Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Vnímání a prevence kyber kriminality na základní škole

Mgr. Tomáš Daňhelka

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Mgr. Tomáš Daňhelka

Informatika

Název práce

Vnímání a prevence kyber kriminality na základní škole

Název anglicky

Perception and Prevention of Cyber Crime at Elementary School.

Cíle práce

Cílem práce je popsat vnímání informační kriminality mezi dětmi a jejich rodiči a porovnání se stávajícím právním řádem. Dále se práce zaměří na prevenci prováděnou organizací Safer internet ve školách, zda prevence ze strany organizace Saferinternet je zaměřená na aktuální problémy informační kriminality. Výstupem práce bude doporučení, kterým směrem zaměřit prevenci v oblasti informační kriminality u dětí školního věku.

Metodika

Budou shromážděny informace z literatury a dalších možných zdrojů. Bude proveden dotazníkový výzkum, týkající se vnímání informační kriminality mezi dětmi. Po analýze situace bude provedena syntéza poznatků, která vyústí v obecná doporučení týkající se této problematiky a shrnutí případných nedostatků na základních školách.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Informační kriminalita, počítačová kriminalita, trestný čin, čin jinak trestný, prevence, internet, saferinternet.cz, vnímání informační kriminality, trestní zákoník, trestní řád, základní školy

---

Doporučené zdroje informací

CRAIG, Paul, HONICK, ROn, Softwarové pirátství bez záhad, Praha: Grada, 2008, 212 s
MATĚJKA, Michal, Počítačová Kriminalita, Praha: Computer Press, 2002, 106 s
POLČÁK R., Internet a proměny práva, vyd. Praha: Auditorium, 2012, ISBN: 978-80-87284-22-3
POLČÁK R., Právo na internetu, vyd. Brno: Computer Press, a.s., 2007, ISBN: 978-80-251-1777-4
POŽÁR J., Základy teorie informační bezpečnosti, vyd. Praha: Policejní akademie ČR, 2007, ISBN: 978-80-7251-250-8
SMEJKAL V., SOKOL T., VLČEK M., Počítačové právo, vyd. Praha: Beck, 1995, ISBN: 80-7179-009-5
Trestní zákoník včetně komentářů a důvodové zprávy
Zákon o soudnictví ve věcech mládeže

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 29. 03. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Vnímání a prevence kyber kriminality na základní škole" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2017 _____

Poděkování

Rád(a) bych touto cestou poděkoval(a) Ing. Tomáši Vokounovi a RNDr. Dagmaře Brechlerové, Ph.D., za vedení práce, dále koordinátorce prevence kriminality hl. m. Prahy Mgr. Janě Štoskové a koordinátorovi prevence kriminality Středočeského kraje JUDr. Milanu Fárovi za spolupráci, své ženě za přínosné připomínky a podporu a všem metodikům prevence na jednotlivých školách, které se zúčastnili výzkumu.

Vnímání a prevence kyber kriminality na základní škole

Souhrn

Diplomová práce se věnuje vnímání a prevenci kybernetické kriminality mezi žáky základní školy. V teoretické části práce definuje pojem kyberkriminalita, popisuje formy kyberkriminality a jejich právní definici a související legislativu. Dále práce popisuje systém prevence kriminality v České republice se zaměřením na základní školství a největší organizace působící v oblasti prevence kyberkriminality.

V praktické části je provedena analýza statistických výstupů Policie ČR s příznakem kyberkriminalita, dále práce popisuje výzkum provedený mezi žáky druhého stupně základní školy na území hlavního města Prahy a Středočeského kraje se zaměřením na okruhy otázek, co žáci považují za kyberkriminalitu a jaké kyberkriminality se sami dopouštějí. Ve svém závěru práce porovnává zjištěné výsledky s popsanými preventivními programy a vyvozuje doporučení, jakým směrem preventivní programy v oblasti kyberkriminality zaměřit.

Klíčová slova: kybernetická kriminalita, kyberkriminalita, prevence, základní škola, E-bezpečí, Seznam se bezpečně!, Safer internet, dotazník, Policejní internetová hotline, ESSK

Perception and Prevention of Cyber Crime at Elementary School

Summary

This thesis is about perception and prevention of cyber crime by primary school pupils. In the theoretical part it defines the term cyber crime, describes its types, their definition by law and legislation related to them. The thesis furthermore describes the system of crime prevention in the Czech Republic with focus on primary education and the largest organizations active in the field of cyber crime prevention.

In the practical part there is an analysis of statistical outcomes with the cyber crime index gained by Police of the Czech Republic. The thesis also describes a research conducted among pupils from upper primary schools in Prague and Central Bohemia with focus on groups of questions about what the pupils understand under cyber crime and what kind of cyber crimes they commit themselves. In the conclusion there is a comparison of research results with the described preventive programmes and a recommendation which way should they go what cyber crime concerns.

Keywords: cybernetic crime, cyber crime, prevention, primary school, E-bezpečí, Seznam se bezpečně!, Safer internet, questionnaire, Police internet hotline, ESSK

Obsah

1 Úvod

Počítače a výpočetní technika zasahují stále do více oblastí našeho života a mnoho činností si již bez nich nedokážeme představit. Generace X, k níž se počítám i já, zažila překotný rozvoj této techniky, kdy vyrůstala ještě bez počítačů, mobilního internetu v každém telefonu. Musela se naučit nové dovednosti, které jsou pro dnešní mladou generaci již samozřejmé. Občas se dnešní děti zeptají, co jsme dělali jako děti my, jak jsme si chatovali s kamarády a je pro ně nepředstavitelné, že nebyly žádné mobilní telefony ani internet.

Děti by se měly učit používání výpočetní techniky, chování na sociálních sítích nebo bezpečné používání facebooku od rodičů, ale ti často těmto věcem zcela nerozumí, také se je učí používat za pochodu. Nestíhají sledovat tento vývoj a děti svými dovednosti v oblasti informačních a komunikačních technologií často předčí své rodiče. Bohužel se však děti sami naučí jen to, co je zajímá. Umí hrát hry, umí si posílat obrázky přes snapchat a mají několik set přátel na facebooku, ale neznají zásady bezpečné práce. Neuvědomují si například, že cokoliv nahrají na internet, zůstane někde uchováno, i když to později ze svého profilu odstraní, a že při komunikaci s jejich virtuálním kamarádem nemusí být na druhé straně skutečně ten, za koho se vydává. Nedostatečný výchovný prvek rodičů by tedy měla zastoupit škola, ale i zde učí učitelé, kteří se naučili používat výpočetní techniku teprve nedávno, mnozí z nich neměli možnost absolvovat výuku informační gramotnosti a její didaktiku v rámci svých pedagogických studií. S ohledem na stav financí ve školství je celkově problém pro školy sehnat zkušené a kvalifikované informatiky, či učitele jiných předmětů, kteří by rozuměli zároveň i problematice informační a výpočetní techniky. Domnívám se, že sami rodiče by měli dětem již od věku, kdy jim půjčí na hraní první tablet nebo telefon, vštěpovat zásady chování s touto technikou, co se na ní může a nesmí dělat, a nepoužívat jí pouze k zabavení času svých dětí.

Při výběru tématu diplomové práce jsem využil své zkušenosti a kontakty ve školách, neboť jsem čtyři roky učil předmět Informatika na druhém stupni základní školy, a pět let jsem působil jako lektor kurzu počítačové gramotnosti pro dospělé. Nyní jako policista pracuji na oddělení informační kriminality. V tématu své diplomové práce jsem se rozhodl spojit tyto dvě pracovní zkušenosti a pokusit se nahlédnout do toho, co děti vědí o

kyberkriminalitě. Jako rodič jsem absolvoval několik seminářů týkající se bezpečného chování na internetu, sledoval jsem různé kurzy a navštívil několik konferencí. Co mne zaujalo, byl fakt, že valná většina preventivních programů hovořila o dítěti na internetu jen jako o potenciální oběti. Děti se učí, co vše jim tam hrozí, čeho se mají vyvarovat. Ale ve své současné práci vidím, že děti jsou sami pachatelé, v oblasti kybernetické kriminality výrazně častěji, než v jiných oblastech. Když s dětmi ze základní škole hovořím na toto téma, zjišťuji, že tolerance k závadovému chování na internetu je vysoká.

Rozhodl jsem se tedy zjistit, zda je prevence v oboru kybernetické kriminality zaměřená na aktuální problémy, zda řeší aktuální témata. Dále zda žáci mají povědomí o tom, co je kybernetická kriminalita a zda se toho jednání sami dopouštějí. Zpočátku jsem měl v úmyslu nabídnout výsledky práce organizaci Safer internet[1], se kterou spolupracovala moje původní vedoucí diplomové práce jako odborný garant, a která mne na toto téma přivedla. Během přípravy jsem při zjištění rozsahu očekávaném výzkumu začal hledat nějaký další subjekt, který by výsledky práce mohl přímo využít. Při hledání jiného subjektu, se kterým bych mohl spolupracovat, jsem se spojil s krajskými metodiky prevence v Praze a ve Středočeském kraji. Těmto se téma práce líbilo a byli vděčni za to, že jim někdo provede výzkum mezi žáky, protože sami nemají v této oblasti žádné informace, ze kterých by mohli dále vycházet. Sami přišli s návrhem, zda by se výzkum nedal využít i pro organizaci Kraje pro bezpečný internet, že by mohlo být zajímavé následně srovnat znalosti a chování dětí v jednotlivých krajích, protože jednotlivé kraje přistupují k prevenci různě a chybí zde srovnání účinnosti jednotlivých preventivních programů.

Jako autor diplomové práce jsem rád, že moje práce bude prakticky využitelná – pomůže dalším lidem podílejícím se na prevenci u žáků základních škola a pravděpodobně přinese i možnost v daném tématu pokračovat dále, například formou výzkumného grantu, nebo přednášek.

[1] http://www.saferinternet.cz/o-nas/10-o-nas.html

2 Cíle práce a metodika

2.1 Cíl práce

Cílem diplomové práce je popsat vnímání kybernetické kriminality u žáků základní školy a analyzovat stávající preventivní programy v této oblasti, zda jejich zaměření odpovídá nejvíce páchané kybernetické kriminalitě. Výsledkem práce bude doporučení, na která témata by bylo vhodné zaměřit pozornost při přípravě preventivních programů. Výsledky dotazníkového šetření budou poskytnuty krajským metodikům prevence, kteří je využijí pří přípravě a výběru vlastních preventivních opatření. Doposud krajští metodikové nemají k dispozici žádná data, na základě kterých by mohli ověřit znalosti žáků, ani zpětnou vazbu, zda preventivní programy ve školách již používané mají nějaký efekt.

V současné době je v jednání možnost budoucího rozšíření výzkumu na celorepublikový projekt pro potřeby organizace Kraje pro bezpečný internet, proto je bráno dotazníkové šetření také jako pilotní, s možností ověřit proveditelnost takovéhoto výzkumu ve větším měřítku.

2.2 Metodika

V teoretické části práci bude provedena rešerše literatury, na základě které bude vytvořen teoretický základ práce. Bude charakterizován pojem kybernetické kriminalita, stanovena právní kvalifikace tohoto pojmu a budou představeny některé organizace, které mají za cíl preventivní působení v oblasti kyberkriminality.

V praktické části bude provedena analýza –(jak kvantitativní, tak kvalitativní) statistických údajů týkajících se kyberkriminality získané od Policie České republiky, ze kterých bude získán obraz momentálně páchané kyberkriminality. Dále bude proveden výzkum kvantitativním dotazníkovým šetřením mezí žáky druhého stupně základní školy s cílem zjistit, o čem se žáci domnívají, že je kybernetická kriminalita, respektive jaké jednání ve vztahu k internetu, sociálním sítím a počítačům je trestné a dále jakého jednání se přímo sami žáci dopouštějí.

V závěru práce budou porovnány výsledky dotazníkového šetření s výsledky analýzy statistických údajů a budou vyvozeny závěry, v kterých oblastech mají žáci špatné povědomí o kyberkriminalitě a jakým směrem zaměřit preventivní programy.

3 Teoretická část

3.1 Vymezení pojmu Kybernetická kriminalita a dalších pojmů

Tato diplomová práce se věnuje kybernetické kriminalitě a hovoří o počítačové, respektive o informační a komunikační technice. Jedná se o velice rychle se rozvíjející obor, kde je dosud nejednoznačné názvosloví. Jde sice o pojmy v hovorové mluvě často používané, avšak někdy v nesprávných souvislostech. Časté je také zaměňování podobných pojmů, například data a informace, případně počítačová a kybernetická kriminalita.

Proto se v první kapitole zaměříme na definování důležitých pojmů. Kde to bude možné, pokusíme se čerpat ze zákona nebo technické normy a nalézt obecně platné definice.

3.1.1 Pojem kybernetická kriminalita

Počítačová technika v současné době zasahuje prakticky do všech oborů lidské činnosti. Dříve byly počítače jasně definovaná zařízení, které nebyl problém popsat. Počítač měl svoji definici, skládal se z předem definovaných součástí. Dnes nalezneme miniaturizované počítače u téměř každého elektronického zařízení, často o tom ani nevíme. Jak roste rozšíření počítačů, roste i množství trestné činnosti páchané na nich a s jejich pomocí. Je proto nutné nějak tuto trestnou činnost pojmenovat. Pro tento typ trestné činnosti se používalo velké množství pojmů, například „počítačová kriminalita“, „informační kriminalita“, „internetová kriminalita“ nebo „kybernetická kriminalita“. Poslední uvedený pojem je nejčastěji užíván v současné době a bude používán i v této práci.

Pojem kybernetická kriminalita je často zaměňován s ostatními podobnými pojmy, avšak tyto názvy nejsou synonymy. Každý má svůj jiný obsah, často se tyto pojmy překrývají. Je to způsobené tím, že dlouhou dobu nebyl pojem kybernetické kriminality definován, a dále tím, že názvosloví často pochází ze zahraničích výrazů a z překladů těchto pojmů. Jako první se ustálil pojem „počítačová kriminalita“ a to v 90. letech 20. století. V naší literatuře definuje autor Vladimír Smejkal počítačovou kriminalitu jako: „*páchání trestné činnosti, v niž figuruje počítač jako souhrn hardwarového a softwarového vybavení včetně dat, případně některá k komponent, případně větší množství počítačů*

samostatných nebo propojených do sítě a to buď jako předmět této trestné činnosti (tj. cíl, oběť zločinného útoku), ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité, nebo jako nástroj trestné činnosti“[2].

Takto popsaná definice však popisuje jen jednání, které je provedeno z počítače (nejčastěji PC) nebo proti počítači. V dnešní době lze tyto činnosti provádět i s jinými zařízeními, ať již pomocí mobilních telefonů, tabletů či herních konzolí. Proto se pojem „počítačová kriminalita“ v odborné literatuře již nepoužívá. Místo pojmu „počítač“ se dnes v této souvislosti využívá pojem „informační a komunikační technologie“ (Information and Comunation Technology), což je ona hojně využívaná zkratka ICT.

Přechod od pojmu počítačová kriminalita k rozšířenějšímu pojetí je znát například již v roce 2000 na definici počítačové kriminality jak jí vydala Rady Evropy: „*Trestný čin namířený buď proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je použito moderních informačních či telekomunikačních technologií*“[3].

V roce 2001 se začíná v mezinárodních úmluvách již plně užívat pojem se „Cyber Crime“, což lze přeložit přesně jako „Kyber Zločin“, užívá se však překlad „Kybernetická kriminalita“ nebo „Kyberkriminalita“. V tomto roce byla také vydána v této oblasti velmi důležitá Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001, která definovala základní pojmy a nastínila skutkové podstaty kybernetických trestných činů. Jedná se o velmi různorodou směsici trestných činů, spojených společným prostředím, kde je tato trestná činnost páchána nebo předmětem útoku. Toto označení tedy můžeme chápat jako skupinové označení, obdobně jako například kriminalitu mladistvých nebo násilnou kriminalitu.

Velmi obecně definuje kybernetickou kriminalitu autor Václav Jirovský jako: „*jakýkoliv čin, směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených.*[4]“

[2] SMEJKAL, Vladimír, Internet @ §§§, str. 64
[3] MATĚJKA, Michal, Počítačová kriminalita, str. 5
[4] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 91

Je však potřeba říct, že ne každé nežádoucí jednání namířené proti informační a komunikační technologii lze postihnout jako trestný čin, nebude jednat pokaždé o kriminální jednání. Chceme-li hovořit o kriminalitě, musíme si ji definovat. Jedná se „*souhrn o soubor všech jednání, která lze podřadit pod některou skutkovou podstatu, upravenou trestním zákonem. Podle tohoto vymezení tedy nejsou kriminalitou taková jednání, která nenaplňují žádnou skutkovou podstatu trestného činu, tedy ani přestupky či jiné správní delikty*“[5].

Tato jednání, která nejsou postižitelná podle trestního nebo přestupkového zákona nejsou definována jako kybernetická kriminalita, protože nejsou kriminalitou vůbec. Jsou však s touto kybernetickou kriminalitou propojeny a často mohou pomoci k jejímu pochopení a objasnění.

V literatuře najdeme velké množství různých verzí definic kybernetické kriminality i obsahu tohoto pojmu, z naší literatury můžeme uvést například autory T. Gřivnu[6], J. Koloucha, V. Jirovského[7] nebo R. Polčáka[8]. Vycházíme-li z této literatury, můžeme kybernetickou kriminalitu definovat následovně. Literatura dále užívá totožný pojem kyberkriminalita, či jeho kratší podobu kybernalita[9].

Pod kybernetickou kriminalitu řadíme:

- **Trestné činy směřující proti důvěrnosti, integritě a důvěryhodnosti počítačových dat a informačních systémů**
- **Trestné činy využívající informačních a komunikačních technologií pro spáchání tradičních trestných činů**
- **Trestné činy vztahující se k obsahu počítačových dat**
- **Trestní činy vztahující se k autorským nebo obdobným právům**

Policie České republiky definuje nově kyberkriminalitu jako „*trestnou činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí, kdy předmětem útoku je samotná oblast informačních a komunikačních*

[5] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 11

[6] GŘIVNA, Tomáš, POLČÁK, Radim, Kyberkriminalita a právo

[7] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou

[8] JIROVSKÝ Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství

[9] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 270

technologií, nebo kdy je páchána trestná činnost za výrazného využití informačních a komunikačních technologií, jakožto významného prostředku k jejímu páchání[10].“

3.1.2 Technické pojmy související s kybernetickou kriminalitou

Technické pojmy jsou definovány v literatuře daleko častěji než výše uvedená definice kybernetické kriminality. Většina technických pojmů je definována v ČSN normách, případně ve výkladových slovnících či encyklopediích. Práce v přehledu těchto definic cituje převážně z knihy Kybernetická kriminalita autora Josefa Smejkala, který v této knize uvádí, že „*v této publikaci naleznete souhrn všech poznatků teoretických i praktických, k nimž jsem dospěl během své práce za takřka 30 let, kdy jsem se této problematice věnoval v rámci svého působení v justici, jako soudní znalec a jako vysokoškolský pedagog.*[11]“.

3.1.2.1 Informace

Informace je jakékoliv sdělení či zpráva. Autoři definují informace různě, často vzhledem ke svému oboru. V českém právním řádu je informace přímo definována v zákoně č. 106/1999 Sb. „*Informací se pro účely tohoto zákona rozumí jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního.*[12]“ Tato definice však pro potřeby zákona hovoří pouze o zaznamenaných informacích. ČSN norma definuje informaci jako „*Poznatek týkající se jakýchkoliv objektů, např. fakt, událostí, věcí, procesů nebo myšlenek, včetně pojmů, který má v daném kontextu specifický význam.*[13]“ Jednoduše chápe informaci sám Smejkal, který o informaci hovoří jako o „*každém energetickém sdělení, které může mít smysl buď pro toho, kdo je činí, nebo pro toho, kdo je přijímá.*[14]“ Autor dále připomíná, že definice nic nevypovídají o pravdivosti informace.

[10] zdroj: http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09MQ%3d%3d
[11] SMEJKAL, Vladimír, Počítačová kriminalita, str. 16
[12] §3 odst. 3 zák. č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů
[13] Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník. Část 1: Základní termíny
[14] SMEJKAL, Vladimír, Počítačová kriminalita, str. 36

3.1.2.2 Data

Data jsou „*fakta, čísla, události, grafy, mapy, transakce, atd., která byla zaznamenány. Jsou základním materiálem, surovinou pro informace*[15]“ Jsou to jakékoliv prvky, které jsou zaznamenány a které je možné znovu interpretovat. Data nemusí mít pokaždé svoji informační hodnotu.

Data jsou uchovávány na nějakém nosiči dat a bývají obvykle organizována v uceleném souboru dat nebo databázi. Soubor dat je uskupení dat stejného typu, „*Pojmenovaná množina vět uložená nebo zpracovaná jako jednotka*[16].“ Databáze je „*souhrn dat uspořádaných podle pojmové struktury, v níž jsou popsány vlastnosti těchto dat a vztahy mezi odpovídajícími entitami; slouží pro jednu nebo více aplikačních oblastí.*[17]“

3.1.2.3 Informační systém

Zjednodušeně lze označit za informační systém jakýkoliv systém, který zpracovává informace[18]. ČSN norma za informační systém označuje „*systém zpracování informací spolu s návaznými organizačními prostředky, např. personálem, technickými a finančními prostředky; takový systém získává a distribuuje informace.*[19]“ V užší definicích bývá informační systém chápán pouze jako systém pro práci s daty, v širších definicích je pod informační systém zahrnuto i okolí systému, které s ním pracuje, tedy jeho tvůrce a uživatele.

3.1.2.4 Počítač

Počítač je dnes slovo obecně známé, užívané v mnoha pramenech. Původní význam počítač se však postupně rozšiřuje, neboť mezi počítače, či spíše počítačové systémy je třeba chápat i mnohá další elektronická zařízení.

Počítač je definován jako „*funkční jednotka, která může provádět rozsáhlé výpočty, včetně mnoha aritmetických či logických operací, bez zásahu člověka.*[20]“ Funkčně je počítač takové zařízení, které má svoji logickou jednotku, která zpracovává informace,

[15] POŽÁR, Josef, Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, str. 5
[16] Norma ČSN ISO/IEC 2382-1, s. 35
[17] Norma ČSN ISO/IEC 2382-1, s. 34
[18] SMEJKAL, Vladimír, Počítačová kriminalita, str. 41
[19] Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník. Část 1: Slovník, s. 11
[20] Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník. Část 1: Základní termíny

obvykle se jedná o procesor a dále paměťové zařízení, na které se dají ukládat ze kterého se dají číst data a programy. K tomuto základu mohou být přidruženy další periferie, které umožňují vkládání a zobrazení dat, propojení počítače s okolím a další funkce. Počítač je dále tvořen na hardwarem, což jsou fyzické části počítače a softwarem, což je veškeré programové vybavení počítače. Zjednodušeně řečeno můžeme říct, že počítač je jakékoliv o zařízení, které zpracovává informace.

3.1.2.5 Počítačový systém

Dle Smejkala není potřeba počítačový systém definovat zvlášť, neboť v dnešní době je téměř každý počítač počítačovým systémem. Počítačový systém je „*funkční jednotka, sestavená z jednoho nebo více technických zařízení a s odpovídajícím programovým vybavením.*[21]“ Smejkal dále doplňuje, že nejméně jedno technické zařízení by mělo být počítačem[22].

Počítačový systém také definuje Úmluva o kybernetické kriminalitě jako „*jakékoliv zařízení nebo skupinu propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu.*[23]“

Jako příklad počítačového systému můžeme uvést stolní počítače, notebooky, tablety a chytré telefony, ale i herní konzole, chytré televize (které se umí připojit na internet), nebo multimediální systémy v autech. Tento výčet je pouze orientační a slouží pro představu, co vše může být počítačovým systémem. Za počítačový systém můžeme považovat i celý internet.

3.1.2.6 Počítačová síť

Počítačová síť je souhrnné označení pro propojené počítače, či obdobná technická zařízení, které spolu mohou komunikovat. Definice dle ČSN normy je to „*síť uzlů zpracování dat, které se při datové komunikaci propojí.*[24]“ Uvedená definice je velmi obecná. Známe velké množství různých typů sítí, dle jejich využití, použité technologie,

[21] SMEJKAL, Vladimír, a kol. Právo informačních a telekomunikačních systémů, str. 43
[22] SMEJKAL, Vladimír, Počítačová kriminalita, str. 25
[23] Úmluva rady Evropy č. 185 o kybernetické kriminalitě ze dne 23.listopadu 2001, kapitola I, Článek 1 - Definice
[24] Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník. Část 1 – Základní termíny, str. 15

topologie atd. Základní dělení sítí, které bude pro nás důležité, je na lokální sítě (LAN) a vzdálené sítě (WAN)

Lokální síť LAN (Local Area Network) je počítačová síť tvořená většinou několika počítači v omezené oblasti. Typický příklad je síť doma, ve škole, nebo ve firmě. Smejkal uvádí definici dle Slovníku výpočetní techniky jako „*Skupinu počítačů a jiných zařízení, rozptýlených v relativně omezené oblasti a spojených komunikační linkou, která umožňuje každém zařízení komunikovat s jakýmkoliv jiným zařízením v síti.*[25]“

Vzdálená síť WAN (Wide Area Network) je počítačová síť, která spojuje počítače na delší vzdálenosti a která propojuje jednotlivé lokální sítě mezi sebou, nepřipojují se k ní jednotlivé počítače přímo. Dle definice se jedná o „*Komunikační síť, která spojuje geograficky oddělené oblasti.*[26]“ Typickým příkladem této sítě je právě Internet. Pro naše potřeby není nutné rozlišovat další typy sítí, postačíme si s tímto základním rozdělením.

3.1.2.7 Internet

Internet je „*celosvětový počítačový systém navzájem propojených počítačových sítí, které spolu komunikují prostřednictvím protokolu TCP/IP.*[27]“ Právně však internet jako takový není nijak definován, Smejkal ho ve své literatuře přirovnává k médiu nebo fyzikální veličině, jako jsou například elektromagnetické vlny, které také využíváme, ale nikomu nepatří. Naše právní normy s pojmem internetu pracují, běžně ho používají, ale není nikde definován.

Internet jako takový nemá právní subjektivitu, nelze ho zařadit mezi hmotné, ani nehmotné statky. Také nepatři žádnému majiteli, pouze jeho jednotlivé části, například servery nebo přípojné body mohou mít konkrétního majitele, který je spravuje. Fungování internetu je z větší části na bázi dobrovolnosti a řídí se definičními normami, které vytváří definiční autority.

Definiční normy jsou normy, které vymezují fungování internetu jako takového. Jsou definovány ve vrstvách, které jsou na sobě závislé. Definiční autority jsou fyzické nebo právnické osoby, které určují, jak bude jimi spravovaná část internetu fungovat, každý poskytoval služeb na internetu je zároveň i definiční autoritou. Význačné postavení

[25] Slovník výpočetní techniky. Microsoft Press, česky Plus s.r.o., Praha, 1993, str. 220
[26] Slovník výpočetní techniky. Microsoft Press, česky Plus s.r.o., Praha, 1993, str. 395
[27] SMEJKAL, Vladimír, Počítačová kriminalita, str. 58

mezi nimi má organizace ICANN, která řídí přidělování a správu doménových jmen a stanovuje pravidla pro využívání systému doménových jmen. „*Specifikem internetu je, že existuje právě jen díky definičním autoritám. Je z nich složen. Žádné operace se neuskuteční bez účasti (provedení či zprostředkování) definiční autority.*[28]*“* Právně podléhají jednotlivé definiční autority, nebo jednoduše poskytovatelé služeb na internetu, právnímu systému státu dle svého sídla. Platí zde však zásada, že pokud poskytovatel služeb neměl ponětí o tom, že poskytovaná informace na internetu je protiprávní, je zbaven své odpovědnosti[29].

3.1.2.8 Kyberprostor

Kyberprostor je novým stále vyvíjejícím se prostředím. Pojem pochází z vědecko-fantastické literatury 80. let., kdy tento pojem užíval William Gibson, zakladatel literárního žánru kyberpunk. Ten použil pojem kyberprostor (Cyber space) pravděpodobně poprvé ve své povídce „Vypálit chrom“, více pak v románu „Neuromancer“, který detailně popisuje kyberprostor, virtuální realitu a chování lidí v nich. Gibson popisuje kyberprostor jako alternativní svět, celý tvořený a ovládaný lidmi a jejich myšlenkami. Gibson pro kyberprostor užívá pojem „matrix“. Uživatelé se připojovali do tohoto světa pomocí elektrod připojených k mozku, případně, pokud se báli pomocí klávesnice a monitoru. Gibsonem se později inspirovali další autoři sci-fi literatury a filmů.

Americká armáda[30] chápe kyberprostor jako pátou globální doménu, spolu se vzduchem, zemí, moři a vesmírem. Tyto domény jsou na sobě závislé. Uzly kyberprostoru jsou umístěny ve všech doménách. Činnosti v jiných doménách mohou vytvářet efekt v kyberprostoru a skrze něj. Kyberprostor si lze v jejich pojetí představit tvořený třemi vrstvami (psychickou, logickou a sociální) s pěti komponenty (geografickými, fyzickými sítěmi, logickými sítěmi, osobami a virtuálními osobami).

Ze světové literatury můžeme uvést například definici kyberprostoru uvedenou v encyklopedii academia.edu, autor Marco Mayer.[31] Kyberprostor je globální a dynamická

[28] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 29

[29] v ČR upravuje §6 zákona č. Zákon č. 480/2004 Sb. o některých službách informační společnosti

[30] Cyberspace Operations Concept Capability Plan 2016-2028, dostupné z http://fas.org/irp/doddir/army/pam525-7-8.pdf, 16.2.2016

[31] Volně přeloženo z https://www.academia.edu/7096442/How_would_you_define_Cyberspace, 16.2.2016

doména, vyznačující se kombinovaným použitím elektronů a elektromagnetického spektra, jejíž cílem je vytváření, ukládání, úprava, výměna, sdílení, získávání, využívání a odstranění informací. Kyberprostor se skládá a) z fyzické infrastruktury a telekomunikačních zařízení, b) počítačových systémů a příslušného softwaru, c) sítěmi mezi počítačovými systémy, d) internetem, e) přístupovými body uživatelů a f) uživatelskými daty.

Z naší literatury můžeme uvést výklad kyberprostoru dle prof. Rudolfa Kohoutka jako „*virtuální svět vytvořený moderními technologickými prostředky (např. počítačem)*[32]“. Náš právní systém pojem kybernetický prostor definuje v zákoně o kybernetické bezpečnosti, jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systém, a službami a sítě elektronických komunikací“*[33].

Z uvedených definic je zřejmé, že kyberprostor je širší pojem než pojem internet, který tvoří jednu z jeho částí. Obdobné je to s činností v kyberprostoru. Z uvedeného plyne, že je důležité nezaměňovat tyto pojmy a nezaměňovat pojmy počítačová kriminalita (vztah jen k počítači), internetová kriminalita (vztah jen k internetu) a kybernetická kriminalita (vztah ke skutkům v celém kyberprostoru).

3.1.2.9 Kybernetický útok

Zabezpečení počítačových dat a informačních systémů se věnuje celý multidisciplinární obor, Informační bezpečnost. Jedná se o „*multidisciplinární obor, usilující o komplexní pohled na problematiku ochrany informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace. Obvykle zahrnuje postupy, zabývající se snižováním rizik vztahujících se k informacím a navrhující příslušná organizační, řídicí, metodická, technická a právní opatření.*[34]“ Rizika, která ovlivňují bezpečnost informací a dat, mají více úrovní rizika, od pouhého narušené bezpečnosti, které nezpůsobí žádnou škodu, až po cílený útok na důvěryhodnost, integritu a dostupnost dat. Každé takové jednání nemusí být nutně trestným činem.

[32] Slovník cizích slov ABZ.cz, dostupné z http://slovnik-cizich-slov.abz.cz/web.php/slovo/kyberprostor, 16.2.2016

[33] §2 písm. a zák. č. 181/2014 Sb.; zákon o kybernetické bezpečnosti

[34] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 270

Náš právní systém definuje v zákoně o kybernetické bezpečnosti bezpečností událost a incident. Bezpečnostní útok jako takový není v našem právním systému definován. *„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.*[35] *“*

Kybernetický útok je nejzávažnější formou takovéhoto narušení bezpečnosti, Kolouch ho definuje jako *„jakékoliv protiprávní jednání útočníka z kyberprostoru, které směřuje proti zájmům osoby. Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného.*[36] *“*

3.2 Dělení kybernetické kriminality

V následující kapitole si vyjmenujeme nejčastější formy kybernetických útoků, které provází kybernetickou kriminalitu. Některá jednání lze podřadit pod konkrétní ustanovení trestního zákoníku a lze ho tedy považovat za kybernetickou kriminalitu, některá jednání však pod ustanovení konkrétního paragrafu podřadit nejdou, alespoň v našem právním systému. I tato jednání je však potřeba sledovat, protože mohou doprovázet kybernetickou kriminalitu, případně být její přípravou, která může ale i nemusí být u konkrétního skutku trestná. I tato jednání mohou v konečném důsledku ohrozit bezpečnost dat.

Jirovský dělí hrozby do tří skupin na základní hrozby, aktivační hrozby a podkladové hrozby a následně definuje čtyři typy základních hrozeb:

- „*Únik informace, kdy informace důvěrného charakteru je prozrazena neautorizovanému subjektu nebo je jím odhalena. Únik informace pak může vést k přímým útokům se značným dopadem.*
- *Narušení integrity, které zahrnuje porušení konzistence dat, kdy mlže dojít k vytvoření nových dat či změně nebo vymazání stávajících dat*

[35] §7 odst. 1, 2 zák. č. 181/2014 Sb. O kybernetické bezpečnosti

[36] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 14

neautorizovaným subjektem.

- *Potlačení služby, ke kterému dochází v případě, kdy je úmyslně bráněno přístupu legitimního subjektu k informacím nebo informačním zdrojům.*
- *Nelegitimní použití, kdy zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem.*[37]*“*

Většina kybernetických útoků obsahuje v sobě nějakou ze základních hrozeb. Aktivační hrozby dále Jirovský dělí na Penetrační hrozby: Maškarádu, Obejití řízení a Narušení autorizace, a na Implementační hrozby: Trojský kůň a Zadní vrátka. Podkladovými hrozbami rozumí takové hrozby, které jsou podkladem více základních hrozeb. Jednotlivé hrozby shrnuje následující přehled. Přehled zahrnuje dle autora všechny známé způsoby formy útoku. Různé metody konkrétního útoku následně mohou patřit do více kategorií, nebo používat prostředky z více kategorií.

Přehled kybernetických útoků

Hrozba	Popis
Porušení autorizace	Osoby, která je autorizována k použití zdroje pro jistý účel jej použije k jinému, neautorizovanému účelu
Obejití řízení	Útočník využije bezpečnostních mezer v systému nebo jeho slabin
Potlačení služby	Omezení legitimního přístupu k informacím nebo jiným zdrojům
Nezákonný odposlech	Informace je získávána monitorováním přenosového kanálu
Emisní nebo VF odposlech	Informace je extrahována z vysokofrekvenčního vyzařování nebo emisí či jiných elektromagnetických jevů, ke kterým dochází při provozu elektronického zařízení
Nelegitimní použití	Zdroj je používá neautorizovanou osobou nebo neautorizovaným způsobem
Indiskrece	Autorizovaná osoba prozradí důvěryhodnou informaci neautorizované osobě z neopatrnosti nebo za úplatu
Únik informace	Získání důvěryhodné informace neautorizovanou osoby nebo systémem
Narušení integrity	Konzistence dat je narušena jejich neautorizovaným vytvořením, úpravou nebo vymazáním
Změna dat při přenosu	Přenášená data jsou během přenosu informačním kanálem změněna, odstraněna nebo zcela vyměněna
Maškaráda	Jedna entita (osoba nebo systém) se představuje jako jiná entita
Vytěžení odpadových médií	Informace je získávána z magnetických nebo papírových medií, vyhozených do odpadu
Fyzický průnik	Útočník získá kontrolu nad systémem proniknutím k jeho ovládacím prvkům

[37] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 21

Replay	Zachycená kopie legitimní transakce je využita pro opětovný přenos s nelegitimním úmyslem
Popření skutečnosti	Strana zúčastněná ve vzájemné komunikaci později popře, že k takové komunikaci došlo
Vyčerpání zdrojů	Jistý zdroj, např. port, je úmyslně zatížen natolik, že je znemožněno používání služby, která je na něj navázána
Podvržení služby	Podvržený systém nebo systémová komponenta, která se vůči uživatelovi chová jako běžná součást systému, slouží k získávání citlivých informací od důvěřivého uživatele
Krádež	Kritický prvek bezpečnostního systému nebo veškerá citlivé informace jsou zcizeny
Analýza provozu	Informace je neautorizovanou entitou získána pomocí sledování provozu a výběrem podstatných jeho částí
Zadní vrátka	Do systému je zabudována vlastnost nebo vložena součást, která při jisté konstelaci vstupních dat umožní obejít bezpečnostní mechanismy
Trojský kůň	Software obsahuje zdánlivě nevinnou nebo neviditelnou část kódu, který – pakliže je spuštěn – ohrozí bezpečnost uživatele.

