberterorismus.[21]

Je zřejmé, že takovéto členění je velmi všeobecné a do značné míry nezohledňuje trestněprávní rovinu problematiky, pouze nahlíží na počítačová zařízení jako na nástroj, který je schopen při určitém způsobu zacházení narušovat i nezávazné normy společenského chování. Tato problematika je dále definována a podrobněji rozpracována v dalších podkapitolách.

[20] McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. s. 43
[21] McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. s. 44

## 4.1 Hacking

Hacking v původním pojetí lze obtížně označit za trestný čin, neboť nelze vyčíslit škodu, která tímto jednáním byla způsobena. Někdy ani správce systému netuší, že mu hacker do systému pronikl. Motivací prvních hackerů nebylo způsobit někomu škodu, ale pouze zvítězit nad technikou a získat obdiv ostatních hackerů. Zjednodušeně lze hacking definovat jako proniknutí do počítačového nebo řídícího systému jinou než standardní cestou s tím, že se obejde nebo prolomí jeho bezpečnostní ochrana.[22]

Hackeři vždy provádějí před pokusem o jakýkoliv manipulační útok průzkum. Tím získávají informace o jakémkoliv subjektu, který chtějí při své činnosti zneužít. Čím více informací mají, tím spíš jsou při své činnosti úspěšní.[23]

Lidé, kteří hackování používají k činům nelegálním, většinou se infiltrují do systémů kvůli vlastnímu obohacení nebo za účelem poškození systému, se nazývají pojmem cracker anglicky black hats. Proti těmto hackerským útočníkům pomáhají etičtí hackeři zabezpečovat systémy. Na rozdíl od etického hackera cracker využívá své schopnosti ke kriminálním účelům. Některé crackovací metody stojí čistě na matematických principech, takže cracker musí mít matematické znalosti. V jiných případech crackerovi stačí, když zná hardwarové registry, to je systém pro ukládání klíčů a hesel v operačním systému windows.[24]

Toto téma je zmíněno v rozhovoru, kde je popsáno podrobněji.

## 4.2 Cracking

S trestnou činností označovanou jako hacking a warez je neoddělitelně spjata další společensky nebezpečná činnost označovaná jako cracking. Jde o prolamování nebo obcházení ochranných prvků elektronických nebo programových produktů za účelem jejich neoprávněného použití. Cracking používá celou řadu metod počínaje prostým debutováním spuštěného programu a konče tzv. reverse engineering. Cracking je často

[22] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007. s 102.
[23] HATCH, B., LEE, J., KURTZ, G. *Linux hackerské útoky. Bezpečnost Linuxu – tajemství a řešení*. Praha, 2002. s. 171.
[24] CRAIG, Paul P a Ron HONICK.*Softwarové pirátství bez záhad.* 1. vyd. Praha: Grada, 2008. s. 56.

používaná metoda při průniku do systému, přičemž jeho cílem není zprovoznit program chráněný softwarovým nebo hardwarovým klíčem, ale zjistit informace důležité pro umožnění neoprávněného přístupu do cílového systému. Nejčastějším typem je tzv. „password cracking“, tj. zjišťování hesla pro přístup do systému. Password cracking zahrnuje mnoho metod, počínaje snahou uhodnout heslo pomocí slovníku nejčastěji používaných hesel, použitím hrubé síly při zkoušení všech možných kombinací znaků, které mohou přicházet v úvahu, až po sofistikované algoritmy, které se snaží o zpětnou rekonstrukci kombinace znaků.

Z hlediska trestního práva může být tato trestná činnost kvalifikována různým způsobem. Případ, kdy tomu, kdo je vlastníkem systému, vůči němuž byl útok crackingem prováděn, nevznikla prokazatelná škoda, nemusí být vůbec jako trestný čin hodnocen.[25] V ostatních případech může jít o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ[26] nebo poškození záznamu v počítačovém sytému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ.[27]

## 4.3 Warez

Moderní počítačové pirátství, které je doprovodným jevem používání informačních technologií a rozšiřuje se s rozmachem internetu, je většinou skupinovou záležitostí. Jedna část pachatelů pracuje na prolamování ochranných prvků programových produktů, kdežto druhá část se specializuje na jejich šíření pomocí www serverů a získávání financí na jejich provoz tím, že umisťuje reklamu na pornografické servery nebo servery, které mají erotický obsah. Tato reklama obvykle nezkušeného uživatele zahltí přívalem samovolně se otevírajících oken, aniž by se dostal k tomu, co hledal.

Warez jsou spíše jakýmsi pozůstatkem minulosti. Dnes jsou používány pro šíření tzv. cracků, to znamená programů umožňujících zrušení ochrany u programových

[25] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007. s. 106.
[26],[27] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 8.2.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

produktů, jejichž plné verze lze stáhnout z internetových stránek dodavatele nebo je získat z reklamních CD, avšak jen na omezenou dobu.[28]

Daleko rozšířenější jsou dnes ale programy pro sítě peer-to-peer, které představují jednoduchý způsob, jak sdílet soubory. Lze je též dobře využít pro stahování hudby, filmů nebo programů.[29]

Matějka **warez** přeneseně označuje jako moderní počítačové pirátství. Dle jeho i dle mého názoru se pak jedná o problém, který se neustále rozrůstá a nedaří se jej potlačovat. V podstatě se jedná o obstarávání pirátských kopií hudby, filmů, software a dalšího. Konkrétně se pak může jednat i o pornografii, počítačové hry atp. Dokonce může nastat i situace, že konkrétní film či hudební soubory jsou pomocí warez poskytovány uživatelům ještě dříve, než dojde k jejich oficiálnímu uvolnění. Matějka dále uvádí, že tato činnost je většinou organizována ve skupinách, kde jednotliví členové mohou mít dále rozděleny úlohy (někdo z nich získává „materiál" a prolamuje různá bezpečnostní opatření, další z nich spravuje internetové stránky, na nichž jsou soubory (či odkazy na ně) umístěny apod.[30]

Postihnout nelegální obsah šíření v síti peer-to-peer je samozřejmě daleko složitější, než když je k šíření použit server warez. Z pohledu trestního práva je vyhodnocení takovéhoto jednání jednoznačné. Jde o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ.[31]

## 4.4 Phishing

Phishing je podvodný způsob, jak prostřednictvím internetu získat citlivé údaje (hesla, čísla kreditních karet, apod.). Jedná se o rozesílání e-mailových zpráv nebo instant messaging*), které nabádají adresáta k zadání jeho osobních údajů na falešnou webovou stránku. Ta bývá téměř totožná s tou oficiální. Často zneužívána bývají zejména

[28] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007., s. 105–106.
[29] Bezpečný internet | Sítě peer-to-peer. *Bezpečný internet | Rady pro bezpečnost na internetu* [online]. Copyright © [cit. 08.02.2020]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/site-peer-to-peer.aspx
[30] MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002. s. 70
[31] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 8.2.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

přihlašovací okénka internetového bankovnictví. Uživatel v dobrém úmyslu do okénka zadá své přihlašovací údaje (jméno a heslo) a tím nevědomky poskytne své údaje útočníkům, kteří následně z jeho účtu vykrádají peníze. Dále se může jednat například o zasílání různých zpráv o výhrách v loterii, nebo vydírání poškozených formou tzv. „ransomware“, kdy virus zablokuje osobní počítač a za odblokování požaduje finanční obnos.[32]

K získání těchto důvěrných informací pachatelé využívají podvodné e-maily, které vyvolávají dojem, že jsou odeslány přímo z banky, a které se snaží přesvědčit uživatele, aby kliknul na určitý odkaz. Jestliže neopatrný uživatel na tento falešný odkaz klikne, dostane se na podvodné stránky, kde je po něm požadováno, aby sdělil své přístupové údaje k účtům, platebním kartám nebo jiné důvěrné informace. Pokud je uživatel naivně sdělí, poskytne je podvodníkům, kteří je následně využijí ve svůj prospěch.[33]

## 4.5 Hoax

Jedná se o jedno z nejrozšířenějších rizikových chování tzv. **hoax** (v překladu z angličtiny „podfuk“), při němž dochází k šíření poplašných nebo smyšlených zpráv, které mají za následek vyvolat paniku, strach, pobouření, manipulovat s názory lidí, nebo poškodit instituci, firmu, značku, výrobek. Hoax se může šířit hromadným rozesíláním emailů, prostřednictvím sociálních sítí. Mezi nejčastější typy hoaxů patří *varování* před smyšlenými viry a různými útoky na počítač, popis nereálného nebezpečí, falešné prosby o pomoc, petice, výzvy, pyramidové hry a nabídky snadného výdělku, řetězové dopisy štěstí, žertovné zprávy, podvodné loterie aj.[34]

Pokud takto šířená zpráva způsobí, že na jejím základě vznikne znepokojení mezi větším počtem lidí, naplňuje skutkovou podstatu trestného činu šíření poplašné zprávy dle § 357 TZ.[35]

---

[32] Počítačová kriminalita - Policie České republiky. *Úvodní strana - Policie České republiky* [online]. Copyright © 2019 Policie ČR, všechna práva vyhrazena [cit. 30.01.2020]. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

[33] HOAX | Phishing | *Co je to phishing*. [online]. [cit. 30.01. 2020] Dostupné z: WWW https://www.hoax.cz/phishing/co-je-to-phishing

[34] ČECH, Ondřej a Nicole ZVONÍČKOVÁ. *Nebezpečí kyberšikany: internet jako zbraň?*. České Budějovice: Theia - krizové centrum, 2017. s. 35.

[35] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

## 4.6 Počítačové pirátství

Ve vztahu k internetovému pirátství je třeba nejprve vymezit problematiku Práva duševního vlastnictví, zejména pak práva autorského. Toto vymezení je nezbytné pro pochopení rozdílu mezi legálním a protiprávním jednání osob, které jsou na Internetu činné.[36]

Právo duševního vlastnictví představuje majetek nehmotné povahy, tzv., „nehmotné statky", které jsou **výsledkem tvůrčí činnosti člověka.** Toto právo je **nezávislé na hmotném substrátu** (může být proto užíváno kdykoliv a kdekoliv na světě) za podmínky, že je jedinečné, neopakovatelné a dostatečně originální. [37]

**Právo duševního vlastnictví je možné rozdělit do dvou oblastí:**

1) Autorská práva (chrání např. původní literární a umělecká díla, hudební skladby, televizní vysílání, počítačové programy, databáze, reklamní výtvory, multimédia aj.)