Tabulka 1: Typické hrozby, Václav Jirovský[38]

3.2.1 Projevy kybernetické kriminality

Výše uvedený přehled kybernetických útoků je pro mnoho lidí špatně představitelný, o jaká jednání se může dělat. Častěji se využívá pojmenování jednotlivých projevů kybernetické kriminality. Tyto projevy v sobě mohou obsahovat více jednotlivých kybernetických útoků, podle toho, jaká je sekvence kroků v jednání pachatele.

Spam

Pojem spam znamená souhrnný název pro veškerou nevyžádanou poštu nezávisle na tom, co je obsahem této pošty. Může jít o neškodnou nevyžádanou reklamu, která nás pouze obtěžuje, ale může jít i o zprávy obsahující například viry nebo phishingové nabídky.

Právní postih spamu je v našem právním systému velmi obtížný. Omezením práva na zasílání elektronické pošty by se jednalo o omezení práva na svobodu projevu dle čl. 17 LZPS. Dle zákona o elektronických komunikací lze postihnout odesílatele spamu pouze za přestupek, kdy přestupek spáchá fyzická osoba, která použije adresu elektronické pošty pro

[38] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 23-24

odeslání zprávy nebo zpráv třetím osobám bez souhlasu držitele adresy elektronické pošty[39], nebo nabídne marketingovou reklamu nebo jiný obdobný způsob nabídky zboží nebo služeb účastníkovi nebo uživateli, který uvedl, že si nepřeje být kontaktován za účelem marketingu[40]. V našem právním systému by šla ještě dále využít náhrada škody v občansko-právním řízení.

Právní postih odesílatele neřeší ani mezinárodní úmluva o kybernetické kriminalitě, neboť nevymezuje zasílání nevyžádané pošty jako trestný čin. K několika odsouzením odesílatele nevyžádané pošty došlo k USA, jejichž právní systém umožňuje toto postihnout[41].

Nelze přesně určit, jakou část z celkového počtu odeslaných emailů tvoří nevyžádaná pošta. Dle různých zdrojů se jedná o 90 % – 95 % veškeré odeslané pošty[42]. Nejnovější výzkumy však udávají číslo menší, kolem 50 %[43] v červnu roku 2015.

Phishing

Se zasíláním nevyžádané pošty souvisí také pojem phishing. Pro daný pojem není přesný český překlad, používá se anglický výraz. Pojmem phishing označuje různé formy podvodů, které končí získáním údajů k internetovému bankovnictví nebo k platební kartě, či obdobný údajům. Útok začíná zpravidla zasláním nevyžádaného emailu, či jiné zprávy. Následně v této zprávě, případně po další komunikaci v následujících zprávách, klikne uživatel na zaslaný odkaz. Tento ho přesměruje na podvržené stránky, které ho vybízejí k zadání údajů do internetového bankovnictví nebo k platební kartě. Stránky jsou vzhledově totožné s originální stránkami například internetového bankovnictví nebo platebního portálu, například PayPal nebo PaySec. Zadané údaje však získá pachatel, který díky nim získá přístup k bankovnímu účtu nebo bankovní kartě, odkud následně odčerpá finanční prostředky na další účty tak, aby zastřel jejich původ[44].

[39] § 119, odst. 1 písm. h) zák. č. 127/2005 Sb. O elektronických komunikacích
[40] § 119, odst. 1 písm. i) zák. č. 127/2005 Sb. O elektronických komunikacích
[41] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 35
[42] Srov. JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 104 srov. KOLOUCH, Jan, Trestně právní ochrana před kybernetickou kriminalitou, str. 34
[43] http://pcworld.cz/novinky/symantec-spamu-je-cim-dal-mene-48487, cit. 21.2.2016
[44] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 37

Phishingový útok patří mezi útoky s využitím prvků sociálního inženýrství. Tyto útoky jsou stále častější, setkáváme se s nimi i u nás. Odhaduje se, že množství phishingových emailů, na které uživatel odpoví, se pohybuje mezi 0,1 % - 0,01 %[45]. Zpočátku se phishingové zprávy vyznačovali špatnou češtinou, nyní jsou již na vysoké úrovni. V poslední době se také prvotní zprávy šíří pomocí sociálních sítí, například pomocí sítě Facebook, nejenom emaily.

Pharming

Pharming je pokročilejší metoda phishingu, při které je napaden DNS server, který překládá IP adresy internetového bankovnictví[46]. Tento následně přesměrovává klienty na podvržené stránky, které jsou k nerozeznání od originálních stránek internetového bankovnictví, avšak data odesílají útočníkovi.

Dalším způsobem pharmingu je napadaní počítače uživatele například virem, který pozmění nastavení prohlížeče, kdy jsou příslušné stránky v prohlížeči přesměrovány rovnou na podvržené stránky falešného internetového bankovnictví. Následuje využití získaných údajů k bankovním účtům a rychlý převod finančních prostředků.

Spear Phishing

Spear phishing[47], nebo také cílený phishing je jednou z forem phishingu, jehož cílem jsou konkrétní osoby, na rozdíl od pharmingu, nebo klasického phishingu, kde cíl útoku není předem vybraný. Útočník si předem z veřejně dostupných zdrojů zjistí co nejvíce informací o napadeném a těchto informací využívá v následné komunikaci, při které vystupuje jako známý napadeného a snaží se tím získat jeho důvěru, aby mu napadený vyzradil důvěrné informace. Následuje opět známý neoprávněný výběr finančních prostředků na základě získaných údajů. Spear phishing bývá také využívaný proti konkrétním organizacím za účelem získání důvěrných informací, které lze následně využít, případně jimi tuto organizaci vydírat.

---

[45] LANCE, James, Phishing bez záhad, str. 35

[46]článek Pharming,, dostupné z http://us.norton.com/cybercrime-pharming

[47] Článek Cílený phishing :podvod, ne sport, dostupné z http://cz.norton.com/spear-phishing-scam-not-sport/article, článek What is Spear Phishing? – Definition, dostupné z https://usa.kaspersky.com/internet-security-center/definitions/spear-phishing

Malware

Malware je souhrnný název pro celé spektrum škodlivého softwaru, různých počítačových virů, červů, trojské koně, spyware a adware a další škodlivý software[48]. Jirovský definuje malware jako „*jakýkoliv software, jenž při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na konkrétní naprogramovanou spouštěcí událost.*[49]*“* Výraz vzniknul

Rozlišujeme několik druhů malwaru[50]. *Počítačoví červi* jsou počítačové viry, které se dokáží sami šířit přes počítačovou síť, na rozdíl od běžných virů, které vyžadují aktivní akci uživatele. K jednomu z prvních útoků pomocí počítačového červa došlo již v roce 1988 v USA[51], kde virus nakazil 2000 počítačů, což při teprve vznikajícím internetu bylo velké číslo. Autor červa byl dokonce usvědčen a odsouzen k trestu vězení a peněžitému trestu.

Dalším druhém počítačového viru jsou *trojští koně.* Jedná se o počítačové programy, které se maskují jako neškodné programy, ale obsahují ještě další škodlivé funkce, které se spouští bez vědomí uživatele a mohou například nainstalovat do počítače další škodlivý software. Zvláštní kategorií trojských koní jsou *backdoor*. Jde o trojské koně, které umožní útočníkovi ovládnout počítač na dálku. Využívají k tomu většinou otevřených komunikačních portů, nebo portů s vysokým číslem[52]. Další kategorií jsou *skenery*, což jsou trojské koně, které sledují provoz, hlavně síťový, na počítači a data odesílají útočníkovi. Ten může takováto data následně využít pro kybernetický útok.

Zvláštním druhem počítačového viru je pak *ransomware*. Jde o vyděračské viry, které uzamknou počítač a znemožní jeho užívání, dokud uživatel nezaplatí určenou finanční částku, kdy mu následně přijde kód pro odblokování. Často se tyto vyděračské viry maskují jako zablokování počítače například policií.

[48] SMEJKAL, Vladimír. Kybernetická kriminalita, str. 138

[49] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 271

[50] KOLOUCH, Jan, Trestně právní ochrana před kybernetickou kriminalitou, str. 42 - 43

[51] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 57

[52] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 63

Další kategorií počítačových virů jsou *rootkity*, což jsou počítačové programy, které mění chování a vzhled systému tak, aby uživatel nevěděl o napadení systému dalšími druhy malwaru, nebo mohou měnit chod antivirového softwaru, aby nemohl tento malware odstranit.

Pojem *spyware* lze přeložit jako špionský software. Jedná se o program, často je součástí volně šířených programů, který odesílá statistické údaje přes internet útočníkovi[53]. Pojem *adware* označuje software, který nám nabízí nechtěnou reklamu, například pomocí neustále se vyskakujících oken.

Scam

Někdy také Scam 419, nebo Nigerijský scam. Jedná se o počítačovou obdobu již dříve existujícího podvodu, kdy jsou odesílány uživatelům dopisy vybízející k zaplacení finanční částky, například jako pomoc při převodu peněz do zahraničí. Jako původ peněz bývá označováno dědictví, obchodní podíl nebo třeba výhra v loterii[54]. Je až obdivuhodné, kolik lidí se na tento typ dopisu nachytá, podvodníci udávají výtěžnost kolem 1 %.

Sniffing

Sniffing, volně přeloženo. „čenichání“ je metoda nelegálního monitorování a sledování veškeré komunikace, které prochází na síti. „*Sniffing je jednoduše řečeno odchytávání komunikace po počítačové síti, především Internetu, subjektem, který není adresát této komunikace.*[55]*“* Mezi sniffing by šlo jistě zařadit i skryté sledování provozu na počítačové síti v zaměstnání nebo ve škole, pokud dochází k prohlížení obsahu přenášených dat.

DoS a DDoS útoky

Zkratka „DoS“ znamená „Denial of Service“, což lze volně přeložit jako „útok s cílem potlačení služby.[56]“ „DDoS“ znamená Distributed Denial of Service.“ Jedná se o útoky, jejichž cílem je zcela znemožnit nebo alespoň omezit činnost prvků informační a komunikační infrastruktury, nejčastěji serverů. Liší se od sebe pouze tím, zda je k útoku

[53] POŽÁR, Josef, Informační bezpečnost, str. 216

[54] Článek Příchod hackerů: nigerijský scam „419“, dostupné z http://www.root.cz/clanky/prichod-hackeru-nigerijsky-scam-419/

[55] MATĚJKA, Michal, Počítačová kriminalita, str. 74

[56] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 47

využit jeden počítač, nebo více počítačů najednou. „*Útoky lze DoS/DDoS lze obecně definovat jako pokusy dočasně nebo trvale znemožnit oprávněným uživatelům přístup k nějaké službě.*[57]“

Je známo několik základních forem DoS/DDos útoků. Všechny mají společné to, že jakmile útok skončí, vše se vrátí do původního stavu a server či služba by měly být nepoškozeny. Mezi nejznámější metody patří následující útoky[58]:

- Zahlcení odesíláním paketů z velkého množství zařízení najednou. Během tohoto útoku jsou najednou odesílány na cílový počítač pakety z množství jiných zařízení najednou. Často jsou pro tento útok využívány botnety. Ke stejnému efektu může ale i dojít legálním způsobem, například když má o danou službu zájem více uživatelů, než na jakou kapacitu je služba nastavena.
- Zahlcení příkazem ping. Během toho útoku jsou na adresu sítě zaslán příkaz ping s podvrženou adresou napadeného počítače. Následně všechny počítače v síti odpovídají na příkaz ping tomuto napadenému počítači, čímž dochází k zahlcení tohoto počítače.
- Zahlcení volných systémových prostředků. Útok spočívá v zaslání SYN paketů s fingovanou hlavičkou na cílový počítač. Tento odešle odpověď a pro potřeby chystaného spojení vyhradí systémové prostředky. V případě odeslání většího množství SYN paketů může dojít k vyčerpání všech volných systémových prostředků.

Cílem DoS/DDoS útoků je způsobit služby nedostupnými, což jako takové může způsobit značné škody, například v případě výpadku služby elektronických obchodů nebo systémů bankovních institucí.

Botnet

Botnet označuje „*síť infikovaných počítačů, ovládaných bez vědomí majitele, které často slouží k rozesílání nevyžádané pošty, ke krádežím identity či k provádění dalších*

[57] SMEJKAL, Vladimír. Kybernetická kriminalita, str. 534
[58] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 47-48

forem kybernetických útoků.[59]*“* Bot je zkrácenina slova robot, tudíž bychom mohli přeložit pojem jako „robotická síť“. Tyto sítě jsou užívány také k realizaci DoS útoků, případně při využití samočinných programů, tzv. botů, například k ovlivnění průzkumů, reklamy apod. klikáním na příslušné odkazy.

Cybersquatting

Cybersquatting znamená, jak napovídá sám pojem, neoprávněné obsazení určitého prostoru v kyberprostoru, nejčastěji k zabrání doménového jména určité společnosti. Pachatel si zaregistruje dříve než oprávněný majitel danou doménu, případně si ji zaregistruje s jinou koncovkou. Následně nabídne právoplatnému uživateli k odprodeji, případně s výhružkou, že na doméně budou umístěny například pornografické stránky. Pravidla k registraci domén upravuje v České republice společnost CZ.NIC[60].

Specifickým případem cybersquatingu je typosquating, který je na stejném principu, jen využívá místo neoprávněně zabraného doménového jména jiné, které je podobné originálnímu, ale s překlepem. Množství přístupů na tuto stránku lze potom využít například v reklamě.

Hacking

Pojem hacking označuje „*proniknutí do počítačového nebo řídicího systému jinou než standardní cestou při obejití nebo prolomení jeho bezpečnostní ochrany.*[61]*“* Motivací hackera nemusí být nutně zisk, zvláště v počátku hackingu šlo spíše o prestiž. Pojem hacker totiž označoval osobu, která měla velké technické znalosti a ovládala daný systém a uměla si upravit jeho fungování ke svému obrazu. Blíže k vývoji hackingu v kapitole 2.3.

Podle motivace jednání hackera můžeme rozlišit tři skupiny těchto osob[62]:

White Hats: Jde o hackery, kteří pomáhají odhalovat slabiny informačních systémů a programů tím, že se do nich pokouší proniknout nestandardní cestou. Často se jedná a zaměstnance nebo spolupracovníky společností, které tyto systémy nebo programy

[59] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 269

[60] Pravidla pro registraci domén, dostupné z http://www.nic.cz/files/nic/doc/Pravidla_registrace_CZ_Pravidla_ADR_20150301.pdf

[61] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 102

[62] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 51

vyvíjejí. Po průniku upozorňují autora na možnou chybu, aby jí mohl autor opravit. Jejich činností nevzniká společnosti žádná škoda.

Black Hats: Jde o hackery, kteří pronikají do informačních systémů za účelem zisku, buď čistě pro sebe, nebo za úplatu pro další osoby, případně s cílem uškodit uživateli daného systému.

Gray Hats: Jde o hackery, kteří se pohybují mezi oběma skupinami, případně spolupracují pro obě strany.

Script Kiddies: Nejedná se o hackery v pravém slova smyslu, jde o uživatele, kteří využívají již hotové skripty vytvořené jiným autorem, bez jejich hlubších znalostí.

V dnešní době je každé neoprávněné proniknutí do informačního systému trestné, pokud není prováděno na přání uživatele nebo majitele systému, a bývá součástí většiny metod kybernetické trestné činnosti. Nejedná se už ale o hacking v jeho historickém smyslu. Také si lze na internetu stáhnout již vytvořené programy, které nám umožní proniknout do systému či obejít zabezpečení systému bez jeho větší znalosti[63].

Cracking

Pojem cracking souvisí s neoprávněným užíváním programů a s jejich šířením. Jedná se o „*zásah do programu, který umožní obejít jeho ochranu proti kopírování či neoprávněnému použití*[64]*.“* Pod cracking spadá i password cracking, což je souhrnný název pro různé vytváření key generátorů a cracků, které umožňují následné užití programu. Časté je také následní sdílení cracknutých programů na warez fórech či prostřednictvím P2P sítí.

Internetové pirátství

Internetové pirátství je obecný pojem, který zahrnuje audiovizuální i softwarové pirátství ve vztahu k šíření děl přes internet. „*Základem k pro softwarové i audiovizuální pirátství je však porušení některého z autorských práv či práv souvisejících s právem*

[63] Například Pět cest, jak proniknout do cizí Wi-Fi sítě, dostupné z http://www.zive.cz/clanky/pet-cest-jak-proniknout-do-cizi-wi-fi-site/sc-3-a-165682/default.aspx, srov. Prolomení WPA/WPA2-PSK přes WPS snadno a rychle (praxe), dostupné z http://www.mrpear.net/cz/blog/435/prolomeni-wpa-wpa2-psk-pres-wps-snadno-a-rychle-praxe

[64] MATĚJKA, Michal. Počítačová kriminalita, str. 73

autorským.[65]*“* Pokud v dané zemi není daná forma kopírování nebo šíření díla přes internet nelegální, nejedná se o internetové pirátství.

Audiovizuální a později softwarové pirátství zde bylo od počátku dostupných technologií, na kterých bylo možné daná díla šířit. S rozvojem internetu však dosáhnul tento fenomén vrcholu. V poslední době však je internetové pirátství, minimálně ve většině evropských zemích, pravděpodobně na ústupu[66]. Jednotlivé státy se pokouší více či méně úspěšně s internetovým pirátstvím bojovat[67], většinou blokováním stránek, přes které dochází ze sdílení pirátského obsahu, avšak tato činnost stáních organizací bývá často na hraně se se zásahy do základních právem a svobod občanů, například na svobodný přístup k informacím či na svobodu vyjadřování.

S internetovým pirátstvím souvisí pojem „warez[68]“. Jedná se o fóra, na kterých se šíří nelegální kopie software a audiovizuálních děl. Na těchto fórech působí profesionálně organizované skupiny, které spolu soutěží o to, kdo nabídne dříve kvalitnější kopii. Často používají pro svoji ochranu důmyslné maskování pomocí skrývání IP adres, přezdívek a prostředníků. Díla jsou ke stažení nabízena většinou zdarma, zisk je generován reklamou, která bývá umístěna na těchto webech. Pro šíření děl je pak následně užíváno P2P sítí. Je zde však velké nebezpečí, že si uživatel kromě hledaného softwaru či filmu stáhne do počítače i nějaký nežádoucí malware, či se stane obětí jiné formy kybernetického útoku.

Racketeering (kybernetické výpalné)

Jedná se o klasický trestný čin, který je však realizovaný prostřednictvím informačních sítí. Pachatel zastrašuje oběť průnikem do systému, zničením či zneužitím dat, přitom vůbec nemusí přijít do styku s obětí trestného činu. Často využívá neznalosti správce systému, neboť tento neví, zda je pachatel hrozbu realizovat, ale raději zaplatí za ochranu[69].

---

[65] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 53

[66] Studie BSA, dostupné z http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf

[67] Srov. Británie čtvrtým rokem blokuje warez, dostupné z http://www.zive.cz/bleskovky/britanie-ctvrtym-rokem-blokuje-warez-popularita-zakazanych-webu-ale-casto-vzrostla/sc-4-a-181503/default.aspx,srov. Konec torrentů v Rusku? Roskomnadzor chce zablokovat 15 největších, dostupné z http://www.zive.cz/bleskovky/konec-torrentu-v-rusku-roskomnadzor-chce-zablokovat-15-nejvetsich-serveru/sc-4-a-180878/default.aspx

[68] MATĚJKA, Michal. Počítačová kriminalita, str. 70

[69] MATĚJKA, Michal. Počítačová kriminalita, str. 65

Šíření závadového obsahu

Šíření závadového obsahu můžeme rozdělit na dva typy. Šíření zakázaných druhů pornografie a šíření nenávistných a extremistických sdělení[70]. Podobně jako u warez zde narážíme na spor s právem na svobodu šíření informací. Daný obsah může být v některých zemích legální a tudíž trestně nepostihnutelný.

V případě šíření zakázaných druhů pornografie se jedná převážně o šíření a držení dětské pornografie, případně dalších zakázaných druhů pornografie, například zobrazující sex se zvířetem.

V případě šíření nenávistných a extremistických sdělení se jedná převážně o texty s tematikou podpory a propagace hnutí, směřující k potlačení práv a svobod člověka, dále o různé rasistické a xenofobní obsahy. Kolouch řadí do této skupiny také šíření pomluv pomocí prostředků informačních technologií a cyberstalking, což je dlouhodobé obtěžování uživatele pomocí informačních prostředků.

Kyberterorismus

Mezi kybernetickou kriminalitu patří taktéž kyberterorismu. Jde o konvenční formu neletální terorismu, jedná se o nebezpečné zneužívání prostředí informačních a komunikačních technologií pro teroristický útok. Podobně jako u klasického konvenčního teroristického útoku mívá kyberteroristický útok stejnou motivaci, ať již politickou nebo náboženskou. Takovýto teroristický útok může ovlivnit větší množství lidí než konvenční útok, proto je užíván stále ve větší míře. [71]

Mezi pravděpodobné cíle lze vyjmenovat následující[72]: Infrastruktura bankovních a finančních institucí, Hlasové a komunikační služby, Elektrická rozvodná síť, Infrastruktura ropného průmyslu, Zdroje vody a ovládání vodních děl a infrastruktura měst.

Pod kyberterorismus můžeme dále zařadit mediální terorismus. Jedná se o ovlivňování veřejného mínění pomocí zneužívání hromadných sdělovacích prostředků.

---

[70] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 55

[71] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 129

[72] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 149

Card skimming

Pojem „card skimming“ můžeme přeložit jako čtení karet. Jedná se o padělání platebních nebo kreditních karet za pomoci čtečky karet, které při platbě kartou nebo při výběru hotovosti z bankomatu, na kterém je čtečka naistalována, zkopírují data z karty, zároveň zachytí PIN. Následně pachatelé vyrobí kopii této karty, a vyberou hotovost, případně ji použijí k platbě na internetu.[73]

Další trestné činy páchané prostřednictvím počítačů

Pod další trestné činy páchané prostřednictvím počítačů můžeme zařadit tradiční trestné činy, při kterých je využíváno informačních a komunikačních technologií[74]. Většina zvláště majetkových trestných činů lze spáchat v současné době na dálku, kdy jsou tyto technologie užívány ke komunikaci, převodu finančních prostředků či vytvoření legendy potřebné k získání potenciálních poškozených.

V dnešní době je prakticky nemožné najít trestný čin, ve kterém by se informační a komunikační technologie nepoužili alespoň ke komunikaci. Zde se ale nejedná kybernetickou kriminalitu dle její definice.

3.2.2 Závadové jednání uskutečňované v prostředí informačních a telekomunikačních technologií

Následující jednání nejsou v současné době popsána v literatuře (Smejkal, Jirovský, Kolouch) jaké samostatné skupiny kybernetické kriminality, avšak jednotlivá jednání jsou zvláště v prostředí sociálních sítí stále častější. Jedná se o škodlivé jednání a chování uskutečňované za pomoci informačních a telekomunikačních technologií, které ve velké míře ohrožuje děti, proto by zde i tato jednání měla být uvedena, přestože se nejedná, alespoň v obecné rovině, o kybernetickou kriminalitu. Jedná se například o sexting, kyberšikanu, kybergrooming. Komplexní studií těchto závadových jednání se zabývá rozsáhlá studie uskutečněná v roce 2015 autorem Kamilem Kopeckým a kol., Rizikové formy chování českých a slovenských dětí v prostředí internetu. Uvedená studie je zajímavá i shrnutím preventivních programů uskutečněných v této oblasti.

[73] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 58

[74] MATĚJKA, Michal. Počítačová kriminalita, str. 60

Kyberšikana

Jedná se „*formu agrese, která je realizována vůči jednotlivci či skupině s použitím informačních a komunikačních technologií a které dochází opakovaně.*[75]*“* Je nutné rozlišovat mezi kyberšikanou, online obtěžováním a online agresí. V případě běžné šikany je důležitým prvkem opakovanost, dlouhodobost a musí být pro oběť vnímána jako ubližující. V případě kyberšikany je zde rozdíl, že k její realizaci postačí i jednotlivý útok, protože ten se může šířit lavinovitě po sociálních sítích. Šikanu, kyberšikanu a boj s nimi řeší metodický pokyn MŠMT č. MSMT-21149/2016, přímo kyberšikanu příloha č. 7 pokynu č. 21291/2010-28. Tento pokyn definu kyberšikanu jako „*zneužití ICT (informačních komunikačních technologií), zejména pak mobilních telefonů a internetu, k takovým činnostem, které mají někoho záměrně ohrozit, ublížit mu. Podobně jako u šikany tváří v tvář se jedná o úmyslné chování, kdy je oběť napadána útočníkem nebo útočníky. Povaha a provedení útoků pak určuje její závažnost*[76].“

Z právního hlediska šikana, ani kyberšikana jako taková není trestný činem. Její jednotlivé útoky dle své závažnosti však trestnými mohou být. Může se jednat o omezování osobní svobody, vydírání, útisk, případně o další skutky. V případě méně závažného jednání se může jednat o přestupek.

Sexting

Jde o fenomén „*elektronické rozesílání textových zpráv, vlastních fotografií či vlastního videa se sexuálním obsahem, ke kterému dochází v prostředí virtuálních elektronických medií – zejména internetu*[77]*“.* Riziko sextingu spočívá v možném zneužití zasílaných fotografií a dalšího obsahu k pozdějšímu kybernetickému útoku, ať již formou kyberšikany, či například vydírání.

Z právního hlediska, pokud se jedná o fotografie nezletilých, se jedná o šíření dětské pornografie a ohrožování mravní výchovy mládeže.

[75] KOPECKÝ Kamil a kol., Rizikové formy chování českých a slovenských dětí v prostředí internetu, str. 11

[76] příloha č. 7 pokynu MŠMT č. MSTM-21291/2010-28, dostupné z http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny

[77] KOPECKÝ Kamil a kol., Rizikové formy chování českých a slovenských dětí v prostředí internetu, str. 43

Kybergrooming

Jde o „*chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přinutit ji k osobní schůzce.*[78]“ Cíle kybergroomerů bývá následně sexuální zneužití oběti. Kybergooming probíhá v několika fázích, ve výše uvedené studii dělí autor Kopecký fáze útoku na „*fázi přípravnou (příprava na kontakt s obětí), fázi kontaktování oběti (zahrnující formování přátelství a formování vztahu či sexuální fázi), fázi přípravy na útok (zlomové formy manipulace oběti) a fázi samotného útoku*[79]“.

Z trestně právního hlediska by byly trestný až samotný útok, pokud by naplňoval některý znak trestného činu dle trestního zákoníku. Právní posouzení komunikace je složité, lze uplatnit postih za navázání nedovolených kontaktů s dítětem, kde je však nutné prokázat úmysl ke spáchání vyjmenovaných trestných činů. Samotná online komunikace by trestná nebyla, pokud by se například nejednalo o sexuální obsah komunikace s nezletilou osobou, či nebyla jinak závadová.

3.3 Vývoj kybernetické kriminality

Stejně, jako v jiných odvětvích, i kybernetická kriminalita kopírovala s určitým zpožděním rozvoj technologií. S tím, jak se objevovali nové technologie, lidé vymýšleli způsoby, jak tyto technologie zneužít, případně zabránit jejich využití. Pokud budeme hovořit o historii kybernetické kriminality, nejedná se pouze o hacking a historický vývoj hackingu, ale i o další nezákonné jednání proti počítačům, či za využití počítačů, ať už jde o sabotáže nebo neoprávněné užití počítačového vybavení. Literatura uvádí různá dělení vývoje kybernetické kriminality, většinou se užívají jako milníky rozvoj nových technologií, například nástup PC, nebo spáchání do té doby neobvyklého skutku, například odcizení větší částky z banky, případně dělí jednotlivá období na jednotlivá desetiletí. Pro tuto práci není detailní zkoumání historie kybernetické kriminality podstatné, je proto užito zjednodušení rozdělení dle autora Matějky[80].

[78] KOPECKÝ Kamil a kol., Rizikové formy chování českých a slovenských dětí v prostředí internetu, str. 25

[79] KOPECKÝ Kamil a kol., Rizikové formy chování českých a slovenských dětí v prostředí internetu, str. 26

[80] MATĚJKA, Michal. Počítačová kriminalita, str. 17

3.3.1 Období do počátku 80.let

První období je spjato převážně s objevováním nových technologií. Rozvoj kybernetické kriminality je ovlivněn vynálezem počítačů, kdy v roce 1946 byl dokončen na Pennsylvánské univerzitě první sálový počítač ENIAC, za kterým následovaly další stroje, konstruované převážně na univerzitách. Kolem těchto výpočetních center vznikaly komunity nadšenců, kteří se snažili využívat chyb v programech, aby nalezli efektivnější řešení. Hledání těchto „hacků“, jak byly tyto efektní a neobvyklé způsoby řešení nazývány, byl věcí cti těchto nadšenců, nelze zde hovořit o nějaké jejich trestné činnosti.[81]

Na přelomu 60. a 70. let se ve Spojených státech amerických rozvíjí hnutí „Phreakers“. Jedná se o skupinu lidí, kteří využívali poznatku, že za pomoci píšťalky, vydávající tón kmitočtu 2600 Hz, která oklamala automatické ústředny, lze spojovat zdarma dálkové hovory. Tito nadšenci následně zkoumali další způsoby, jak daný systém funguje a jak přeprogramovat telefonní ústředny. Z komunity „Phrakerů“ následně vzešla řada odborníků, ať už vývojářů, jak například Steve Jobs a Steve Wozniak, nebo skutečných hackerů, jako Kevin David Mitnick.

Kromě této relativně neškodné činnosti se rozmáhají sabotáže proti počítačům a počítačovým centrům, kdy škoda se vzhledem k ceně těchto počítačů pohybuje v řádu jednotek milionů dolarů[82].

V prostředí Československa lze z této doby dohledat první skutky sabotáží proti počítačům, kdy pracovníci poškozovali záznamy na magnetických páskách[83], klasifikováno jako trestné činy sabotáže a poškozování majetku v socialistickém vlastnictví, případně nelegální užití počítačů, spočívající například v tisku obrázků, ve výpočtu diplomových pracích, nebo vedení účetnictví[84]. Smejkal zde také zmiňuje první případy tzv. „dokladových“ deliktů, kdy pracovníci páchají podvody, spočívající v manipulaci záznamů v databázích, například faktury, výplat a podobně.

[81] JIROVSKÝ, Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, str. 48-49
[82] KABAY, M.E: A Brief History of Computer Crime: An Introduction for Students, str. 5
[83] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 76
[84] SMEJKAL, Vladimír, Internet a §§§, str. 67.

3.3.2 Období od počátku 80. let do pol. 90 let 20. století

Další období rozvoje počítačové kriminality je ohraničeno skokovým rozvojem techniky. Na přelomu 70 a 80. let přichází několik novinek. Na konci 70. let to rozvoj prvních BBS (Bulletin Board System), systému umožňující propojit počítače mezi sebou do sítě přes telefonní linky, dále je to rozvoj osobních počítačů, ať už uvedení prvních IBM PC nebo Maců. Postupně vznikají standarty Internetu a jednotlivé protokoly pro komunikaci mezi počítači a jednotlivými sítěmi.

Spolu s rozšíření počítačů a možnosti komunikace mezi nimi vzniká v této době několik hackerských skupin, které zpočátku zkoumali možnosti vznikajících technologií, upozorňovali na různé nedostatky a tyto poznatky také publikovali pomoví BBS sítí, aby byla dostupné ostatním. Z literatury lze zmínit například skupinu Chaos Computer Club z Hamburku, kteří upozornili na vážné slabiny nového systému Bundespost, kdy prostřednictvím chyby systému převedli finanční prostředky a následně veřejně prostředky vrátili a věc zveřejnili[85], nebo skupinu Legions of Doom, kteří vydávají LOD Technical Journal, ve kterém zveřejňují různé chyby v systémech. Zlomový bod následuje v roce 1990, kdy po vyšetřování provedla americká FBI akci Sundevil, ve které se zaměřila na BBS sítě se závadovým obsahem, zabavila 42 počítačů a 23 000 disků. Skutečný přínos akce byl mizivý, avšak ukázal snahu policie přestat jednání hackerů přehlížet. Tyto kroky policie, spolu se snahou nadále omezovat svobodu slova na síti, daly vzniknout nadaci Electronic Frontier Foundation (EFF), která se snaží soudními procesy bránit svobodu projevu na sítích[86].

Na konci toho období jsou již počítače rozšířené jak mezi jednotlivci, tak mezi společnostmi a začínají se objevovat první skutečné kybernetické zločiny, které mají za účel prosté obohacení. Jak jeden z prvních lze zmínit čin Vladimira Levina, jehož skupině se podařilo v roce 1994 proniknout do systému banky Citibank a zde odcizit přes 10 milionů dolarů[87].

[85] KABAY, M.E: A Brief History of Computer Crime: An Introduction for Students, str. 41
[86] Informace o organizaci dostupné na https://www.eff.org/about/history
[87] KABAY, M.E: A Brief History of Computer Crime: An Introduction for Students, str. 18

3.3.3 Období od poloviny 90. let do současnosti

Od poloviny 90. let, kdy je již běžně rozšířený internet i počítače, dochází k velkému nárůstu kybernetické kriminality, a to jak do kvality, tak do kvantity.[88] Kromě skutečných hackerů může tuto trestnou činnost provádět i nezkušená osoba, která si na internetu stáhne již vytvořený nástroj, který jen „spustí“, tzv. Script Kiddies. Dále dochází k rozvoji technologie CD a DVD disků, které se stávají běžnou výbavou domácích počítačů a spustí tak lavinu nelegálního kopírování softwaru i audiovizuálních děl. S rozvojem internetu dále souvisí rozšíření počítačových virů, šířených zpočátku na médiích, v současné době však ji převážně prostřednictvím emailové komunikace a v neposlední řadě rozvoj DoS a DDoS útoků.

Jednotlivým druhům kybernetické trestné činnosti se budeme věnovat podrobně v další kapitole.

3.4 Trestně právní úprava kybernetické kriminality

Jak již bylo uvedeno výše a jak píše autor Smejkal, „*Internet jako takový není subjektem práva – nemá právní subjektivitu.*[89]“ To však nebrání tomu, aby zde byl a ovlivňoval náš život, čím dál více. Přes internet je uskutečňována komunikace, jsou skrze něj realizovány obchody, ale je využíván i k páchání zločinu. Z počátku si zakládal na své svobodě, kterou se organizace jako EFF, snaží nadále hájit, Avšak čím více se internet zapojuje do každodenního života, tím více se logicky jeho fungování prolíná s různými oblastmi práva., které se ho více či méně úspěšně snaží jistou formou regulovat. Je nutné často řešit, jaké a čí právo na internetu platí, díky tomu, že internet, respektive celý kyberprostor, nerespektuje hranice a jednotlivé státy mají různé právní systémy.

3.4.1 Působnost práva na internetu

Internet jako takový nemá právní subjektivitu, je to však „*informační a telekomunikační systém, který se skládá ze subjektů práva, tedy účastníků právních vztahů v podobě fyzických a právnických osob.*[90]“ Na tyto subjekty se již právní systémy vztahují.

[88] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 128
[89] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 59
[90] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 26

Je zde však problém s principem teritoriality, neboť internet jako takový nemá hranice a informace na něm se mohou nacházet v jednu chvíli na více místech a během okamžiku svoje místo změnit. Pokud chce tedy nějaký subjekt hájit své zájmy, musí často využít mezinárodní spolupráce. Proto také vznikají jednotlivé mezinárodní úmluvy, které mají pomoci společnému boji proti kybernetické kriminalitě a mají harmonizovat jednotlivé právní systémy v oblasti práva v kyberprostoru.

V dnešní době moderní státy uznávají princip teritoriality, dle které se právo určitého státu vztahuje na všechny, kdo v daném státu pobývají. Taktéž na základě tohoto principu postihují státy trestné činy, které se na jejich území staly, to znamená, kde se pachatel dopustil jednání, nebo kde nastal následek.[91] Postačí, když na území daného státu byla spáchána jen část jednání. Často se tedy může stát, že jeden trestný činu bude prošetřovat více států, neboť jednání či následek nastaly na více místech zároveň. O to více musí při vyšetřování takovéto trestné činnosti jednotlivé orgány činné v trestním řízení využívat možností mezinárodní spolupráce, například Interpolu nebo Europolu.

Státní orgány jsou také nuceny spolupracovat s jednotlivými definičními autoritami na internetu a s poskytovali služeb, kteří vlastně řídí fungování internetu. Na základě příslušného rozhodnutí, nejčastěji vydaného soudem, mohou být tyto poskytovatelé služeb přinuceni poskytnout orgánům činným v trestním řízení informace o uživatelích, obsah informací, které poskytovatel přenáší nebo uchovává, nebo může být poskytovateli přikázáno, aby nějakou svoji službu omezil, například blokoval příslušnou webovou stránku či IP adresu. V našem právní systému upravuje vyžadování a poskytování informací Trestní řád a zákon o Policii České republiky.

V další kapitole budou popsány jednotlivé kybernetické útoky, jak byly vyjmenovány v kapitole 2.2, a bude uvedena úprava v Trestním zákoníku, které dané jednání v našem právním systému postihuje.

3.4.2 Úprava v zákoně č. 40/2009 Sb. Trestní zákoník

Dříve platný trestní zákon č. 140/1961 Sb., účinný do konce roku 2009, se dlouho kybernetickou trestnou činností nezabýval, s výjimkou později přidaného ustanovení

[91] §4 trestního zákoníku č. 40/2009 Sb.

§ 257a které praví, že „*Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch*

a) takových informací neoprávněně užije,

b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo

c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,

bude potrestán“. Dané ustanovení chránilo jak softwarové, tak hardwarové vybavení počítače, avšak vyžadovalo úmysl pachatele, aby způsobil škodu nebo jinou újmu, nebo úmysl k tomu, aby získal pro sebe nebo jiného neoprávněný prospěch. Pokud nebyl prokázán tento úmysl, nemohl být pachatel pro tento paragraf stíhán a odsouzen.

S příchodem nového trestního zákoníku č. 40/2009 Sb., účinného od 1. 1. 2010, došlo k výrazné změně. Nový trestní zákoník zavádí ve zvláštní části ryze počítačové trestné činy - § 230, § 231 a § 232, u dalších mění skutkové podstaty, aby tyto v některém svém bodě také chránily před kybernetickou kriminalitou. Celkem je v trestním zákoníku zařazeno 21 skutkových podstat, mající vztah ke kybernetické kriminalitě. Jednotlivé trestné činy a skutkové podstaty lze třídit podle různých kritérií.

Autor Kolouch dělí kybernetické trestné činy na trestné činy, při jejich páchání představují prostředky informačních a komunikačních technologií předmět ochrany, a na trestné činy, při jejich páchání jsou prostředky informačních a komunikačních technologií užity ke spáchání trestného činu[92]. Některé skutkové podstaty autor zařazuje do obou kategorií, neboť skutkové podstaty chrání informační a komunikační technologie a zároveň obsahují ustanovení o zneužití těchto technologií.

Jedná se o následující skutkové podstaty:

Trestné činy, při jejich páchání představují prostředky informačních a komunikačních technologií předmět ochrany:

- § 182 Porušení tajemství dopravovaných zpráv
- § 183 Porušení tajemství listin a jiných dokumentů zachovávajících

[92] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 78

soukromí

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- § 232 Poškození záznamu v počítačovém systému a nosiči informací a zásah do vybavení počítače z nedbalosti
- § 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- § 311 Teroristický útok

Trestné činy, při jejich páchání jsou prostředky informačních a komunikačních technologií užity ke spáchání trestného činu:

- § 180 Neoprávněné nakládání s osobními údaji
- § 182 Porušení tajemství dopravovaných zpráv
- § 184 Pomluva
- § 191 Šíření pornografie
- § 192 Výroba a jiné nakládání s dětskou pornografií
- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 236 Výroba a držení padělatelského náčiní
- § 287 Šíření toxikomanie
- § 345 Křivé obvinění
- § 348 Padělání a pozměnění veřejné listiny
- § 354 Nebezpečné pronásledování
- § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 Podněcování nenávisti vůči skupině osob nebo k omezování práv a svobod
- § 407 Podněcování útočné války

Nyní se pokusíme k jednotlivým projevům kybernetické kriminality najít odpovídající ustanovení trestního zákoníku.

Spam

Obecně zasílání nevyžádané pošty, tzv. Spamu, není v našem právním systému trestné z pohledu trestního zákoníku. Zasahování do práva na odesílán pošty, i nevyžádané, by se dalo považovat za omezování práva na svobodu projevu. Z hlediska správního práva by bylo možné postihnout jako přestupek dle zákona č. 480/2004 Sb. zasílání nevyžádaných obchodních sdělení, u kterých zákon vyžaduje předchozí souhlas uživatele[93]. Dále by dle zákona č. 127/2005 bylo přestupkem použití adresy elektronické pošty k odesílání zpráv bez souhlasu držitele této adresy[94].

Scam

Jedná se o formu spamu, avšak zde se již pachatel dopouští podvodu dle § 209 trestního zákoníku (dále jen TrZ), pokud vznikla oběti nějaká škoda.

Phishing

Phishingové útoky nevyžadují, aby pachatel napadl počítač oběti, oběť mu sama sdělí nevědomky přístupové údaje do internetového bankovnictví, případně potřebné údaje k platebním kartám. Jedná se o podvod spáchaný pomocí ICT zařízení, nejčastěji pomocí počítače, internetu a sociálních sítí.

Právně lze phishingové útoky postihovat dle naší právní úpravy jako podvod dle § 209 TrZ a dále v případě získání údajům k internetové bankovnictví či platební kartě jako neoprávněné opatření, padělání a pozměňování platebního prostředku dle § 234 TrZ.

V současné době jsou phishingové útoky rozšířené na síti Facebook, kdy pachatelé napodobují stránky banky, vyzývají klienty ke zlepšení bezpečnosti svého bankovnictví, často se slibem odměny. Napadeny takto byly v létě 2016 banky Česká spořitelna, mBank, i další banky, které varují klienty na svých webových stránkách před podvodnými phishingovými útoky[95]. Dalším druhem phishingového útoku je prosba od kamaráda na facebooku, ať již z napadeného facebookového účtu nebo z podvrženého účtu, na zaslání

[93] §7 odst. 2 zák. č. 480/2004 Sb. O některých službách informační společnosti
[94] § 119 odst. 1, písm. h), i) zák. č. 127/2005 Sb. O elektronických komunikacích
[95] http://www.csas.cz/banka/content/inet/internet/cs/sc_17573.xml?archivePage=phishing&navid=nav00156_phishing_aktuality, http://www.mbank.cz/blog/post,659,pozor-phishingovy-utok-na-mbank.html

malé finanční částky. Následuje odkaz na stránky, tvářící se jako stránky platebních společností, kde poškozený zadá své údaje k platební kartě či internetovému bankovnictví.[96]

Pharming

Jedná se o kombinaci podvodu, jako v případě phishingu, avšak pachatel již také potřebuje získat přístup k počítači poškozeného, nejčastěji instalací viru zaslaného spolu s phishingovým emailem, nebo napadením DNS serveru.

Právně lze pharming postihnout jako podvod dle § 209 TrZ v souběhu s neoprávněném přístupu k počítačovému systému a nosiči informací dle § 230 TrZ a neoprávněné opatření, padělání a pozměňování platebního prostředku dle § 234 TrZ.

Klienti České spořitelny byli napadeni takto například v létě 2015, kdy byl rozesílán email s varováním na nezaplacené splátky, jeho přílohou byl virus, který následně po přihlášení do internetového bankovnictví přesměroval poškozené na podvodné stránky, kde zadali údaje k internetovému bankovnictví a následně vybídnul klienty k instalaci programu do mobilního telefonu, který se tvářil jako doplněk zabezpečení účtu. Tímto však pachatel získal přístup k účtu i k ověřujícím zprávám sms[97]. Obdobný útok byl uskutečněn i v létě 2014 tentokrát s emailem s výzvou od exekutora.

Spear phishing

Stejně jako v případě běžného phishingu je trestně právní postih za podvod dle § 209 a neoprávněné opatření, padělání a pozměňování platebního prostředku dle § 209 a § 234 TrZ. Pokud pachatel využije získané informace k vydírání společnosti nebo jednotlivce, mohlo by se jednat i o trestný čin vydírání § 175 TrZ.

Za formu spear phishingu by se dali považovat i phishingové útoky prostřednictvím facebooku, kdy pachatel napadne některý facebookový účet. Z něj si zjistí informace o přátelích napadeného, které následně kontaktuje, vydávající se poškozeného. Komunikace končí zasláním žádostí o půjčku, s odkazem na phishingovou stránku, jak bylo uvedeno u phishingu.

[96] http://www.lidovky.cz/zada-vas-facebooky-pritel-o-penize-jde-o-podvod-varuje-policie-pu5-/zpravy-domov.aspx?c=A140601_163704_ln_domov_sk

[97] http://www.securitymagazin.cz/technologie/ceska-sporitelna-varuje-nova-podoba-podvodneho-emailu-1404043728.html

Malware

Právní postih za malware souvisí s účelem, který má daný malware. U většiny virů přichází v úvahu postih dle § 230 TrZ za neoprávněný přístup k počítačovému systému a nosiči informací[98]. V případě ransomware lze pachatele stíhat pro trestný čin vydírání dle § 175 TrZ [99]. Dále zmiňuje autor Kolouch další právní postihy, například při získávání utajovaných informací například postih za teroristický útok (§311), vyzvědačství (§316) nebo ohrožení utajené informace (§317 TrZ).

Jako příklad útoku pomocí malware lze zmínit některé případy phishingu, jak bylo uvedeno již výše, případně útok ransomwaru, který zablokuje počítač a zobrazí pouze stránku s výzvou, že počítač byl zablokován policií, neboť se v něm nachází nezákonný obsah a oběť má zaplatit určitou částku, aby jí byl počítač odblokován, jinak se vystavuje trestnímu stíhání[100]. Tento typ ransomwaru je rozšířený nejenom v ČR, ale v celé EU.

Sniffing

Sniffing jako neoprávněný odposlech dat lze postihnout dle § 182 TrZ jako porušování tajemství doručovaných zpráv, případně § 183 porušování tajemství listin a jiných dokumentů uchovávaných v soukromí. Je zde nutné zkoumat hledisko neoprávněného odposlechu, neboť se tohoto skutku mohou dopouštět i společnosti, které sledují například komunikaci svých zaměstnanců.

V nedávné době bylo možné pomocí sniffingových programů snadno sledovat komunikaci na síti, v dnešní době již jednoduché sledování není možné, neboť většina komunikace, například na sociálních sítích je realizována prostřednictvím https protokolu, který komunikaci šifruje, aby tomuto sledování zabránil. V úvahu připadají různé viry, které mohou také sledovat komunikace, nebo například keyloggery, odchytávající zadaná hesla.

DoS a DDos útoky

Jedná se o kybernetické útoky, které směřují přímo proti telekomunikačnímu zařízení, které se snaží svým útokem vyřadit z provozu. Takovýto útok může být kvalifikován jako teroristický čin dle § 311 TrZ, pokud by směřoval proti ústavnímu

[98] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 394
[99] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 149
[100] http://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/

zřízení nebo obranyschopnosti České republiky[101]. V případě, že čin nesměřuje přímo proti České republice, ale proti konkrétním společnostem, či zařízením, přichází v úmyslu postih za trestný čin poškození a ohrožení provozu obecně prospěšného zařízení dle § 276 a 277 TrZ, jelikož mezi tato zařízení spadají také zařízení a sítě elektronických komunikací, a koncová telekomunikační a rádiová zařízení, případně i zařízení držitele poštovní licence[102]. V případě útoků na společnosti, nebo zařízení, které nespadají pod obecně prospěšné zařízení, připadá v úvahu pouze postih za poškození cizí věci dle § 228, kde však je složitější prokazování způsobené škody, která poškozením či dočasným vypnutím zařízení vznikla.

Jako příklad je možné připomenout případ z roku 2013, kdy byla napadena většina českých zpravodajských serverů, přičemž se má za to, že útoky směřovali na tyto servery z Ruska[103].

Cybersquatting

V případě neoprávněného obsazení doménového jména, se právně jedná většinou o obchodně právní spor. Spory jsou převážně řešeny mimosoudní cestou, případně Rozhodčím soudem při Hospodářské komoře ČR a Agrární komoře ČR[104]. Domény registrované s příponou .cz zpravuje spol. CZ.NIC, která také pomáhá případně spory řešit.

V trestně právní rovině by se v případě neoprávněné registrace doménového jména a jeho zneužití mohlo jednat o Porušení práv k ochranné známce a jiným označením dle § 268 TrZ, případně o Porušení předpisů o pravidlech hospodářské soutěže dle § 248 TrZ. Pokud by dále majitel nelegálně registrované domény vyhrožoval majiteli značky například tím, že pokud si doménu neodkoupí, umístí na ní nevhodný obsah, mohl by se dopustit trestného činu vydírání dle § 175 TrZ.

Hacking

Jedná se o přístup do počítačového systému jinou, než standartní cestou, většinou prolomením bezpečnostního opatření. Jak již bylo řečeno výše, nemusí se vždy jednat o trestnou činnost, tzv. „white hats“ přistupují k systému se svolením jeho správce, vyhledávají bezpečnostní skuliny a tím se snaží zlepšit jeho zabezpečení. V ostatních

[101] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 107
[102] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 117
[103] http://www.lupa.cz/clanky/ihned-cz-je-nedostupny-zrejme-celime-utoku-rika-redakce/
[104] https://www.nic.cz/page/314/pravidla-a-postupy/

případech se však „hacker“ dopouští trestného jednání, nezávisle na tom, zda způsobil nějakou škodu, neboť již pouze „překonání bezpečnostního opatření a tím nelegální získání přístupu k počítačovému systému nebo jeho části“ je trestné jde § 230 odst. 1 TrZ. Dále jsou trestná další jednání, při nichž pachatel využije například volně přístupného uživatelského účtu a v něm provede neoprávněně změny, například neoprávněně užije data, nebo vloží data do systému, dle § 230 odst. 2 TrZ. V případě způsobení škody, či získání prospěchu přichází úvahu již naplnění kvalifikované skutkové podstaty. Prolomení zabezpečení a získání přístupu k systému muže být jediným cílem hackera, jak bývalo častější v dřívějších dobách. Nyní to však bývá většinou začátek jeho jednání, je tedy častý souběh s dalšími trestnými činy, podle toho, jakého dalšího jednání se pachatel po nelegálním přístupu do systému dopustí[105].

Jako příklad jednání lze zmínit například phishingové útoky, při nichž je prolomeno zabezpečení facebookového účtu, z něhož je následně komunikováno s poškozenými, jak bylo uvedeno u phishingových útoků.

Cracking

Cracking souvisí s pojmem hacking, neboť hackeři „black hats[106]“ bývají často označování v literatuře jako „crackeři“. Druhé chápání pojmu souvisí s porušování autorských práv, kde „crack“ je označování pro prolomení zabezpečení daného programu, či jiného obcházení ochranných prvků, například chránícím před vytvářením nelegálních kopií[107].

V trestně právní rovině lze úmysl pachatele postihnou dle § 230 TrZ jako Neoprávněný přístup k počítačovému systému a nosiči informací, případně dle § 231 TrZ jako Opatření a přechovávání přístupového zařízení a hesla k počítačovému sytému a jiných takových dat. Dále by mohlo dojít k porušení § 270 TrZ Porušení autorského práva a práv souvisejích s právem autorským a práv k databázi, při nelegálním šíření díla.

Internetové pirátství

Obecný pojem označuje trestné činy týkající se porušování autorských práv za předpokladu, že je k činnosti využíván internet. Postih této trestné činnosti je

[105] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 406
[106] http://www.pctools.com/security-news/crackers-and-hackers/
[107] KOLOUCH Jan. VOLOVECKÝ Petr, Trestně právní ochrana před kybernetickou kriminalitou, str. 52

problematický vzhledem k rozdílné právní úpravě v jednotlivých státech, kdy například v České republice stažení kopie audiovizuální díla pouze pro vlastní potřebu nemusí být trestné. Celková problematika autorských práv je poměrně rozsáhlá[108] a její podrobný rozbor je mimo zaměření této práce.

Trestně právní postih přichází v úvah za trestný čin Porušování autorského práva, práv souvisejících s právem autorským a práv k databází dle § 270 TrZ. V případě nižší intenzity porušení autorského zákona jde jednání klasifikovat dle správního práva jako přestupek.

Racketeering

Jedná se o klasický trestný čin vydírání dle § 175 TrZ, s případným souběhem trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TrZ, za předpokladu, že pachatel skutečně do systému vnikne.

Šíření závadového obsahu

V souvislosti se šířením závadového obsahu lze z hlediska trestního práva postihnout dvě skupiny trestných činů.

První skupina souvisí se šířením zakázané pornografie, zejména dětské pornografie a souvisejícího jednání. Jedná se o trestné činy dle § 191 až 192b TrZ. Trestné může být jak šíření, tak již prosté držení zakázaného materiálu.

Druhou skupinu tvoří šířeních nenávistných a extremistických sdělení. Jedná se například o Založení, podporu a propagaci hnutí směřujícího k potlačení práv a svobod dle § 403 TrZ, projev sympatií k takovémuto hnutí dle § 404 TrZ, ale i další činy související například další trestní činy uvedené v § 352 až § 356 TrZ, jako hanobení národa, rasy, etnické a jiné skupiny osob, podněcování nenávisti a další.

Jako šíření závadového obsahu by také bylo možné klasifikovat další klasické trestné činy prováděné prostřednictvím ICT, například pomluva § 184 TrZ, ale i nebezpečné vyhrožování § 185 TrZ, nebezpečné pronásledování § 254 TrZ a další. Způsobů spáchání těchto trestných činů je celá řada, závadový obsah je možné šířit prostřednictvím snad všech užití ICT.

[108] Např. SMEJKAL, Vladimír, Kybernetická kriminalita, str. 357 a dále

Kyberterorismus

Kyberterorismus je teroristický čin za užití informačních či komunikačních technologií. Za účelem ochrany před kybernetickými útoky byl přijat zákon č. 181/2014 Sb., který upravuje celou řadu oblastí týkajících se kyberprostoru a bezpečnosti v něm. Za kyberterorismus lze považovat i řadu jednání zde již uvedenou, například DoS útoky, pokud směřují proti státnímu zřízení s cílem je destabilizovat, případně proti větší skupině obyvatelstva, například s cílem je zastrašit[109]. V souvislosti s kyberterorismem je třeba zmínit i mediální terorismus, jehož cílem je mediální prezentace teroristů a jejich útoků s cílem zasáhnout strachem větší skupinu lidí, než na které míří skutečná teroristický hrozba[110]. V dnešní době se tak děje nejčastěji za pomoci internetu a dalších telekomunikačních zařízení.

Teroristický útok naplňuje znaky trestného činu dle § 311 TrZ, v případě méně závažné motivace pachatelů se může jednat o Obecné ohrožení dle § 272 TrZ.

Card skimming

Card skimming úzce souvisí s phishingem, od něhož se liší pouze v získávání údajů o platebních kartách. V případě card skimmingu se jedná o kopírovací zařízení, které je umístěné na bankomatu nebo platebním terminálu. Dále je již postup pachatele stejný jako u phishingového, kdy pachatel za pomoci těchto údajů o kartě odčerpá z účtu finanční prostředky.

Z hlediska trestního práva se jedná o trestný čin neoprávněného opatření, padělání a pozměňování platebního prostředku dle § 234 TrZ, případně o podvod dle § 209 TrZ.

Card skimmingové útoky jsou běžné[111], složitá je jejich mezinárodní provázanost, kdy je v jednom státě prováděno kopírování karet a jejich užití je následně v jiném státě, tak aby bylo ztíženo vysledování pachatele.

3.4.3 Úprava v dalších zákonech

Ve vztahu ke kybernetické kriminalitě je třeba zmínit i další zákony, které se této oblasti dotýkají. Některé již byly zmíněny u jednotlivých druhů kybernetické kriminality,

[109] SMEJKAL, Vladimír, Kybernetická kriminalita, str. 86

[110] http://www.ozbrojeneslozky.cz/clanek/atraktivita-terorismu-pro-medialni-zpravodajstvi-vyvoj-vztahu-mezi-terorismem-a-medii

[111] http://karvinsky.denik.cz/z-regionu/zlocinci-napichli-bankomat-v-centru-ostravy-vybrali-penize-nic-netusicim-lidem-2-449s.html

pokud se tato kriminalita zákona přímo dotýká. Souvisejících zákonů a vyhlášek bychom nalezli jistě nepočetně více[112], zde uvedeme jen několik, z pohledu autora významných, které se přímo týkají kybernetické kriminality, případně toho, jak jí lze předcházet.

Zákon č. 121/2000 Sb., Autorský zákon

Autorské právo chrání jednotlivá díla, dále počítačové programy a databáze, jak je uvedeno v § 2 tohoto zákona. V autorský zákon upravuje, za jakých podmínek je možné šířit chráněná díla, za jakých podmínek je možné vytvářet kopie těchto děl. Dále jsou v zákoně uvedeny správní delikty, kterých se dopustí fyzická nebo právnická osoba při porušení tohoto zákona.

Na autorský zákon se odkazuje trestní zákoník v § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi a následujících. Bez autorského zákona, který upřesňuje autorské právo, by nebyl možný postih v této oblasti.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon vymezuje pojmy v oblasti kybernetické bezpečnosti. Vztahuje se na právnické a fyzické osoby, které jsou brány jako kritická informační struktura, nebo významná síť. V zákoně jsou popsány bezpečnostní opatření, druhy kybernetických incidentů a útoků a kroky, které je třeba učinit, když k útokům nastane.

Spolu se zákonem byly vydány související prováděcí vyhlášky a to vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti a vyhláška č. 317/2014 Sb. o významných informačních systémech. Zejména vyhláška o kybernetické bezpečnosti uvádí organizační opatření a opatření technické povahy, která mohou být užitečná nejenom subjektům, na které se zákon a vyhláška vztahují, ale mohou být i pomocí pro další společnosti, které chtějí svojí kybernetickou bezpečnost pojímat komplexně.

Zákon č. 127/2005 Sb., o elektronických komunikacích

Zákon upravuje podmínky podnikání a výkon státní správy v oblasti elektronických komunikací. Upravuje činnost poskytovatelů internetového i televizního vysílání a

[112] Smejkal uvádí, že pojem Internet se vyskytuje v české legislativě více než 2000x, SMEJKAL, Vladimír, Kybernetická kriminalita, str. 65

mobilních operátorů a zřizuje Český telekomunikační úřad, který na trh v oblasti elektronických komunikací dohlíží a rozhoduje případně spory. Kromě regulace komunikačních činností obsahuje i ustanovení o právech a povinnostech spotřebitelů a podnikatelů, ustanovení o ochraně údajů, služeb a sítí elektronických komunikací. V neposlední řadě uvádí správní delikty, kterých se jednotlivé subjekty dopustí při porušení zákona.

Zákon č. 480/2004 Sb., o některých službách informační společnosti

Zákon upravuje odpovědnost a práva a povinnosti osob, které šíří obchodní sdělení elektronickými prostředky. Také někdy bývá nazýván médii Antispamový zákon. Upravuje, kdy nám může být zasíláno obchodní sdělení (většinou nabídka), kdy je a kdy není potřeba souhlas k zasílání těchto sdělením. Obsahuje také správní delikty, kterých se právnické osoby mohou při porušení tohoto zákona dopustit.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Zákon o službách vytvářejícím důvěru pro elektronické transakce nahradil zákon č. 227/2000 Sb. o elektronickém podpisu, tak aby jednotlivá ustanovení byla v souladu s evropským právem. Kromě ustanovení o elektronickém podpisu obsahuje zákon ustanovení o elektronickém časovém razítku a elektronické pečeti.

V souvislosti se zabezpečením informačních systémů je třeba zmínit také ustanovené Občanského zákoníku, který nám kromě ustanoveních o občanské odpovědnosti a o náhradě škody hovoří také o svépomoci: „*Každý si může přiměřeným způsobem pomoci k svému právu sám, je-li jeho právo ohroženo a je-li zřejmé, že by zásah veřejné moci přišel pozdě.*[113]“

Vzhledem k rychlosti a komplexnosti, se kterou se dějí jednotlivé útoky kybernetické kriminality, mělo by být hlavně na uživatelích, aby se sami snažili předcházet těmto útokům a sami si zajistili svoji bezpečnosti. Státní orgány těžko mohou zastavit již probíhající útok, vždy budou jen napravovat škody a zjišťovat viníka.

[113] § 14 odst. 1) zákona č. 89/2012 Sb., Občanský zákoník

3.4.4 Právní úprava v mezinárodních dokumentech

Z pohledu České republiky jsou nejdůležitější mezinárodní dokumenty dvě úmluvy přijaté Radou Evropy a to Úmluva Rady Evropy o kybernetické kriminalitě[114], přijatá v listopadu 2001 a Dodatkový protokol[115], k této úmluvě. Tyto dokumenty mají pomoci sladit jednotlivé právní systémy zemí EU, aby mohl být boj proti kybernetické kriminalitě efektivnější. Jednotlivé země Evropské unie upravují svoje právní systémy tak, aby byly v souladu s těmito úmluvami a umožnily jednotné stíhání vymezených kybernetických trestných činů. Česká republika ratifikovala Úmluvu v roce 2013, s účinnosti dokumentu od 1.12.2013.

Úmluva o kybernetické kriminalitě.

Úmluva se skládá z preambule a 48 článků, které se dělí do čtyř kapitol.

- Kapitola I – Užití pojmů
- Kapitola II – Opatření, která mají být přijata na vnitrostátní úrovni
- Kapitola III – Mezinárodní spolupráce
- Kapitola IV – Závěrečná ustanovení

První kapitola obsahuje definice základních pojmů počítačový systém, počítačová data, poskytovatel služby a provozní data.

Druhá kapitola v první části, týkající se trestního práva hmotného, definuje čtyři skupiny kybernetických trestných činů a popisuje následně v jednotlivých článcích jednotlivé trestné činy, upřesňuje jejich skutkové podstaty. Dále je zde ustanovení o pokusu, účastenství, trestní odpovědnosti právnických osob a o trestech. V druhé části, týkající se trestního práva procesního, jsou ustanovení o působnosti, dále jednotlivá ustanovení, která mají umožnit státům lépe zajišťovat a vyhodnocovat zájmová data. Ve třetí části hovoří úmluva o stanovení trestní soudní pravomoci.

Třetí kapitola hovoří o mezinárodní spolupráci orgánů činných v trestním řízení, o vydávání osob, vzájemné pomoci v oblasti vyřizování žádostí, vyšetřování a poskytování zajištěných dat.

[114] Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001
[115] Dodatkový protokol k Úmluvě o kybernetické kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů ze dne 28. ledna 2003

Závěrečná kapitola popisuje působnost Úmluvy, platnost, účinky a hovoří o řešení sporů o výklad úmluvy.

Dělení kybernetických trestných činů dle Úmluvy o kybernetické kriminalitě:

1) Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů
   a) Nezákonný přístup
   b) Nezákonný odposlech
   c) Zasahování do dat
   d) Zasahování do systému
   e) Zneužívání zařízení
2) Trestné činy související s počítačem
   a) Počítačové padělání
   b) Počítačový podvod
3) Trestné činy související s obsahem
   a) Trestné činy související s dětskou pornografií
4) Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským
   a) Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

Dodatkový protokol k Úmluvě o kybernetické kriminalitě

Dodatkový protokol k úmluvě byl přijat v lednu 2003, aby vyplnil mezeru v Úmluvě o kybernetické kriminalitě, která v souvislosti s šířením závadového obsahu obsahuje ustanovení pouze o šíření dětské pornografie, neobsahuje však zmínku o šíření dalšího závadového obsahu. Dodatkový protokol k Úmluvě doplňuje Úmluvu a vymezuje znaky trestných činů, týkajících se šíření rasistického a xenofobního materiálu.

Dodatkový protokol se skládá ze čtyřech kapitol. V první kapitole je popsán účel Protokolu a definován rasistický a xenofobní materiál. V druhé kapitole jsou definovány trestné činy šíření rasistických a xenofobních materiálů pomocí počítačových systémů, dále rasisticky a xenofobně motivované vyhrožování, rasisticky xenofobně motivované útoky a popírání, snižování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti. Třetí kapitola popisuje vztah mezi Úmluvou a Protokolem, kdy se některé

části a články Úmluvy přiměřeně užijí i na Protokol. Poslední kapitola obsahuje ustanovení týkající s účinnosti, platnosti, podobně jako Úmluva.

Česká republika ratifikovala Dodatkový protokol k Úmluvě o kybernetické kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů dne 7. srpna 2014 s platností od 1. prosince 2014.

Právní úprava kyberkriminality Spojených států amerických

Jedna z prvních zemí, které přijali právní úpravu týkajících se počítačových trestných činů, byly Spojené státy americké (USA). V současné době nadále platí, že právní úprava USA a mezinárodní smlouvy, které USA ratifikovaly, určují hlavní směr, kterým se ICT ubírá, neboť zde sídlí největší společnosti podnikající v ICT, a také velké množství definičních autorit internetu, které všechny podléhají právnímu systému USA.

První právní úprava USA, týkající se počítačové kriminality, pochází již z roku 1986, kdy byl přijat Kongresem Zákon o počítačových podvodech The Computer Fraud and Abuse Act (CFAA)[116]. Zákon by několikrát novelizován a je stále platný. Popisuje sedm počítačových aktivit, které jsou trestné[117]: neoprávněný přístup k počítači za účelem získání informace z národní bezpečnosti v úmyslu poškodit USA nebo zajistit prospěch jinému státu; neoprávněný přístup k počítači za účelem získání finanční nebo úvěrové informace; neoprávněný přístup k počítači užívanému federální vládou; neoprávněný přístup k chráněnému počítači v úmyslu se obohatit na úkor jiného; úmyslné poškození chráněného počítače; podvodné obchody s počítačovými hesly nebo jinými informacemi umožňující přístup k chráněnému počítači; ohrožování chráněného počítače v úmyslu vynucení poskytnutí peněz nebo jiných hodnot. Jako chráněný počítač popisuje zákon počítač užívaný finanční institucí nebo vládou USA nebo počítač užívaný v mezistátním či mezinárodním obchodu. Na následné novelizaci zákona CFAA již spolupracovala organizace EFF, která dohlíží na dodržování základních práv a svobod na internetu.

V roce 1986 byl také přijat federální zákon, který zajišťuje soukromí elektronické komunikace. Další státy, které postupně zaváděli právní normy týkající se počítačové kriminality, vycházeli většinou alespoň částečně z právní úpravy USA, které jsou v této

[116] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers, dostupný na https://www.law.cornell.edu/uscode/text/18/1030

[117] https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29,

oblasti průkopníkem. Jako jedna z dalších zemí, která následovala USA, bylo Spojené království v roce 1990[118]. V roce 2014 Kongres schválil čtyři nové zákony týkající se kybernetické bezpečnosti. Jedná se o zákon o modernizaci federální informační bezpečnosti, zákon o ochraně národní kybernetické bezpečnosti, zákon o posílení kybernetické bezpečnosti a zákon o posouzení kybernetické bezpečnosti pracovní síly.

V těchto nových zákonech je jasný posun v chápání kybernetické bezpečnosti, zesílení důrazu na celou tuto oblast a snaha o sjednocení spolupráce soukromého i veřejného sektoru. Lze očekávat, že podobný vývoj bude následovat i právní úprava Evropské unie.

3.5 Metody prevence kriminality dětí a mladistvých v oblasti informační kriminality

Prevence kriminality tvoří důležitou součást boje proti kriminalitě. V České republice je tradice prevence kriminality od počátku vzniku samostatné České republiky v roce 1993, odkdy je pravidelně formována jako součást vládní politiky. Od roku 1996, kdy byla přijata první Strategie prevence kriminality, se rozvíjí systém spolupráce mezi jednotlivými složky vlády i státní samosprávy a organizací. „*V oblasti kriminality vláda deklarovala, že považuje za „výhodnější zaměření na prevenci, zejména v oblasti kriminality mladistvých.*[119]“ Strategie se zaměřuje na kriminalitu obecně, neřeší jednotlivé druhy kriminality, pro které jsou následně přijaty konkrétní dokumenty ze strany organizací, které se zaměřují na danou oblast.

3.5.1 Základní terminologie

Pojem prevence je definován jako: „*všechna opatření směřující k předcházení a minimalizace jevů spojených s rizikovým chováním a jeho důsledky. Prevencí může být jakýkoliv typ výchovné, vzdělávací, zdravotní, sociální či jiné intervence směřující k předcházení výskytu rizikového chování, zamezující jeho další progresi, zmírňující již existující formy a projevy rizikového chování nebo pomáhající řešit jeho důsledky.*[120]“

[118] International Comparison of Cyber Crime, str. 17
[119] Strategie prevence kriminality v České republice na léta 2016 až 2020, str. 3
[120] Národní strategie primární prevence rizikového chování na období 2013-2018, str. 8

Pojem **rizikové chování** znamená všechny formy chování, které mají negativní dopad na zdraví, sociální nebo psychologické fungování jedince a jeho okolí.

Prevenci jako takovou děláme do tří skupin na primární, sekundární a terciální[121]. **Primární prevence** je zaměřena na celou populaci, snaží se působit ještě před vznikem nebezpečné situace, tak aby k ní ani nedošlo. **Sekundární prevence** se zaměřuje již na vybrané rizikové skupiny obyvatelstva, vybrané dle věku, ohrožení, sociálního či situačního prostředí. **Terciální prevence** představuje programy, zaměřené na osoby, které již byly pachateli, nebo oběťmi, aby se znovu do dané situace nedostali.

Ve vztahu k tématu práce se z těchto tří skupin budeme hovořit o primární prevenci, neboť ta působí ještě před vznikem nebezpečné situace a snaží se jí předcházet. Primární prevenci dále dělíme na nespecifickou, která není konkrétně zaměřena a na specifickou, která je již zaměřena na konkrétní cílovou skupinu, v našem případě děti a mládež. Ministerství školství dělí dále specifickou prevenci do tří úrovní na[122]:

- **Všeobecnou primární prevenci** – je zaměřena na běžnou populaci dětí a mládeže, zohledňuje pouze věková kritéria. Jedná se většinou o programy pro větší počet účastníků (obvykle třída, skupiny do 30 účastníků).
- **Selektivní primární prevenci** – je zaměřena na skupiny osob, u kterých jsou ve zvýšené míře přítomny rizikové faktory pro vznik a vývoj různých forem rizikového chování a jsou většinou více ohrožené než jiné skupiny populace. Pracujeme zde s menšími skupinami, případně i jednotlivci.
- **Indikovanou primární prevenci** – je zaměřena na jedince, u kterých se již vyskytly projevy rizikového chování. Jedná se o práci s populací s výrazně zvýšeným rizikem výskytu či počínajících projevů rizikového chování. Jedná se o individuální práci s klientem

Oblasti, na které se primární prevence se u žáků zaměřuje, jsou následující skupiny rizikového chování u dětí a mládeže:

- Interpersonální agresivní chování - agrese, šikana, kyberšikana a další rizikové formy komunikace prostřednictvím multimédií, násilí, intolerance,

[121] Strategie prevence kriminality v České republice na léta 2016 až 2020, str. 38
[122] Národní strategie primární prevence rizikového chování na období 2013-2018, str. 9

antisemitismus, extremismus, rasismus a xenofobie, homofobie

- Delikventní chování ve vztahu k hmotným statkům – vandalismus, krádeže, sprejerství a další trestné činy a přečiny
- Záškoláctví a neplnění školních povinností
- Závislostní chování – užívání všech návykových látek, netolismus, gambling
- Rizikové sportovní aktivity, prevence úrazů
- Rizikové chování v dopravě, prevence úrazů
- Spektrum poruch příjmu potravy
- Negativní působení sekt
- Sexuální rizikové chování

Z uvedeného přehledu je patrné, že prevence kybernetické kriminality bude spadat do více skupin rizikového chování, zejména do Interpersonálního agresivního chování a Delikventní chování ve vztahu k hmotným statkům.