2) Průmyslová práva (chrání např. patenty na vynálezy, vzory, průmyslové modely, ochranné známky, zeměpisný původ aj.) Z hlediska zaměření této monografie se dále budu primárně zabývat pouze právem autorským a zásahům do tohoto práva.

Ochrana autorských děl je realizovatelná v rámci občanskoprávního řízení, a to různými druhy právních nástrojů, jako jsou žaloby určovací (kdo je autorem), zdržovací (zákaz šíření či užívání), odstraňovací (zničení neoprávněně vyrobených kopií programů), na náhradu škody, na přiměřené zadostiučinění, atd.[38]

Právo na náhradu škody a na vydání bezdůvodného obohacení podle zvláštních právních předpisů zůstává nedotčeno; podle nového Autorského zákona, zákon číslo 121/2000 Sb.[39] Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů ve znění pozdějších předpisů (dále jen „autorský zákoník“ nebo „AZ“), výše bezdůvodného obohacení vzniklého na straně toho, kdo neoprávněně

[36],[36] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 277.

[38] SMEJKAL, Vladimír. *Internet a §§§*. Praha: 2. aktualizované a rozšířené vydání, Grada, 2001. s. 80
[39] Zákony pro lidi. *Zákon č. 121/2000 Sb*. Autorský zákon. © AION CS, s.r.o. 2010-2020 [cit. 22.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121

nakládal s dílem, aniž by k tomu získal potřebnou licenci, činí dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného nakládání s dílem. Je zde tedy vysloveně určena částka, kterou je možné žalovat. Nový autorský zákon reflektuje i technologické změny, podle kterých do práva autorského neoprávněně též zasahuje ten, kdo vyvíjí, vyrábí, nabízí k prodeji, pronájmu nebo půjčení, dováží, rozšiřuje nebo využívá pro dosažení majetkového prospěchu poskytováním služeb nebo jiným způsobem pomůcky zamýšlené k odstranění, vyřazení z provozu nebo omezení funkčnosti technických zařízení nebo jiných prostředků k ochraně práv. Přitom za jiné prostředky se považují jakýkoli postup, výrobek nebo součástka vložené do postupu, přístroje nebo výrobku, jež mají předcházet, omezit nebo zabránit neoprávněnému zásahu do práva autorského k dílu, které je zpřístupňováno jen s použitím kódu nebo jiným způsobem umožňujícím odkódování.

Toto je zakotveno v § 43 AZ[40]. Rovněž je postihováno jednání spočívající v tom, že pachatel a) odstraní nebo změní jakékoli elektronické informace o identifikaci práv k dílu, b) bude rozšiřovat rozmnoženiny díla včetně jejich dovozu, jakož i sdělování díla veřejnosti, u nichž byly elektronické informace o identifikaci práv k dílu odstraněny nebo pozměněny, bez svolení autora.[41]

## 4.7 Kyberšikana

S nástupem a rozvojem moderních technologií a s ohledem na jejich snadnou přístupnost a každodenní využívání se v dnešní době více než kdy dříve zvyšuje pravděpodobnost, že uživatelé v kyberprostoru přijdou do styku s kyberšikanou. Stejně jako v reálném životě, i ve virtuálním světě by měla být dodržována určitá pravidla, bez kterých hrozí ohrožení uživatele, a to někdy až velmi vážným způsobem. Pachatelům trestné činnosti (agresorům) navíc vše usnadňuje vysoká míra anonymity, která se k pobytu v kyberprostoru váže. Není pro ně nijak těžké vydávat se za přítele, tím získat důvěru běžného uživatele a dostat ho do nepříjemné situace.[42]

[40] Zákony pro lidi. *Zákon č. 121/2000 Sb*. Autorský zákon. © AION CS, s.r.o. 2010-2020., [cit. 22.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121
[41] SMEJKAL, Vladimír. *Internet a §§§*. Praha: 2. aktualizované a rozšířené vydání, Grada, 2001. s. 81-82
[42] ROGERS, Vanessa. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty*. Praha: Portál, 2011. s. 34.

Může se projevovat různými způsoby a ze začátku může působit nenápadně a neškodně. Může se jednat o komentáře u fotografií, které člověka zarazí, ale může pokračovat až zveřejňováním ponižujících fotografií nebo osobních informací, které uživatele mohou přivézt do velmi nepříjemné situace. Tyto osobní fotografie nebo informace se pak prostřednictvím sociálních sítí šíří neskutečnou rychlostí a mohou pak silně negativně ovlivnit veškerý společenský i osobní život.[43]

### 4.7.1 Definice kyberšikany

Jedná se o zvláštní druh šikany, kdy se agresor snaží ublížit psychickým nátlakem a týráním své oběti prostřednictvím internetu a informačních technologií. Dochází při ní k vážnému ohrožení psychického zdraví, které může mít trvalé psychické následky. Nejčastějšími nástroji kyberšikany jsou zprávy SMS, MMS, opakované telefonní hovory online interaktivní hry, webové stránky, blogy, elektronická pošta (e-maily), internetové ankety, dotazníky a sociální sítě jako je Facebook, Instagram nebo Twitter.

Cíle zůstávají stejné jako u klasické šikany, a to ublížení, zesměšnění a ponížení oběti. Kyberšikana v mnoha případech začíná jako klasická šikana a někdy se její projevy prolínají a doplňují. Mezi klasickou šikanou a kyberšikanou jsou ale zásadní rozdíly, které znesnadňují její rozpoznání a zásah proti ní: *„anonymita, nezávislost na místě a čase, technická zdatnost dětí a absence fyzické konfrontace.“*[44]

## 4.8 Druhy kyberšikany

### 4.8.1 Kyberstalking

Je hlavní možností ohrožení v kyberprostoru a zejména na sociálních sítích. Jedná se o sledování všech jeho aktivit a neustálé obtěžování uživatele, které může vyústit až ve vyhrožování. Agresor (stalker) je většinou osoba, která je nebo byla oběti blízká (partner, kamarád) a z nějakého důvodu není schopná akceptovat ukončení vztahu (milostného, přátelského). Stalkeři také umí své počínání velmi dobře skrývat, na ostatní

[43] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013., Psyché (Grada). s. 28.
[44] ČECH, Ondřej a Nicole ZVONÍČKOVÁ. *Nebezpečí kyberšikany: internet jako zbraň?*. České Budějovice: Theia - krizové centrum, 2017. s. 35.

působí velmi sympaticky a mile, a bývá proto někdy velmi těžké tohoto agresora odhalit, nebo vůbec uvěřit, že zrovna tento člověk může být pachatelem.[45]

Pokud se kyberstalking nechá zajít příliš daleko, může mít opravdu děsivé následky, dochází k absolutní ztrátě soukromí, ztrátě pocitu bezpečí a každodenní nejistotě a strachu. Oběť kyberstalkingu pak začne selhávat i v běžných věcech a kvalita života je tím velmi omezena. Při řešení podobné situace je ze všeho nejdůležitější rozvázat veškeré kontakty s agresorem, nepodněcovat ho k hovoru, nediskutovat s ním, měnit trasu do školy/ práce nebo pokud možno mít doprovod, ale hlavně je třeba si shromažďovat veškerý materiál, který by později mohl sloužit jako důkaz agresorova počínání (kopie konverzací a výhružným e-mailů, vzkazy, výpisy hovorů atd.).[46]

Kyberstalking, je od 1. 1. 2010 klasifikován jako trestný čin. Je zakotven v trestním zákoníku, konkrétně v **§ 354 Nebezpečné pronásledování**, odst. 1. písm. c) *„vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje‘‘*. Trestní sazba se pohybuje od odnětí svobody na půl roku až na tři léta.[47]

### 4.8.2 Kybergrooming

Jde o velmi nebezpečnou praktikou v oblasti kyberšikany. Jedná se o takové chování, kdy agresor manipuluje s nic netušící obětí, snaží se získat její důvěru a dostat se do úzkého okruhu jejích blízkých. Poté, co se mu to povede, snaží se oběť vylákat na osobní schůzku, kde jí nějakým způsobem zneužije (krádež, fyzické napadení, sexuální zneužití atd.).[48]

Samotný kybergrooming má několik fází. V první fázi si agresor vybírá oběť podle veřejně viditelných informací. Ve druhé fázi navazuje s obětí kontakt, snaží se sblížit a navodit pocit důvěry. V další fázi se snaží získat od oběti kompromitující materiál

[45] ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013. s. 67.
[46] BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014. s. 14-15.

[47] 40/2009 Sb. Trestní zákoník. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © [cit. 08.02.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[48] KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci, 2015. s. 25.

(fotografie, informace), na základě kterého pak může vyžadovat osobní schůzku, což je fáze čtvrtá.[49]

Nejdůležitější prevencí proti kybergroomingu je neposkytovat nikomu cizímu žádné soukromé materiály, s tím souvisí i nastavení soukromí na sociálních sítích, kdy je důležité zabezpečit si své profily tak, aby naše příspěvky, informace či fotografie viděli jen naši přátelé. Zvýšená pozornost by také měla být v případě, že si osoba, která nás kontaktovala, nepřeje, aby o vašem vztahu někdo věděl. Rovněž je nutné dávat si mimořádný pozor, když má dojít ke schůzce s osobou, kterou znáte pouze z internetu, nejlépe se podobným schůzkám úplně vyhnout nebo zvolit veřejné a frekventované místo. Tím eliminujeme potenciální nebezpečí.

### 4.8.3 Sexting

Sexting je „*elektronické rozesílání textových zpráv, vlastních fotografií či vlastního videa se sexuálním obsahem, ke kterému dochází ve virtuálním prostředí.*“[50] Ti, kteří se účastní podobné komunikace, riskují zneužití takto citlivých osobních materiálů k vydírání, zesměšnění nebo k jinému poškození své osoby, které může mít vliv i na budoucí život poškozené osoby. V rámci anonymity v kyberprostoru je také velmi lehké se dopustit šíření dětské pornografie, jelikož v dnešní době opravdu není věk mladistvých snadno rozpoznatelný.