3.5.2 Popis současné situace v oblasti prevenci kybernetické kriminality

Součástí **Strategie prevence kriminality v České republice na léta 2016 až 2020** je globální cíl: „*Česká republika se řadí mezi moderní demokratické země, které v zajišťování bezpečnosti a veřejného pořádku podporují preventivní přístupy, k čemuž vytváří vhodné systémové, organizační i finanční předpoklady*[123].“ Je možné polemizovat s tímto názorem, zvláště se zajištěním finančních předpokladů. Dlouhodobý trend kriminality však skutečně vykazuje pokles, dle Vyhodnocení strategie pro rok 2012 až 2015 dokonce o téměř 15 %[124]. Jediné dvě oblasti, kde dochází k vzestupu kriminality, jsou drogová kriminalita, kde dle Vyhodnocení zaznamenáváme nárůst o 46 % a pak kybernetické kriminalita, kde je patrný nárůst o téměř 30 % každý rok. Dále je odhadováno, že velké množství této kriminality zůstává latentní (skryté), dle Vyhodnocení se jedná o až 90 % z celkového množství.

Koncepci a koordinaci preventivní politiky má na starost mezirezortní Republikový výbor pro prevenci kriminality. Tento na úrovni vlády předkládá zprávy, které jsou projednávány také v Poslanecké sněmovně Parlamentu České republiky. Rozvoj systému

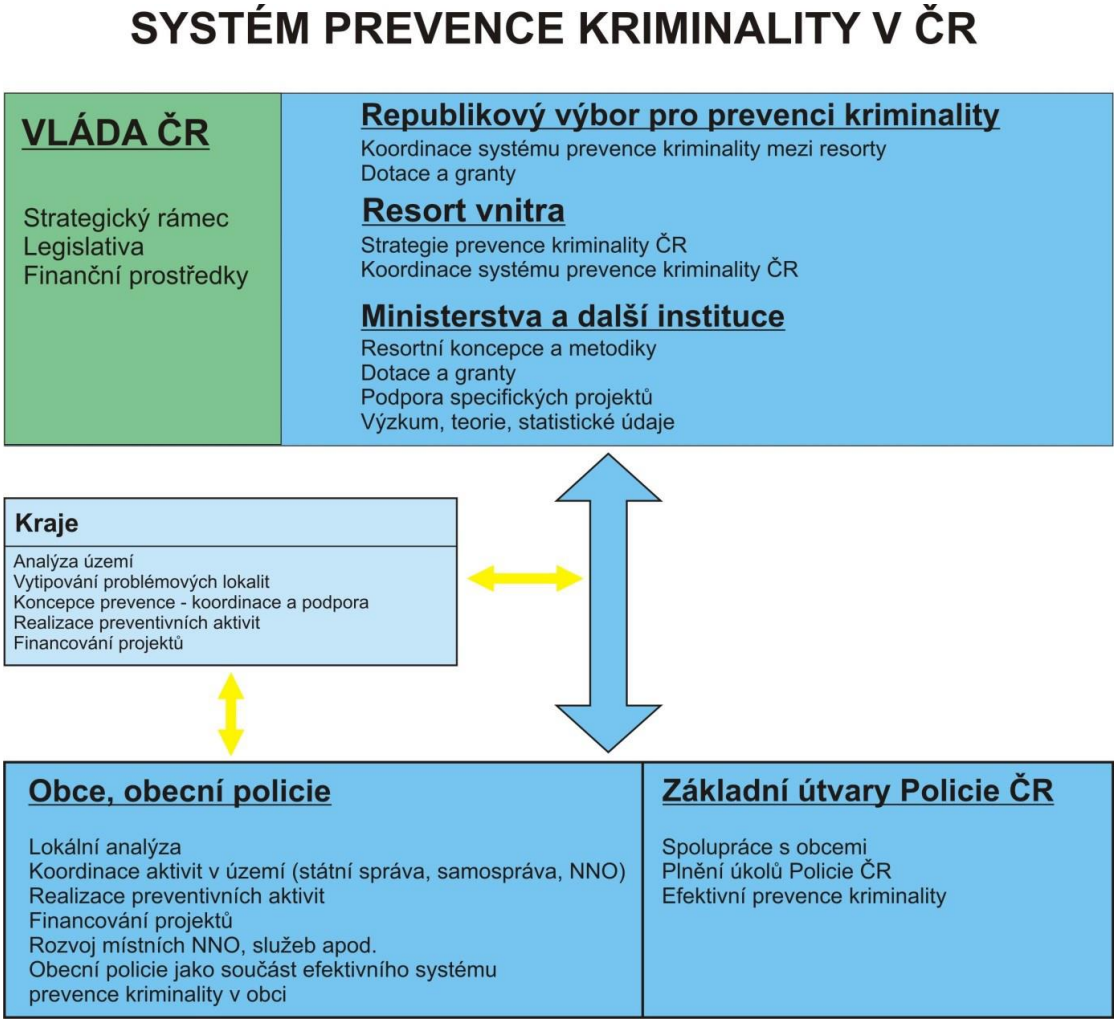
[123] Strategie prevence kriminality v České republice na léta 2016 až 2020, str. 6
[124] Vyhodnocení Strategie prevence kriminality v České republice na léta 2012 až 2015, str. 4

dále zajišťuje Ministerstvo vnitra, které koordinuje součinnost jednotlivých subjektů. Ministerstvo vnitra také zastupuje Českou republiky v rámci mezinárodních orgánů v rámci OSN (Komise OSN pro prevenci kriminality a trestní justici a dalších) a Evropské unie, kde je Česká republika součástí Evropské sítě prevence kriminality (EUropean Crime Prevention Network, dále EUCPN).

EUCPN stanovuje úkoly členským zemím prostřednictvím víceletých strategií a snaží se posílit a zefektivnit prevenci napříč Evropskou unií, což vzhledem k rozdílným právním systémům i kulturně historickým tradicím je náročný úkol. Tato organizace také každoročně vyhlašuje soutěž o Evropskou cenu prevence kriminality a na projekty přispívá z prostředku Evropské unie. Za Českou republiku lze zmínit například projekt E-Bezpečí, který se zabývá nebezpečnými internetovými fenomény[125], a který získal v roce 2015 1 místo v mezinárodním kolem Evropské ceny prevence kriminality.

Schéma spolupráce mezi jednotlivými subjekty v oblasti prevenci popisuje přehledně následující schéma.

[125] https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu



Obrázek 1: Schéma systému prevence kriminality v ČR, zdroj: Strategie prevence kriminality v České republice na léta 2016 až 2020

Policie ČR se prevencí zabývá v rámci plnění svých úkolů, jednotlivá opatření však byla v kompetenci jednotlivých krajských ředitelství a byla vykonávána různě. V současné době již byla přijata **Koncepce prevence kriminality Policie ČR pro léta 2014 – 2016** a která „*pojímá prevenci kriminality jako princip, který prostupuje všemi hlavními oblastmi policejní práce, přičemž preventivní dopady má mnoho policejních aktivit, a zároveň Koncepce přiznává, že dosud formálně a v každodenní praxi tyto aktivity jako prevence ještě chápány nejsou.*[126]“ Prevence ze strany Policie ČR fungovala na dobré úrovni v rámci lokálních problémů, kdy je běžná spolupráce s obcemi i s Obecními a Městskými policiemi. Strategie prevenci kriminality dále hodnotí Koncepci prevence kriminality

[126] Strategie prevence kriminality v České republice na léta 2016 až 2020, str. 16

Policie ČR tak, že „*obsahuje pouze vize, strategické cíle, jak se s těmito problémy vypořádat, avšak bez konkrétních úkolů, termínů a odpovědností*.“ Plošněji se Policie ČR věnuje pouze různým preventivním akcím v oblasti bezpečnosti provozu.

Ministerstvo vnitra ČR se také v oblasti prevence kriminality se věnuje informování občanů o možnostech ochrany před trestnou činností a upozorňuje prostřednictvím informačních kampaní na nové druhy kriminality. V letech 2012 – 2015 jednalo o prevenci kriminality rizikových jevů v oblasti virtuální komunikace. Bylo partnerem projektu E-Synergie (E-Bezpečí), který realizovalo Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci. O projektu bude podrobněji hovořeno dále. Dále Ministerstvo vnitra podporuje kraje a obce v rámci dotačních titulů.

Stěžejní úlohu v prevenci kriminality u dětí a mladistvých má Ministerstvo školství, mládeže a tělovýchovy (dále MŠMT). MŠMT stanovuje strategie, na základě kterých pak postupují podřízené orgány. Přijímá jako hlavní dokument Národní strategii, momentálně **Národní strategii primární prevence rizikového chování na období 2013 – 2018**, ve které „*vychází ze závěrů pravidelných jednání s krajskými školskými koordinátory prevence a metodiky prevence, z dlouhodobých cílů stanovených Strategiemi meziresortních orgánů*.[127]“ MŠMT hlavně koordinuje jednotlivé subjekty podílející se na prevenci. V Národní strategii je uvedeno, že aby byla primární prevence účinná, musí být realizována ve spolupráci mnoha subjektů, např. škol, školských poradenských zařízení, zákonných zástupců, neziskových organizací, OSPODů, Policie ČR, vysokými školami a dalšími subjekty.

Systém koordinace, jak je popsán v Národní Strategii probíhá na horizontální a vertikální úrovni. Na horizontální úrovní spolu spolupracují MŠMT, Ministerstvo zdravotnictví, Ministerstvo vnitra a Úřad vlády České republiky. Většinou se jedná o projekty, které se netýkají prevence před kybernetickou kriminalitou, s výjimkou projektů Ministerstva vnitra.

Na vertikální úrovni je prevence koordinována tak, aby byly jednotlivé aktivity přiblíženy problémům v konkrétní oblasti, na regionální i místní úrovni. MŠMT na

[127] Národní strategie primární prevence rizikového chování na období 2013-2018, str. 3

vertikální úrovni metodicky řídí činnost krajských školských koordinátorů prevence, což jsou pracovníci krajských úřadů, metodiků prevence, což jsou pracovníci konkrétních pedagogicko-psychologických poraden, a prostřednictvím krajských školských koordinátorů prevence a metodiků prevence metodicky vedou činnost školních metodiků prevence, což jsou přímo učitelé, kteří vykonávají tuto činnost ve školách.

Školní metodik prevence vytváří a realizuje prevenci prováděnou v konkrétní škole, každá škola musí mít svého školního metodika prevence. Standardní činnosti školního metodika prevence jsou vymezeny ve vyhlášce č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních. Podílí se na přípravě Školního preventivního programu, což je dlouhodobý preventivní program, který je i součástí školního vzdělávacího programu, který má každá škola vytvořený a dle kterého se řídí vzdělávací proces ve škole. Dále se podílí na vytváření Minimálního preventivního programu, což je dokument školy, který škola vytváří vždy na aktuální školní rok a za který zodpovídá metodik. V tomto dokumentu lze reagovat na aktuální problémy ve škole, obsahuje konkrétní aktivity prováděné v průběhu roku a měl by obsahovat i seznam spolupracujících organizací, které se spolupodílí na prevenci ve škole. Minimální preventivní plán obsahuje i výčet vzdělávacích oblastí dle Školního vzdělávacího plánu, ve kterých bude v průběhu roku realizována preventivní činnost v rámci výuky jednotlivých předmětů. Důležitou součástí práce školního metodika by měla být také komunikace s ostatními učiteli a koordinace jednotlivých vzdělávacích pořadů a preventivních akcí, kterých se škola účastní.

3.5.3 Působící organizace a jejich programy

Různých organizací, které se podílí na prevenci kriminality, je velké množství a mají různá zaměření. Zde byly vybrány některé známější organizace zaměřené konkrétně na prevenci kybernetické kriminality, které působí v celé České republice a které spolupracují se základními školami na krajské nebo celostátní úrovni.

Seznam se bezpečně

Jedná se projekt českého internetového portálu Seznam.cz[128], který vznikl v roce 2008 v reakci na vzestup nebezpečného chování na sociálních sítích tohoto portálu, převážně na chatech serveru Lidé.cz. Cílem projektu je varovat před nebezpečnými jevy na

[128] http://www.seznamsebezpecne.cz/o-projektu

internetu, se zaměřením hlavně na děti, co jim hrozí, čeho se mají vyvarovat a jak mají postupovat, když se stanou svědky nežádoucího jednání. Součástí projektu jsou besedy s žáky, vzdělávání pedagogů, odborné konference a další činnosti. Nejviditelnější činností projektu jsou jejich filmy, vzdělávací „Seznam se bezpečně“, který má již tři díly a je určen pro prevenci ve školách byl dokonce doporučen MŠMT jako vzdělávací pomůcka a krátké video spoty „Křečci v síti“, který je distribuován po internetu a je srozumitelný i pro děti na prvním stupni školy. Dále se projekt snaží zviditelňovat závažný témata rizikového chování na internetu, například spolupráci s divadlem Studio Ypsilon, se kterým vznikla divadelní hra #jsi_user.

Za svou práci v oblasti prevence škodlivých internetových jevů byl projekt v roce 2013 oceněn Zlatým záchranářským křížem.

Při přípravě práce bylo hovořeno s Martinem Kožíškem, manažerem pro internetovou bezpečnost společnosti Seznam.cz. Při krátkém rozhovoru popsal Kožíšek fungování jednotlivých preventivních programů, které společnost provádí. Zaměřuje se cíleně na žáky škol a v poslední době i na seniory. Témata, kterými se budou jednotlivé pořady zabývat, nemají celkovou koncepci. Při přípravě dalšího programu či video spotu se vychází dle pana Kožíška „z toho, o čem se zrovna hodně mluví, co je momentálně problém“. Zpětnou vazbu, zda je daný program úspěšný, již společnost Seznam.cz nedělá. Ověřuje si, zda byly úspěšné video spoty dle počtu vyhledávání klíčových slov ve spotu a dle počtu zhlédnutí videí. Dle pana Kožíška jsou jejich programy a besedy pro školy úspěšné, neboť mají objednány termíny na celý rok dopředu. Při besedách využívají spolupráce se známými osobnostmi, které žáci znají, například s – Benem Cristovalem, Mirkem Vaňurou nebo Braněm Holičkem.

Témata, kterým se projekty Seznam se bezpečně a Křečci v síti věnují, jsou následující:

- varování před anonymním seznamováním a před zasíláním intimních fotografií
- varování před sociálním inženýrstvím a dětskou prostitucí
- varování před kyberšikanou
- varování před možností zneužití veškerých materiálů nahraných na síť

Všeobecně lze shrnout, že se preventivní programy vytvářené internetovým portálem Seznam.cz se zaměřují pouze na dítě jako oběť.

Projekt E-Bezpečí

Jde o projekt Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého, která na něm spolupracuje i s dalšími organizacemi[129]. Projekt funguje od roku 2008. Cílovou skupinou projektu jsou žáci základních škol, učitelé a pracovníci organizací, podílející se na prevenci, například pracovníci OSPOD, metodici prevence a další. Hlavní náplní projektu je práce v terénu, různé semináře, školení. Kromě vzdělávání zajišťuje tento projekt E-Bezpečí také celorepublikové výzkum v oblasti kybernetického bezpečí, s velmi vysokými počty respondentů, přes 20000 dětí. Každoročně provádí výzkum Nebezpečí internetové komunikace, nebo Výzkum rizikového chování českých dětí v prostředí internetu 2014.

Projekt E-Bezpečí se specializuje zejména na: kyberšikanu a sexting, kybergrooming, kyberstalking a stalking, rizika sociálních sítí, hoax a spam a zneužití osobních údajů v prostředí elektronických médií. Spolupracuje s celou řadou organizací, je podporován MŠMT a MVČR jako celorepublikový preventivní projekt, spolupracuje i s Policií ČR. Dále je partnerem a společně sdílí data s projekty Seznam se bezpečně a s projekty Centra bezpečnosti Google, podporují ho i další soukromé subjekty.

Projekt v roce 2015 získal první místo v národním kole soutěže Evropská cena prevence kriminality (ECPA - European Crime Prevention Award).

Program E-bezpečí má větší množství témat, než Seznam se bezpečně, ale opět je zaměřený pouze na děti a další osoby jako na oběti. Zabývá se tématy, které cílovým skupinám hrozí a jak se těmto hrozbám vyhnout. Při přípravě témat je tento projekt postavený na vědeckých metodách, jeho pracovníci provádí každoročně výzkumy, na základě kterých dále vytváří preventivní programy.

Při přípravě práce byly autoři projektu opakovaně osloveni s žádostí o spolupráci, avšak neúspěšně.

[129] https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

Saferinternet.cz

Projekt uskutečněný neziskovým sdružením Národním centrem bezpečnějšího internetu (NCBI). Cílem projektu je zvyšování povědomí o bezpečnějším užívání internetu, podporuje vzdělávání v této oblasti, a to zejména dětí. Kromě toho sdružení provozuje linku Online helpline, zaměřenou na pomoc obětem kybernetického násilí a spolupracují s linkou Helpline Policie ČR. Projekt se zaměřuje hlavně na konference a školení pro děti a rodiče ve školách, je partnerem preventivního programu Praha bezpečně online, Evropského měsíce kybernetické bezpečnosti a dalších mezinárodních organizací.

Preventivní programy v oblasti kybernetické bezpečnosti poskytuje převážně v Praze, kde je jediným partnerem několika městských částí v této oblasti. Veřejně viditelnější je spíše činnost NCIB jako pořadatele konferencí, než přímo preventivních programů pro děti. Saferinternet se podílí na přípravě pravidelných akcí, například Praha bezpečně online, Evropský měsíc kyberbezpečnosti a Code Week CZ a dalších. Tyto akce však v prevenci nepůsobí na žáky přímo. Dále se podílí na provozu linky Stop online.cz, která slouží převážně pro nahlášení a přímé pomoci při případech kyberšikany a výskytu dětské pornografie.

Během přípravy této práce byly autorem navštívena přednáška pořádaná pro rodiče žáků i přednáška přímo pro žáky na škole v Praze 5. Dále se autor zúčastnil workshopu pořádaného na Praze 13 a konference v Senátu České republiky. Konference zde nebudou hodnoceny, na prevenci se nepodílejí přímo. Během přednášek bylo zaměření témat kyberšikana, sexting, kybergrooming. Přednášky byly doprovázeny reálnými případy, což bylo pro žáky zajímavé a někdy šokující. Přednáška pro rodiče měla v náplni obdobná témata jako přednáška pro žáky. Přednáška pro rodiče byla pro zvýšení její atraktivity spojená s losováním tiskárny na konci přednášky, od čehož si pořadatelé slibovali větší účast rodičů. Posluchače navíc to však na přednášku nepřilákalo, tato forma zakončení působila trapně a rušivě.

Státní organizace

Na prevenci v oblasti kybernetické kriminality se podílejí také státní organizace. Jako gestor problematiky kybernetické bezpečnosti a národní autorita pro tuto oblast byl rozhodnutím vlády zvolen Národní bezpečností úřad a jím řízené Národní centrum

kybernetické bezpečnosti. Jako národní koordinátor kybernetické bezpečnosti má na starosty následující oblasti[130]:

- podílí se na koordinaci a zpracování koncepce zajišťování bezpečnosti státu v oblasti kybernetické bezpečnosti
- koordinuje spolupráci v kybernetické bezpečnosti na národní i mezinárodní úrovni
- koordinuje spolupráci se školami všech stupňů v oblasti vzdělávání v kybernetické bezpečnosti
- koordinuje zapojení NCKB do projektů výzkumu a vývoje

Pracovníci NBU se pravidelně účastní konferencí, připravují témata pro školy. V současné době probíhá například preventivní program pro žáky školy zaměřený na představení naší digitální stopy. Nabídka spolupráce autora s NBU při přípravě této diplomové práce byl z jejich strany vítána, nakonec byla neuskutečněna z důvodů přílišného pracovního vytížení pracovníků NBU, mající tuto problematiku na starost. Národní centrum kybernetické bezpečnosti se potýká s nedostatkem pracovníků, kdy má v rámci prevence na starost i pořádání cvičení kybernetické bezpečnosti.

Oblasti prevence se věnuje i Policie České republiky, konkrétně Oddělení tisku a prevence Policejního prezidia České republiky. Hlavní náplní tohoto oddělení je spíše poskytování informačního servisu sdělovacím prostředkům a zajištění komunikace Policejního prezidia ČR s medii a veřejností[131]. Preventivní působení je spíše okrajovou záležitostí, věnuje se spíše koordinaci. Silná prevence probíhá v oblasti silničního provozu, případně v oblasti ochrany seniorů. Autor práce na toto oddělení obrátil s nabídkou spolupráce, kdy mu bylo sděleno, že kybernetickou kriminalitou se toto oddělení nezabývá, celý oblast kybernetické kriminality přešla pod odbor NCOZ. Zde na prevenci není prostor, odbor se také potýká s nedostatkem pracovníků, prevence je až na posledním místě. Odbor v poslední době zlepšil svoji prezentaci, na webových stránkách policie má uvedeny základní údaje týkající se kybernetické kriminality[132].

[130] zdroj: https://www.nbu.cz/cs/onas/organizacni-struktura-a-hlavni-ukoly-organizacnich-celku/1146-narodni-koordinator-kyberneticke-bezpecnosti/

[131] zdroj: http://www.policie.cz/clanek/preventivne-informacni-skupina-policejniho-prezidia-ceske-republiky.aspx

[132] zdroj: http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09MQ%3d%3d

Prevenci ze strany Policie České republiky se nesystémově taktéž věnují jednotlivá krajská ředitelství, která připravují své vlastní projekty. Jako příklad lze zmínit videospoty vytvořené v roce 2015[133] od krajského ředitelství policie Královehradeckého a Pardubického kraje, případně Poldík webík z krajského ředitelství policie Moravskoslezského kraje.

[133] dostupné z http://www.policie.cz/clanek/prevenci-k-bezpeci.aspx

4 Vlastní práce

V praktické části práce bude provedena analýza statistických dat získaných z policejních statistik, konkrétně z výstupů z Policejní internetové hotline a ze systému Evidenčně statistický systém kriminality (ESSK). Z těchto statických dat bude získán obraz kybernetické kriminality, která je v současné době aktuálně řešena policií včetně poměrného rozložení jednotlivých skutků.

V druhé části budou představeny výsledky dotazníkového šetření prováděného mezi žáky základní školy. Cílem dotazníkového šetření bylo zjistit povědomí žáků, co je to kyberkriminalita a dále jakého závadového jednání v této oblasti se sami dopouští.

Závěrem budou porovnány poměrné rozložení páchané kyberkriminality se zaměřeními preventivních programů představených v teoretické části a se znalostmi a zkušenosti žáků s kybernetickou kriminalitou.

4.1 Analýza

Jako podkladová data pro analýzu byly vybrány dva zdroje, které mohou nastínit poměrné rozložení páchané kybernetické kriminality v České republice. Absolutní čísla, kolik jednotlivých skutků je spácháno, nelze přesně určit. Veškerá kriminalita má i svojí latentní část, která není nikdy nahlášena ani objevena. Je předpokládáno, že v případě kybernetické kriminality je toto číslo výrazně vyšší než u ostatních druhů kriminality.

Jako jeden ze zdrojů byly vybrány statické výstupy Policejní internetové hotline. Jako druhý zdroj byly vybrány roční přehledy z Evidenčně statistického systému kriminality (ESSK) Policie ČR.

4.1.1 Analýza statických výstupů Policejní internetové hotline

Na základě úkolu Ministerstva vnitra ČR byla v srpnu roku 2012 zřízena Policejní internetová HotLine. Jejím cílem mělo být centralizování poznatků z oblasti kybernetické, v té době se ještě užíval pojem informační, kriminality a následná koordinace prověřování a vyšetřování jednotlivých případů. Záměrem hotline bylo poskytnout občanům snadno dostupný a anonymní způsob, jak oznámit podezření z jednotlivých případů kybernetické kriminality. Policejní internetovou hotline provozoval útvar Policejního prezidia ČR, oddělení informační kriminality, v roce 2015 se provoz přesunul pod nově vzniklý odbor

kybernetické kriminality zřízeny při Národní centrále proti organizovanému zločinu (NCOZ).

„*Služba má přispívat ke zvýšení úspěšnosti odhalování informační kriminality, pomocí včasné reakce na jednotlivé poznatky, a to prostřednictvím činnosti policistů, kteří na základě zaslaných podnětů provádí jejich prvotní vyhodnocení, zajištění důkazního materiálu, který bývá v prostředí internetu velmi rychle přesouván či mazán, a dále spočívající v komunikaci s provozovateli služeb a poskytovateli internetového připojení*.[134]“

Aplikace je dostupná na webových stránkách policie, http://aplikace.policie.cz/hotline/, kde je umístěný Formulář pro hlášení závadového obsahu a aktivit v síti internet.

Jednotlivá hlášení jsou specializovanými pracovníky prověřena, případně je kontaktován oznamovatel, aby hlášení doplnil, jestliže nebylo oznámení anonymní. Dle svého charakteru jsou hlášení postoupena na příslušné součásti policie k dalšímu prověřování, případně uložena ad acta, jestliže se nejedná o relevantní podání.

Kvantitativní analýza

Policejní hotline funguje od poloviny roku 2012. Celkem za dobu fungování bylo přijato 18 580 hlášení. Počty jednotlivých oznámení jsou uvedeny v následující tabulce, ve které jsou uvedeny počty oznámení v daném roce a procentuální vyjádření relevantních oznámení, a procentuální vyjádření oznámení, které byly postoupeny k dalšímu prověření příslušnými součástmi policie.

Rok	Počet oznámení	% relevantních	% postoupených
2013	3829	46 %	22 %
2014	6590	64 %	39 %
2015	3173	39 %	19 %
2016	3378	40 %	10 %

Tabulka 2: Počty oznámení na Policejní internetovou hotline

S výjimkou roku 2014 je počet oznámení relativně stále stejný. Výkyv v roce 2014 je zapříčiněn vlnou falešných exekučních výzev, která se šířila prostřednictvím emailového

[134] ze zprávy: POLICEJNÍ INTERNETOVÁ HOTLINE, Statistický výstup za rok 2014, v přílohách

spamu. Spam obsahoval malware, který při instalaci následně napadal internetový prohlížeč a internetové bankovnictví.

Problém hlášení spočívá v tom, že větší část hlášení jsou nesmyslná oznámení, případně hlášení jednání nepřislušející řešit policii a dále že služba je využívána občany k oznamování jiných protiprávních jednání, které nepřísluší do oboru kybernetické kriminality.

Kvalitativní analýza

Rozložení oblastí relevantních oznámení je uvedeno v následující tabulkách a grafech získaných z jednotlivých statistických zpráv. Výstupy za jednotlivé roky se liší, neboť ve zprávách není jednotná forma vyhodnocení, správa hotline byla předávána mezi různými součástmi a každý rok byla ve statistickém výstupu použita jiná pojmenování sledovaných oblastí.

rok 2013

Skutková podstata trestného činu	Počet
podvod	564
neoprávněný přístup k počítačovému systému a nosiči informací	450
zneužití dítěte k výrobě pornografie	202
hanobení národa, rasy, etnické nebo jiné skupiny osob	147
šíření pornografie	93
porušení autorského práva, práv souvisejících s právem autorským a práv k databázi	47
padělání a pozměnění veřejné listiny	29
pomluva	22
popírání, zpochybňování, schvalování a ospravedlňování genocidia	20
podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod	14
založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka	14
nebezpečné pronásledování	13
nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy	10

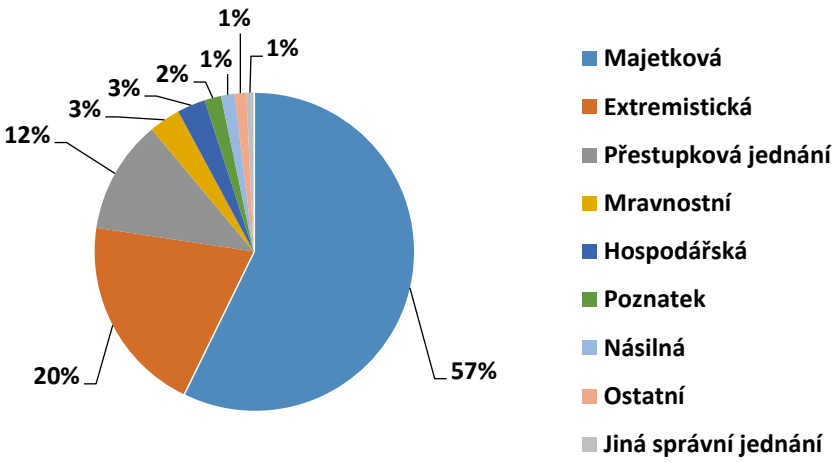
Tabulka 3: Skutky oznamované na Policejní internetovou hotline za rok 2013, zdroj: Policie ČR, Policejní internetová hotline - Statistický výstup za rok 2013

rok 2014

Oblast	Počet
Hospodářská	3522
Amorální jednání právně nepostihnutelná	2087
Majetková	218
Extremistická	189
Přestupkové jednání	177
Hlášené nesmyslnosti	128
Mravnostní	118
Ostatní	68
Poznatek	55
Násilná	25
Jiná správní jednání	3
Celkem	6590

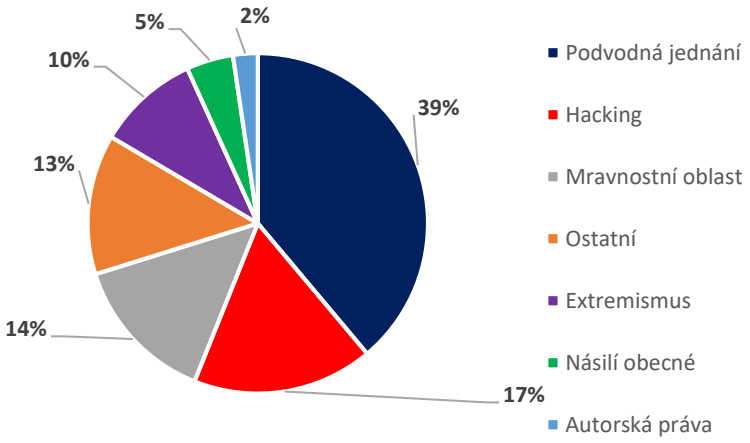
Tabulka 4: Skutky oznamované na Policejní internetovou hotline za rok 2014, zdroj: Policie ČR, Policejní internetová hotline - Statistický výstup za rok 2014

rok 2015



Obrázek 2: Skutky oznamované na Policejní internetovou hotline za rok 2015, zdroj: Policie ČR, Policejní internetová hotline - Statistický výstup za rok 2015

rok 2016



Obrázek 3: Skutky oznamované na Policejní internetovou hotline za rok 2016, zdroj: Policie ČR, Policejní internetová hotline - Statistický výstup za rok 2016

Nejčastější právní kvalifikace podaných jednání, tak jak byly postoupeny příslušným součástem Policie ČR:

1. **Neoprávněný přístup k počítačovému systému a nosiči informací:** v roce 2015 a 2016 se jednání potencionálně kvalifikované dle § 230 TrZ stalo nejčastěji přijímaným druhem protiprávních skutků, a to zejména v souvislosti s různými phishingovými útoky a ransomwarovými útoky. Tato skutková podstata bývá většinou v souběhu s dalšími trestnými činy, například s Podvodem, Vydíráním a dalšími.

2. **Podvod:** oznámení podvodu ve smyslu ust. § 209 TrZ představuje jeden z nejrozšířenějších druhů podání. Je nutná komunikace s podatelem, v mnoha případech s poskytovateli inzertních služeb, jelikož tato podvodná jednání se nejčastěji vyskytují na serverech – www.aukro.cz, www.sbazar.cz, www.bazos.cz a dalších.

3. **Hanobení národa, rasy, etnické nebo jiné skupiny osob:** tato trestná činnost většinou zasahuje do více skutkových podstat extremistické povahy a v největší míře se vyskytuje na Facebooku. Často se jedná rovněž o trestné činy ve vztahu k různým pravicovým či levicovým extremistickým hnutím. V této oblasti je část poznatků předávána dalším odborům NCOZ.

4. **Přestupková jednání** podání, která spadají do oblasti přestupkové – proti majetku. Častá jsou hlášení o možných inzertních podvodech v částkách několika stokorun.

Policejní internetová hotline neposkytuje vzhledem k počtu podaných oznámení ucelený obraz o páchané kybernetické kriminalitě, zvláště proto, že většina podání je s ní nesouvisejících.

4.1.2 Analýza statistiky prověřovaných trestných činů s příznakem Kybernetická kriminalita

Jako statistický zdroj o aktuálním nápadu kybernetické trestné činnosti byl vybrán ESSK, Evidenčně statistický systém kriminality, který je jeden z informačních systémů, které provozuje Policie ČR. Systém obsahuje údaje o všech skutcích, ke kterým vedli policejní orgány trestné řízení, tj. které měli zahájeny úkony trestního řízení dle trestního řádu. Informace do evidencí jsou doplňována automaticky a jsou verifikována specializovanými pracovníky, kteří mají na starost statistiku, aby byly minimalizovány nepřesnosti při vykazování. Systém eviduje druhy trestné činnosti, jednotlivé paragrafy trestných činů a speciální příznaky, dle kterých lze údaje dále třídit.

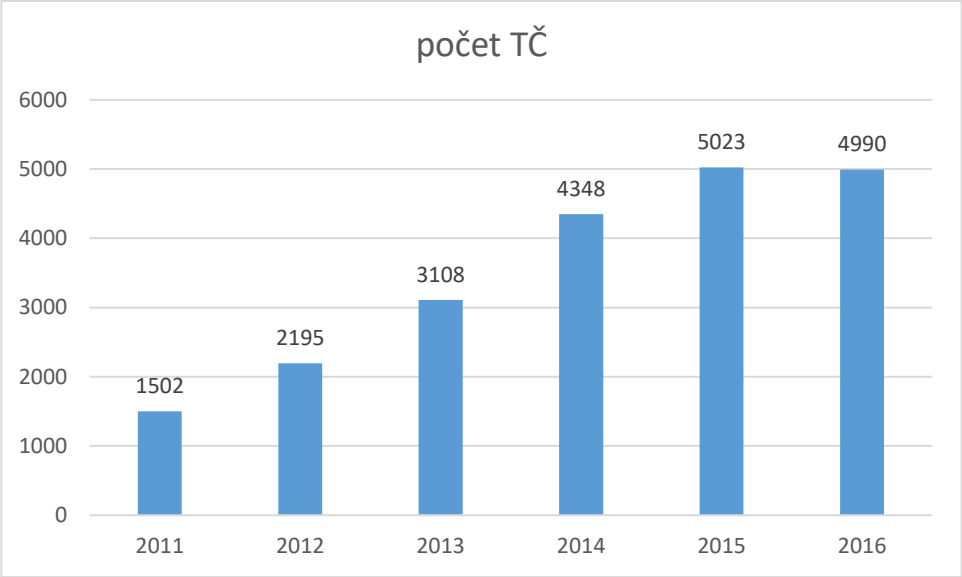
Výstupem z ESSK jsou sestavy, exportované v kontingenčních tabulkách. Část těchto sestav je volně dostupná na webových stránkách policie[135]. Dále je možní v rámci Policie získat specializované sestavy například trestné činnosti spáchané dětmi, na dětech, či na seniorech. Spáchaná kybernetická kriminalita se jako podskupina sleduje od roku 2011. Sestavy od roku 2011 do roku 2016 jsou v přílohách této práce.

Pro potřeby analýzy byly vybrány sestavy trestných činů, které mají sledovanou událost 07 IT kriminalita. Dále byly vybrána sestava s trestnými činy spáchanými dětmi od 1 do 17 let. V této sestavě však chybí počítačové trestné činy, nemají zde samostatnou skupinu, není tedy pro potřeby analýzy v této práci využitelná. Sestavy s příznakem IT kriminalita jsou v přílohách pojmenovány „A B *rok*“ sestavy s kriminalitou spáchanou dětmi „*rok*“.

[135] http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2016.aspx

Kvantitativní analýza

Z tabulek získaných z ESSK byly zjištěny počty spáchané kybernetické kriminality, která byla policii známá a které byla v daném roce prověřována.



Obrázek 4: Počty skutků spáchané kybernetické kriminality

Počty spáchaných trestných činů s výjimkou posledního roku stále stoupají. Tento vzestup neodpovídá vývoji trestné činnosti v České republice, kde je zřejmý stálý pomalý pokles.