Co se týče bezpečnosti, platí prakticky stejná pravidla jako u **kybergroomingu**. Vždy je důležité neposkytovat nikomu cizímu osobní informace a kompromitující fotografie. Bohužel by tato opatrnost v dnešní době měla platit nejen ohledně cizích osob, ale také u partnerů či rodiny. Vždy totiž může dojít k ukončení dobrých vztahů, rozhádání se a poté může snadno skrze tyto informace dojít ke zneužití.[51]

[49] BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014. s. 16-17.
[50] KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci, 2015. s. 43.
[51] Vybrané typy kyberšikany a její preventivní opatření. *Medium – Get smarter about what matters to you*. [online]. Dostupné z: https://medium.com/edtech-kisk/vybran%C3%A9-typy-kyber%C5%A1ikany-a-jej%C3%AD-preventivn%C3%AD-opat%C5%99en%C3%AD-bbd1254eb227

### 4.8.4 Flaming

Jako flaming se označuje agresivní chování projevující se urážkami, nadávkami, ponižováním a vyhrožováním. Jedná se o jev v dnešní době velmi častý a běžný uživatel se s tímto chování může setkat u komentářů fotografií nebo přímo při konverzaci. Často lze na flaming narazit na sociálních sítích v komentářích příspěvků, kde často názory hraničí se zákonem. Flaming nemá za cíl nic jiného než rozčílit, naštvat, ponížit oběť a to zcela beztrestně a většinou i anonymně. *Podle výzkumu je flaming jako slovní napadení ve virtuálním prostředí čtyřikrát častější než v reálném životě.*[52] Právě anonymita je to, co ve většině případů hraje klíčovou roli v kyberšikaně a způsobuje tenkou hranici mezi běžným uživatelem a agresorem.

Oběť flamingu by si měla v první řadě uvědomit, že není potřeba každého přesvědčovat o své pravdě, i kdyby byl sebevíc v právu. Agresorovi, který se dopouští flamingu, většinou stejně nezáleží na argumentech, jde mu pouze o vyprovokování hádky a urážení. Proto by si uživatelé sociálních sítí měli udržet zdravý nadhled a vměšovat se do co nejmenšího množství hromadných diskusí a diskutovat raději osobně, kde si podobné nádavky většina agresorů nedovolí.[53]

# 5 Kyberterorismus

Souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem je tzv. „kyberprostor“, neboli jde o teroristické aktivity zaměřené proti a prováděné prostřednictvím počítačové sítě a touto sítí řízených systémů („informační elektronické síťové struktury“).[54] Tedy daný zločin se neodehrává ve skutečném světě, ale ve světě virtuálním, i když cílem útoku mohou být skutečné věci.

[52] ŠMAHEL, David. *Psychologie a internet: děti dospělým, dospělí dětmi.* Praha: Triton, 2003. s. 13.
[53] Vybrané typy kyberšikany a její preventivní opatření. *Medium – Get smarter about what matters to you.* [online]. Dostupné z: https://medium.com/edtech-kisk/vybran%C3%A9-typy-kyber%C5%A1ikany-a-jej%C3%AD-preventivn%C3%AD-opat%C5%99en%C3%AD-bbd1254eb227

[54] Kybernetický terorismus, kyberterorismus - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 05.12.2019]. Dostupné z: https://www.mvcr.cz/clanek/kybernetic ky-terorismus-kyberterorismus.aspx

Klasická nebo chcete-li oficiální definice kyberterorismu formulovaná Dorothy E. Denningovou zní následovně: *„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“*[55]

Bohužel, tato známá americká analytička dění v kyberprostoru chápe jako akty kyberterorismu téměř výhradně útoky směrované proti kritické infrastruktuře, jež mají za cíl získání informační nadvlády. Paradoxně častěji jsou na internetu zaznamenávány útoky narušující funkci určité služby či jejích součástí, aniž by daný útok byl veden proti konkrétní společnosti nebo vládě s konkrétním účelem (např. vydírání).[56]

## 5.1 Jak chápat kyberterorismus

Samotné počítače za nic nemohou, kdyby existovaly jen ty nebo i chytré mobilní telefony, tablety či notebooky, moc bychom s tím nesvedli. A to je právě ono, hlavní podíl na to má samotný internet. Tedy uměle vytvořená ,,věc‘‘, virtuální prostor, ke kterému se připojíme svým zařízením a je jedno o které se jedná, zda notebook nebo chytrý mobilní telefon, jsme schopni vyhledávat a získávat informace. Toto připojení tedy i určité propojení všech zařízení, které jsou k internetu připojeny. Proto jsou hackeři schopni ovládat nebo získávat cenné informace z jakéhokoli zařízení na světě a to odkudkoli. A to, jak už jsem zmínil v úvodu, v dnešní době moderních technologií a snaze všechno usnadnit a zjednodušit může být od serverů bank, pojišťoven, státních institucí, škol, ale i chytrých domácností, pomocí kterých jsme schopni ovládat celý dům či byt pomocí aplikace ve svém chytrém telefonu, kdy si můžeme zapnout pračku nebo uvařit kávu, velké riziko. Když se najde někdo, kdo chce tyto technologie zneužít a dělat jisté naschvály nebo v horším případě získávat cenná nebo citlivá data a ty dále zneužívat pro svoji potřebu.

[55] Kybernetická kriminalita IV*: Hacktivismus a kyberterorismus*. [online]. Copyright ©2011 [cit. 08.12.2019]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php

[56] Kybernetická kriminalita IV*: Hacktivismus a kyberterorismus*. [online]. Copyright ©2011 [cit. 08.12.2019]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php

**Kyberterorismus je tedy úmyslný a často i politicky motivovaný útok**, který je vedený proti počítačovým systémům, programům a v neposlední řadě i uživatelům v rámci celého kyberprostoru.

## 5.2 Příklad kyberterorismu

Typickým příkladem kyberterorismu může být napadení bankovních sektorů, státní či vojenské infrastruktury, zejména tajných informací nebo různých bezpečnostních systémů, což je velmi nebezpečným kyberkriminálním zločinem. A nejen to, ale i napadení domácností či mnoha státních institucí, úřadů nebo škol.
V nejhorším možném případě může kyberterorismus vést ke ztrátě na lidském životu, a to se děje v momentě, kdy napáchaná kyberkriminalita v kyberprostoru si začíná vybírat svoji daň (nehledě na to, zda jde o teroristické aktivisty, samostatné crackery, či pachatele kyberšikany apod.) i mimo svět virtuálního prostředí.

# 6 Darknet

Darknet neboli jinak řečeno temný internet, podsvětí internetu. Je část internetu, kam se běžný uživatel nedostane, a to z několika důvodů. Jsou přístupné pouze prostřednictvím speciálního softwaru nebo konfigurace.

Nejprve si ovšem vyjasněme pojmy. Darknet se někdy zaměňuje s Deep Webem (hlubokým webem, neviditelným webem). Deep Web obsahuje rozsáhlé databáze knihoven, institucí, archivů, institucí, které nejsou běžnému uživateli přístupné. Jsou zde uchována ta nejcennější data, např. vědecko-výzkumného charakteru, které si tyto instituce chrání, a proto na jejich stránkách nefunguje indexování vyhledávacími roboty. Databáze poskytují svůj obsah jen po přihlášení na heslo nebo vyžadují speciální oprávnění. Možná je to pro někoho novinka, ale hluboký web pokrývá drtivou většinu internetu, podle odhadů až 95 %.

Darknet je také „hluboko“, ale jak bylo zmíněno na začátku, je to místo, ve kterém probíhá kromě jiného ilegální činnost. Funguje na bázi anonymního připojení přes šifrované sítě, ve kterých probíhá komunikace mezi jednotlivými uživateli (P2P), a je

dostupný jen přes speciální software a konfiguraci komunikačních protokolů a portů. Jinými slovy, přes Google se na něj nedostanete. Tak jako ve skutečném světě zde probíhá prodej zbraní, drog, ilegální sázení, obchod s bílým masem, šíří se zde dětská pornografie nebo se sdílejí kódy ke škodlivému softwaru (malwaru, spywaru, ransomwaru…). V neposlední řadě tu čile komunikují teroristé. A platí se zde digitální měnou bitcoiny.[57]

## 6.1 Jak se dostat na Darknet

Jednou z aplikací, která umožňuje přístup je nejběžnější internetový prohlížeč Tor (The Onion Router). Jedná se tedy o internetový prohlížeč, je volně ke stažení, doporučuje se stahovat z oficiální stránky, aby byla zaručena oficiální verze a s ní zaručena nonymita. Kdybyste si do počítače nenainstalujete originální prohlížeč, ale nějakou jeho mutaci, která nemusí být tak bezpečná, bude sledovat, co se snažíte navštívit.[58]

Další možností jak se dostat na Darknet je jeden z nejznámějších vyhledávačů Torch. Do tohoto vyhledávače se ručně indexují „onion‘‘ webové stránky. Existuje samozřejmě mnoho dalších vyhledávačů a stránek pro přístup na Darknet. Doporučuje se procházet různá internetová fóra a proklikat se k tomu, co vás zajímá.

Obsahy webů a jejich adresy se velmi často mění, při hledání to chce trpělivost a vše si poznamenávat, může se vám stát, že narazíte na něco zajímavého, odejdete a poté už se vám nepodaří vrátit zpět. Buďte také velice obezřetní! Vyhýbejte se webům s nelegálním obsahem a dejte si pozor na podvodné webové stránky a tzv. mirrory. Mirror (zrcadlo) je web, který kopíruje jeho originál. Většinou se jedná o naprosto identickou kopii zajeté stránky, kterou lidé používají, ale navrženou pouze za účelem vás podvést. [59]

## 6.2 Darknet nerovná se „ilegální‘‘

[57] Darknet – podsvětí internetu – oTechnice.cz. *oTechnice.cz – Nejnovější zprávy ze světa technologií* [online]. Copyright © 2020 [cit. 29.01.2020]. Dostupné z: https://otechnice.cz/darknet-podsveti-internetu/
[58] idnes.cz, *Jak se připojit na neviditelný internet*, publikováné: 14. června 2016 © 2020 [cit. 29.01.2020] Dostupné z https://www.idnes.cz/technet/software/jak-se-pripojit-na-neviditelny-internet.A160602_150524_tec_technika_baha
[59] idnes.cz, *Jak se připojit na neviditelný internet*, publikováné: 14. června 2016 © 2020 [cit. 29.01.2020] Dostupné z https://www.idnes.cz/technet/software/jak-se-pripojit-na-neviditelny-internet.A160602_150524_tec_technika_baha

Jedním dechem je nutné dodat, že Darknet nevznikl za účelem páchání zločinů, ani jej nevynalezli zločinci. Byl zamýšlen „jen“ jako prostor bez regulací, cenzury a státního dohledu, zkrátka jako bezpečný anonymní digitální prostor, na který se zločin postupně „nabalil“. Domov zde dříve našli např. anarchisté různých odstínů, zastánci stahování čehokoli bez omezení nebo příslušníci různých subkultur. I dnes je možné jej využít pozitivně. Je aktivní tam, kde dochází k porušování lidských práv, používá se k ochraně soukromí nebo zde našly útočiště oběti domácího násilí.

Svůj název dostal Darknet od inženýrů Microsoftu před 15 lety v článku *The Darknet and Future of Content Distribution* (Darknet a budoucnost distribuce obsahu). Později došlo k jeho různým definicím, ale v digitálním mainstreamu se uchytil právě Darknet. První „temnou sítí“ se stal v roce 2000 Freenet. Byl primárně vytvořen na ochranu nepohodlných politických oponentů v nedemokratických režimech. Byl na rozdíl od „standardního internetu“ pomalý a nenabízel zdaleka tolik obsahu. Už Freenet vyžadoval speciální konfiguraci a software. S příchodem kryptoměn začaly vznikat tzv. freemarkety, na kterých bylo možné obchodovat prakticky s čímkoli.[60]

# 7 Fenomenologie počítačové kriminality

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

## 7.1 Trestné činy související s počítačovou kriminalitou a jejich skutkové podstaty

[60] Darknet – podsvětí internetu – oTechnice.cz. *oTechnice.cz – Nejnovější zprávy ze světa technologií* [online]. Copyright © 2020 [cit. 29.01.2020]. Dostupné z: https://otechnice.cz/darknet-podsveti-internetu/

### 7.1.1 § 230 TZ Neoprávněný přístup k počítačovému systému a nosiči informací [61]

*(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán: odnětím svobody až na dvě léta, zákazem činnosti nebo, propadnutím věci.*

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

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

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

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

*d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán: odnětím svobody až na tři léta, zákazem činnosti nebo, propadnutím věci.*

*(3) Odnětím svobody na šest měsíců až čtyři léta, zákazem činnosti nebo propadnutím věci bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2*

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

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

*(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,*

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

*b) způsobí-li takovým činem značnou škodu,*

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

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

[61] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.03.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

*e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.*

*(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,*

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

*b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.*

## Skutková podstata

Tato norma je zaměřena na ochranu informací v počítačových systémech. **Objektem** tohoto trestného činu je tedy ochrana počítačových systémů a jejich dat, a to je právě zájem, který je chráněn státem. **Objektivní stránka** jednání a následek, mezi nimiž musí být příčinná souvislost neboli kauzální nexus. Jednání je v tomto případě překonávání bezpečnostního opatření, a tím neoprávněné získání přístupu k počítačovému systému nebo jeho části. Následkem je porušení objektu neboli práva na ochranu počítačových systému a jejich dat. **Předmětem** je nosič informací, respektive jeho obsahové a technické vybavení. **Subjektem** je osoba starší patnácti let a musí být příčetná, která takový čin spáchá. **Subjektivní stránka** neboli zavinění ve formě úmyslu. Tento trestný čin je závažnější, pokud pachatel data v počítači zneužije, vymaže, pozmění, vloží, páchá-li tento čin s úmyslem způsobit někomu škodu, sobě nebo jinému neoprávněný prospěch nebo s úmyslem omezit funkčnost počítačového systému.

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

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

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

### 7.1.2 § 231 TZ Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat [62]

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

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

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

*bude potrestán: odnětím svobody až na dvě léta, propadnutím věci nebo, zákazem činnosti.*

*(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci bude pachatel potrestán,*

*a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo*

*b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.*

*(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.*

## Skutková podstata

Ke splnění skutkové podstaty tohoto činu není třeba získat přístup k počítačovým systémům jako v § 231 TZ, ale stačí, když si někdo opatří nebo přechovává zařízení s programovým vybavením, počítačové heslo nebo podobný prostředek, pomocí kterého lze získat přístup k počítačovému systému a to vše s úmyslem spáchat trestný čin neoprávněného přístupu k počítačovému systému. V téhle situaci jde vlastně o formu

[62] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.03.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

přípravy, pachatel si obstarává nástroj k neoprávněnému přístupu do počítačového systému a už tato forma přípravy je definována jako trestný čin. **Objekt** tohoto trestného činu je ochrana počítačových systémů a jejich dat. **Jednáním** je výroba, přechovávání, prodávání nebo opatřování prostředku, kterým se lze neoprávněně dostat to počítačového systému a následkem je porušení práva na ochranu počítačových systémů a jejich dat. **Předmět** útoku je nosič informací, respektive jeho obsahové a technické vybavení. **Subjekt** je osoba starší patnácti let a příčetná, která tento čin spáchá a **subjektivní stránka** je zavinění ve formě úmyslu. Odstavce 2 a 3 už obsahují pouze kvalifikovanou skutkovou podstatu, tedy i vyšší trest, pokud pachatel spáchá čin v odstavci 1 jako člen organizované skupiny nebo získá takovým činem pro sebe či pro jiného značný prospěch nebo prospěch velkého rozsahu.

### 7.1.3 § 232 TZ Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti [63]

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

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

*b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,*

*a tím způsobí na cizím majetku značnou škodu, bude potrestán: odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci.*

*(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.*

## Skutková podstata

**Objektem** tohoto trestného činu je ochrana počítačových systémů a jejich dat. **Jednání** je porušení povinnosti, a tím znehodnocení dat v počítačovém systému nebo učinění zásahu do technického nebo programového vybavení počítače nebo jiného technického zařízení, a tím způsobení značné škody na cizím majetku. **Následek** je

[63] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.03.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

porušení práva na ochranu počítačových systémů a jejich dat. **Předmět** útoku je nosič informací, respektive jeho obsahové a technické vybavení, v tomto konkrétním případě znehodnocení dat v počítačovém systému nebo učinění zásahu do technického nebo programového vybavení počítače nebo jiného technického zařízení a tím způsobení značné škody na cizím majetku. **Subjekt** je osoba starší patnácti let a příčetná, která tento trestný čin spáchala a **subjektivní stránka** je zavinění ve formě hrubé nedbalosti.

**Definice hrubé nedbalosti** z trestního zákoníku § 16 odst. 2, zní takto: *„Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.“*[64]

## 7.2 Analyzování policejní statistiky

V této části práce jsou analyzovány policejní statistiky, konkrétně poškozování a zneužívání záznamu na nosiči informací za posledních deset let. Tedy od roku 2009 do roku 2019. Tyto statistické záznamy obsahují zjištěné trestné činy od 1. 1. do 31. 12. daného roku. Statistický záznam poškozování a zneužívání záznamu na nosiči informací obsahuje všechny tři trestné činy, které byly rozebrány v předešlé kapitole (§ 230-232 TZ).[65]

[64] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.03.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[65] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

**Tabulka č. 1[66] - Poměr zjištěných a objasněných trestných činů v kategorii poškozování a zneužívání záznamu na nosiči informací (§ 230-232 TZ)[67]**

| Poš. a zneuž. záz. na nos.informací | Zjištěno | Objasněno | Objasněnost v procentech |
|---|---|---|---|
| **2019** | 1092 | 208 | 19,1% |
| **2018** | 893 | 231 | 25,9% |
| **2017** | 784 | 206 | 26,3% |
| **2016** | 635 | 157 | 24,7% |
| **2015** | 707 | 144 | 20,4% |
| **2014** | 669 | 192 | 28,7% |
| **2013** | 301 | 76 | 25,2% |
| **2012** | 178 | 45 | 25,3% |
| **2011** | 134 | 54 | 40,3% |
| **2010** | 101 | 30 | 29,7% |
| **2009** | 62 | 20 | 32,3% |

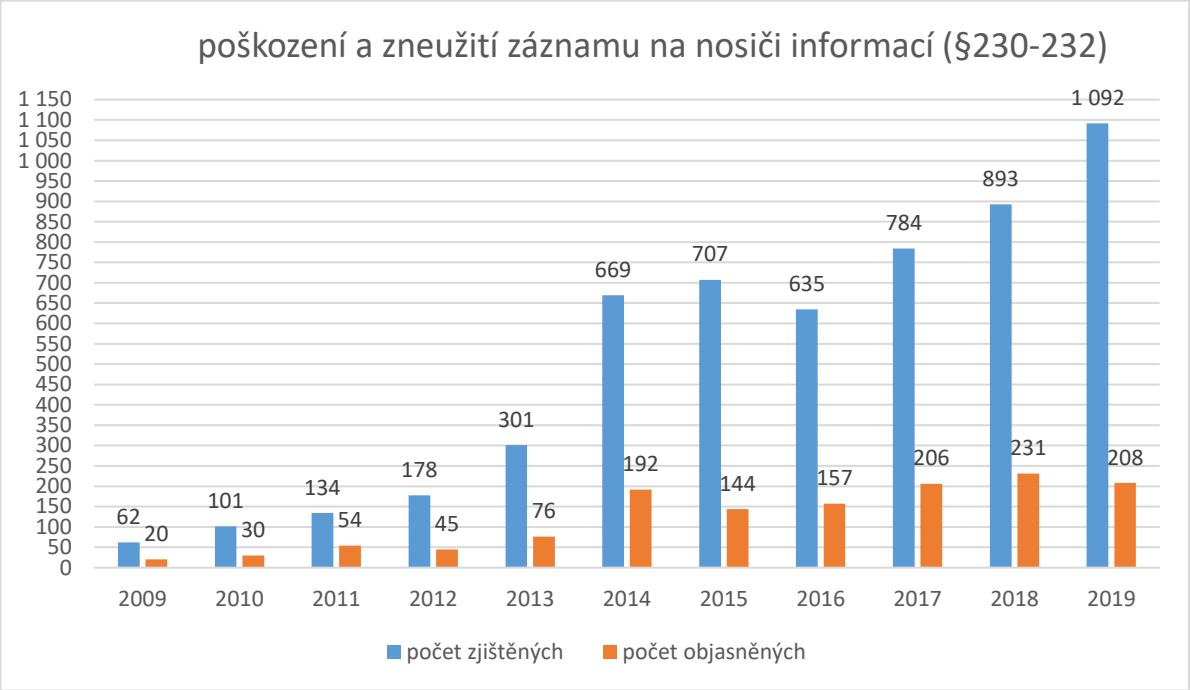
Z tabulky je patrné, jak se počítačové systémy a počítačová kriminalita rychle rozrůstá. Za rok 2009 bylo zjištěno pouhých 62 trestných činů v kategorii poškozování a zneužívání záznamu na nosiči informací. V dalších letech postupně přibýval jejich počet a za rok 2019 je jich zjištěno 1092, to je sedmnáckrát více než za rok 2009. Jedná se tedy o enormní nárůst. Objasněnost těchto činů naproti tomu nestoupá, ale spíše kolísá mezi 20% až 30%. Výjimkou je rok 2011, kdy byla nejvyšší objasněnost za celé desetileté

[66] Kriminalita - Policie České republiky. *Úvodní strana - Policie České republiky* [online]. Copyright © 2020 Policie ČR, všechna práva vyhrazena [cit. 20.04.2020]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx?q=Y3BpPTE%3d

[67] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

období, a to 40,3%. Naopak nejmenší objasněnost byla v roce 2019, kdy dosáhla pouze 19,1%. Podle těchto zjištěných statistických výsledků se průměrná objasněnost pohybuje okolo 29,8%. To je zapříčiněno zřejmě vysoce anonymním prostředím v počítačovém světě.