Kvalitativní analýza

V rámci této analýzy byly vybrány nejčastější druhy trestné činnosti, které je páchána. Jde o trestnou činnost, které není latentní. Některé oblasti jsou sloučené do jedné, protože dané činy spolu často souvisejí, například podvodné jednání shrnuje podvod (§ 209 TrZ), úvěrový podvod (§ 210 TrZ) a pojistný podvod (§ 211 TrZ). Mravnostní činy shrnují šíření pornografie (§ 191 TrZ), ohrožování výchovy dítěte (§ 201, 202 TrZ) a skupinu ostatních mravnostních činů patřící ve statistice pod jednu skupinu – prostituce ohrožující mravní vývoj dítěte (§ 190 TrZ), výroba a jiné nakládání s dětskou pornografií (§ 192 TrZ), zneužití dítěte k výrobě pornografie (§ 193 TrZ). Bylo by zajímavé vzhledem k zaměření preventivních programů samostatně skupinu trestných činů týkající se dětské pornografie, či navazování nedovolených kontaktů s dítětem (§ 193b TrZ), ta se však samostatně nesleduje. Ryze počítačové činy zahrnují Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TrZ), Opatření a přechovávání přístupového zařízení a

hesla k počítačovému systému a jiných takových dat (§ 231 TrZ) a Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TrZ)

rok	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
celkový počet trestných činů	1502	2195	3108	4348	5023	4990
podvodná jednání	**899**	**1292**	**1856**	**2458**	**2915**	**2989**
	59,9%	58,9%	59,7%	56,5%	58,0%	59,9%
porušován autorských práv	**155**	**241**	**181**	**262**	**315**	**234**
	10,3%	11,0%	5,8%	6,0%	6,3%	4,7%
mravnostní trestné činy	**132**	**145**	**247**	**305**	**313**	**323**
	8,8%	6,6%	7,9%	7,0%	6,2%	6,5%
ryze počítačové trestné činy	**64**	**107**	**215**	**552**	**588**	**518**
	4,3%	4,9%	6,9%	12,7%	11,7%	10,4%
neoprávněné držení platebního prostředku	**28**	**51**	**71**	**103**	**173**	**210**
	1,9%	2,3%	2,3%	2,4%	3,4%	4,2%
nebezpečné vyhrožování	**22**	**30**	**42**	**56**	**52**	**67**
	1,5%	1,4%	1,4%	1,3%	1,0%	1,3%
nebezpečné pronásledování	**23**	**33**	**40**	**50**	**45**	**47**
	1,5%	1,5%	1,3%	1,1%	0,9%	0,9%
vydírání	**24**	**28**	**35**	**53**	**80**	**98**
	1,6%	1,3%	1,1%	1,2%	1,6%	2,0%
krádeže	**33**	**76**	**132**	**160**	**168**	**133**
	2,2%	3,5%	4,2%	3,7%	3,3%	2,7%

Tabulka 5: Nejčastější druhy kybernetické kriminality

Z tabulky je patrné, že nejčastější páchané skutky kybernetické kriminality jsou různá podvodná jednání, na druhém místě počítačové trestné činy jako neoprávněný přístup k počítačovému systému (§ 230, 231, 232 TrZ) následované mravnostními trestnými činy. Pokud bychom skupinu mravnostních trestných činů rozdělili, počty jednotlivých skutků této oblasti by byly rozloženy tak, že skupina ostatních mravnostních činů (§ 191, 192 a 193 TrZ) tvoří 70 % toho čísla, šíření pornografie 10 % a ohrožování výchovy dítěte 20 %. Trestný čin neoprávněné držení platebního prostředku Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 TrZ) zahrnuje většinou odčerpání finančních prostředků z účtu pomocí odcizených nebo cardskimmingovými či phishingovými útoky získaných čísel platebních karet.

Celkově převažuje mezi spáchanou trestnou činností, kterou Policie ČR sleduje jako kybernetickou kriminalitu nejrůznější majetková trestná činnost.

4.2 Výzkum

Součástí praktické části práce je výzkum, uskutečněný mezi žáky druhého stupně základní školy. Výzkum je pojat jako pilotní projekt k možnému celorepublikovému výzkumu, provedenému pro potřeby organizace Kraje pro Bezpečnější internet (KPBI), s jehož krajskými koordinátory byl výzkum konzultován a kteří se podíleli na distribuci dotazníků. Vzhledem ke skutečnosti, že se jedná o pilotní projekt, nebyly předem jisté počty respondentů a návratnost z jednotlivých škol. Během výzkumu byly zjištěny značně rozdílné výsledky v rámci Hlavního města Prahy a Středočeské kraje. Zda bude v projektu pokračováno, je v současné době předmětem jednání mezi zúčastněnými stranami.

Výsledky dotazníků budou poskytnuty krajským koordinátorům prevence kriminality a jednotlivým školám, které o výsledky projevili zájem. V návaznosti na dotazníkové šetření byl připraven materiál pro kantory, aby mohli po vypracování dotazníků žákům vysvětlit jednotlivé pojmy a jejich trestnost. Je dále plánována přednáška výsledků na celorepublikové konferenci Řešení elektronického násilí a kyberkriminality v Jihlavě a pro potřeby KPBI.

4.2.1 Vymezení cílů výzkumu

Při přípravě cílů výzkumu byly analyzovány již provedené výzkumy organizacemi, které se zabývají prevencí, konkrétně E-bezpečí a Saferinternet, tak aby nedošlo k opakovanému dotazování na již známá témata.

Konkrétně projekt organizace E-bezpečí zkoumal v rozsáhlém výzkumu prováděném v letech 2014 a 2015 chování dětí na facebooku[136] a komunikaci na internetu a kyberšikanu[137], organizace Saferinternet prováděla v roce 2014 v rámci Evropského měsíce kybernetické bezpečnosti 2014 průzkum týkající se obecně internetové bezpečnosti[138].

[136] dostupné z https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/ceske-deti-na-facebooku-2015
[137] dostupné z https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/2017-02-19-08-00-11
[138] dostupné z http://www.saferinternet.cz/ecsm-2014/467-vysledky-pruzkumu-v-ramci-ecsm-2014.html

Cíle prováděného výzkumu s ohledem na téma práce byly zvoleny následující tři:

- zjistit povědomí žáků o tom, co je kyberkriminalita, konkrétně, jaké jednání a chování v prostředí počítačů, internetu a sociálních sítí je dle našeho právního řádu trestné
- Zjistit jakého závadového jednání v oblasti kyberkriminality se již dopustili žáci, či jejich vrstevníci.
- Ověření proveditelnosti výzkumu z hlediska distribuce, návratnosti a zpracování dotazníků pro zamýšlený celorepublikový výzkum pro potřeby organizace Kraje pro bezpečnější internet

Výsledky výzkumu budou poskytnuty krajským metodikům prevence kriminality a školám, které projevili o výsledky zájem. Na základě výsledků bude krajskými metodiky zohledněn výběr preventivních programů, které jsou školám nabízeny.

4.2.2 Charakteristika výzkumného vzorku

Jako cílová skupina byly zvoleni žáci druhého stupně základní školy, tj. ve věku od 11 do 16 let navštěvující základní školu nebo víceletá gymnázia v Hlavním městě Praze a ve Středočeském kraji. Mladší žáci nebyli do výzkumu zahrnuti, neboť z již proběhlých výzkumů, například organizace E-Bezpečí je zřejmé, že výpočetní techniku používají ve velké míře pouze jako zábavní prostředek, není zde předpoklad znalostí ohledně kybernetické kriminality ani zkušeností se závadovým jednáním jako takovým, případně by tato zkušenost byla ojedinělá a statistiku by nijak neovlivnila. S ohledem na skutečnost, že se jedná o pilotní projekt rozsáhlejšího výzkumu, bylo ponecháno na dobrovolnosti jednotlivých škol, zda se do projektu zapojí, což ovlivnilo návratnost dotazníků. Očekáváná návratnost dotazníků byla kolem 5%.

Celkem z území Hlavního města Prahy se výzkumu zúčastnilo 248 respondentů ze 7 škol. 45,2 % vzorku tvořili chlapci, 54, 8% dívky, což odpovídá genderovému rozložení obyvatelstva v České republice. Z věkového hlediska bylo rozložení vzorku následující: 11 let 16,1 %; 12 let 40,7 %; 13 let 21,4 %; 14 let 10,5 %; 15 let a více 11,3 %. Věkové rozložení bylo ovlivněno výběrem tříd, které se zúčastnily výzkumu, neodpovídá věkovému rozložení žáků na základní škole.

Z území Středočeského kraje se výzkumu zúčastnilo 3898 respondentů ze všech okresů kraje. Aktuální počet žáků druhého stupně základní školy je na území Středočeského kraje 38 817, výzkumný vzorek tedy tvoří více jak 10 % žáků druhého stupně základní školy v daném kraji. 51,9 % vzorku tvořili chlapci, 48,1 % tvořily dívky, cože neodpovídá zcela genderovému rozložení obyvatelstva. Rozložení může být ovlivněno typem škol, nebo tříd, které se do výzkumu zapojili. Z věkového hlediska je rozložení vzorku následující: : 11 let 10,7 %; 12 let 24,3 %; 13 let 21,5 %; 14 let 25,9 %; 15 let a více 17,6 %. Věkové rozložení bylo ovlivněno výběrem tříd, které se zúčastnily výzkumu, neodpovídá věkovému rozložení žáků na základní škole.

4.2.3 Metodika výzkumu

Vlastní výzkum s ohledem na očekávané množství respondentů, byl orientován kvantitativně, a byla zvolena explorativní výzkumná metoda. S ohledem na kvantitativní vyhodnocení byly zvoleny pouze uzavřené otázky. Dotazník byl rozdělen na tři části, v první části byly otázky pro statistické třídění, druhá část obsahovala jednu otázku s více správnými odpověďmi, třetí část obsahovala 48 dichotomických otázek.

Vlastní dotazník byl zpracován v programu Google Forms, který umožňuje automatické zpracování odpovědí do grafů a celkový výstup do tabulky. Distribuce dotazníků byla provedena ve spolupráci s krajským metodikem prevence kriminality Hlavního města Prahy a Středočeského kraje. Dotazníky byly šířeny prostřednictvím odkazu s průvodním dopisem, který vysvětloval školám, k čemu dotazníky budou využity. Průvodní dopisy jsou v přílohách práce. Pro potřeby využití jednotlivých krajů byly vytvořeny dvě shodné kopie dotazníků, které byly šířeny v jednotlivých krajích.

Dotazníky jsou anonymní, pro potřeby krajských metodiků v něm respondenti uváděli školu, kterou navštěvují. S ohledem na předem neznámý seznam škol, které se do výzkumu zapojí, vyplňoval název školy respondent, tudíž pro třídění dotazníků dle škol je nutné ručně upravit jednotné názvy škol.

Příprava výzkumu byla zahájena koncem roku 2016, sběr dat a průběžné vyhodnocování probíhalo od 23. 2. 2017 do 16. 3. 2017. Při přípravě byly analyzovány již výzkumy v oblasti internetové bezpečnosti a byly pro dotazník zvoleny pouze otázky týkající se přímo kybernetické kriminality, neboť otázky týkající se zabezpečení či používání výpočetní techniky dětmi již zkoumali výše uvedené výzkumy.

Před provedení samotného výzkumu byl vytvořen pilotní dotazník, který vyplnilo v lednu 2017 19 žáků 7. a 9. třídy. Při vyplňování pilotních dotazníků byl autor přítomen, po vyplnění získal zpětnou odezvu od respondentů, na základě kterého byla upravena formulace otázek, aby byly uchopitelnější pro cílovou skupinu a byla stanovena doba nutná pro vyplnění dotazníku. Pečlivé vyplnění dotazníku zabralo žákům od 15 do 25 minut. Výsledky pilotního dotazníku jsou v přílohách práce.

S výsledky bude dále pro potřeby krajských metodiků pracováno, kdy budou upraveny a tříděny po jednotlivých školách. Očekávané předání krajským metodikům je v dubnu 2017, zpracované výsledky pro jednotlivé školy je ve čtvrtém čtvrtletí 2017.

Jako prvotní zpětná vazba pro potřeby školních metodiků prevence byl po vyplnění dotazníků zaslán materiál, obsahující okomentované otázky s vysvětlením, zda jedná o závadové jednání a jakou právní kvalifikaci by dané jednání mohlo naplňovat. Materiál je v přílohách práce.

Při přípravě otázek byly cíleně voleny podobně formulované otázky, aby bylo ověřeno, zda žáci v dotaznících odpovídají konzistentně. Dále byly zvoleny otázky, které se sice týkají stejného jednání, ale byly přeformulovány s ohledem k různým tématům, ke kterým mohou být žáci různě tolerantní. Například nabourání se do facebookového profilu kamaráda a nabourání se do cizích webových stránek. Cíleně byly do dotazníku umístěny i příklady jednání, které není trestným činem, ale může být například nemorální, aby byl získán komplexní obraz názoru žáků na tuto oblast.

V úvodní části dotazníku jsou uvedeny statistické údaje, které jsou potřebné pro další využití dat metodiky prevence. Prevence je připravována vzhledem k věku jejích příjemců, proto je zde rozdělení dle věku, dále je zde název školy, který je potřebný pro porovnání výsledků mezi okresy, případně školami, kde již proběhnul nějaký preventivní program a kde dosud neproběhnul. Dotazníky umožňují dále třídění dle pohlaví, dle toho, zda respondent absolvoval preventivní program. Otázka, zda má respondent facebookový účet je přidána do dotazníku s ohledem na dotaz, zda žáci uvádí při registracích nepravdivé údaje, neboť je při založení facebookového účtu vyžadován věk alespoň 13 let. Otázka má ověřit, zda žáci lžou v dotazníku. Skutečnost, že má facebookový účet uvedlo 84,3 % žáků Středočeského kraje a 71,8 % žáků z Prahy. Rozdíl ve výsledcích může být způsoben jiným věkovým rozložení respondentů a nízkým množstvím respondentů v Praze.

Výsledek ze středočeského kraje odpovídá výsledkům výzkumu projektu E-bezpečí z roku 2015, který uvádí množství facebookových účtů u dětí starších 10 let 78,9[139] %, přičemž počet dětských uživatelů facebooku stále roste.

Otázky, kterého jednání se dopustili žáci, nebo jejich vrstevníci byly zvoleny cíleně tak, aby pokrývali všechny příklady kybernetické kriminality. Lze očekávat, že žáci nebudou chtít uvést, že se něčeho dopustili, avšak sdělí to na svého vrstevníka, proto jsou jednotlivé otázky uvedeny vždy ve formě, zda se jednání dopustil respondent dotazníku a zda jednání dopustil některý jeho vrstevník.

4.2.4 Shrnutí výsledků výzkumu

Kompletní výsledky byly vytvořeny pomocí programu Google Forms, který umožňuje export do tabulek a dále byla vyexportován přehled s grafickým vyjádřením výsledků. Kompletní výsledky výzkumu jsou v přílohách této práce.

Výsledky z dotazníkového šetření získané ze škol v Praze a Středočeském kraji byly porovnány mezi sebou a přes řádový rozdíl mezi počtem získaných vyplněných dotazníků si výsledky vzájemně odpovídaly. V jednotlivých odpovědích se liší maximálně o 10 %, většinou se jedná o jednotky procent.

Otázky zaměřené na znalost trestného jednání

Znalosti žáků o tom, co je kybernetická kriminalita, se pohybuje mezi 10 % až 80 % v případě Prahy a 13 % až 70 % v případě Středočeského kraje. Nižší znalost byla zjištěna u příkladů porušení autorských práv, pohybovala se zde mezi 10 % a 30 %, znalost týkající se příkladů neoprávněného přístupu k různým informačním systémům se pohybovala většinou mezi 40 % a 60 %. Nejvíce žáci věděli, že je trestné vytváření phishingových stránek, 80 % v případě Prahy. Zajímavé je rozdílné určení například u příkladu „zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky“, který za trestný označilo 32,2 % žáků v případě Středočeského kraje a 33,5 % žáků v případě Prahy a „náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu jeho zprávy a místo nich dám odkazy na porno“ které jako trestný označilo 58,3 % / 64,1 % žáků. Za zmínku stojí také množství odpovědí, které označili netrestné jednání, například přepsání článku na wikipedii (33,7 % / 35,1 %), instalace vlastní počítačové hry

[139] Kamil Kopecký; České děti a facebook 2015 výzkumná zpráva, str.10

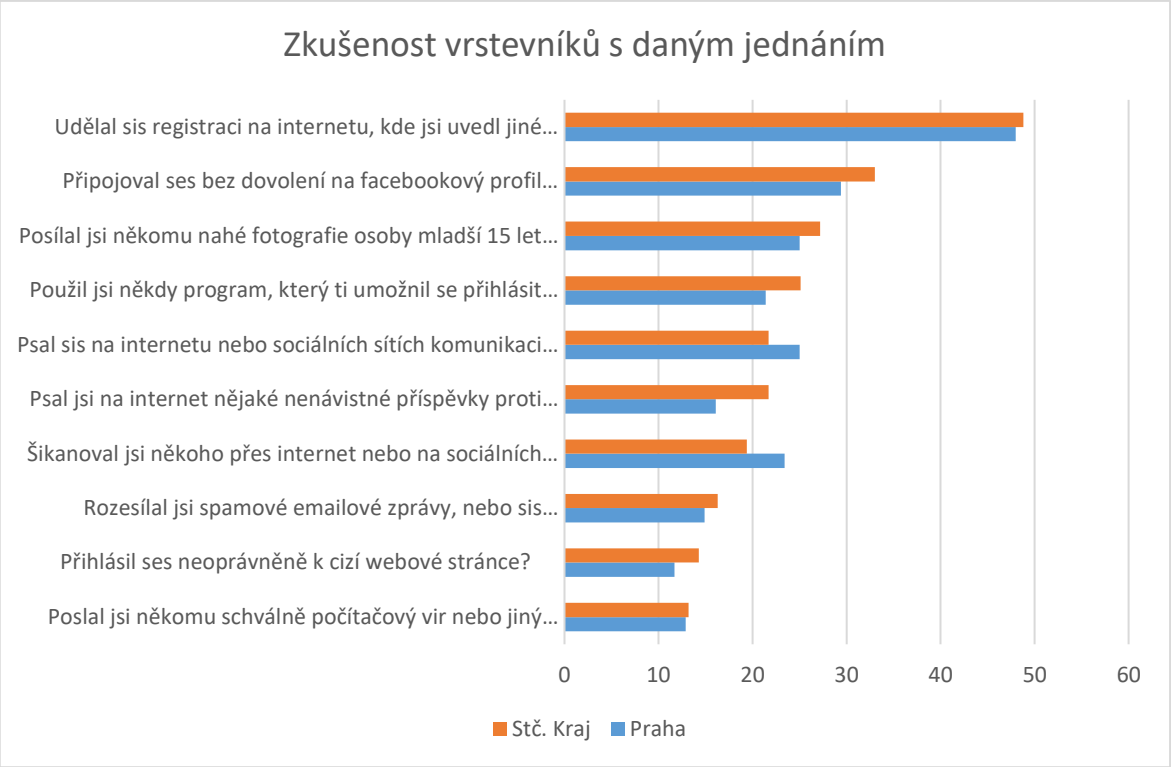
v rozporu se školním řádem (38,2 % / 36,3 %). Velmi častý byl i výskyt odpovědi „spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat na sociálních sítích zprávy, že je fakt strašný a měl by se raději zabít“, 61,4 % / 59,3 %, v daném případě se jedná o kyberšikanu.

Výběr jednotlivých oblastí a jeho procentuální výskyt v odpovědích je uveden v následujícím grafu:

Obrázek 5: Co žáci považují za kyberkriminalitu

Otázky zaměřené na zkušenost s kyberkriminalitou

Procentuální vyjádření zkušeností s jednotlivými příklady kybernetické kriminality relativně vzájemně odpovídá u dotazníků z Prahy i Středočeského kraje. Výsledky se od sebe liší v jednotkách procent. Pro vyhodnocení byly vybrány možnosti uvedené u jednání spáchaného vrstevníkem, kde byly dle předpokladu zjištěny vyšší procentuální výsledky. Prokázalo se, že žáci sami na sebe nechtějí sdělit, že se jednání dopouštějí, výsledky u odpovědí čeho se dopustili oni ve srovnání s tím, čeho se dopustil jejich vrstevník, jsou většinou poloviční až třetinové s výjimkou otázky „Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, než skutečné“, kde byl výsledek o 2 % vyšší. Nejčastější kladné odpovědi jsou uvedené v následujícím grafu.



Obrázek 6: Zkušenosti žáků s kyberkriminalitou

Pokud bychom porovnali výsledky z obou částí dotazníku výsledky z Prahy a Středočeského kraje, vykazují žáci v Praze většinou vyšší znalosti toho, co je trestné jednání a mezi jejich vrstevníky je méně jedinců, kteří mají s tímto jednáním zkušenost. Porovnání však není objektivní, neboť se liší řádově množství vrácených dotazníků (3898 ve Středočeském kraji proti 248 v Praze), výsledek bude pravděpodobně ovlivněn výběrem škol, které se do výzkumu zapojily, neboť se v Praze zapojily jen ty školy, které měly o dané téma zájem a které se mu ve výuce věnují (tyto školy projevily i zájem o výsledky výzkumu, neboť by s ním chtěly dále pracovat).

Z provedeného výzkumu vyplývá, že mezi žáky druhého stupně základní školy je zkušenost s neoprávněným přístupem k cizí webové stránce 14,3 %, respektive 11,7 % v případě výsledků z Prahy. Neoprávněný přístup k cizímu facebookému účtu, které je stejným jednáním, se vyskytuje v 33 % respektive 29,3 %. Neoprávněný přístup k cizí Wifi síti se vyskytuje v 25,1 % / 21,4 %. Z vyšší zkušeností s kyberkriminalitou a dalším nežádoucím jednáním lze zmínit ještě zkušenost se zasílání fotografií nahé osoby mladší 15 let 27,7 % / 25 %, se sextingem 21,7 % / 25 %, s kyberšikanou 19,4 % / 23,4 %, zasílání nenávistných příspěvků 21,7 % / 16,1 %. Zkušenosti s další trestnou činností se pohybuje

kolem 10 %, a pod touto hranicí. Zajímavé je uvedení rozdílného výsledku ještě u neoprávněného přístupu k cizímu internetovému bankovnictví 2,9 % / 2,4 % oproti neoprávněnému použití cizího internetového bankovnictví 3,5 % / 4,4 %. Vytvoření registrace na jiné údaje, než jsou skutečné, uvedlo 48,8 % / 48 % žáků, což naznačuje velkou ochotu dětí na internetu lhát.

Stahování hudby přiznalo 84,8 % / 81,5 %, stahování videa 56,1 % / 58,1 %. Tato otázka byla do dotazníku přidána za účelem porovnání odpovědí s jinými výzkumy prováděnými v této oblasti. Výsledek odpovídá obecně předpokládaným výsledkům (výzkum EU Kids online uvádí procento stahování hudby a videa 44% dětí ve věku 9-16, ve věku 13-16 je to 58,5 %)[140], případně další výzkum prováděný touto organizací uvádí u dětí sledování videí na internetu v 59 %[141].

[140] Výzkum EU Kinds online, dostupné z http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/DigitalSkillsShortReport.pdf, /

[141] https://lsedesignunit.com/EUKidsOnline

5 Výsledky a diskuse

V přechozích kapitolách byla provedena analýza statistických údajů týkající se kybernetické kriminality získané od Policie České republiky a provedeno dotazníkové šetření mezi žáky druhého stupně základní školy. Z analýzy vyplynulo, že nejčastější jednání spadající pod kybernetickou kriminalitu, jsou majetkové trestné činy, převážně podvodná jednání dle § 209, § 210 a § 211 TrZ. Druhý nejčastější druh kriminality, v poslední době stále narůstající, tvoří skupina ryze počítačových trestných činů jako Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 TrZ, který je sledován s trestnými činy dle § 231 a 232 TrZ, které s touto skutkovou podstatou souvisejí. Tyto trestné činy jsou charakteristické pro téměř každý komplexnější skutek kyberkriminality, neboť vždy pachatel potřebuje přistoupit neoprávněně k nějakému počítačovému systému, ať již získání přístupu k cizímu počítači, facebookovému účtu, nebo do internetového bankovnictví pro odčerpání finančních prostředků. Vyšetřovatelé se tyto činy učí také častěji odhalovat a připojovat je v usneseních o zahájení trestních stíhání k dalším skutkovým podstatám, které daný skutek naplní, ať se již jedná o podvod (jako jsou například phishingové útoky), či vydírání (například ransomwarové útoky), proto roste podíl těchto činů rychleji, než celkový počet kyberkriminality. Na dalších místech následují trestné činy související s porušením autorských práv a mravnostní trestné činy.

Jestliže porovnáme tyto skupiny trestných činů se zaměřením prevence prováděné organizacemi, které byly v práci zmiňované, je zde patrný nedostatek, kdy se prevence zaměřuje převážně na děti jako na oběti kyberkminality. Z témat je to kyberšikana, která však ve své běžné podobě není trestným činem. Další skupina preventivních programů je zaměřená na riziko zasílání intimních fotografií a další intimní komunikace, případně před rizikem anonymního seznamování. Zde je toto na místě, neboť kyberkriminalita související s mravnostními trestnými činy je na třetím místě v počtu prověřovaných trestných činů a je na předních místech i oznamovaných trestných činů přes Policejní hotline. I zde však je třeba zaměřit se na dítě i jako na pachatele než jen jako na oběť. S touto kriminalitou souvisí také trestné činy vydírání a sexuálního útisku spojená s následným požadováním zaslání dalších fotografií.

Z první části výzkumu, provedeného dotazníkovým šetřením mezi žáky základních škol, vyplynulo, že s výjimkou několika případů se znalost trestnosti jednání související

s kybernetickou kriminalitou pohybuje kolem 50 % či méně. Dále z výsledků plyne, že žáci více tolerují pro ně zřejmě slabší formy téhož jednání. Například méně jich označilo za trestný neoprávněný přístup k počítačovému systému, kdy se nabourají do profilu kamaráda a umístím mu tam nějaký vtipný obsah, v porovnání se stejným jednáním, ale umístěním odkazů na porno místo zpráv kamaráda. Celkově je znalost trestnosti jednání v oblasti kybernetické kriminality nízká, je zde prostor pro zlepšení.

V druhé části výzkumu, kde bylo zjišťováno, jakého jednání se žáci a jejich vrstevníci dopouštějí, byla zjištěna největší zkušenost se sextingem, kyberšikanou a zasíláním nahých fotografií osob mladších 15 let, což značí, že toto zaměření preventivních programů je správné. Opět je ale na místě zmínit, že dítě je zde působí i jako pachatel, ne jen oběť. Dále byla zjištěna oproti ostatním dotazovaným formám jednání velká zkušenost s neoprávněným přístupem k počítačovému systému, v dotazníku byl konkrétně zmíněn přístup do cizího facebookového účtu a neoprávněný přístup k cizí wifi sítí. Vzhledem k tomu, že toto jednání doprovází páchaní většiny složitějších skutků kybernetické kriminality, je na místě se zaměřit komplexněji i na tuto oblast. V neposlední řadě byla zjištěna vyšší zkušenost se zasíláním nenávistných příspěvků proti nějaké skupině osob. Z výsledků je patrné, že žáci na internetu uvádějí nepravdivé údaje, což sice není trestným činem, ale jistě není žádoucí, aby si na toto chování žáci navykli.

Poslední cíl práce bylo ověřit proveditelnost většího dotazníkového šetření šířeného formou spolupráce s krajskými metodiky prevence kriminality ve školách. Osvědčila se forma distribuce, kterou použil středočeský kraj, který kladl větší důraz na důležitost výsledků v průvodním dopise, dále požadoval po jednotlivých okresních pracovnících prevenci kriminality, aby byl přidán do kopie pro kontrolu, zda skutečně dotazník školám byl odeslán. V Praze byl dotazník šířen dle průvodního dopisu více na bázi dobrovolnosti, nebyla provedena kontrola, zda školy dotazník dostaly a že pochopily důležitost vyplnění pro potřeby kraje. Ze škol byla získána zpětná vazba, že by potřebovali většího vysvětlení pojmů a důvodu, k čemu výsledky budou sloužit. Všechny školy, které měli k dotazníku doplňující otázky, vyplnili následně dotazník. Problémy s vyplněním žáci neměli, neobjevila se ani stížnost na přílišnou náročnost nebo délku dotazníku.

Dotazníkové šetření prováděné plošně na základních školách ve spolupráci s krajskými a následně okresními metodiky prevence je proveditelné. Pro pokračování

výzkumu by bylo vhodné zvolit větší kontrolu nad formou šíření dotazníků, dále získat kompletní adresář škol a tyto ještě jednou oslovit a ověřit, zda dotazníkům porozuměly a zda nepotřebují dovysvětlení pojmů a další komentář. Pokud by se provedlo dotazníkové šetření ve všech krajích, výsledkem by byl v našem prostředí pravděpodobně jeden z největších vzorků respondentů, které se zúčastnili dotazníkového šetření na téma počítačové bezpečnosti a kyberkriminality.

5.1 Doporučení pro praxi

Současné preventivní programy jsou zaměřené převážně na to, co dětem hrozí na internetu a sociálních sítích. Prevence prováděná organizacemi uvedenými v teoretické části je zaměřena převážně na následující oblasti: kyberšikana, sexting, kybergrooming, nebezpečí anonymního seznamování na sociálních sítích, nebezpečí zneužití osobních údajů a dalších citlivých materiálů v sociálních sítích.

Děti se však mohou snadno stát sami pachateli kybernetické kriminality. Výsledky dotazníkové šetření ukazují, že s kybernetickou kriminalitou mají již na druhém stupni základní školy zkušenosti sami žáci, případně jejich vrstevníci.

Oblasti kyberkriminality, u kterých uvedli žáci, že s ní má zkušenost více jak 20 % jejich vrstevníků, jsou následující:

- Stahování hudby a videí (to nemusí být nutně nezákonné, záleží na obsahu)
- Neoprávněný přístup k počítačovému systému
- Zasílání nahých fotografií osob mladších 15 let
- Sexting
- Psaní nenávistných příspěvků proti nějaké skupině osob
- Kyberšikana.

Oblasti, ve kterých je nejčastěji páchána kriminalita, kterou lze považovat za kyberkriminalitu, dle statistik Policie České republiky, jsou následující:

- Podvodná jednání
- Ryze počítačové trestné činy
- Mravnostní trestní činy

- Porušování autorských práv
- Neoprávněné držení platebního prostředku

Na tyto oblasti je vhodné zaměřit preventivní působení. V některých oblastech jsou působící organizace aktivní, některé oblasti jsou dosud zcela bez zájmu. Vzhledem k tomu, že již na druhém stupni základní školy mají žáci s kyberkriminalitou zkušenosti, někde i přes 30 %, je vhodné začít s prevencí již v raném školním věku. Hledání vhodných metod a forem prevence je již na odbornících z těchto oblastí.

6 Závěr

V teoretické části byla provedena rešerše literatury a byl vytvořen teoretický základ práce, popsány formy kybernetické kriminality a stanovena její právní kvalifikace. Byly popsány největší organizace, které působí v oblasti prevence kyberkriminality v České republice a představeny jejich preventivní programy. V praktické části byla provedena analýza statistických údajů ze systému ESSK Policie ČR týkající se kyberkriminality. Byl proveden výzkum za pomoci dotazníkového šetření, ze kterého bylo zjištěno, jaké jednání v oblasti kyberkriminality vnímají žáci jako trestné a jakého se sami dopouštějí. Bylo ověřeno, že dotazníkové šetření prováděné touto formou je proveditelné a návratnost vyplněných dotazníků je dostatečná i pro provedení většího dotazníkového zkoumání.

Porovnáním současného nápadu v oblasti kybernetické kriminality a znalostí a zkušeností žáků druhého stupně základní školy byly nalezeny oblasti, na které by bylo vhodné zaměřit pozornost při preventivním působení. Jedná se o oblast majetkových trestných činů, zejména podvodného jednání, dále neoprávněného přístupu k počítačovému systému a dalším ryze počítačovým trestným činům. Oblast kyberšikany preventivní programy již řeší, taktéž oblast související s mravnostními trestnými činy. Chybí informovanost a preventivní zaměření v oblasti porušování autorských práv. Celkově by bylo vhodné začít s prevencí již v nižším školním věku na základní škole, neboť na druhém stupni již mají žáci s kyberkriminalitou zkušenosti. Žáci nejsou jen oběti, ale dle informací, které sami uvedli v dotaznících, někteří z nich jsou pravděpodobně také pachatelé kyberkriminality.

Výsledky dotazníkového šetření byly poskytnuty krajským metodikům prevenci kriminality Středočeského kraje a hlavního města Prahy, kteří na dotazníkovém šetření spolupracovali. Ti výsledky zohlední při přípravě vlastních preventivních programů. Dále bude připravena prezentace výsledků formou přednášky pro odborné konference v rámci prevence kybernetické kriminality, například v Jihlavě, případně dle zájmu i jinde. V jednání je dosud pokračování výzkumu jeho rozšířením na další kraje ve spolupráci s KPBI a poskytnutí výsledků dalším organizacím.

Práce si neklade za cíl určovat, jak by měla být prevence prováděna, ani neuvádí, že je prováděna špatně. Autor pouze upozorňuje na oblasti, ve kterých jsou dle výsledků jeho práce nedostatky a kterým směrem by bylo vhodné preventivná působení zaměřit. Jedná se

o problematiku neoprávněného přístupu k počítačovým systémům, problematiku autorských práv a problematiku podvodného jednání páchanými prostřednictvím ICT. Prevence v těchto oblastech by měla být vedena s pohledem na žáky, jako potenciální pachatele této kriminality.