**Graf č. 1.[68] Poměr zjištěných a objasněných trestných činů v kategorii poškozování a zneužívání záznamu na nosiči informací (§230-232 TZ)**




Na grafu je vidět, řekl bych, až enormní nárůst počítačové kriminality za období deseti let. Podle mých předpokladů se bude v průběhu let dále navyšovat, jde o to, do jaké míry.

V následující **tabulce č. 2.** jsou podrobně rozpracovány další hodnoty počítačové kriminality. Celkový počet registrované kriminality, podrobný počet objasněné kriminality, kriminality spáchané nezletilými, mladistvými a jaký počet z celkového počtu trestných činů spáchaly děti, počet činů spáchaných opakovaně trestanými osobami, cizinci a počet činů spáchaných pod vlivem alkoholu.

[68] Kriminalita - Policie České republiky. *Úvodní strana - Policie České republiky* [online]. Copyright © 2020 Policie ČR, všechna práva vyhrazena [cit. 20.04.2020]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx?q=Y3BpPTE%3d

**Tabulka č. 2[69] - Podrobný poměr zjištěných a objasněných trestných činů v kategorii poškozování a zneužívání záznamu na nosiči informací (§ 230-232 TZ)[70]**

| rok | REGISTROVÁNO | OBJASNĚNO (registrováno => z toho objasněno) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | POČET | POČET | tj. v % (objasněnost) | spácháno nezletilými | spácháno mladistvými | spácháno dětmi | spácháno opakov. trest. osobami | spácháno cizinci | spácháno pod vlivem alkoholu |
| **2019** | 1 092 | 208 | 19,1 | 7 | 7 | 14 | 33 | 27 | 0 |
| **2018** | 893 | 231 | 25,9 | 8 | 11 | 19 | 41 | 31 | 3 |
| **2017** | 784 | 206 | 26,3 | 2 | 17 | 19 | 41 | 31 | 0 |
| **2016** | 635 | 157 | 24,7 | 9 | 8 | 17 | 37 | 9 | 0 |
| **2015** | 707 | 144 | 20,4 | 17 | 9 | 26 | 36 | * | 0 |
| **2014** | 669 | 192 | 28,7 | 5 | 9 | 14 | 28 | * | 1 |
| **2013** | 301 | 76 | 25,2 | 4 | 6 | 10 | 11 | * | 1 |
| **2012** | 178 | 45 | 25,3 | 2 | 0 | 2 | 12 | * | 0 |
| **2011** | 134 | 54 | 40,3 | 6 | 5 | 11 | 12 | * | 0 |
| **2010** | 101 | 30 | 29,7 | 2 | 0 | 2 | 13 | * | 0 |
| **2009** | 62 | 20 | 32,3 | 0 | 0 | 0 | 3 | * | 0 |

(data označena * nejsou uvedena v policejních statistikách)

**Výpočet podílu, neboli indexu** – dospělí vs děti u této kriminality, podíl dětí na trestné činnosti a podíl počítačové kriminality na celkové kriminalitě za rok 2019.

děti ÷ všichni pachatelé **x** 100

**14 ÷ 208 x 100 = 6,73%**

děti ÷ celková kriminalita **x** 100

**3361 ÷ 93202 x 100 = 3,6%**

počítačová kriminalita ÷ celková kriminalita x 100

**208 ÷ 93202 x 100 = 0,22%**

[69] Kriminalita - Policie České republiky. *Úvodní strana - Policie České republiky* [online]. Copyright © 2020 Policie ČR, všechna práva vyhrazena [cit. 20.04.2020]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx?q=Y3BpPTE%3d

[70] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

Výpočtem těchto indexů bylo zjištěno, že dětí je u počítačové kriminality větší množství než u celkové kriminality, z čehož vyplývá závěr, že mladá generace více inklinuje k počítačové kriminalitě než ostatní kriminalitě. Konkrétně na počítačové kriminalitě se podílela **6,73%**, kdežto podíl dětí na celkové kriminalitě je pouze **3,6%**. Podíl počítačové kriminality na celkové kriminalitě je **0,22%,** což není nijak závratné číslo, ale postupem času se podíl zvětšuje.

# 8 Příčiny počítačové kriminality

Smejkal uvádí: *„Motivem bývá nejčastěji osobní obohacení, ale jsou známy i další časté motivy, patří k nim zejména pocit převahy nad zaměstnavatelem či veřejnými orgány, pocit beztrestnosti, snaha kompenzace nespokojenosti s prací, názor, že firmě nemohou uškodit malé ztráty a touha po riziku.“*[71]

Shrnutí příčin počítačové kriminality. Pachatele vedou k jejímu páchání, nejčastěji osobní obohacení, touha pachatele o vlastní zviditelnění, neoprávněný prospěch, získání informací jak pro osobní potřebu, tak pro průmyslovou špionáž, snadný zisk, ublížit jinému, pocit převahy nad zaměstnavatelem či veřejnými orgány, pocit beztrestnosti, snaha kompenzace nespokojenosti s prací, názor, že firmě nemohou uškodit malé ztráty a touha po riziku. Počítačů lze dále užít jako prostředků pro vydírání, nebezpečné pronásledování a kyberšikanu. Mezi další patří šíření dětské či jiné pornografie. Dochází tedy k uspokojení vlastní deviace. Mimo obvyklou počítačovou kriminalitu dále stojí tzv. internetové podsvětí nazvané „Dark Net“, na kterém lze např. nelegálně zakoupit zbraně či drogy. Tedy svým způsobem lehčí dostupnost než v reálném prostředí. Hlavní „výhodou“ kyberkriminality je, že pomocí sítě můžou provádět útoky či jiné páchání na dálku, tedy odkudkoli na světě. Celkově malý počet zjištěné kriminality na rozdíl od té skryté. Tedy velká pravděpodobnost, že se na daný útok nebo čin vůbec nepřijde.

Hlavním motivem je určitý pocit anonymity a pocit nedotknutelnosti, že nemůže být pachatel odhalen, do určité míry tomu tak může být. Zvolení jiné identity, možnosti různých skrytých nebo přesměrovávaných IP adress. To uvádí i Jirovský: *„Útočník nebo*

[71] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015., Pro praxi. s. 135

*pachatel pracuje v globálním prostředí, může se v kyberprostoru velmi rychle a nepozorovatelně pohybovat, měnit identity nebo i mizet.“*[72]

## 8.1 Pachatelé počítačové kriminality

Pachatelé počítačové kriminality bývají nejčastěji mladší lidé, s odborným vzděláním souvisejícím s tímto oborem. Dalším znakem pachatele je problematičnost v oblasti začleňování se do společnosti, ale není to pravidlem.

Dnes je velmi těžké určit profil pachatele počítačové kriminality, jak již bylo zmiňováno, žijeme v době, kdy je obrovský rozmach informačních technologií a s tím i přibývá více sfér, kam může počítačová kriminalita proniknout. V některých oblastech počítačové kriminality pachatelé ani nepotřebují odborné vědomosti nebo speciální programy. Například v oblasti počítačového pirátství stačí, pokud pachatel nějakým způsobem sdílí chráněný obsah. Z tohoto důvodu není už dnes možné profily pachatelů příliš zobecňovat jako dříve, když byly počítače a internet využívány malým počtem lidí. A v dnešní době má přístup k internetu každý, proto i počítačovou kriminalitu páchají i děti.

# 9 Rozhovor

V rámci bakalářské práce byl proveden rozhovor s bezpečnostním analytikem (Security analyst) Martinem Kuncem z CZ.NIC a jeho kolegou Petrem Špringerem specialistou počítačové bezpečnosti z CZ.NIC. Oba pánové souhlasili s uveřejněním své identity v rozhovoru, jež je součástí této bakalářské práce.

[72] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007. s. 19.

## Jaká je Vaše práce a co má na starosti Vaše společnost?

**Martin Kunc**: *„Naše společnost je CZ.NIC, což je správce domény. Za doménu se platí, asi 160Kč ročně. Kdokoli si ji může zaregistrovat a z toho jsou samozřejmě peníze, takže CZ.NIC vymyslel, že ty peníze budeme vracet komunitě. Což dělá především prostřednictvím open sears projektů. Tyto projekty se docela hojně využívají. Když na to přišlo, tak to dopadlo tak, že národní cirt team České republiky se založil pod CZ.NICkem. Krom národního CSIRT team (CSIRT.CZ ) máme v ČR ještě GovCERT (GovCERT.CZ), což je Národní centrum kybernetické bezpečnosti, ten řeší, řekněme, ty vládní věci a soukromí společností a jednotlivé uživatele řešíme my jako CSIRT team. Oni dále mají ty tajné a utajované věci, do kterých my nezasahujeme, ani nemáme jak.“*

*„Dále máme na starost evropské projekty, spolupracujeme na zvyšování bezpečnosti. Tady s Petrem máme na starosti Honeypoty.* ***Honeypot*** *je zařízení nebo softwar, který se tváří, že to je to zranitelné zařízení, toto zařízení láká útočníky, aby si na ně vyzkoušeli svoje útoky a třeba tam poslali nějaký nový malware a my to takhle můžeme posbírat a dělat analýzy nebo to dost poslat antivirům ke zpracování. Loňským rokem jsme odstartovali penetrační testování, kdy firmám a institucím nabízíme službu. Kdy se jim pokoušíme dostat do sítě a zjistit slabá místa jejich zabezpečení.“*

*„Dále děláme scanner webu, na kterém pracuje Petr, kdy školám za symbolickou jednu korunu zkontrolujme web a popřípadě opravíme chyby. Do toho děláme Incident handling. Incident handling má na starosti zvládání incidentů. Úkolem je zabezpečit hladký životní cyklus incidentů, a to příjem hlášení, jejich řešení, až po návrh nápravných opatření. Tým incident handlingu vystupuje v rámci vládního CERT týmu jako spojka se zástupci kritické informační infrastruktury a významných informačních systémů. Dále také zajišťuje komunikaci s národními a mezinárodními partnery. Což je o tom, že nám… že nám píšou, ať už firmy nebo lidi nebo zahraniční firmy, které mají s něčím problém nebo našli jsme tady server, který je nejspíš napadený,…. zkuste s tím něco udělat. My pak zase kontaktujeme tu českou firmu. Jenom v zásadě přepošleme zprávu. Případně ještě zajistíme komunikace mezi těmi subjekty. To má primárně na starost Incident handling.*“

**Petr Špringer:** *„Chodíme do škol školit o bezpečnosti na internetu a snažíme se vzdělávat i veřejnost, jako CSIRT team. Máme kolegyni, která se zabývá kyberšikanou,*

*která chodí po školách a dalších institucích a vysvětluje, co je kyberšikana a že vůbec něco takového existuje. Na to konto máme i miniseriál: „ Jak bezpečně na internet“.“*

*„Spolupracujeme i s policií, snažíme se v rámci této spolupráce i zablokovat škodlivé domény, což je teoreticky pro nás o něco snazší, jakožto národní CSIRT team jsme součástí CZ.NICu, což je správce domény, a pokud přijde příkaz od policie, tak můžeme velice rychle danou stránku vypnout.*

*Každých 14 dní vydáváme zprávy o bezpečnosti na ROOT.cz a spolupracuje s námi CES.NET*

*Každý rok pořádáme IT Konference ohledně bezpečnosti*.“

## Zabezpečujete i státní instituce, nebo jen soukromé uživatele?

**Martin Kunc** *„Prakticky nám může napsat kdokoliv. Například scanner webu, o to si může napsat i jakékoli ministerstvo. Tam dále je ale problém kybernetické bezpečnosti, takže v případě, že se tam něco najde, tak se to musí hlásit i GovCERTu.*

*PROKY – projekt predikce a ochrany před kybernetickými incidenty, tam sbíráme obrovské množství dat, která jsou pro CSIRT team dostupná zdarma a stejně tak pro některé subjekty. 2x týdně rozesíláme správcům koncových sítí informace o tom, zda mají nějaký otevřený port nebo nějakou jinou chybu a oni sami si musí zkontrolovat, zda je to tak, jak to má být.*

*Dále řešíme prevenci a snažíme se dělat osvětu a informovat uživatele a vzdělávat uživatele v naší akademii CZ.NIC, kde máme i několik kurzů zaměřených na bezpečnost. Teď kolega z Prahy udělal nový kurz na forenzní analýzu operační paměti.*

**Petr Špringer***: Penetrační testy - máme placenou službu chovat se jako útočník, nemusím najít všechny chyby, ale stačí mi najít jen nějakou jednu chybu webu a dostat se k co nejvíce oprávněním v té síti, a pak samozřejmě v rámci zprávy musíme říct, kam jsme se dostali, čeho jsme nezneužili, proč to tak šlo a tak dále.*

*CSIRT team si může založit kdokoli, ČR jich má v celé Evropě nejvíce. Začíná se to rozmáhat a je to jedině dobře, když mají na sebe kontakty a můžou spolupracovat.“*

## Jak si stojí Česká republika oproti světu?

**Martin Kunc:** *„Velmi dobrá otázka! Je několik žebříčků. Česká republika si vede velice dobře a je na předních příčkách spolu s Estonskem. Z krátkodobý historie svět velice zaujala naše kauza s Huawei, tím jsme si asi taky udělali dobré jméno ve světě. Pokud budeme hodnotit Českou republiku z pohledu odborníků, tak stojí za zmínku cvičení Lockt Shealt, který je pořádaný CCDCOE, což je jakousí součástí NATO, i když úplně není, protože se na tom ještě neshodly všechny státy, k čemuž ještě nedošlo, každý rok se pořádá několik cvičení. V tom cvičení má každý stát, který se účastní, má dva týmy, jeden modrý- obranný a jeden červený- útočný. Je vytvořená infrastruktura, která je pro každý stát stejná. K této síti se tyto týmy připojí a simulují situace útoků, červený útočí a modrý se brání. Za poslední tři roky jsme byli na předních příčkách, do třetího místa. A těchto cvičení je více, ať už celosvětových nebo evropských.“*

## Zvyšuje-li se index reálné hrozby útoku, zvyšuje se předpoklad útoku?

**Martin Kunc:** *„Je zde více parametrů, jedna z věcí jsou zájmy států a státem organizovaných skupin, které se zlepšujou. Otázka je, jestli rychleji než obrana jednotlivých států. Druhou věcí je klasická kriminalita, kde nedokážu posoudit, zda je to lepší nebo horší. Jsou zajímavější útoky, protože je to potřeba, počítače jsou čím dál více bezpečnější. Nicméně furt i v dnění době jde i o případy, kdy někomu přijde email s přílohou a příjemce otevře přílohu, a tím aktivuje narušení.“*

**Petr Špringer***: „Je to pořád a pokud budou mít lidi možnost získat peníze nebo prospěch, tak to zůstane. Hlavně je jednoduché si založit email a rozesílat tyto, ať už podvodné nebo škodlivé emaily, a bez větší práce jich posílat tisíce. Jsou i čím dál více sofistikované, lepší se vzhled nebo i jazyk, vypadají hodně důvěryhodně.“*

*„Je hlavně i větší četnost, může za to i větší dostupnost dat. Poslat podvodný email není nic těžkého, děje se to i mezi velkými firmami a holdingy. I rozesílání škodlivých malwarů pomocí těchto podvodných emailů.“*

*„Jde to jedno s druhým, zlepšuje se technika zabezpečení, ale i s tím souběžně se zlepšují i ty útoky, například zabezpečení - je jednodušší odemykat chytrý mobilní telefon*

*nebo vstupovat do zabezpečených objektů pomocí skenu obličeje nebo otisku prstu, ale to se všechno dá zneužít a všechno z obyčejné fotky jak obličeje, tak kvalitnější fotky ruk,y kdy po zvětšení bude schopné rozeznat otisky prsů, proto stále nejbezpečnější zůstává heslo, silné heslo s kombinací čísel, písmen a speciálních znaků. A pokud mi někdo kompromituje heslo, tak se dá změnit, ale to u obličeje, otisků prstů, sítnice nebo duhovky nejde.“*

## Je možný útok v takové míře, aby došlo k ochromení celého státu?

**Martin Kunc:** *„Toho se zas tak moc nebojím, veškeré systémy nepůjdou napadnou jedním virem. Každý program funguje na trochu jiné bázi a je dost složité, aby fungoval správně na jednom systému, samozřejmě každý používá i trochu jiný operační systém, což je taky překážka, ale rozhodně se nebojím, že by došlo ke shození všech počítačů v České republice najednou. Hacker bude hledat tu nejjednodušší cestu, jak toho docílit, takže si rozhodně nebude dávat tu práci, abych shodil všechny počítače, ale bude stačit, aby shodil například jenom rozvodnou síť. Což může způsobit velké škody a bude mnohem jednodušší než napadat velké množství institucí.“*

*Bezpečnostní vstupy- záleží na zabezpečení dané instituce. Pokud je vstup dveří pomocí karet, tak projde více lidí najednou a je možná infiltrace někoho zvenčí, zato při vstupu, kde jsou turnikety, tak projde vždy jen jeden. Je důležité zvolit adekvátní způsob.“*

## Jaký je Váš názor na Darkweb?

**Martin Kunc**: *„Není to v zásadě zas tak super, jak to zní. Darkweb, jak se dneska používá, je v zásadě jen Thor síť. Thor klienta si může kdokoli stáhnout, je to opensours a může se připojit k té síti. Popravdě neznám žádné webové stránky, a ani nevím, jak přesně funguje vyhledávání. Momentálně se tomu asi přisuzuje příliš velká váha, stejně tak může posloužit uzavřený kanál, v zásadě to funguje podobně. Ten Thor zvládá velmi dobře anonymizaci a je velice těžké dohledat, kdo se připojoval a odkud se připojoval, ale pokud vím, tak česká policie ve spolupráci s USA mají nějaké určité možnosti, ne úplně identifikovat daného člověka, ale zúžit okruh podezřelých. Ale jak říkám, není to zas tak nic extra, je tomu jen připisována velká váha. Nemá to pro mě zas takovou jiskru.“*

**Během studia tohoto téma jsem narazil na to, že dnes už to není jen o počítačích, tabletech a chytrých telefonech, ale i o chytrých domácích spotřebičích, chytrých domácnostech. Máte nějaká doporučení jak chránit tato zařízení a předcházet možným útokům?**

**Petr Špringer**: *„Na stánkách CSIRTu máme pro uživatele doporučení jak se starat a zabezpečit o svá zařízení, a jak zabezpečit zařízení dětem. Je vydané doporučení, že stačí jedno zranitelné zařízení v síti, které může způsobit narušení sítě, i když všechna ostatní zařízení můžou být zabezpečena správně.“*

**Martin Kunc**: *„Zase se spoléhat na zabezpečení sítě přes router není správné. Jakmile se někdo dostane dovnitř, tak má s velikou pravděpodobností přístup ke všem zařízením v síti, ale pokud jsou všechny zařízení dostatečně zabezpečena, tak se není čeho bát. Ale je to opravdu o tom, že když se najde jedno nezabezpečené zařízení, u kterého nepředpokládáme, že by k němu mohlo dojít, například při tom penetračním testu, a najde se například chytrá ledničkа, pračka, kávovar nebo něco dalšího, co se dá ovládat na dálku pomocí sítě, tak …. Množství útoků se zvyšuje, ale to souvisí i s nárůstem těchto zařízení.*