7 Seznam použitých zdrojů

Tištěné zdroje

- CRAIG, Paul, HONICK, Ron, Softwarové pirátství bez záhad, Praha: Grada, 2008, 212 s., ISBN 978-80-247-1765-4
- JAISHANKAR, K., Cyber Criminology Exploring Internet Crimes and Criminal Behavior, vyd. CRC Press 2011, 461 s., ISBN 978-1-4398-2949-3
- MATĚJKA, Michal, Počítačová Kriminalita, vyd. Praha: Computer Press, 2002, 106s. ISBN 80-7226-419-2
- POLČÁK R., Internet a proměny práva, vyd. Praha: Auditorium, 2012, 388 s., ISBN: 978-80-87284-22-3
- POLČÁK R., Právo na internetu – spam a odpovědnost ISP, vyd. Brno: Computer Press, a.s., 2007, 150 s., ISBN: 978-80-251-1777-4
- POŽÁR J., Základy teorie informační bezpečnosti, vyd. Praha: Policejní akademie ČR, 2007, 219 s., ISBN: 978-80-7251-250-8
- SMEJKAL V., SOKOL T., VLČEK M., Počítačové právo, vyd. Praha: Beck, 1995, 99 s., ISBN: 80-7179-009-5
- JIROVSKÝ Václav, Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství, vyd. Praha 2007, 284 s., ISBN: 978-80-247-1561-2
- ZOUBKOVÁ I., FIRSTOVÁ J. a kol., Kriminologie – aktuální problémy, vyd. Praha: Policejní akademie 2013, 270 s., ISBN 978-80-7251-395-6
- ŠTĚDROŇ B., LUDVÍK M., Právo v informačních technologiích, vyd. Computer Media 2008, 132 s., ISBN: 978-80-86686-36-3
- SMEJKAL Vladimír, Internet @ §§§, vyd. Grada 1999, 168 s., ISBN: 80-7169-765-6
- KOLOUCH J. VOLOVECKÝ P., Trestně právní ochrana před kybernetickou kriminalitou, vyd. Policejní akademie 2013, 117 s., ISBN: 978-80-7251-402-1
- GŘIVNA, Tomáš a POLČÁK, Radim, Kyberkriminalita a právo, vyd. Praha: Auditorium 2008, 220 s., ISBN 978-809-0378-674,
- SMEJKAL, Vladimír. Kybernetická kriminalita. vyd. Plzeň: Aleš Čeněk, 2015, 636 s., ISBN 978-80-7380-501-2
- KOLOUCH, Jan. Cybercrime. vyd. CZ.NIC, z.s.p.o., 2016, 528 s., ISBN 978-80-88168-18-8, dostupné z https://knihy.nic.cz/files/edice/cybercrime.pdf
- JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef, Výkladový slovník kybernetické bezpečnosti, vyd. Policejní akademie 2015, 242 s., ISBN 978-80-7251-436-6 dostupné z http://www.cybersecurity.cz/data/slovnik_v310.pdf

- SMEJKAL V., a kol. Právo informačních a telekomunikačních systémů, 2. vyd. Praha: C.H.Beck 2004, 770 s., ISBN 978-80-7179-765-4
- Slovník výpočetní techniky: (výklad standardních pojmů pro vědu, školství a obchod), vyd. Microsoft Press, Plus s.r.o., Praha, 1993, 421 s., ISBN 80-85297-48-5
- LANCE, James, Phishing bez záhad, vyd.: Praha. Grada Publishing, 2007, 281 s., ISBN: 978-80-247-1766-1
- POŽÁR, Josef, Informační bezpečnost, vyd. Plzeň: Aleš Čeněk, 2005, 311 s., ISBN 80-86898-38-5
- KOPECKÝ Kamil a kol., Rizikové formy chování českých a slovenských dětí v prostředí internetu, Univerzita Palackého v Olomouci, 2015, 172 s., ISBN 978-80-244-4868-8, dostupné z
- KOPECKÝ Kamil; České děti a facebook 2015 výzkumná zpráva, [cit. 2016-12-15], dostupné z https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/76-eske-dti-a-facebook-2015
- KABAY, M.E: A Brief History of Computer Crime: An Introduction for Students, 2008, [cit. 2016-12-15], dostupné z http://www.mekabay.com/overviews/history.pdf
- Strategie prevence kriminality v České republice na léta 2016 až 2020, [cit. 2016-12-15], dostupné z http://www.mvcr.cz/soubor/strategie-prevence-kriminality-2008-2011-strategie-pdf.aspx
- Národní strategie primární prevence rizikového chování na období 2013-2018, [cit. 2017-03-27], dostupné z http://www.msmt.cz/file/28077
- Strategie prevence kriminality v České republice na léta 2016 až 2020, [cit. 2016-12-15], dostupné z http://www.mvcr.cz/soubor/strategie-prevence-kriminality-2008-2011-strategie-pdf.aspx
- Vyhodnocení Strategie prevence kriminality v České republice na léta 2012 až 2015, [cit. 2016-12-15], dostupné z http://www.mvcr.cz/soubor/vyhodnoceni-strategie-2012-az-2015-vlada-final-docx.aspx
- Výzkum EU Kinds online, [cit. 2017-03-27], dostupné z http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/DigitalSkillsShortReport.pdf
- Výzkum EU Kinds online, [cit. 2017-03-27], dostupné z https://lsedesignunit.com/EUKidsOnline/
- Metodický pokyn MŠMT č. MSTM-21291/2010-28, [cit. 2017-03-27], dostupné z http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny
- Avner LEVIN, Daria ILKINA,: International Comparison of Cyber Crime, Privacy and Cyber Crime Institute of Ryerson University, [cit. 2017-03-27], dostupné z http://www.ryerson.ca/content/dam/tedrogersschool/privacy/AODAforms/Ryerson_International_Comparison_ofCyber_Crime_-March2013%20AODA.pdf

Právní normy, aktuální znění k 16. 3. 2017

- Zákon č. 40/2009 Sb. Trestní zákoník
- Zákon č. 121/2000 Sb., Autorský zákon
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 218/2003 Sb. Zákon o soudnictví ve věcech mládeže
- Zákon č. 89/2012 Sb., Občanský zákoník
- Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001
- Dodatkový protokol k Úmluvě o kybernetické kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů ze dne 28. ledna 2003

Elektronické zdroje

• https://us.norton.com/cybercrime-pharming

• http://pcworld.cz/novinky/symantec-spamu-je-cim-dal-mene-48487

• http://slovnik-cizich-slov.abz.cz/web.php/slovo/kyberprostor

• https://www.academia.edu/7096442/How_would_you_define_Cyberspace

• http://fas.org/irp/doddir/army/pam525-7-8.pdf

• http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09MQ%3d%3d

• http://www.saferinternet.cz/o-nas/10-o-nas.html

• http://cz.norton.com/spear-phishing-scam-not-sport/article

• https://usa.kaspersky.com/internet-security-center/definitions/spear-phishing

• http://www.root.cz/clanky/prichod-hackeru-nigerijsky-scam-419/

• http://www.nic.cz/files/nic/doc/Pravidla_registrace_CZ_Pravidla_ADR_20150301.pdf

• z http://www.zive.cz/clanky/pet-cest-jak-proniknout-do-cizi-wi-fi-site/sc-3-a-165682/default.aspx

• http://www.mrpear.net/cz/blog/435/prolomeni-wpa-wpa2-psk-pres-wps-snadno-a-rychle-praxe

• http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf

• z http://www.zive.cz/bleskovky/britanie-ctvrtym-rokem-blokuje-warez-popularita-zakazanych-webu-ale-casto-vzrostla/sc-4-a-181503/default.aspx

• http://www.zive.cz/bleskovky/konec-torrentu-v-rusku-roskomnadzor-chce-zablokovat-15-nejvetsich-serveru/sc-4-a-180878/default.aspx

• http://www.csas.cz/banka/content/inet/internet/cs/sc_17573.xml?archivePage=phishing&navid=nav00156_phishing_aktuality

• http://www.mbank.cz/blog/post,659,pozor-phishingovy-utok-na-mbank.html

• http://www.lidovky.cz/zada-vas-facebooky-pritel-o-penize-jde-o-podvod-varuje-policie-pu5-/zpravy-domov.aspx?c=A140601_163704_ln_domov_sk

• http://www.securitymagazin.cz/technologie/ceska-sporitelna-varuje-nova-podoba-podvodneho-emailu-1404043728.html

• http://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/

• http://www.lupa.cz/clanky/ihned-cz-je-nedostupny-zrejme-celime-utoku-rika-redakce/

• https://www.nic.cz/page/314/pravidla-a-postupy/

• http://www.pctools.com/security-news/crackers-and-hackers/

• http://www.ozbrojeneslozky.cz/clanek/atraktivita-terorismu-pro-medialni-zpravodajstvi-vyvoj-vztahu-mezi-terorismem-a-medii

• http://karvinsky.denik.cz/z-regionu/zlocinci-napichli-bankomat-v-centru-ostravy-vybrali-penize-nic-netusicim-lidem-2-449s.html

• http://www.seznamsebezpecne.cz/o-projektu

• https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

• https://www.nbu.cz/cs/onas/organizacni-struktura-a-hlavni-ukoly-organizacnich-celku/1146-narodni-koordinator-kyberneticke-bezpecnosti/

• http://www.policie.cz/clanek/preventivne-informacni-skupina-policejniho-prezidia-ceske-republiky.aspx

• http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09MQ%3d%3d

• http://www.policie.cz/clanek/prevenci-k-bezpeci.aspx

• http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2016.aspx

• https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/ceske-deti-na-facebooku-2015

• https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/2017-02-19-08-00-11

• http://www.saferinternet.cz/ecsm-2014/467-vysledky-pruzkumu-v-ramci-ecsm-2014.html

8 Přílohy

Příloha 1 – seznam obrázků

Příloha 2 – seznam tabulek

Příloha 3 – pilotní dotazník

Příloha 4 – výsledky pilotního dotazníku

Příloha 5 – finální verze dotazníku

Příloha 6 – průvodní dopis k dotazníku pro metodiky prevence a ředitele škol

Příloha 7 – kompletní výsledky výzkumu, školy na území hl. m. Prahy

Příloha 8 – kompletní výsledky výzkumu, školy na území Středočeského kraje

Příloha 9 – dopis se zpětnou vazbou pro školní metodiky prevence

Příloha 10 – shrnuté výsledky z části výzkumu Označ co je kyberkriminalita

Příloha 11 – shrnuté výsledky z části výzkumu Zkušenost s kyberkriminalitou

Přílohy uložené na CD:

Příloha 12 – statistické výstupy z ESSK, kyberkriminalita za rok 2011

Příloha 13 – statistické výstupy z ESSK, kyberkriminalita za rok 2012

Příloha 14 – statistické výstupy z ESSK, kyberkriminalita za rok 2013

Příloha 15 – statistické výstupy z ESSK, kyberkriminalita za rok 2014

Příloha 16 – statistické výstupy z ESSK, kyberkriminalita za rok 2015

Příloha 17 – statistické výstupy z ESSK, kyberkriminalita za rok 2016

Příloha 18 – statistické výstupy z ESSK, kriminalita dětí za rok 2011

Příloha 19 – statistické výstupy z ESSK, kriminalita dětí za rok 2012

Příloha 20 – statistické výstupy z ESSK, kriminalita dětí za rok 2013

Příloha 21 – statistické výstupy z ESSK, kriminalita dětí za rok 2014

Příloha 22 – statistické výstupy z ESSK, kriminalita dětí za rok 2015

Příloha 23 – Statistický výstup za rok 2013 Policejní internetové hotline

Příloha 24 – Statistický výstup za rok 2014 Policejní internetové hotline

Příloha 25 – Statistický výstup za rok 2015 Policejní internetové hotline

Příloha 26 – Statistický výstup za rok 2016 Policejní internetové hotline

Příloha 27 – odevzdané dotazníky, školy na území hl. m. Prahy

Příloha 28 – odevzdané dotazníky, školy na území Středočeského kraje

Příloha 1 – Seznam obrázků

Příloha 2 – Seznam Tabulek

Příloha 3

Dotazník Vnímání kyber kriminality

Vyplň všechny položky. Dotazník je zcela anonymní, základní údaje jsou pouze pro statistické třídění.

*Povinné pole

1. **Název školy** *

2. **Věk** *
   Označte jen jednu elipsu.
   - 11
   - 12
   - 13
   - 14
   - 15 a více

3. **Pohlaví** *
   Označte jen jednu elipsu.
   - Chlapec
   - Dívka

4. **Absolvoval jsi v rámci výuky nějaký preventivní program, zaměřený na nežádoucí jednání na počítači** *
   Označte jen jednu elipsu.
   - Ano
   - Ne

5. **Máš účet na facebooku/messengeru?** *
   Označte jen jednu elipsu.
   - Ano
   - Ne

Označ jednání, které považuješ v ČR za trestné - za kyberkriminalitu

Trestné jednání je takové, za které může uložit český soud trest.

6. **Kyberkriminality je když,** *

Zaškrtněte všechny platné možnosti.

- [ ] stáhnu si písničku z internetu a pouštím si ji.
- [ ] staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout
- [ ] stáhnu si počítačovou hru z internetu
- [ ] stahuji si s internetu programy pro crackování her
- [ ] nahraju na internet do diskuzního fora cracky k počítačovým hrám ke stažení
- [ ] nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy
- [ ] nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačové hře.
- [ ] mám hodně stažených filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami
- [ ] nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu
- [ ] někdo mi poslal email, který vypadá jako z facebooku a já přes něj zadám svoje jméno a heslo a on se dostane do mého facebooku
- [ ] vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo
- [ ] vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele
- [ ] použiju heslo a uživatelské jméno jiného uživatele, které mi poslaly mnou vytvořené stránky, které udělal můj kamarád
- [ ] použiju heslo a uživatelské jméno jiného uživatele, které mi poslali mnou vytvořené stránky, které jsem si udělal a dal na internet
- [ ] nahraju kamarádovi bez jeho vědomí do počítače volně stažitelný program, abych se mohl dívat, co na počítači dělá
- [ ] náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil ve škole
- [ ] náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo do jeho facebooku, použiju ho a podívám se na jeho facebook
- [ ] náhodou uvidím, jaké rodiče mají uživatelské jméno a heslo na internetové bankovnictví a podívám se na jejich účet
- [ ] zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj
- [ ] přijdu k počítači, uvidím, že se kamarád neodhlásil z facebooku, tak se mu něco napíšu na jeho facebook
- [ ] přijdu k počítači ve škole, je otevřený prohlížeč a když dám zpět, tak se mi otevře spolužákův facebook. Když už jsem na jeho facebooku, tak si ho prohlédnu
- [ ] na počítači doma , je otevřený prohlížeč a když dám zpět, tak se mi otevře facebook rodičů, který si prohlédnu
- [ ] na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské, tak se zkusím přihlásit za ní, abych se podíval, co tam může zadávat
- [ ] na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské, tak se zkusím přihlásit za ní a přepíšu nějaké známky
- [ ] zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená
- [ ] změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni
- [ ] udělám si doma sbírku cracků k programům nebo hrám
- [ ] napíšu program, který umí odemknout nelegálně stažené windows
- [ ] nahraju na internet program, který umí odemknout zkušební verzi windows, aby šla používat pořád

- [ ] omylem jsem si stáhnul do počítače počítačový vir
- [ ] počítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokoval
- [ ] stáhnu si z internetu volně dostupný kod počítačového viru a pošlu ho kamarádovi
- [ ] použiju volně dostupný program, který mi jistí heslo do cizí wifi sítě
- [ ] z legrace pošlu kamarádovi program s počítačovým virem
- [ ] použiju volně dostupný program, který zablokuje provoz nějaké webové stránky svými stálými dotazy
- [ ] na kamarádovu zeď na facebooku vložím nějakou nadávku
- [ ] na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v nějaké trapné situaci
- [ ] dám na svůj facebook zprávu, že učitelka je pitomá
- [ ] dám na svůj facebook zprávu, že by měli jít cikáni do plynu
- [ ] dám na kamarádův facebookovou zeď zprávu, že by měli být uprchlíci nahnáni zpět do moře
- [ ] spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat zprávy, že je fakt strašný a měl by se raději zabít
- [ ] nahraju na wikipedii článek o tom, jak je škola pitomá
- [ ] přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky, místo skutečností
- [ ] náhodou zjistím heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky
- [ ] náhodou zjistím heslo k blogu kamaráda a na jeho blog smažu mu jeho zprávy a místo nich dám odkazy na porno
- [ ] použiju volně stažitelný program, který mi ve školní síti zjistí, kdo si co píše na chatu
- [ ] použiju volně stažitelný program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě
- [ ] Pošlu své kamarádce (14 let) svojí fotku ve spodním prádle
- [ ] Kamarádka (14 let) mi pošle svojí fotku ve spodním prádle
- [ ] Pošlu spolužákovi zprávu, že si na něj před školou počkáme a že do stane pěstí
- [ ] Píši si na internetu s dospělým člověkem
- [ ] Pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý
- [ ] Kamarádka (14 let) mi pošle svojí fotku, na které se sprchuje
- [ ] Napíšu své kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslala, zveřejním ve škole
- [ ] založím si webové stránky s doménou, která je stejná jako slavná zahraniční značka a umístím si na ně svůj vlastní obsah
- [ ] založím si webové stránky s doménou, jako je česká firma u zahraničního registrátora (třeba s koncovkou .eu) a budu chtít po české firmě, aby si ji koupila
- [ ] registruji si doménu se jménem nového výrobku dříve, než výrobce a budu mu jí nabízet na prodej. Když si ji nechce koupit, dám si na ní svůj obsah
- [ ] pošlu email do školy, že tam mají bombu
- [ ] pošlu email na policii, že na letišti je bomba
- [ ] Nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru
- [ ] někdo si zkopíruje cizí platební kartu
- [ ] na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačové hry

☐ rodiče mi na dají svoje číslo platební karty, abych ho mohl používat, a já si s ním zaplatím počítačovou hru na telefon

Uveď, zda jsi již danou věc zkoušel, nebo zda znáš nějakého svého vrstevníka, který toto dělal

Odpověz, ano/ne. Dotazník je anonymní, není možné určit, kdo jak hlasoval.

7. **Rozesílal jsi hromadně emailové zprávy, nebo si nainstaloval program, který toto dělá** *
   Označte jen jednu elipsu.
   - ◯ Ano
   - ◯ Ne

8. **Rozesílal nějaký tvůj vrstevník hromadně emailové zprávy, nebo si nainstaloval program, který toto dělá** *
   Označte jen jednu elipsu.
   - ◯ Ano
   - ◯ Ne

9. **Vytvořil jsi někdy stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje** *
   Označte jen jednu elipsu.
   - ◯ Ano
   - ◯ Ne

10. **Vytvořil tvůj vrtevník někdy stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje** *
    Označte jen jednu elipsu.
    - ◯ Ano
    - ◯ Ne

11. **Připojoval jsi se bez dovolení na facebookový profil někoho jiného** *
    Označte jen jednu elipsu.
    - ◯ Ano
    - ◯ Ne

12. **Připojoval se tvůj vrstevník se bez dovolení na facebookový profil někoho jiného** *
    Označte jen jednu elipsu.
    - ◯ Ano
    - ◯ Ne

13. **Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě** *
    Označte jen jednu elipsu.
    - ◯ Ano
    - ◯ Ne

14. **Použil tvůj vrstevník někdy program, který ti umožnil se přihlásit do cizí wifi sítě** *
Označte jen jednu elipsu.

- Ano
- Ne

15. **Zkoušel jsi odposlouchávat provoz v počítačové síti** *
Označte jen jednu elipsu.

- Ano
- Ne

16. **Zkoušel tvůj vrstevník odposlouchávat provoz v počítačové síti** *
Označte jen jednu elipsu.

- Ano
- Ne

17. **Přihlásil jsi se k cizí webové stránce** *
Označte jen jednu elipsu.

- Ano
- Ne

18. **Přihlásil se tvůj vrstevník k cizí webové stránce** *
Označte jen jednu elipsu.

- Ano
- Ne

19. **Přihlásil jsi se do cizího internetového bankovnictví** *
Označte jen jednu elipsu.

- Ano
- Ne

20. **Přihlásil se tvůj vrstevník do cizího internetového bankovnictví** *
Označte jen jednu elipsu.

- Ano
- Ne

21. **Použil jsi bez svolení cizí platební kartu na internetu** *
Označte jen jednu elipsu.

- Ano
- Ne

22. **Použil tvůj vrtevník bez svolení cizí platební kartu na internetu** *
Označte jen jednu elipsu.

- Ano
- Ne

23. **Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)** *
Označte jen jednu elipsu.

- Ano
- Ne

24. **Posílal tvůj vrstevník někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)** *
Označte jen jednu elipsu.

- Ano
- Ne

25. **Zkusil jsi někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků** *
Označte jen jednu elipsu.

- Ano
- Ne

26. **Zkusil tvůj vrstevník někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků** *
Označte jen jednu elipsu.

- Ano
- Ne

27. **Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program** *
Označte jen jednu elipsu.

- Ano
- Ne

28. **Poslal tvůj vrstevník někomu schválně počítačový vir nebo jiný škodlivý program** *
Označte jen jednu elipsu.

- Ano
- Ne

29. **Registroval jsi si doménu, jejíž jméno by mohlo patřit jinému** *
Označte jen jednu elipsu.

- Ano
- Ne

30. **Registroval si tvůj vrstevník doménu, jejíž jméno by mohlo patřit jinému** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

31. **Pozměnil jsi bez oprávnění nějaký počítačový program** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

32. **Pozměnil tvůj vrstevník bez oprávnění nějaký počítačový program** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

33. **Stahuješ si hudbu z internetu** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

34. **Stahuješ si videa z internetu** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

35. **Nahráváš staženou hudbu na internet, nebo nahráváš tam odkazy, odkud je lze stáhnout** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

36. **Nahráváš stažená videa na internet, nebo nahráváš tam odkazy, odkud je lze stáhnout** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

37. **Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

38. **Psal tvůj vrstevník na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)** *

Označte jen jednu elipsu.

- Ano
- Ne

39. **Nahrával jsi někomu jinému, nebo umisťoval na internet, počítačové cracky** *

Označte jen jednu elipsu.

- Ano
- Ne

40. **Nahrával tvůj vrstevník někomu jinému, nebo umisťoval na internet, počítačové cracky** *

Označte jen jednu elipsu.

- Ano
- Ne

41. **Poslal jsi někdy přes internet zprávu, že je někde bomba?** *

Označte jen jednu elipsu.

- Ano
- Ne

42. **Poslal tvůj vrstevník někdy přes internet zprávu, že je někde bomba?** *

Označte jen jednu elipsu.

- Ano
- Ne

43. **Požadoval jsi prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)** *

Označte jen jednu elipsu.

- Ano
- Ne

44. **Požadoval tvůj vrstevník prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)** *

Označte jen jednu elipsu.

- Ano
- Ne

45. **Šikanoval jsi někdo přes internet nebo na sociálních sítích**

Označte jen jednu elipsu.

- Ano
- Ne

46. **Šikanoval tvůj vrtevník někdo přes internet nebo na sociálních sítích** *
Označte jen jednu elipsu.

- Ano
- Ne

47. **Psal jsi si na internetu nebo sociálních sítích komunikaci s erotickým obsahem** *
Označte jen jednu elipsu.

- Ano
- Ne

48. **Psal tvůj vrstevník si na internetu nebo sociálních sítích komunikaci s erotickým obsahem** *
Označte jen jednu elipsu.

- Ano
- Ne

49. **Zkoušel jsi použít na internetu kódy platebních karet cizí osoby** *
Označte jen jednu elipsu.

- Ano
- Ne

50. **Zkoušel tvůj vrstevník použít na internetu kódy platebních karet cizí osoby** *
Označte jen jednu elipsu.

- Ano
- Ne

51. **Stahoval jsi si z internetu kódy platebních karet cizí osoby** *
Označte jen jednu elipsu.

- Ano
- Ne

52. **Stahoval si tvůj vrstevník z internetu kódy platebních karet cizí osoby** *
Označte jen jednu elipsu.

- Ano
- Ne

53. **Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí** *
Označte jen jednu elipsu.

- Ano
- Ne

54. **Použil tvůj vrstevník internetové bankovnictví cizí osoby bez jejího vědomí** *
Označte jen jednu elipsu.

- Ano
- Ne

55. **Udělal jsi si registraci na internetu, kde jsi uvedl jiné údaje, než skutečné** *
Označte jen jednu elipsu.

- Ano
- Ne

56. **Udělal si tvůj vrstevník registraci na internetu, kde uvedl jiné údaje, než skutečné** *
Označte jen jednu elipsu.

- Ano
- Ne

57. **Objednal jsi si na internetu zboží na jiné údaje než skutečné** *
Označte jen jednu elipsu.

- Ano
- Ne

58. **Objednal si tvůj vrstevník na internetu zboží na jiné údaje než skutečné** *
Označte jen jednu elipsu.

- Ano
- Ne

Příloha 4

tomas.danhelka@gmail.com

Upravit formulář

Počet odpovědí: 19

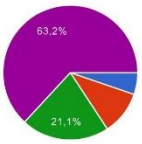
Zobrazit všechny odpovědi Publikovat analýzu

Souhrn

Název školy

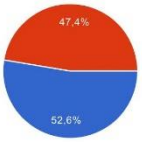
ZŠ Kořenského
Zš Kořenského
Pokus
Já
ZŠ Kořenského Líba
ZŠ Kořenského - Lenka
zs korenskeho
Kořernského
ZŠ a MŠ Kořenského
ZŠ Korenského
Kořenského
žš kořenskeho
Zš Kořenského

Věk



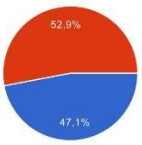
11	1	5.3 %
12	2	10.5 %
13	0	0 %
14	4	21.1 %
15 a více	12	63.2 %

Pohlaví



Chlapec	10	52.6 %
Dívka	9	47.4 %

Absolvoval jsi v rámci výuky nějaký preventivní program, zaměřený na nežádoucí jednání na počítači



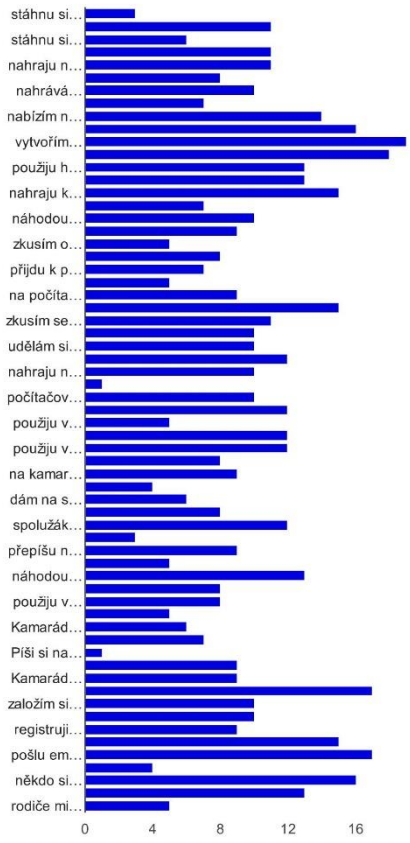
Ano	8	47.1 %
Ne	9	52.9 %

Máš účet na facebooku/messengeru?

Ano	17	100 %
Ne	0	0 %

Označ jednání, které považuješ v ČR za trestné - za kyberkriminalitu

Kyberkriminality je když,



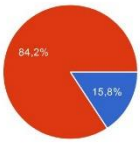
stáhnu si písničku z internetu a pouštím si ji.	3	15.8 %
staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout	11	57.9 %
stáhnu si počítačovou hru z internetu	6	31.6 %
stahuji si s internetu programy pro crackování her	11	57.9 %
nahraju na internet do diskuzního fora cracky k počítačovým hrám ke stažení	11	57.9 %
nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy	8	42.1 %
nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačové hře.	10	52.6 %
mám hodně stažených filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami	7	36.8 %
nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu	14	73.7 %
někdo mi poslal email, který vypadá jako z facebooku a já přes něj zadám svoje jméno a heslo a on se dostane do mého facebooku	16	84.2 %
vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo	19	100 %
vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele	18	94.7 %

použiju heslo a uživatelské jméno jiného uživatele, které mi poslaly mnou vytvořené stránky, které udělal můj kamarád	13	68.4 %
použiju heslo a uživatelské jméno jiného uživatele, které mi poslali mnou vytvořené stránky, které jsem si udělal a dal na internet	13	68.4 %
nahraju kamarádovi bez jeho vědomí do počítače volně stažitelný program, abych se mohl dívat, co na počítači dělá	15	78.9 %
náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil ve škole	7	36.8 %
náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo do jeho facebooku, použiju ho a podívám se na jeho facebook	10	52.6 %
náhodou uvidím, jaké rodiče mají uživatelské jméno a heslo na internetové bankovnictví a podívám se na jejich účet	9	47.4 %
zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj	5	26.3 %
přijdu k počítači, uvidím, že se kamarád neodhlásil z facebooku, tak se mu něco napíšu na jeho facebook	8	42.1 %
přijdu k počítači ve škole, je otevřený prohlížeč a když dám zpět, tak se mi otevře spolužákův facebook. Když už jsem na jeho facebooku, tak si ho prohlédnu	7	36.8 %
na počítači doma , je otevřený prohlížeč a když dám zpět, tak se mi otevře facebook rodičů, který si prohlédnu	5	26.3 %
na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské, tak se zkusím přihlásit za ní, abych se podíval, co tam může zadávat	9	47.4 %
na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské, tak se zkusím přihlásit za ní a přepíšu nějaké známky	15	78.9 %
zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená	11	57.9 %
změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni	10	52.6 %
udělám si doma sbírku cracků k programům nebo hrám	10	52.6 %
napíšu program, který umí odemknout nelegálně stažené windows	12	63.2 %
nahraju na internet program, který umí odemknout zkušební verzi windows, aby šla používat pořád	10	52.6 %
omylem jsem si stáhnul do počítače počítačový vir	1	5.3 %
počítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokoval	10	52.6 %
stáhnu si z internetu volně dostupný kod počítačového viru a pošlu ho kamarádovi	12	63.2 %
použiju volně dostupný program, který mi jistí heslo do cizí wifi sítě	5	26.3 %
z legrace pošlu kamarádovi program s počítačovým virem	12	63.2 %
použiju volně dostupný program, který zablokuje provoz nějaké webové stránky svými stálými dotazy	12	63.2 %
na kamarádovu zeď na facebooku vložím nějakou nadávku	8	42.1 %
na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v nějaké trapné situaci	9	47.4 %
dám na svůj facebook zprávu, že učitelka je pitomá	4	21.1 %
dám na svůj facebook zprávu, že by měli jít cikáni do plynu	6	31.6 %
dám na kamarádův facebookovou zeď zprávu, že by měli být uprchlíci nahnáni zpět do moře	8	42.1 %
spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat zprávy, že je fakt strašný a měl by se raději zabít	12	63.2 %
nahraju na wikipedii článek o tom, jak je škola pitomá	3	15.8 %
přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky, místo skutečností	9	47.4 %
náhodou zjistím heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky	5	26.3 %
náhodou zjistím heslo k blogu kamaráda a na jeho blog smažu mu jeho zprávy a místo nich dám odkazy na porno	13	68.4 %
použiju volně stažitelný program, který mi ve školní síti zjistí, kdo si co píše na chatu	8	42.1 %
použiju volně stažitelný program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě	8	42.1 %
Pošlu své kamarádce (14 let) svojí fotku ve spodním prádle	5	26.3 %
Kamarádka (14 let) mi pošle svojí fotku ve spodním prádle	6	31.6 %
Pošlu spolužákovi zprávu, že si na něj před školou počkáme a že do stane pěstí	7	36.8 %
Píši si na internetu s dospělým člověkem	1	5.3 %

Pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý	9	47.4 %
Kamarádka (14 let) mi pošle svojí fotku, na které se sprchuje	9	47.4 %
Napíšu své kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslala, zveřejním ve škole	17	89.5 %
založím si webové stránky s doménou, která je stejná jako slavná zahraniční značka a umístím si na ně svůj vlastní obsah	10	52.6 %
založím si webové stránky s doménou, jako je česká firma u zahraničního registrátora (třeba s koncovkou .eu) a budu chtít po české firmě, aby si ji koupila	10	52.6 %
registruji si doménu se jménem nového výrobku dříve, než výrobce a budu mu jí nabízet na prodej. Když si ji nechce koupit, dám si na ní svůj obsah	9	47.4 %
pošlu email do školy, že tam mají bombu	15	78.9 %
pošlu email na policii, že na letišti je bomba	17	89.5 %
Nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru	4	21.1 %
někdo si zkopíruje cizí platební kartu	16	84.2 %
na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačové hry	13	68.4 %
rodiče mi na dají svoje číslo platební karty, abych ho mohl používat, a já si s ním zaplatím počítačovou hru na telefon	5	26.3 %

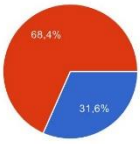
Uveď, zda jsi již danou věc zkoušel, nebo zda znáš nějakého svého vrstevníka, který toto dělal

Rozesílal jsi hromadně emailové zprávy, nebo si nainstaloval program, který toto dělá



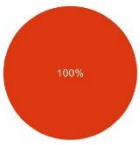
Ano	3	15.8 %
Ne	16	84.2 %

Rozesílal nějaký tvůj vrstevník hromadně emailové zprávy, nebo si nainstaloval program, který toto dělá



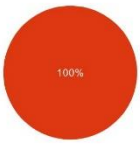
Ano	6	31.6 %
Ne	13	68.4 %

Vytvořil jsi někdy stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje



Ano	0	0 %
Ne	19	100 %

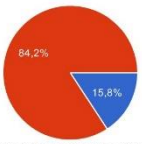
Vytvořil tvůj vrtevník někdy stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje



Ano	0	0 %
Ne	19	100 %

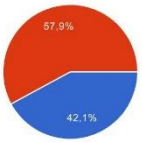
Připojoval jsi se bez dovolení na facebookový profil někoho jiného

Ano	3	15.8 %
Ne	16	84.2 %



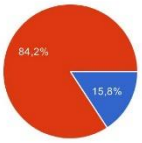
Připojoval se tvůj vrstevník se bez dovolení na facebookový profil někoho jiného

Ano	**8**	42.1 %
Ne	**11**	57.9 %



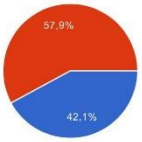
Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě

Ano	**3**	15.8 %
Ne	**16**	84.2 %



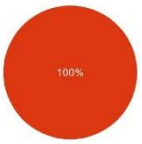
Použil tvůj vrstevník někdy program, který ti umožnil se přihlásit do cizí wifi sítě

Ano	**8**	42.1 %
Ne	**11**	57.9 %



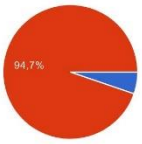
Zkoušel jsi odposlouchávat provoz v počítačové síti

Ano	**0**	0 %
Ne	**19**	100 %



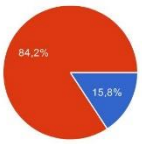
Zkoušel tvůj vrstevník odposlouchávat provoz v počítačové síti

Ano	**1**	5.3 %
Ne	**18**	94.7 %



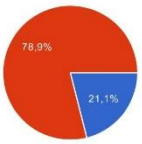
Přihlásil jsi se k cizí webové stránce

Ano	**3**	15.8 %
Ne	**16**	84.2 %



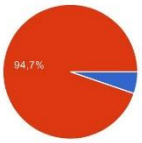
Přihlásil se tvůj vrstevník k cizí webové stránce

Ano	**4**	21.1 %
Ne	**15**	78.9 %

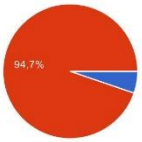


:tví

Ano	**1**	5.3 %
Ne	**18**	94.7 %

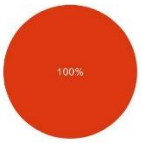


Přihlásil se tvůj vrstevník do cizího internetového bankovnictví



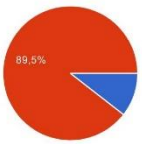
Ano	**1**	5.3 %
Ne	**18**	94.7 %

Použil jsi bez svolení cizí platební kartu na internetu



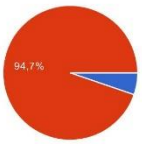
Ano	**0**	0 %
Ne	**19**	100 %

Použil tvůj vrtevník bez svolení cizí platební kartu na internetu



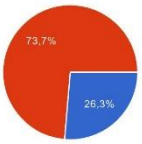
Ano	**2**	10.5 %
Ne	**17**	89.5 %

Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)



Ano	**1**	5.3 %
Ne	**18**	94.7 %

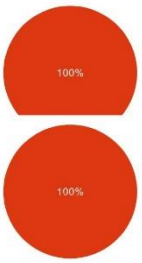
Posílal tvůj vrstevník někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)



Ano	**5**	26.3 %
Ne	**14**	73.7 %

Zkusil jsi někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků

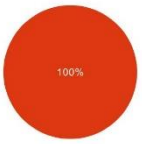
Ano	**0**	0 %
Ne	**19**	100 %



ou síť nebo webovou stránku odesíláním velkého množství požadavků

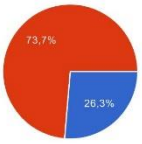
Ano	**0**	0 %
Ne	**19**	100 %

Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program



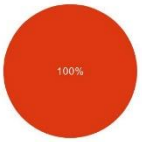
Ano	**0**	0 %
Ne	**19**	100 %

Poslal tvůj vrstevník někomu schválně počítačový vir nebo jiný škodlivý program



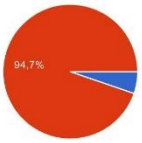
Ano	**5**	26,3 %
Ne	**14**	73,7 %

Registroval jsi si doménu, jejíž jméno by mohlo patřit jinému



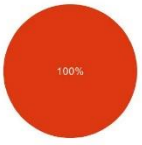
Ano	**0**	0 %
Ne	**19**	100 %

Registroval si tvůj vrstevník doménu, jejíž jméno by mohlo patřit jinému



Ano	**1**	5,3 %
Ne	**18**	94,7 %

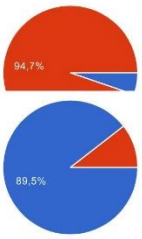
Pozměnil jsi bez oprávnění nějaký počítačový program



Ano	**0**	0 %
Ne	**19**	100 %

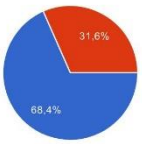
Pozměnil tvůj vrstevník bez oprávnění nějaký počítačový program

Ano	**1**	5,3 %
Ne	**18**	94,7 %



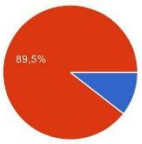
Ano	**17**	89.5 %
Ne	**2**	10.5 %

Stahuješ si videa z internetu



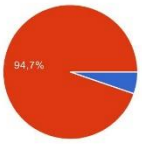
Ano	**13**	68.4 %
Ne	**6**	31.6 %

Nahráváš staženou hudbu na internet, nebo nahráváš tam odkazy, odkud je lze stáhnout



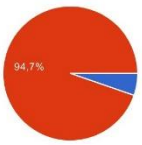
Ano	**2**	10.5 %
Ne	**17**	89.5 %

Nahráváš stažená videa na internet, nebo nahráváš tam odkazy, odkud je lze stáhnout



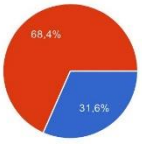
Ano	**1**	5.3 %
Ne	**18**	94.7 %

Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)



Ano	**1**	5.3 %
Ne	**18**	94.7 %

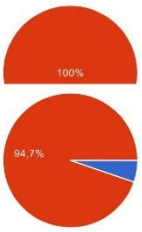
Psal tvůj vrstevník na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)



Ano	**6**	31.6 %
Ne	**13**	68.4 %

Nahrával jsi někomu jinému, nebo umisťoval na internet, počítačové cracky

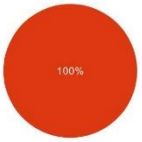
Ano	**0**	0 %
Ne	**19**	100 %



isťoval na internet, počítačové cracky

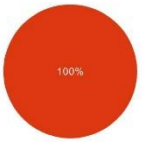
Ano	**1**	5.3 %
Ne	**18**	94.7 %

Poslal jsi někdy přes internet zprávu, že je někde bomba?