*Velmi často se stává to, že člověk někam nainstaluje právě router nebo jiné chytré zařízení (ledničku, pračku,…) a zapomene na to, nebo neví, že je to připojený k internetu, a to je právě ten problém.“*

**Doporučení expertů**: *„Zablokovat přístup zařízení k síti/internetu, které to nepotřebují. Je otázka, jestli moje pračka potřebuje připojení k internetu. Já si myslím, že opravdu ho nepotřebuje. U některých zařízení to přímo jde vypnout, aby se nepřipojovala k internetu, v jiných případech to jde nastavit i na routeru, aby se dané zařízení nepřipojovalo. Pokud to jde, tak to odpojit, pokud to nejde, tak segmentovat, což znamená udělat lokální uzavřenou síť pouze pro to jedno zařízení, aby se z něho nedalo dostat na jiné zařízení v síti, nebo připojit pomocí síťového kabelu. Aktualizovat, pokud to jde, aby software nebo antivir byl aktuální. Pokud to nejde u starších zařízení, tak zařízení vyměnit.“*

## Jaké jsou největší příčiny počítačové kriminality?

**Martin Kunc:** *„Těžko říct, které jsou největší. To co mě napadá je 1) vlastní obohacení, 2) špionáž, ať už korporátní nebo státní (nebo jak se jí říká) 3) vandalismus (?) … a možná „hacktivism“.*

*Otázka je, jestli tam pak nezahrnout i vydírání, očerňování, stalking, kyberšikana, dětská pornografie (šíření a vlastnění).*

*Taky jestli to neformulovat spíš do „motivace“ než příčiny.“*

## Mohl byste seřadit příčiny podle důležitosti?

**Martin Kunc: „***To asi nedokážu. Důležitost můžeme určit buď dle finančních důsledků (jednotlivce, firmy, maximálně celkem nebo jednotlivě), ekonomických dopadů na celý stát (když se jim rozbijou centrifugy na obohacování uranu, tak to bude mít ekonomické dopady na celou zemi), důležitosti dle znepřístupnění – když nepůjdou platby kartama, českej internet, Česká pošta... , pozice armádních jednotek? (v případě válečného konfliktu asi důležitější než zašifrované disky uživatelů). Na druhou stranu zašifrované disky nemocnice v případě nouze můžou udělat taky dost velké potíže.“*

## Lze příčiny rozlišovat například také podle věku uživatelů?

**Martin Kunc:** *„Asi ne. I když zatím ještě žijeme v době, kdy u lidí nad 70 se nedá očekávat zapojení do aktivit spojených s počítačovou kriminalitou. Naopak ti mladší to zvládají velmi dobře, někdy od druhého stupně základní školy.“*

## Jaké byste navrhoval opatření ke snížení kriminality páchané prostřednictvím počítačů?

**Martin Kunc:** *„Vzdělávání uživatelů. Což je mimo jiné jedním z poslání sdružení CZ.NIC.“*

**Jaké navrhujete opatření a doporučení jak se chovat , abychom se nestali obětí kyberkriminality?**

**Martin Kunc:** *„Nikomu neposílat peníze. Prověřovat si emaily od banky, vždy kontrolovat přes internetové bankovnictví a hned nerozklikávat. S tím souvisí celkově si dávat pozor na emaily jak od neznámých adresátů, tak i podezřelých příloh, nikdy neklikat na odkazy v emailu. Je to jako zásada se vždycky rozhlídnout, když jdeš přes silnici, nejde se spoléhat jen na to, zda něco slyším, nebo ne. Ale někdy jdou lidi zamyšlený a nerozhlídnou se a to je stejný i u tý bezpečnosti na internetu. Zálohovat data, zálohovat, pokud možno i off-line, když už dojde k nějaké ztrátě dat, tak aby to způsobilo co nejmenší škodu. Zkontrolovat, jestli zálohy opravdu fungují. Mít aktuální software. Používat antivir. V zařízení mít vždy software a programy, co doopravdy používám.“*

**Petr Špringer***: „Používat heslo, které je silné, kombinace číslic, písmen a speciálních znaků, tím se zvyšuje bezpečnost, v ideálním případě na každou službu jiné heslo. Dříve se doporučovalo každý rok heslo změnit, ale od toho se už tak nějak opustilo. Používat dvoufaktorovou autentizaci, někteří experti říkají, že použití SMS zprávy už není příliš bezpečné z důvodu, že jde převzít kontrolu nad číslem, ale to nehrozí u běžných uživatelů. Je možný tzv. SIM swaping, útočník přesvědčí telekomunikační společnost, že je majitelem čísla, a přesvědčí je, aby přepnuli číslo na jiné zařízení.“*

Tímto bych chtěl oběma pánům velice poděkovat za poskytnutí tohoto zajímavého a přínosného rozhovoru do bakalářské práce.

# 10 Diskuse k etiologii a fenomenologii počítačové kriminality a k navrhovaným opatřením

Během zpracovávání této práce jsem se snažil přijít na hlavní příčiny, tedy co je hlavním motivem páchání této kriminality.

Martin Kunc v rozhovoru uvedl, že podle něj jsou příčiny této kriminality „ *1) vlastní obohacení, 2) špionáž ať už korporátní nebo státní (nebo jak se jí říká) 3) vandalismus"*[73]

Smejkal uvádí: „*Motivem bývá nejčastěji osobní obohacení, ale jsou známy i další časté motivy, patří k nim zejména pocit převahy nad zaměstnavatelem či veřejnými orgány, pocit beztrestnosti, snaha kompenzace nespokojenosti s prací, názor, že firmě nemohou uškodit malé ztráty a touha po riziku."*[74]

Dle mého shrnutí vede pachatele k páchání počítačové kriminality nejčastěji osobní obohacení, touha pachatele o vlastní zviditelnění, neoprávněný prospěch, získání informací jak pro osobní potřebu, tak pro průmyslovou špionáž, snadný zisk, touha ublížit jinému, pocit převahy nad zaměstnavatelem či veřejnými orgány, pocit beztrestnosti, snaha kompenzace nespokojenosti s prací, dokonce i názor, že firmě nemohou uškodit malé ztráty a touha po riziku. Počítačů lze užít jako prostředku pro vydírání, nebezpečné pronásledování a kyberšikanu. Mezi další patří šíření dětské či jiné pornografie. Prostředek k získání nelegálních prostředků na tzv. internetové podsvětí nazvané „Dark Net", na kterém lze např. nelegálně zakoupit zbraně či drogy. Hlavní „výhodou" a důvodem kyberkriminality je, že pomocí sítě můžou pachatelé provádět útoky či jiné páchání na dálku, tedy odkudkoli na světě. Výsledkem je celkově malý počet zjištěné kriminality, na rozdíl od té skryté. Tedy velká pravděpodobnost, že se na daný útok nebo čin vůbec nepřijde.

To uvádí i Jirovský:*„Útočník nebo pachatel pracuje v globálním prostředí, může se v kyberprostoru velmi rychle a nepozorovatelně pohybovat, měnit identity nebo i mizet."*[75]

V kapitole **7.2** , kde byly analyzovány policejní statistiky za posledních deset let, tedy od roku 2009 do roku 2019, vždy od 1. ledna do 31. prosince daného roku, konkrétně vybrané trestné činy související s počítačovou kriminalitou § 230-232 TZ76 bylo prokazatelně zjištěno, že dochází ke každoročnímu nárůstu této kriminality. A to ve velké

[73] Rozhovor v této bakalářské práci
[74] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. s. 135.
[75] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007. s. 19.
[76] Zákony pro lidi. *Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

míře. Od roku 2009 do roku 2019 byl sedmnáctinásobný nárůst. V roce 2009 bylo zjištěno pouhých 62 trestných činů a za rok 2019 jich bylo zjištěno 1092. Průměrná objasněnost za celé desetileté období se pohybuje okolo 29,8%. Překvapením ze statistiky je, že pomocí idexu bylo zjištěno, že **6,73%** z celkového počtu trestných činů bylo spácháno dětmi. Kdežto podíl dětí na celkové kriminalitě je pouze **3,6%**. Podíl počítačové kriminality na celkové kriminalitě v ČR je **0,22%,** což není nijak závratné číslo, ale postupem času se podíl zvětšuje.

Další věcí, která však víceméně souvisí s vývojem dané oblasti, je i rozvoj konkrétních zařízení, která mohou být v rámci kyberkriminality zneužita. Zatímco dříve nebylo standardem mít doma vlastní stolní počítač, dnes je zpravidla v běžné rodině i více než jeden počítač, dále pak notebooky, tablety, chytré mobilní telefony.

Obecně se pak domnívám, že by bylo vhodné zlepšit osvětu mezi běžnými uživateli informačních technologií. Nepopiratelně existuje mnoho informačních zdrojů, ať už přímo internetových nebo z jiných médií, nicméně je otázkou, nakolik jsou dostupné pro běžné uživatele. Respektive je otázkou, nakolik se jimi běžný uživatel zabývá a nepovažuje je pouze za zbytečné plýtvání jeho časem. Jak jsem již navrhl v textu práce, domnívám se, že v případě dětí by bylo vhodné této problematice věnovat zvýšenou pozornost ve škole v rámci relevantních předmětů. Varovat je hlavně před možnými hrozbami, které zde hrozí. Vysvětlit základní pravidla u materiálů podléhajícím licenčnímu nebo duševnímu vlastnictví, tedy u filmů, hudby, programů, obrázků, atd. U ostatních sociálních skupin je toto mírně problémovější, neboť neexistuje prostředek, který by donutil uživatele dbát na jeho „kybernetickou bezpečnost“ – snad vyjma používání informačních technologií v zaměstnání, kde se dá předpokládat zájem zaměstnavatele na prevenci kyberkriminality. Ale to se nedotkne celé této skupiny a spíše je nutno se zaměřit na hrozbu pro tyto jedince, kteří můžou uvěřit podvodným emailům a naletět podvodníkům nebo mohou nevědomě šířit pirátské kopie souborů. Tento problém se nedá ale zcela vyřešit. A je jednoduchá odpověď proč tak činit. Protože rychlost, kterou se stále rozvíjí a zdokonaluje IT technologie a s ní spojené hrozby a další možnosti útoků a podvodů, se zvyšuje. Je ale možné tento problém, i když ne , ale z větší části eliminovat a v maximální možné míře potlačit.