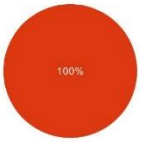
Ano	**0**	0 %
Ne	**19**	100 %

Poslal tvůj vrstevník někdy přes internet zprávu, že je někde bomba?



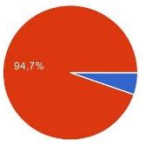
Ano	**0**	0 %
Ne	**19**	100 %

Požadoval jsi prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)



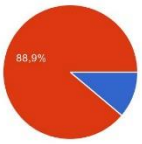
Ano	**0**	0 %
Ne	**19**	100 %

Požadoval tvůj vrstevník prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)



Ano	**1**	5.3 %
Ne	**18**	94.7 %

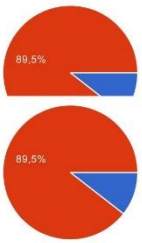
Šikanoval jsi někdo přes internet nebo na sociálních sítích



Ano	**2**	11.1 %
Ne	**16**	88.9 %

Šikanoval tvůj vrtevník někdo přes internet nebo na sociálních sítích

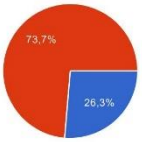
Ano	**2**	10.5 %
Ne	**17**	89.5 %



ıunikaci s erotickým obsahem

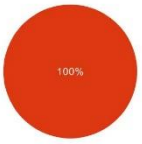
Ano	**2**	10.5 %
Ne	**17**	89.5 %

Psal tvůj vrstevník si na internetu nebo sociálních sítích komunikaci s erotickým obsahem



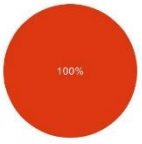
Ano	**5**	26.3 %
Ne	**14**	73.7 %

Zkoušel jsi použít na internetu kódy platebních karet cizí osoby



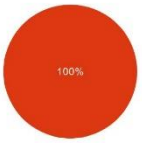
Ano	**0**	0 %
Ne	**19**	100 %

Zkoušel tvůj vrstevník použít na internetu kódy platebních karet cizí osoby



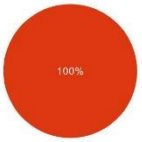
Ano	**0**	0 %
Ne	**19**	100 %

Stahoval jsi si z internetu kódy platebních karet cizí osoby



Ano	**0**	0 %
Ne	**19**	100 %

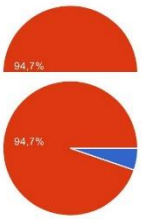
Stahoval si tvůj vrstevník z internetu kódy platebních karet cizí osoby



Ano	**0**	0 %
Ne	**19**	100 %

Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí

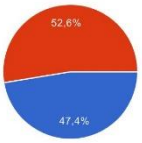
Ano	**1**	5.3 %
Ne	**18**	94.7 %



zí osoby bez jejího vědomí

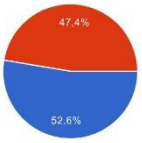
Ano	**1**	5.3 %
Ne	**18**	94.7 %

Udělal jsi si registraci na internetu, kde jsi uvedl jiné údaje, než skutečné



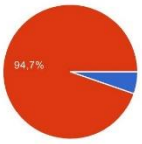
Ano	**9**	47.4 %
Ne	**10**	52.6 %

Udělal si tvůj vrstevník registraci na internetu, kde uvedl jiné údaje, než skutečné



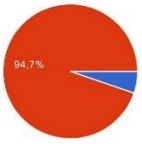
Ano	**10**	52.6 %
Ne	**9**	47.4 %

Objednal jsi si na internetu zboží na jiné údaje než skutečné



Ano	**1**	5.3 %
Ne	**18**	94.7 %

Objednal si tvůj vrstevník na internetu zboží na jiné údaje než skutečné



Ano	**1**	5.3 %
Ne	**18**	94.7 %

Počet odpovědí za den

Příloha 5

Dotazník Vnímání a prevence kyberkriminality

Vyplň všechny položky. Dotazník je zcela anonymní, základní údaje jsou pouze pro statistické třídění. Za pečlivé vyplnění předem děkuji.

Dotazníkové šetření je součástí diplomové práce na téma Vnímání a prevence kyberkriminality na základní škole. V přípravné fázi bylo šetření konzultováno s příslušným krajským koordinátorem prevence kriminality, který se na distribuci dotazníků podílí a který bude využívat výsledky této práce pro další působení v oblasti prevence kyberkriminality, výsledky budou taktéž využity v rámci Policie ČR.

*Povinné pole

1. **Název školy** *

2. **Věk** *
   Označte jen jednu elipsu.
   - 11
   - 12
   - 13
   - 14
   - 15 a více

3. **Pohlaví** *
   Označte jen jednu elipsu.
   - Chlapec
   - Dívka

4. **Absolvoval jsi v rámci výuky nějaký preventivní program, zaměřený na bezpečné chování v prostředí internetu a výpočetní techniky.** *
   Označte jen jednu elipsu.
   - Ano
   - Ne

5. **Máš účet na facebooku/messengeru?** *
   Označte jen jednu elipsu.
   - Ano
   - Ne

Co je podle tebe kyberkriminalita? Označ jednání, o kterém si myslíš, že je v ČR trestné.

Trestné jednání je takové, za které může uložit český soud trest.

6. **Kyberkriminalita je když,** *

Zaškrtněte všechny platné možnosti.

- [ ] stáhnu si počítačovou hru z internetu
- [ ] přijdu k počítači ve škole, je otevřený prohlížeč a když dám zpět, tak se mi otevře spolužákův facebook. Když už jsem na jeho facebooku, tak si ho prohlédnu
- [ ] nahraju kamarádovi bez jeho vědomí do počítače volně stažitelný program, abych se mohl dívat, co na počítači dělá
- [ ] nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy
- [ ] vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele
- [ ] mám hodně stažených filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami
- [ ] použiju heslo a uživatelské jméno jiného uživatele, které mi poslali webové stránky, které napodobují vzhled facebooku
- [ ] nahraju na internet do diskuzního fora cracky k počítačovým hrám ke stažení
- [ ] náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil ve škole
- [ ] stáhnu si písničku z internetu a pouštím si ji
- [ ] zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená
- [ ] náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo do jeho facebooku, použiju ho a podívám se na jeho facebook
- [ ] nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu
- [ ] nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačové hře
- [ ] počítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokoval
- [ ] zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj
- [ ] náhodou uvidím, jaké rodiče mají uživatelské jméno a heslo na internetové bankovnictví a podívám se na jejich účet
- [ ] dám na svůj facebook zprávu, že učitelka je pitomá
- [ ] přijdu k počítači, uvidím, že se kamarád neodhlásil z facebooku, tak mu něco napíšu na jeho facebook
- [ ] na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské a zkusím se přihlásit za ni, abych se podíval, co tam může zadávat
- [ ] stahuji si z internetu programy pro crackování her
- [ ] na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské a zkusím se přihlásit za ni a přepíšu nějaké známky
- [ ] vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo
- [ ] udělám si doma sbírku cracků k programům nebo hrám
- [ ] napíšu program, který umí odemknout nelegálně stažené windows
- [ ] někdo vytvořil počítačoví vir, který jsem si omylem stáhnul do počítače
- [ ] stáhnu si z internetu volně dostupný kod počítačového viru a pošlu ho z legrace kamarádovi
- [ ] na kamarádovu zeď na facebooku napíši nějakou nadávku
- [ ] použiju volně dostupný program, který mi zjistí heslo do cizí wifi sítě
- [ ] nahraju na internet program, který umí odemknout zkušební verzi windows, aby šla používat pořád

- [ ] na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v nějaké trapné situaci
- [ ] dám na svůj facebook zprávu, že by měli jít cikáni do plynu
- [ ] spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat na sociálních sítích zprávy, že je fakt strašný a měl by se raději zabít
- [ ] použiju volně dostupný program, který zablokuje provoz nějaké webové stránky svými stálými dotazy
- [ ] změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni
- [ ] nahraju na wikipedii článek o tom, jak je škola pitomá
- [ ] zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky
- [ ] dám na facebookovou zeď kamaráda zprávu, že by měli být uprchlíci nahnáni zpět do moře
- [ ] náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu jeho zprávy a místo nich dám odkazy na porno
- [ ] použiju volně stažitelný program, který mi ve školní síti zjistí, kdo si co píše na chatu
- [ ] použiju volně stažitelný program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě
- [ ] pošlu své kamarádce (14 let) svojí fotku ve spodním prádle
- [ ] na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačové hry
- [ ] pošlu spolužákovi zprávu, že si na něj před školou počkáme a že do stane pěstí
- [ ] přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky, místo skutečností
- [ ] píši si na internetu s dospělým člověkem
- [ ] pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý
- [ ] napíšu své kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslala, zveřejním ve škole
- [ ] založím si webové stránky s doménou, která je stejná jako slavná zahraniční značka a umístím si na ně svůj vlastní obsah
- [ ] registruji si doménu se jménem nového výrobku dříve, než výrobce a budu mu jí nabízet na prodej. Když si ji nechce koupit, dám si na ní svůj obsah
- [ ] staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout
- [ ] kamarádka (14 let) mi pošle svojí fotku ve spodním prádle
- [ ] pošlu email na policii, že na letišti je bomba
- [ ] nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru
- [ ] rodiče mi dají svoje číslo platební karty, abych ji mohl používat, a já si s ní zaplatím počítačovou hru na telefon
- [ ] založím si webové stránky s doménou, jako je česká firma u zahraničního registrátora (třeba s koncovkou .eu) a budu chtít po české firmě, aby si ji koupila
- [ ] kamarádka (14 let) mi pošle svojí fotku, na které se nahá sprchuje

Uveď, zda jsi již danou věc zkoušel, nebo zda znáš nějakého svého vrstevníka, který to dělal

Odpověz, ano/ne. Dotazník je anonymní, není možné určit, kdo jak hlasoval.

7. **Rozesílal jsi spamové emailové zprávy, nebo sis nainstaloval program, který to dělá** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

8. **Rozesílal nějaký tvůj vrstevník spamové emailové zprávy, nebo si nainstaloval program, který to dělá?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

9. **Vytvořil jsi někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

10. **Vytvořil tvůj vrtevník někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

11. **Připojoval jsi se bez dovolení na facebookový profil někoho jiného?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

12. **Připojoval se tvůj vrstevník se bez dovolení na facebookový profil někoho jiného?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

13. **Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

14. **Použil tvůj vrstevník někdy program, který ti umožnil se přihlásit do cizí wifi sítě?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

15. **Zkoušel jsi odposlouchávat provoz v počítačové síti?** *
Označte jen jednu elipsu.

- Ano
- Ne

16. **Zkoušel tvůj vrstevník odposlouchávat provoz v počítačové síti?** *
Označte jen jednu elipsu.

- Ano
- Ne

17. **Přihlásil jsi se neoprávněně k cizí webové stránce?** *
Označte jen jednu elipsu.

- Ano
- Ne

18. **Přihlásil se tvůj vrstevník neoprávněně k cizí webové stránce** *
Označte jen jednu elipsu.

- Ano
- Ne

19. **Přihlásil jsi se neoprávněně do cizího internetového bankovnictví?** *
Označte jen jednu elipsu.

- Ano
- Ne

20. **Přihlásil se tvůj vrstevník neoprávněně do cizího internetového bankovnictví?** *
Označte jen jednu elipsu.

- Ano
- Ne

21. **Použil jsi bez svolení cizí platební kartu na internetu?** *
Označte jen jednu elipsu.

- Ano
- Ne

22. **Použil tvůj vrtevník bez svolení cizí platební kartu na internetu?** *
Označte jen jednu elipsu.

- Ano
- Ne

23. **Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

24. **Posílal tvůj vrstevník někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

25. **Zkusil jsi někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

26. **Zkusil tvůj vrstevník někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

27. **Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

28. **Poslal tvůj vrstevník někomu schválně počítačový vir nebo jiný škodlivý program?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

29. **Pozměnil jsi bez oprávnění nějaký počítačový program?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

30. **Pozměnil tvůj vrstevník bez oprávnění nějaký počítačový program?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

31. **Stahuješ si hudbu z internetu?** *

Označte jen jednu elipsu.

- Ano
- Ne

32. **Stahuješ si videa z internetu?** *

Označte jen jednu elipsu.

- Ano
- Ne

33. **Nahráváš staženou hudbu na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?** *

Označte jen jednu elipsu.

- Ano
- Ne

34. **Nahráváš stažená videa na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?** *

Označte jen jednu elipsu.

- Ano
- Ne

35. **Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?** *

Označte jen jednu elipsu.

- Ano
- Ne

36. **Psal tvůj vrstevník na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?** *

Označte jen jednu elipsu.

- Ano
- Ne

37. **Poslal jsi někdy přes internet zprávu, že je někde bomba?** *

Označte jen jednu elipsu.

- Ano
- Ne

38. **Poslal tvůj vrstevník někdy přes internet zprávu, že je někde bomba?** *

Označte jen jednu elipsu.

- Ano
- Ne

39. **Požadoval jsi prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

40. **Požadoval tvůj vrstevník prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

41. **Šikanoval jsi někoho přes internet nebo na sociálních sítích?**

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

42. **Šikanoval tvůj vrtevník někdo přes internet nebo na sociálních sítích?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

43. **Psal sis na internetu nebo sociálních sítích komunikaci s erotickým obsahem?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

44. **Psal tvůj vrstevník na internetu nebo sociálních sítích komunikaci s erotickým obsahem?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

45. **Zkoušel jsi použít na internetu kódy platebních karet cizí osoby?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

46. **Zkoušel tvůj vrstevník použít na internetu kódy platebních karet cizí osoby?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

47. **Stahoval sis z internetu kódy platebních karet cizí osoby?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

48. **Stahoval si tvůj vrstevník z internetu kódy platebních karet cizí osoby?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

49. **Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

50. **Použil tvůj vrstevník internetové bankovnictví cizí osoby bez jejího vědomí?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

51. **Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, než skutečné?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

52. **Udělal si tvůj vrstevník registraci na internetu, kde uvedl jiné údaje, než skutečné?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

53. **Objednal sis na internetu zboží na jiné údaje než skutečné?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

54. **Objednal si tvůj vrstevník na internetu zboží na jiné údaje než skutečné?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

Děkuji za spolupráci a pečlivé vyplnění.

kpt. Mgr. Tomáš Daňhelka

Příloha 6

Vážená paní, vážený pane.

Obracím se na Vás se žádostí o spolupráci na **dotazníkovém šetření na téma Vnímání a prevence kyberkriminality na základní škole**. Cílová skupina jsou žáci druhého stupně základní školy, cílem dotazníkového šetření je zjistit povědomí dětí o tom, co to je kyberkriminalita, jaká je jejich zkušenost s ní.

Dotazníkové šetření bude probíhat v rámci Hl. m. Prahy a Středočeského kraje. **V přípravné fázi bylo konzultováno s příslušným krajským koordinátorem prevence kriminality, který se na distribuci dotazníků podílí a který bude taktéž využívat výsledky této práce pro další působení v oblasti prevence kyberkriminality, výsledky budou taktéž využity v rámci Policie ČR.**

Odkaz na dotazník

https://docs.google.com/forms/d/e/1FAIpQLSc_sTY2UIdAxuZoGhIrdPf4uKLKWimJwClNbGMvl3r5Sh9YVg/viewform?c=0&w=1

Dotazník přepošlete prosím svému metodiku prevence nebo informatikovi, kteří budou dotazník s žáky vyplňovat.

Dotazník je zpracovaný v programu google forms, je šířen formou odkazu na něj, očekávaná doba vyplnění je cca 15 minut. Vhodná forma vyplnění dotazníku je v rámci výuky informatiky či obdobného předmětu vyučovaného na Vaší škole, ideálně s dohledem příslušného učitele, který může výrazy, kterým by žáci nerozumněli, vysvětlit. K vyplnění je zapotřebí počítač či jiné zařízení připojené k síti internet. Dotazníky jsou anonymní, neumožňují identifikaci autorů jednotlivých odpovědí. Žáci by měli vyplňovat dotazníky samostatně, jde o zjištění jejich znalostí a jejich zkušeností. **Prosím o vyplnění dotazníků do 15. března 2017.**

Dotazník umožňuje třídit výsledky dle škol, samozřejmostí je zpětná vazba pro Vaši školu, na které oblasti se zaměřit při preventivním působení v oblasti kyberkriminality. Výsledky budou za jednotlivé školy zpracovány po celkovém vyhodnocení dotazníků, pravděpodobně ve 4. čtvrtletí 2017. Máte-li zájem o zpětnou vazbu, napište mi email s kontaktem na Vašeho pracovníka, kterému mají být výsledky zaslány, a se kterým se dá případně dále spolupracovat. **Pro zpětnou vazbu je nutné v dotazníku správně vyplnit název školy.**

Dotazníky jsou součástí diplomové práce na téma Vnímání a prevence kyberkriminality na základní škole, kterou jako student oboru Informatika České zemědělské univerzity v Praze a zároveň vrchní komisař SKPV oddělení informační kriminality Krajského ředitelství policie Středočeského kraje zpracovávám. Pro další informace mne kontaktujte, budu vděčný za každou zpětnou vazbu z Vaší strany.

Děkuji za Vaši pozornost a spolupráci.

S pozdravem
kpt. Mgr. Tomáš Daňhelka
vrchní komisař
tomas.danhelka@gmail.com

Příloha 7

tomas.danhelka@gmail.com

Upravit formulář

Počet odpovědí: 248

Zobrazit všechny odpovědi Publikovat analýzu

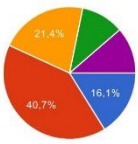
Souhrn

Název školy

Základní škola, Praha 10, Jakutská 2/1210
ZŠ Kořenského
Základní škola, Praha 2, Londýnská 34
ZŠ Lipence
ZŠ Praha Lipence
Zš Kořenského
ZŠ Karla Čapka
zš praha lipence
ZŠ, Hauptova 591, Praha - Zbraslav
Zš Praha Lipence
Zš Lipence
Zš a Mš Kořenského
ZŠ a MŠ Kořenského Praha 5
Základní škola,Praha 10,Jakutská 2/1210
ZŠ A MŠ KOŘENSKÉHO
ZŠ-Lipence
Základní škola,Praha 10, Jakutská 2/1210
Základní škola Lipence
zš Lipence
ZŠ a MŠ Kořenského
ZŠ Vladislava Vančury
Zš Vladislava Vančury
ZŠ,Hauptova591 Praha-Zbraslav
Základní Škola, Praha 2, Londýnská 34
Zš Karla Čapka
zs karla capka
ZŠ Kořenského
Základní škola Praha 10 Jakutská 2/1210
Zakladní škola, Praha 10, Jakutská 2/1210
základní škola, Praha 10, Jakutská 2/1210
Jakutská
Základní škola ,Praha ,Jakutská 2/1210
ZŠ Praha - Lipence
ZŠ MŠ Kořenského Praha 5
ZŠ Praha-Lipence
ŽŠ Lipence
ZŠ Praha Lipnce
ZŠ Praha Lipence
ZŠ- Lipence Praha5
zškořenskeho
ZšKořenského
ZS Kořenského
Základní škola, Praha 10, Jakutská 2/1210
10, Jakutská 2/1210
základní škola, praha 10,Jakutská 2/1210
Základní škola Lipence
Zš Praha-Lipence
Žš Praha Lipence
zš Praha Lipence
Zš a Mš kořenského
Zs Kořenského
Kořeského
Zš Mš kořenského

zs křenského
Zš kořenského
ZŠ Krořenského
Základní škola, Praha 10, Jakutska2/1210
Základní škola, Praha 10, Jakutská 2/1210
Základní škola, Praha 10 ,Jakutská 2/1210
Základní škola, Praha 10, Jakutská /
Základní škola, Praha10, Jakutská 2/1210
Základní škola, PRAHA 10, Jakutská 2/1210
Základní škola, Praha 10 Jakutská 2/1210
Základní škola, Praha 10,Jakutská 2/1210
Základní škola, Praha 10, Jakutská2/1210
Základní škola , Praha 10 , Jakutská 2/1210
Základní škola ,Praha 10, Jakutská 2/1210
Základní škola Praha 10, Jakutská 2/1210
ZŠ PRAHA LIPENCE
ZŠ s RVJ K Míličovu
ZŠ londýnská
Hauptova591 Praha 5
Hauptova 561 Praha 5
Zš, Hauptova 591, Praha Zbraslav
Hauptova 591 Praha 5
Vladislava Vančury
Zš-Hauptova 591 Praha 5
Zš-Hauptova 591-Praha Zbraslav
zš Vladislava Vančury
ZŠ, Hauptova591, Praha-Zbraslav
ZŠ, Haptova 591, Praha-Zbraslav
ZŠ,Hauptova591, Praha-Zbraslav
Zš-Hauptova 591 Praha zbraslav
Zš Londýnská
Základní škola, Praha2,Londýnská 34
Zakladní škola,Praha2,Londýnská 34
základní škola praha 2,londýnská 34
základní škola,Praha 2,Londýnská 34
Karla Čapka
Zš karla Čapka
zskodanska
Karla Čapka Zš
ZŠ Londynska, Praha 2, Londýnská 34
Zš Londýnská, Praha2, Londýnská 34
ZŠ Londýnská Praha 2 Londýnská 34
Základní škola,Praha 2, Londýnská 34
Základní škola, Praha2, Londýnská 34
Základní škola, Praha 2, Londýnska 34
zs kodanska
KARLA CAPKA
ZŠ Kodaňská
ZS KARLA CAPKA

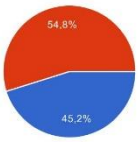
Věk



11	**40**	16.1 %
12	**101**	40.7 %
13	**53**	21.4 %
14	**26**	10.5 %
15 a více	**28**	11.3 %

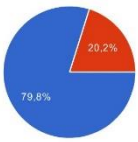
Pohlaví

Chlapec	**112**	45.2 %
Dívka	**136**	54.8 %

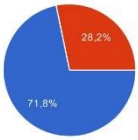


rogram, zaměřený na bezpečné chování v prostředí internetu a výpočetní techniky.

Ano	**198**	79.8 %
Ne	**50**	20.2 %



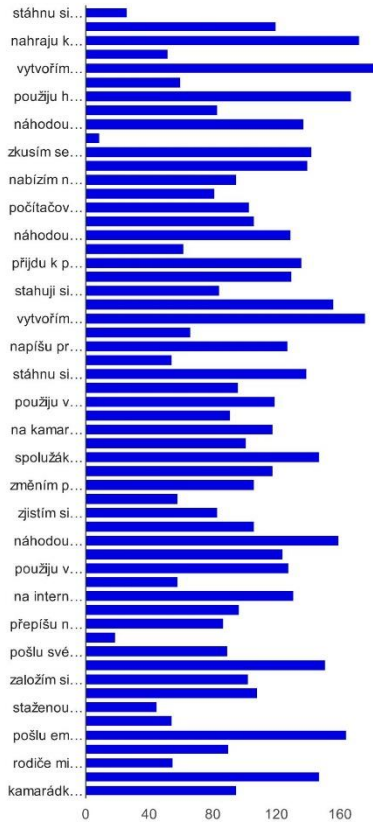
Máš účet na facebooku/messengeru?



Ano	**178**	71.8 %
Ne	**70**	28.2 %

Co je podle tebe kyberkriminalita? Označ jednání, o kterém si myslíš, že je v ČR trestné.

Kyberkriminalita je když,

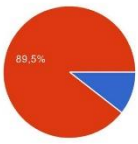


stáhnu si počítačovou hru z internetu	26	10.5 %
k se mi otevře spolužáků facebook. Když už jsem na jeho facebooku, tak si ho prohlédnu	120	48.4 %
eho vědomí do počítače volně stažitelný program, abych se mohl dívat, co na počítači dělá	172	69.4 %
nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy	52	21 %
ánka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele	199	80.2 %
tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami	60	24.2 %
méno jiného uživatele, které mi poslali webové stránky, které napodobují vzhled facebooku	167	67.3 %
nahraju na internet do diskuzního fora cracky k počítačovým hrám ke stažení	83	33.5 %
uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil ve škole	137	55.2 %
stáhnu si písničku z internetu a pouštím si ji	9	3.6 %
zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená	142	57.3 %
al uživatelské jméno a heslo do jeho facebooku, použiju ho a podívám se na jeho facebook	140	56.5 %
nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu	95	38.3 %
nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačové hře	81	32.7 %
čítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokoval	103	41.5 %
zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj	106	42.7 %
liče mají uživatelské jméno a heslo na internetové bankovnictví a podívám se na jejich účet	129	52 %
dám na svůj facebook zprávu, že učitelka je pitomá	62	25 %
tači, uvidím, že se kamarád neodhlásil z facebooku, tak mu něco napíšu na jeho facebook	136	54.8 %
elektronické žákovské a zkusím se přihlásit za ni, abych se podíval, co tam může zadávat	130	52.4 %
stahuji si z internetu programy pro crackování her	84	33.9 %
telka heslo do elektronické žákovské a zkusím se přihlásit za ni a přepíšu nějaké známky	156	62.9 %
vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo	176	71 %
udělám si doma sbírku cracků k programům nebo hrám	66	26.6 %
napíšu program, který umí odemknout nelegálně stažené windows	127	51.2 %
někdo vytvořil počítačoví vir, který jsem si omylem stáhnul do počítače	54	21.8 %
stáhnu si z internetu volně dostupný kod počítačového viru a pošlu ho z legrace kamarádovi	139	56 %
na kamarádovu zeď na facebooku napíši nějakou nadávku	96	38.7 %
použiju volně dostupný program, který mi zjistí heslo do cizí wifi sítě	119	48 %
nahraju na internet program, který umí odemknout zkušební verzi windows, aby šla používat pořád	91	36.7 %
na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v nějaké trapné situaci	118	47.6 %
dám na svůj facebook zprávu, že by měli jít cikáni do plynu	101	40.7 %
spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat na sociálních sítích zprávy, že je fakt strašný a měl by se raději zabít	147	59.3 %
použiju volně dostupný program, který zablokuje provoz nějaké webové stránky svými stálými dotazy	118	47.6 %
změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni	106	42.7 %
nahraju na wikipedii článek o tom, jak je škola pitomá	58	23.4 %
zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky	83	33.5

		%
dám na facebookovou zeď kamaráda zprávu, že by měli být uprchlíci nahnáni zpět do moře	106	42.7 %
náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu jeho zprávy a místo nich dám odkazy na porno	159	64.1 %
použiju volně stažitelný program, který mi ve školní síti zjistí, kdo si co píše na chatu	124	50 %
použiju volně stažitelný program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě	128	51.6 %
pošlu své kamarádce (14 let) svojí fotku ve spodním prádle	58	23.4 %
na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačové hry	131	52.8 %
pošlu spolužákovi zprávu, že si na něj před školou počkáme a že do stane pěstí	97	39.1 %
přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky, místo skutečností	87	35.1 %
píši si na internetu s dospělým člověkem	19	7.7 %
pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý	89	35.9 %
napíšu své kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslala, zveřejním ve škole	151	60.9 %
založím si webové stránky s doménou, která je stejná jako slavná zahraniční značka a umístím si na ně svůj vlastní obsah	102	41.1 %
registruji si doménu se jménem nového výrobku dříve, než výrobce a budu mu jí nabízet na prodej. Když si ji nechce koupit, dám si na ní svůj obsah	108	43.5 %
staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout	45	18.1 %
kamarádka (14 let) mi pošle svojí fotku ve spodním prádle	54	21.8 %
pošlu email na policii, že na letišti je bomba	164	66.1 %
nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru	90	36.3 %
rodiče mi dají svoje číslo platební karty, abych ji mohl používat, a já si s ní zaplatím počítačovou hru na telefon	55	22.2 %
založím si webové stránky s doménou, jako je česká firma u zahraničního registrátora (třeba s koncovkou .eu) a budu chtít po české firmě, aby si ji koupila	147	59.3 %
kamarádka (14 let) mi pošle svojí fotku, na které se nahá sprchuje	95	38.3 %

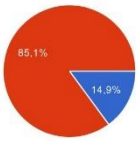
Uveď, zda jsi již danou věc zkoušel, nebo zda znáš nějakého svého vrstevníka, který to dělal

Rozesílal jsi spamové emailové zprávy, nebo sis nainstaloval program, který to dělá



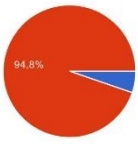
Ano	26	10.5 %
Ne	222	89.5 %

Rozesílal nějaký tvůj vrstevník spamové emailové zprávy, nebo si nainstaloval program, který to dělá?



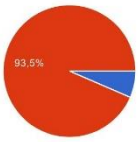
Ano	37	14.9 %
Ne	211	85.1 %

Vytvořil jsi někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?



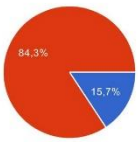
Ano	13	5.2 %
Ne	235	94.8 %

Vytvořil tvůj vrstevník někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?



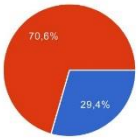
Ano	**16**	6.5 %
Ne	**232**	93.5 %

Připojoval jsi se bez dovolení na facebookový profil někoho jiného?



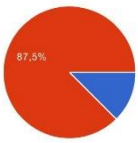
Ano	**39**	15.7 %
Ne	**209**	84.3 %

Připojoval se tvůj vrstevník se bez dovolení na facebookový profil někoho jiného?



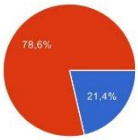
Ano	**73**	29.4 %
Ne	**175**	70.6 %

Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě?



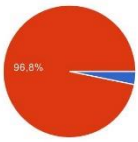
Ano	**31**	12.5 %
Ne	**217**	87.5 %

Použil tvůj vrstevník někdy program, který ti umožnil se přihlásit do cizí wifi sítě?



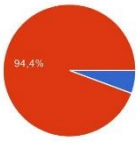
Ano	**53**	21.4 %
Ne	**195**	78.6 %

Zkoušel jsi odposlouchávat provoz v počítačové síti?



Ano	**8**	3.2 %
Ne	**240**	96.8 %

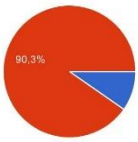
Zkoušel tvůj vrstevník odposlouchávat provoz v počítačové síti?



Ano	**14**	5.6 %
Ne	**234**	94.4 %

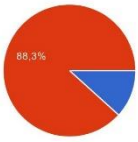
Přihlásil jsi se neoprávněně k cizí webové stránce?

Ano	**24**	9.7 %
Ne	**224**	90.3 %



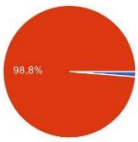
Přihlásil se tvůj vrstevník neoprávněně k cizí webové stránce

Ano	**29**	11.7 %
Ne	**219**	88.3 %



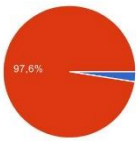
Přihlásil jsi se neoprávněně do cizího internetového bankovnictví?

Ano	**3**	1.2 %
Ne	**245**	98.8 %



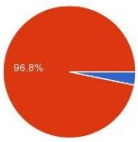
Přihlásil se tvůj vrstevník neoprávněně do cizího internetového bankovnictví?

Ano	**6**	2.4 %
Ne	**242**	97.6 %



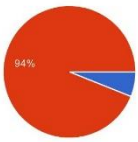
Použil jsi bez svolení cizí platební kartu na internetu?

Ano	**8**	3.2 %
Ne	**240**	96.8 %



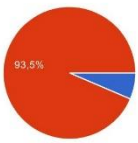
Použil tvůj vrstevník bez svolení cizí platební kartu na internetu?

Ano	**15**	6 %
Ne	**233**	94 %



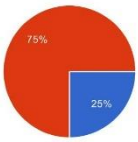
Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)?

Ano	**16**	6.5 %
Ne	**232**	93.5 %



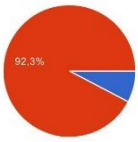
Posílal tvůj vrstevník někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)?

Ano	**62**	25 %
Ne	**186**	75 %



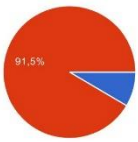
webovou stránku odesíláním velkého množství požadavků?

Ano	**19**	7.7 %
Ne	**229**	92.3 %



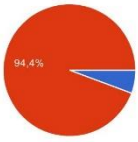
Zkusil tvůj vrstevník někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků?

Ano	**21**	8.5 %
Ne	**227**	91.5 %



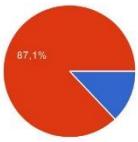
Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program?

Ano	**14**	5.6 %
Ne	**234**	94.4 %



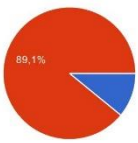
Poslal tvůj vrstevník někomu schválně počítačový vir nebo jiný škodlivý program?

Ano	**32**	12.9 %
Ne	**216**	87.1 %



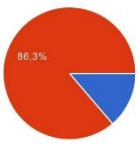
Pozměnil jsi bez oprávnění nějaký počítačový program?

Ano	**27**	10.9 %
Ne	**221**	89.1 %



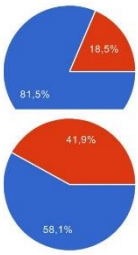
Pozměnil tvůj vrstevník bez oprávnění nějaký počítačový program?

Ano	**34**	13.7 %
Ne	**214**	86.3 %



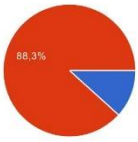
Stahuješ si hudbu z internetu?

Ano	**202**	81.5 %
Ne	**46**	18.5 %



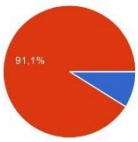
Ano	**144**	58.1 %
Ne	**104**	41.9 %

Nahráváš staženou hudbu na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?



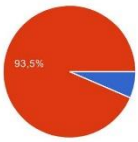
Ano	**29**	11.7 %
Ne	**219**	88.3 %

Nahráváš stažená videa na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?



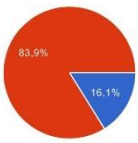
Ano	**22**	8.9 %
Ne	**226**	91.1 %

Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?



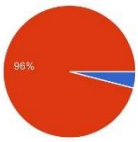
Ano	**16**	6.5 %
Ne	**232**	93.5 %

Psal tvůj vrstevník na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?



Ano	**40**	16.1 %
Ne	**208**	83.9 %

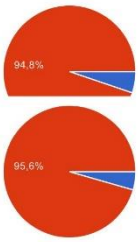
Poslal jsi někdy přes internet zprávu, že je někde bomba?



Ano	**10**	4 %
Ne	**238**	96 %

Poslal tvůj vrstevník někdy přes internet zprávu, že je někde bomba?

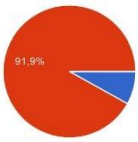
Ano	**13**	5.2 %
Ne	**235**	94.8 %



ciálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného apod.)?

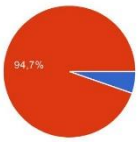
Ano	**11**	4.4 %
Ne	**237**	95.6 %

Požadoval tvůj vrstevník prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejniš jeho fotografie nebo video, apod.)?



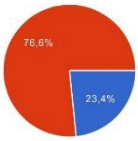
Ano	**20**	8.1 %
Ne	**228**	91.9 %

Šikanoval jsi někoho přes internet nebo na sociálních sítích?



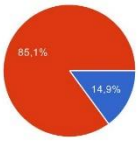
Ano	**13**	5.3 %
Ne	**231**	94.7 %

Šikanoval tvůj vrstevník někdo přes internet nebo na sociálních sítích?



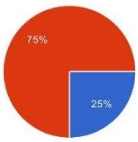
Ano	**58**	23.4 %
Ne	**190**	76.6 %

Psal sis na internetu nebo sociálních sítích komunikaci s erotickým obsahem?



Ano	**37**	14.9 %
Ne	**211**	85.1 %

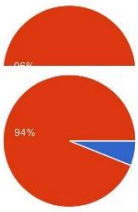
Psal tvůj vrstevník na internetu nebo sociálních sítích komunikaci s erotickým obsahem?



Ano	**62**	25 %
Ne	**186**	75 %

Zkoušel jsi použít na internetu kódy platebních karet cizí osoby?

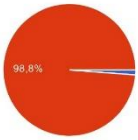
Ano	**10**	4 %
Ne	**238**	96 %



latebních karet cizí osoby?

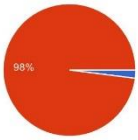
Ano	**15**	6 %
Ne	**233**	94 %

Stahoval sis z internetu kódy platebních karet cizí osoby?