# 11 Návrhová opatření

Hlavním opatřením, jak se chránit, abychom se nestali obětí počítačové kriminality je hlavně obezřetnost a maximální zabezpečení svých zařízení, která jsou připojena k internetu, tedy ta, která mohou být napadena vzdáleně odkudkoli ze světa, ať už se jedná o ta v naší domácí síti, veřejné síti např. v kavárně, zaměstnání nebo hromadné dopravě. U zařízení, může jím být chytrý mobilní telefon, tablet nebo laptop, je důležité mít spolehlivý, a hlavně aktuální antivir, který chrání zařízení. Právě ten, když už k nějakému útoku dojde, zabrání škodám, ke kterým by mohlo dojít. Zároveň je potřeba mít i aktuální verzi softwaru v zařízení. Jak již bylo zmíněno, doporučuje se pozorně kontrolovat elektronickou komunikaci, kdo nám email, fotku,posálá přes sociální sítě nebo cokoli jiného posílá, zda toho člověka známe a můžeme mu věřit. Aby nedocházelo k našemu zastrašovaní pomocí Hoax nebo jiné dezinformaci, je důležité sledovat zdroj odkud autor článku čerpá, zda se jedná o důvěryhodný zdroj a můžeme mu věřit. To bylo opatření spíše pro koncové uživatele, ti ale jsou největší a nejzranitelnější skupinou, i když si člověk řekne, že nemůže být pro hackera důležitý, tím se hluboce mýlí. Právě tito obyčejní uživatelé, jako jsme my lidé, a ne velké firmy a korporace, jsme snazším cílem něž větší firma nebo holding, který investuje nemalé peníze do zabezpečení svých systémů a sítí.

Dalším aspektem, který je zmiňován i v rozhovoru s experty, je potřeba zlepšit osvětu mezi běžnými uživateli informačních technologií, už od základních škol je potřeba se věnovat bezpečnosti na internetu v rámci relevantních předmětů. U ostatních sociálních skupin je toto mírně problémovější, neboť neexistuje prostředek, který by donutil uživatele dbát na jeho „kybernetickou bezpečnost“ – snad vyjma používání informačních technologií v zaměstnání, kde se dá předpokládat zájem zaměstnavatele na prevenci kyberkriminality.

# Závěr

Počítačová kriminalita je velmi obsáhlé a aktuální téma a vyžaduje znalosti z trestního práva, kriminologie a prevence kriminality, ale i technické znalosti v oblasti kyberprostoru.

V úvodu této práce byl vysvětlen význam počítačové kriminality, její vznik, jakými prostředky k ní dochází a základní vymezení pojmů. Dále pak základní společné znaky počítačové kriminality. V další kapitole došlo k vymezení pojmů jako kyberprostor a jeho vznik, jeho původ z Arpanetu. S tím úzce souvisí i vznik internetu, proto byla jedna celá kapitola věnována pouze tomuto známému pojmu, bez kterého si dnes již neumíme náš život představit. Nevynechali jsme ani zavedení internetu u nás v ČR, jeho začátky a rozvoj. Od čtvrté kapitoly jsem se již věnoval formám počítačové kriminality, kdy z prostředku běžného života se stal nástroj pro páchání trestné činnosti. Zde jsou i zahrnuty podkapitoly, kde jsou uvedeny formy jakými lze počítačovou kriminalitu páchat, a i přes to, že kapitola je obsáhlá, tak neobsahuje úplně všechny formy, ale pouze ty nejznámější a nejvíce využívané způsoby jako je hacking, hoax, warez, cracking, phishing počítačové pirátství, kyberšikanu a její druhy. Další velkou kapitolou je kyberterorismus, v této kapitole je vysvětlení tohoto pojmu a jeho vymezení s příklady. Významnou kapitolou je Darknet, tedy část temného internetu, kam není umožněn přístup každému, pokud tedy k tomu nevyužije speciální prostředky. Jednou z nejdůležitějších kapitol této práce je fenomenologie počítačové kriminality, kde jsou podrobně rozebrány jejich skutkové podstaty a provedena analýza statistických dat za posledních deset let. V kapitole osm jsou shrnuty hlavní příčiny počítačové kriminality z rozhovoru a literatury, tedy co pachatele vede k jejímu páchání. V rámci této práce byl proveden rozhovor s bezpečnostním analytikem Martinem Kuncem a Petrem Špringerem, specialistou počítačové bezpečnosti z CZ.NIC. Předposlední kapitola je věnována diskuzi, kde bylo provedeno shrnutí práce a její objasnění. V poslední kapitole jsou zpracována návrhová opatření k této problematice.

Cíle této práce byly objasnit základní pojmy, zejména pojem počítačová kriminalita, objasnit její příčiny, analyzovat nejčastější nelegální konání proti počítačům nebo páchané na počítači nebo prostřednictvím počítače, zpracovat fenomenologii počítačové kriminality za posledních deset let a navrhnout příslušná opatření, která by měla směřovat ke snížení počítačové kriminality. Dle mého názoru byly cíle bakalářské práce splněny.

# Seznam použitých zdrojů

## Literární zdroje


BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014. 43 s. ISBN 978-80-904864-9-2.

CRAIG, Paul P. a Ron HONICK. *Softwarové pirátství bez záhad*. Praha: Grada, 2008. 212 s. ISBN 978-80-247-1765-4.

ČECH, Ondřej a Nicole ZVONÍČKOVÁ. *Nebezpečí kyberšikany: internet jako zbraň?*. České Budějovice: Theia - krizové centrum, 2017. 131 s. ISBN 978-80-904854-4-0.

ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem.* Praha: Grada, 2013. 150 s., Psyché (Grada). ISBN 978-80-210-6374-7.

ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013. 224 s. ISBN 978-80-251-3804-5.

HATCH, Brian, James LEE a George KURTZ. *Linux - hackerské útoky: bezpečnost Linuxu - tajemství a řešení*. Praha: SoftPress, c2002. 576 s. ISBN 80-86497-17-8.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. 217 s. ISBN 978-80-7387-545-9.

JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. 524 s., CZ.NIC. ISBN 9788088168157.

MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.

McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. 232 s. ISBN 978-0313339745

PEKÁREK, Oldřich a Vladimír ČÍŽEK. *Práce s agenturními a elektronickými informacemi* [online]. České Budějovice: Vysoká škola evropských a regionálních studií, 2007. 138 s., [cit. 2020-04-20]. ISBN 978-80-86708-40-9.

ROGERS, Vanessa. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty*. Praha: Portál, 2011. 104 s. ISBN 978-80-7367-984-2.

ROSENZWEIG, Paul. *Cyber warfare: how conflicts in cyberspace are challenging America and changing the world*. Santa Barbara, Calif.: Praeger, c2013. 290 s. ISBN 9780313398964.

SMEJKAL, Vladimír. *Internet a §§§*. Praha: 2. aktualizované a rozšířené vydání, Grada, 2001. 284 s. ISBN 8024700581.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. 636 s., Pro praxi. ISBN 78-80-7380-501-2.

SVATOŠ, Roman. *Kriminologie ve světle nového trestního zákoníku*. České Budějovice: Vysoká škola evropských a regionálních studií, 2010. 174 s. ISBN 978-80-86708-21-8.

ŠÁMAL, Pavel. *Trestní zákoník*: komentář.2. vyd. Praha: C.H. Beck, 2012. 3632 s., Velké komentáře. ISBN 9788074004285.

**Elektronické zdroje:**

Jak se připojit na neviditelný internet, *idnes.cz* 14. června 2016 © 2020 [cit. 29.01.2020] Dostupné z https://www.idnes.cz/technet/software/jak-se-pripojit-na-neviditelny-internet.A160602_150524_tec_technika_baha

Počítačová kriminalita - Policie České republiky. *Úvodní strana - Policie České republiky* [online]. Copyright © 2019 Policie ČR, všechna práva vyhrazena [cit. 30.01.2020]. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

Darknet – podsvětí internetu – oTechnice.cz. *oTechnice.cz – Nejnovější zprávy ze světa technologií* [online]. Copyright © 2020 [cit. 29.01.2020]. Dostupné z: https://otechnice.cz/darknet-podsveti-internetu/

Kybernetická kriminalita IV*: Hacktivismus a kyberterorismus*. [online]. Copyright ©2011 [cit. 08.12.2019]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php

Vybrané typy kyberšikany a její preventivní opatření. *Medium – Get smarter about what matters to you.* [online]. Dostupné z: https://medium.com/edtech-kisk/vybran%C3%A9-typy-kyber%C5%A1ikany-a-jej%C3%AD-preventivn%C3%AD-opat%C5%99en%C3%AD-bbd1254eb227

IP adresa – Wikipedie. [online]. Copyright © 2020 [5.4, 2020]. Dostupné z https://cs.wikipedia.org/wiki/IP_adresa

Kybernetický terorismus, kyberterorismus - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 05.12.2019]. Dostupné z: https://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx

Kriminalita - Policie České republiky. *Úvodní strana - Policie České republiky* [online]. Copyright © 2020 Policie ČR, všechna práva vyhrazena [cit. 20.04.2020]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx?q=Y3BpPTE%3d

Bezpečný internet | Sítě peer-to-peer. *Bezpečný internet | Rady pro bezpečnost na internetu* [online]. Copyright © [cit. 08.02.2020]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/site-peer-to-peer.aspx

HOAX | Phishing | Co je to phishing. [online]. [cit. 30.01. 2020] Dostupné z: WWW https://www.hoax.cz/phishing/co-je-to-phishing

## Legislativní dokumenty

*Zákon č. 40/2009 Sb., trestní zákoník* [online]. © AION CS, s.r.o. 2010-2020 [cit. 10.03.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

*Zákon č. 121/2000 Sb*. Autorský zákon. © AION CS, s.r.o. 2010-2020 [cit. 22.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121

*Zákon č. 181/2014 Sb.* Zákon o kybernetické bezpečnosti © AION CS, s.r.o. 2010-2020 [cit. 22.04.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

## Ostatní zdroje:

**Rozhovor** s experty na počítačovou bezpečnost.

Martin Kunc

Bezpečnostní analytik (Security analyst)

CZ.NIC

Petr Špringer

Specialista počítačové bezpečnosti

CZ.NIC

# Seznam tabulek a grafů