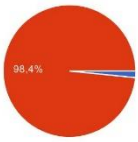
Ano	**3**	1.2 %
Ne	**245**	98.8 %

Stahoval si tvůj vrstevník z internetu kódy platebních karet cizí osoby?



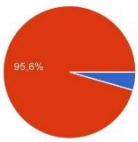
Ano	**5**	2 %
Ne	**243**	98 %

Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí?



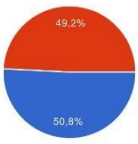
Ano	**4**	1.6 %
Ne	**244**	98.4 %

Použil tvůj vrstevník internetové bankovnictví cizí osoby bez jejího vědomí?



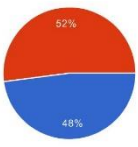
Ano	**11**	4.4 %
Ne	**237**	95.6 %

Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, než skutečné?



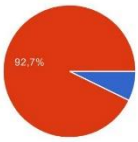
Ano	**126**	50.8 %
Ne	**122**	49.2 %

Udělal si tvůj vrstevník registraci na internetu, kde uvedl jiné údaje, než skutečné?



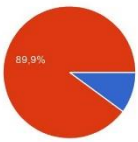
Ano	**119**	48 %
Ne	**129**	52 %

Objednal sis na internetu zboží na jiné údaje než skutečné?



Ano	**18**	7.3 %
Ne	**230**	92.7 %

Objednal si tvůj vrstevník na internetu zboží na jiné údaje než skutečné?



Ano	**25**	10.1 %
Ne	**223**	89.9 %

Děkuji za spolupráci a pečlivé vyplnění.

Počet odpovědí za den

Příloha 8

tomas.danhelka@gmail.com

Upravit formulář

Počet odpovědí: 3898

Zobrazit všechny odpovědi Publikovat analýzu

Souhrn

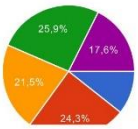
Název školy

ZŠ Žižkov Kutná Hora
ZŠ 28. října NERATOVICE
Gymnázium Zikmunda Wintra Rakovník
Gymnázium Mnichovo Hradiště
Gymnázium Jana Palacha Mělník
Základní škola Václava Havla Poděbrady
ZŠ Generála Klapálka
ZŠ Dolní Břežany
ZŠ Luštěnice
ZŠ Zásmuky
ZŠ Juventa Milovice
ZŠ Pečky, okres Kolín
Základní škola Pečky, okres Kolín
ZŠ Václava Havla
ZŠ Davle
Gymnázium Karla Čapka Dobříš
ZŠ Kolín III., Lipanská 420
ZŠ Uhlířské Janovice, okres Kutná Hora
ZŠ Všetaty
ZŠ Zbraslavice
ZŠ a MŠ Čistá u Rakovníka
ZŠ Kostelec nad Černými lesy
ZŠ Březnice
Gymnázium Příbram
Zš Zásmuky
Generála Klapálka
ZŠ Průhonice
ZŠ Uhlířské Janovice okres Kutná Hora
Základní škola Kolín V., Ovčárecká 374
Základní škola Letců R.A.F. v Nymburce
ZŠ Městec Králové
ZŠ Týnec nad Labem
ZŠ a MŠ Dolní Břežany
ZŠ Pečky
ZŠ Pečky,okres Kolín
Kostelec nad Černými lesy
ZŠ 28. října NERATOVICE
Zš Průhonice
ZŠ a MŠ Nečín
ZŠ Tyršova 446 Nymburk
ZŠ Libušín
ZŠ Žižkov
Gymnázium Příbram, Legionářů 402
ZŠ Cerhenice
generála klapálka
Základní škola, Kosova Hora, okres Příbram
ZŠ a MŠ v Novém Strašecí
ZŠ Ing.M.Plesingera-Božinova Neratovice
ZŠ Žižkov, Kutná Hora
ZŠ Ing. M. Plesingera-Božinova Neratovice
Gymnázium Jana Palacha
Základní škola Kolín III., Lipanská 420
Základní škola T. G. Masaryka Poděbrady, Školní 556, okres Nymburk

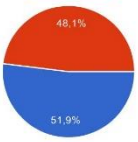
Masarykova základní škola a mateřská škola Obecnice
7.zš Kolín
Základní škola Letců R.A.F v Nymburce
Dolní Břežany
ZŠ a MŠ Kácov
ZŠ Jílové u Prahy
7.ZŠ Kolín
ZŠ Václava Havla Poděbrady
Základní škola Městec Králové
ZŠ KOLÍN 5., OVČÁRECKÁ 374
Gymnázium Karla Čapka, Dobříš
ZŠ Kosova Hora, okres Příbram
ZŠ Kolín 5 Ovčárecká 374
ZŠ Žehušice
Zš Zbraslavice
GJP Mělník
ZŠ Tyršova 446, Nymburk
ZŠ
Zš Juventa Milovice
Václava Havla
ZŠ Kolín 3, Masarykova 412
2.zš Rakovník
Základní škola Komenského náměstí 35, Dobříš
Zš Všetaty
Zš Pečky, okres Kolín
7 ZŠ Kolín
Zásmuky
ZŠ Kolín V, Ovčárecká 374
Zš Žižkov Kutná Hora
Zš Generála Klapálka
ZŠ Kolín 5., Ovčárecká 374
Základní škola Luštěnice
Zš a Mš Dolní Břežany
2. Základní škola Rakovník
8zsmb
Základní škola Šanov
Šanov
Všetaty
7 zš kolín
Zš a Mš v Novém Strašecí
Základní škola Václava Havla
14. ZŠ Kladno
ZŠ a PrŠ, Kutná Hora
ŽŠ Žižkov Kutná Hora
zš generála klapálka
Zš Žižkov
ZŠ Žižkov Kutná Hora
ZŠ Kostelec n. Č. l.
zš zbraslavice
Gymnázium Zikmunda Wintra
Základní škola Dobříš, Komenského nám. 35, okres Příbram
ZŠ Václava Havla Kralupy
zš Václava Havla
Zš a Mš Kácov
ZŠ T.G.MASARYKA,MILOVICE
2zš Rakovník
Ostatní

Věk

11	**416**	10.7 %
12	**948**	24.3 %
13	**837**	21.5 %
14	**1011**	25.9 %

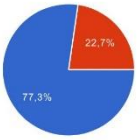


15 a více **686** 17.6 %



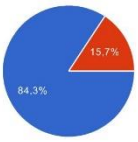
Chlapec **2023** 51.9 %
Dívka **1875** 48.1 %

Absolvoval jsi v rámci výuky nějaký preventivní program, zaměřený na bezpečné chování v prostředí internetu a výpočetní techniky.



Ano **3014** 77.3 %
Ne **884** 22.7 %

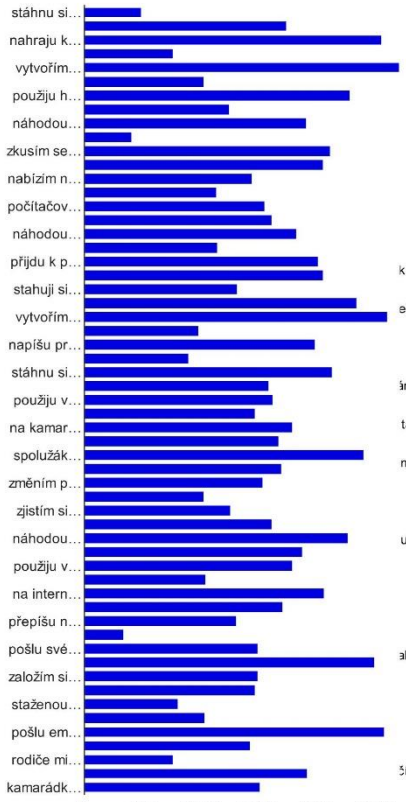
Máš účet na facebooku/messengeru?



Ano **3286** 84.3 %
Ne **612** 15.7 %

Co je podle tebe kyberkriminalita? Označ jednání, o kterém si myslíš, že je v ČR trestné.

Kyberkriminalita je když,

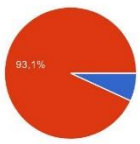


stáhnu si počítačovou hru z internetu	494	12.7 %
k se mi otevře spolužákův facebook. Když už jsem na jeho facebooku, tak si ho prohlédnu	1747	44.8 %
eho vědomí do počítače volně stažitelný program, abych se mohl dívat, co na počítači dělá	2566	65.8 %
nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy	764	19.6 %
ánka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele	2715	69.7 %
tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami	1029	26.4 %
méno jiného uživatele, které mi poslali webové stránky, které napodobují vzhled facebooku	2288	58.7 %
nahraju na internet do diskuzního fora cracky k počítačovým hrám ke stažení	1254	32.2 %
uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil ve škole	1911	49 %
stáhnu si písničku z internetu a pouštím si ji	409	10.5 %
zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená	2122	54.4 %
al uživatelské jméno a heslo do jeho facebooku, použiju ho a podívám se na jeho facebook	2058	52.8 %
nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu	1451	37.2 %
nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačové hře	1139	29.2 %
čítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokoval	1561	40 %
zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj	1616	41.5 %
liče mají uživatelské jméno a heslo na internetové bankovnictví a podívám se na jejich účet	1832	47 %
dám na svůj facebook zprávu, že učitelka je pitomá	1146	29.4 %
přijdu k počítači, uvidím, že se kamarád neodhlásil z facebooku, tak mu něco napíšu na jeho facebook	2019	51.8 %
na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské a zkusím se přihlásit za ni, abych se podíval, co tam může zadávat	2063	52.9 %
stahuji si z internetu programy pro crackování her	1315	33.7 %
na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské a zkusím se přihlásit za ni a přepíšu nějaké známky	2351	60.3 %
vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo	2611	67 %
udělám si doma sbírku cracků k programům nebo hrám	991	25.4 %
napíšu program, který umí odemknout nelegálně stažené windows	1988	51 %
někdo vytvořil počítačovi vir, který jsem si omylem stáhnul do počítače	900	23.1 %
stáhnu si z internetu volně dostupný kod počítačového viru a pošlu ho z legrace kamarádovi	2136	54.8 %
na kamarádovu zeď na facebooku napíši nějakou nadávku	1590	40.8 %
použiju volně dostupný program, který mi zjistí heslo do cizí wifi sítě	1623	41.6 %
nahraju na internet program, který umí odemknout zkušební verzi windows, aby šla používat pořád	1476	37.9 %
na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v nějaké trapné situaci	1800	46.2 %
dám na svůj facebook zprávu, že by měli jít cikáni do plynu	1675	43 %

spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat na sociálních sítích zprávy, že je fakt strašný a měl by se raději zabít	**2407**	61.7 %
použiju volně dostupný program, který zablokuje provoz nějaké webové stránky svými stálými dotazy	**1701**	43.6 %
změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni	**1541**	39.5 %
nahraju na wikipedii článek o tom, jak je škola pitomá	**1028**	26.4 %
zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky	**1257**	32.2 %
dám na facebookovou zeď kamaráda zprávu, že by měli být uprchlíci nahnáni zpět do moře	**1618**	41.5 %
náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu jeho zprávy a místo nich dám odkazy na porno	**2274**	58.3 %
použiju volně stažitelný program, který mi ve školní síti zjistí, kdo si co píše na chatu	**1883**	48.3 %
použiju volně stažitelný program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě	**1798**	46.1 %
pošlu své kamarádce (14 let) svojí fotku ve spodním prádle	**1049**	26.9 %
na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačové hry	**2068**	53.1 %
pošlu spolužákovi zprávu, že si na něj před školou počkáme a že do stane pěstí	**1713**	43.9 %
přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky, místo skutečností	**1313**	33.7 %
píši si na internetu s dospělým člověkem	**338**	8.7 %
pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý	**1495**	38.4 %
napíšu své kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslala, zveřejním ve škole	**2498**	64.1 %
založím si webové stránky s doménou, která je stejná jako slavná zahraniční značka a umístím si na ně svůj vlastní obsah	**1494**	38.3 %
registruji si doménu se jménem nového výrobku dříve, než výrobce a budu mu jí nabízet na prodej. Když si ji nechce koupit, dám si na ní svůj obsah	**1472**	37.8 %
staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout	**810**	20.8 %
kamarádka (14 let) mi pošle svojí fotku ve spodním prádle	**1038**	26.6 %
pošlu email na policii, že na letišti je bomba	**2587**	66.4 %
nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru	**1434**	36.8 %
rodiče mi dají svoje číslo platební karty, abych ji mohl používat, a já si s ní zaplatím počítačovou hru na telefon	**762**	19.5 %
založím si webové stránky s doménou, jako je česká firma u zahraničního registrátora (třeba s koncovkou .eu) a budu chtít po české firmě, aby si ji koupila	**1922**	49.3 %
kamarádka (14 let) mi pošle svojí fotku, na které se nahá sprchuje	**1515**	38.9 %

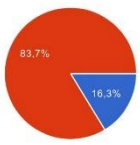
Uveď, zda jsi již danou věc zkoušel, nebo zda znáš nějakého svého vrstevníka, který to dělal

Rozesílal jsi spamové emailové zprávy, nebo sis nainstaloval program, který to dělá



Ano	**268**	6.9 %
Ne	**3630**	93.1 %

Rozesílal nějaký tvůj vrstevník spamové emailové zprávy, nebo si nainstaloval program, který to dělá?

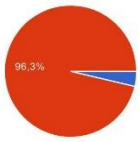


Ano	**635**	16.3 %
Ne	**3263**	83.7 %

Vytvořil jsi někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?

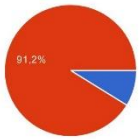
Ano	**145**	3.7 %

Ne **3753** 96.3 %



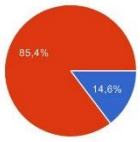
Vytvořil tvůj vrstevník někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?

Ano **343** 8.8 %
Ne **3555** 91.2 %



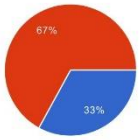
Připojoval jsi se bez dovolení na facebookový profil někoho jiného?

Ano **571** 14.6 %
Ne **3327** 85.4 %



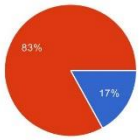
Připojoval se tvůj vrstevník se bez dovolení na facebookový profil někoho jiného?

Ano **1285** 33 %
Ne **2613** 67 %



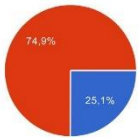
Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě?

Ano **661** 17 %
Ne **3237** 83 %



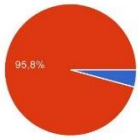
Použil tvůj vrstevník někdy program, který ti umožnil se přihlásit do cizí wifi sítě?

Ano **977** 25.1 %
Ne **2921** 74.9 %



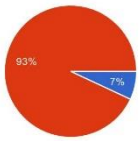
Zkoušel jsi odposlouchávat provoz v počítačové síti?

Ano **164** 4.2 %
Ne **3734** 95.8 %



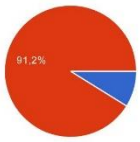
Zkoušel tvůj vrstevník odposlouchávat provoz v počítačové síti?

Ano **272** 7 %
Ne **3626** 93 %



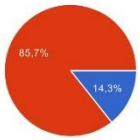
e?

Ano	**344**	8.8 %
Ne	**3554**	91.2 %



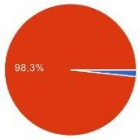
Přihlásil se tvůj vrstevník neoprávněně k cizí webové stránce

Ano	**558**	14.3 %
Ne	**3340**	85.7 %



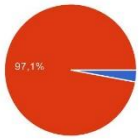
Přihlásil jsi se neoprávněně do cizího internetového bankovnictví?

Ano	**66**	1.7 %
Ne	**3832**	98.3 %



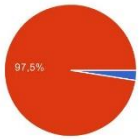
Přihlásil se tvůj vrstevník neoprávněně do cizího internetového bankovnictví?

Ano	**112**	2.9 %
Ne	**3786**	97.1 %



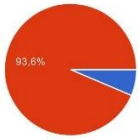
Použil jsi bez svolení cizí platební kartu na internetu?

Ano	**96**	2.5 %
Ne	**3802**	97.5 %



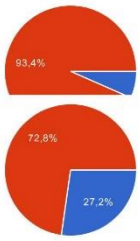
Použil tvůj vrstevník bez svolení cizí platební kartu na internetu?

Ano	**248**	6.4 %
Ne	**3650**	93.6 %



Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)?

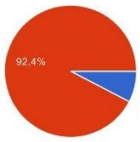
Ano	**258**	6.6 %
Ne	**3640**	93.4 %



oby mladší 15 let (svoje nebo i cizí)?

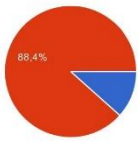
Ano	**1061**	27.2 %
Ne	**2837**	72.8 %

Zkusil jsi někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků?



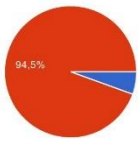
Ano	**298**	7.6 %
Ne	**3600**	92.4 %

Zkusil tvůj vrstevník někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků?



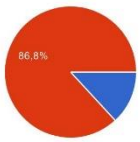
Ano	**452**	11.6 %
Ne	**3446**	88.4 %

Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program?



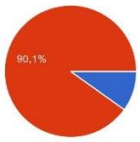
Ano	**215**	5.5 %
Ne	**3683**	94.5 %

Poslal tvůj vrstevník někomu schválně počítačový vir nebo jiný škodlivý program?



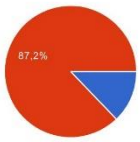
Ano	**513**	13.2 %
Ne	**3385**	86.8 %

Pozměnil jsi bez oprávnění nějaký počítačový program?



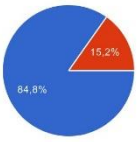
Ano	**386**	9.9 %
Ne	**3512**	90.1 %

Pozměnil tvůj vrstevník bez oprávnění nějaký počítačový program?



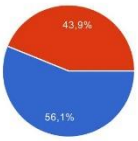
Ano	**499**	12.8 %
Ne	**3399**	87.2 %

Stahuješ si hudbu z internetu?



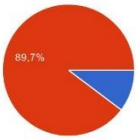
Ano	**3306**	84.8 %
Ne	**592**	15.2 %

Stahuješ si videa z internetu?



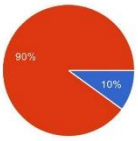
Ano	**2187**	56.1 %
Ne	**1711**	43.9 %

Nahráváš staženou hudbu na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?



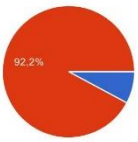
Ano	**401**	10.3 %
Ne	**3497**	89.7 %

Nahráváš stažená videa na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?



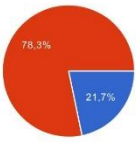
Ano	**389**	10 %
Ne	**3509**	90 %

Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?



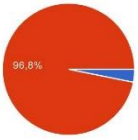
Ano	**305**	7.8 %
Ne	**3593**	92.2 %

Psal tvůj vrstevník na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?



Ano	**846**	21.7 %
Ne	**3052**	78.3 %

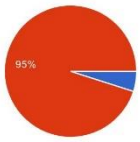
Poslal jsi někdy přes internet zprávu, že je někde bomba?



Ano	**124**	3.2 %
Ne	**3774**	96.8 %

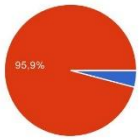
Poslal tvůj vrstevník někdy přes internet zprávu, že je někde bomba?

Ano **193** 5 %
Ne **3705** 95 %



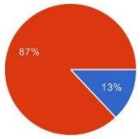
Požadoval jsi prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)?

Ano **161** 4.1 %
Ne **3737** 95.9 %



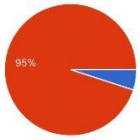
Požadoval tvůj vrstevník prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)?

Ano **506** 13 %
Ne **3392** 87 %



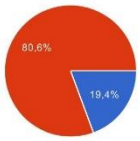
Šikanoval jsi někoho přes internet nebo na sociálních sítích?

Ano **192** 5 %
Ne **3655** 95 %



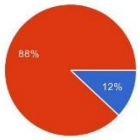
Šikanoval tvůj vrstevník někdo přes internet nebo na sociálních sítích?

Ano **755** 19.4 %
Ne **3143** 80.6 %



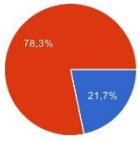
Psal sis na internetu nebo sociálních sítích komunikaci s erotickým obsahem?

Ano **467** 12 %
Ne **3431** 88 %



Psal tvůj vrstevník na internetu nebo sociálních sítích komunikaci s erotickým obsahem?

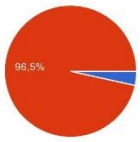
Ano **847** 21.7 %
Ne **3051** 78.3 %



Zkoušel jsi použít na internetu kódy platebních karet cizí osoby?

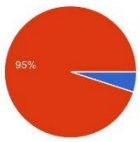
Ano **135** 3.5 %

Ne **3763** 96.5 %



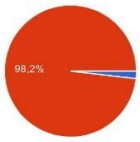
Zkoušel tvůj vrstevník použít na internetu kódy platebních karet cizí osoby?

Ano **193** 5 %
Ne **3705** 95 %



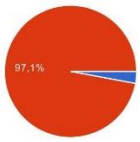
Stahoval sis z internetu kódy platebních karet cizí osoby?

Ano **72** 1.8 %
Ne **3826** 98.2 %



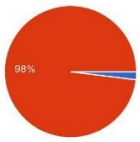
Stahoval si tvůj vrstevník z internetu kódy platebních karet cizí osoby?

Ano **114** 2.9 %
Ne **3784** 97.1 %



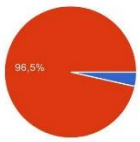
Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí?

Ano **77** 2 %
Ne **3821** 98 %



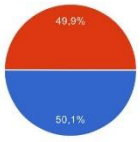
Použil tvůj vrstevník internetové bankovnictví cizí osoby bez jejího vědomí?

Ano **138** 3.5 %
Ne **3760** 96.5 %



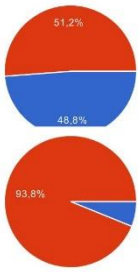
Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, než skutečné?

Ano **1951** 50.1 %
Ne **1947** 49.9 %



Udělal si tvůj vrstevník registraci na internetu, kde uvedl jiné údaje, než skutečné?

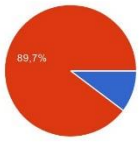
Ano **1901** 48.8 %
Ne **1997** 51.2 %



skutečné?

Ano	**240**	6.2 %
Ne	**3658**	93.8 %

Objednal si tvůj vrstevník na internetu zboží na jiné údaje než skutečné?



Ano	**401**	10.3 %
Ne	**3497**	89.7 %

Děkuji za spolupráci a pečlivé vyplnění.

Počet odpovědí za den

Příloha 9

Vážená paní, vážený pane.

Děkuji Vám za účast na prováděném dotazníkovém šetření. Z několika škol se mi ozvali kantoři, že by rádi otázky ještě jednou probrali s žáky a mohli jim sdělit, o jaké trestné činy by mohlo daným jednáním jít. Nejedná se o dogmatické rozdělení, při určení trestnosti daného skutku se posuzují další okolnosti, například společenská nebezpečnost činu, způsobená škoda, úmysl a podobně.

V návaznosti na dotazník Vám zasílám stručně okomentované otázky z dotazníku, abyste je mohli probrat s žáky. Otázky jsem pro přehlednost označil barevně:

není trestné
trestné za určitých podmínek
trestné

Snad Vám daný komentář bude užitečný, V případě dotazů mne klidně kontaktujte na emailu uvedeném u dotazníků.

S pozdravem

kpt. Mgr. Tomáš Daňhelka

Okomentované otázky:

stáhnu si počítačovou hru z internetu – záleží na tom, zda se jedná o volně stažitelnou verzi hry nebo pirátskou verzi, užívání pirátské verze je trestné, porušování autorského zákona

přijdu k počítači ve škole, je otevřený prohlížeč, a když dám zpět, tak se mi otevře spolužákův facebook. Když už jsem na jeho facebooku, tak si ho prohlédnu – trestné, neoprávněný přístup k počítačovému systému. Pokud by se mi to stalo omylem a hned se odhlásím, tak to ještě není trestné. Pokud si ho ale již prohlížím, tak jednám úmyslně a jednání je trestné.

nahraju kamarádovi bez jeho vědomí do počítače volně stažitelný program, abych se mohl dívat, co na počítači dělá - trestné ,neoprávněný přístup k počítačovému systému.

nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy – trestné, pokud se nejedná o volně šiřitelné filmy.

vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele – trestné, neoprávněný přístup k počítačovému systému, případně neoprávněné opatření, padělání a pozměnění platebního prostředku.

mám hodně stažených filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami – trestné, pokud se nejedná o volně šiřitelné filmy.

použiju heslo a uživatelské jméno jiného uživatele, které mi poslali webové stránky, které napodobují vzhled facebooku – trestné. Neoprávněný přístup k počítačovému systému.

nahraju na internet do diskuzního fóra cracky k počítačovým hrám ke stažení – trestné, porušování autorských práv, pokud se nejedná o volně šiřitelné hry.

náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil ve škole – trestné, neoprávněný přístup k počítačovému systému.

stáhnu si písničku z internetu a pouštím si ji – není trestné. Nahrávání již je. Stahování pirátských kopií celých alb již trestné bude, ale jednalo by se spíše o správní delikt.

zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená – trestné, neoprávněný přístup k počítačovému systému.

náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo do jeho facebooku, použiju ho a podívám se na jeho facebook – trestné. Neoprávněný přístup k počítačovému systému.

nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu – trestné, pokud se nejedná o volně šiřitelné filmy či programy. Porušení autorských práv.

nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačová hře – trestné, pokud se nejedná o volně šiřitelné hry. porušování autorských práv.

počítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokoval – trestné, ten, autor počítačového viru se dopouští neoprávněného přístupu k počítačovému systému a vydírání.

zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj – trestné, neoprávněný přístup k počítačovému systému.

náhodou uvidím, jaké rodiče mají uživatelské jméno a heslo na internetová bankovnictví a podívám se na jejich účet – trestné, neoprávněný přístup k počítačovému systému.

dám na svůj facebook zprávu, že učitelka je pitomá – není trestné, nemorální.

přijdu k počítači, uvidím, že se kamarád neodhlásil z facebooku, tak mu něco napíšu na jeho facebook – trestné, neoprávněný přístup k počítačovému systému.

na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské, a zkusím se přihlásit za ni, abych se podíval, co tam může zadávat – trestné, neoprávněný přístup k počítačovému systému.

stahuji si z internetu programy pro crackování her – trestné, porušování autorských práv, pokud se nejedná o hry, které vlastním. Samotné stažení ještě trestné není, užití či šíření již je.

na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské a zkusím se přihlásit za ni a přepíšu nějaké známky – trestné, neoprávněný přístup k počítačovému systému.

vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo – trestné, podvod, neoprávněný přístup k počítačovému systému, případně neoprávněné opatření , padělání a pozměnění platebního prostředku.

udělám si doma sbírku cracků k programům nebo hrám – trestné, pokud se nejedná o moje hry, autorská práva.

napíšu program, který umí odemknout nelegálně stažené windows – trestné, porušování autorských práv, případně Opatření a přechovávání přístupového zařízení a hesla k počítačovému sysému a jiných takových dat.

někdo vytvořil počítačoví vir, který jsem si omylem stáhnul do počítače – autor viru se dopustil trestného činu Neoprávněný přístup k počítačovému systému, případně Opatření a přechovávání přístupového zařízení a hesla k počítačovému sysému a jiných takových dat.

stáhnu si z internetu volně dostupný kód počítačového viru a pošlu ho z legrace kamarádovi – trestné Neoprávněný přístup k počítačovému systému, případně Opatření a přechovávání přístupového zařízení a hesla k počítačovému sysému a jiných takových dat.

na kamarádovu zeď na facebooku napíši nějakou nadávku – není trestné, nemorální.

použiju volně dostupný program, který mi zjistí heslo do cizí wifi sítě – trestné, Neoprávněný přístup k počítačovému systému, případně Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

nahraju na internet program, který umí odemknout zkušební verzi windows, aby šla používat pořád – trestné, porušení autorských práv, případně Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v nějaké trapné situaci – není trestné. Může být v rozporu s ochranou osobnostních práv.

dám na svůj facebook zprávu, že by měli jít cikáni do plynu – trestné, podněcování rasové nesnášenlivosti.

spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat na sociálních sítích zprávy, že je fakt strašný a měl by se raději zabít – záleží na závažnosti, může být trestné, účast na sebevraždě.

použiju volně dostupný program, který zablokuje provoz nějaké webové stránky svými stálými dotazy – může být trestné, dle napadených stránek například obecné ohrožení, pokud se jedná o kriticky důležitou infrastrukturu.

změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni – trestné, porušování autorských práv.

nahraju na wikipedii článek o tom, jak je škola pitomá – není trestné.

zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky – trestné, neoprávněný přístup k počítačovému systému.

dám na facebookovou zeď kamaráda zprávu, že by měli být uprchlíci nahnáni zpět do moře – trestné, podněcování rasové nesnášenlivosti.

náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu jeho zprávy a místo nich dám odkazy na porno – trestné, neoprávněný přístup k počítačovému systému, může být ohrožování mravní výchovy, pokud se jedná o stránky, kam mají přístup děti.

použiju volně stažitelný program, který mi ve školní síti zjistí, kdo si co píše na chatu – trestné, neoprávněný přístup k počítačovému systému, Porušování tajemství dopravované zprávy, případně Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

použiju volně stažitelný program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě – trestné, neoprávněný přístup k počítačovému systému, případně Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

pošlu své kamarádce (14 let) svojí fotku ve spodním prádle – není trestné, pokud se nejedná o erotické pózy.

na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačová hry – trestné, neoprávněné opatření, padělání a pozměnění platebního prostředku.

pošlu spolužákovi zprávu, že si na něj před školou počkáme a že do stane pěstí – není trestné, pokud to opravdu neuskutečníme.

přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky, místo skutečností – není trestné.

píši si na internetu s dospělým člověkem – není trestné, ale může být nebezpečné.

pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý – trestné, zvláště pokud jsou na fotce zobrazeny detailně pohlavní orgány, případně v erotické pozici.

napíšu svá kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslala, zveřejním ve škole - trestné, vydírání, případně sexuální nátlak.

založím si webové stránky s doménou, která je stejná jako slavná zahraniční značka a umístím si na ně svůj vlastní obsah –porušování práv ke značce, spíše jako správní delikt, případně zde hrozí občansko-správní žaloba.

registruji si doménu se jménem nového výrobku dříve, než výrobce a budu mu jí nabízet na prodej. Když si ji nechce koupit, dám si na ní svůj obsah - trestné, porušování práv ke značce, případně vydírání.

staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout – trestné, porušování autorských práv, pokud se nejedná o volně šiřitelnou skladbu.

kamarádka (14 let) mi pošle svo jí fotku ve spodním prádle - legální, může být trestné v případě erotických pozicí.

pošlu email na policii, že na letišti je bomba – trestné, šíření poplašné zprávy.

nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru – není trestné, jedná se o porušení školního řádu.

rodiče mi dají svoje číslo platební karty, abych ji mohl používat, a já si s ní zaplatím počítačovou hru na telefon - není trestné

založím si webová stránky s doménou, jako je česká firma u zahraničního registrátora (třeba s koncovkou .eu) a budu chtít po české firmě, aby si ji koupila – trestné vydírání.

kamarádka (14 let) mi pošle svojí fotku, na které se nahá sprchuje – trestné, pokud fotografie zabírá pohlavní orgány, rozhodně nebezpečné.

část s výběrem

Rozesílal jsi spamové emailové zprávy, nebo sis nainstaloval program, který to dělá? – příklad šíření spamu. Trestnost záleží na obsahu šíření zprávy.

Vytvořil jsi někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje? – podvod, případně další trestné činy podle toho, jaké údaje stránka shromažďuje. Příklad phishingu.

Připojoval ses bez dovolení na facebookový profil někoho jiného? – neoprávněný přístup k počítačovému systému. Často bývá součástí phishingových útoků šířených přes facebook.

Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě? – neoprávněný přístup k počítačovému systému, případně opatření a přechovávání přístupového zařízení a hesla k počítačovému systému.

Zkoušel jsi odposlouchávat provoz v počítačové síti? - neoprávněný přístup k počítačovému systému, případně opatření a přechovávání přístupového zařízení a hesla k počítačovému systému.

Přihlásil ses neoprávněně k cizí webové stránce? – neoprávněný přístup k počítačovému systému.

Přihlásil ses neoprávněně do cizího internetového bankovnictví? – neoprávněný přístup k počítačovému systému, případně neoprávněné opatření, padělání a pozměnění platebního prostředku.

Použil jsi bez svolení cizí platební kartu na internetu? - neoprávněné opatření, padělání a pozměnění platebního prostředku.

Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)? – Výroba a jiné nakládání s dětskou pornografií.

Zkusil jsi někdy zahltit něčí počítačovou síť nebo webovou stránku odesíláním velkého množství požadavků? – neoprávněný přístup k počítačovému systému, obecné ohrožení.

Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program? – neoprávněný přístup k počítačovému systému, případně pokus k danému jednání, pokud není virus spuštěn.

Pozměnil jsi bez oprávnění nějaký počítačový program? – porušování autorských práv.

Stahuješ si hudbu z internetu? – porušování autorských práv.

Stahuješ si videa z internetu? – pro vlastní účely legální, pokud je zároveň nešíříš, například používáním P2P sítí, torrentů. V případě pouhého sledování stažených filmů se bude jednat spíše o správní delikt (přestupek). Šíření chráněných filmů už trestné je, pokud se nejedná volně šiřitelné filmy.

Nahráváš staženou hudbu na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout? – porušování autorských práv.

Nahráváš stažená videa na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout? – porušování autorských práv.

Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťané, apod.)? – podněcování nenávisti.

Poslal jsi někdy přes internet zprávu, že je někde bomba? – šíření poplašné zprávy.

Požadoval jsi prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)? – vydírání, pokud by pachatel požadoval erotické fotografie, tak i sexuální útisk.

Šikanoval jsi někoho přes internet nebo na sociálních sítích? – nemorální, kyberšikana.

Psal sis na internetu nebo sociálních sítích komunikaci s erotickým obsahem? – sexting, není trestné, ale může být nebezpečné.

Zkoušel jsi použít na internetu kódy platebních karet cizí osoby? – neoprávněné opatření, padělání a pozměnění platebního prostředku.

Stahoval sis z internetu kódy platebních karet cizí osoby? – neoprávněné opatření, padělání a pozměnění platebního prostředku.

Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí? – neoprávněné opatření, padělání a pozměnění platebního prostředku, podvod.

Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, než skutečné? – může se jednat o podvod, pokud vznikla škoda. Jedná se o porušení podmínek užívání služby, může dojít ke zrušení účtu provozovatelem služby. Časté na příklad s datem narození (např. facebook až od 13 let).

Objednal sis na internetu zboží na jiné údaje než skutečné? – může se jednat o podvod, pokud vznikla škoda.

Příloha 10

Příloha 10 - shrnuté výsledky z části výzkumu Označ, co je kyberkriminalita

kyberkriminalita je když:	Praha	Stč.
stáhnu si počítačovou hru z internetu	10,5	12,7
přijdu k počítači ve škole, je otevřený prohlížeč, a když dám zpět, tak se mi otevře spolužákův fac	48,4	44,8
nahraju kamarádovi bez jeho vědomí do počítače volně stažitelný program, abych se mohl dívat,	69,4	65,8
nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy	21	19,6
vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, a	80,2	69,7
mám hodně stažených filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nen	24,2	26,4
použiju heslo a uživatelské jméno jiného uživatele, které mi poslali webové stránky, které napod	67,3	58,7
nahraju na internet do diskuzního fóra cracky k počítačovým hrám ke stažení	33,5	32,2
náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil ve šk	55,2	49
stáhnu si písničku z internetu a pouštím si ji	3,6	10,5
zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená	57,3	54,4
náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo do jeho facebooku, použiju ho a	56,5	52,8
nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu	38,3	37,2
nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačová hře	32,7	29,2
počítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokova	41,5	40
zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj	42,7	41,5
náhodou uvidím, jaké rodiče mají uživatelské jméno a heslo na internetová bankovnictví a podíva	52	47
dám na svůj facebook zprávu, že učitelka je pitomá	25	29,4
přijdu k počítači, uvidím, že se kamarád neodhlásil z facebooku, tak mu něco napíšu na jeho face	54,8	51,8
na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské, a zkusím se přihlásit	52,4	52,9
stahuji si z internetu programy pro crackování her	33,9	33,7
na počítači ve škole uvidím, jaké má učitelka heslo do elektronické žákovské a zkusím se přihlásit	62,9	60,3
vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a	71	67
udělám si doma sbírku cracků k programům nebo hrám	26,6	25,4
napíšu program, který umí odemknout nelegálně stažené windows	51,2	51
někdo vytvořil počítačoví vir, který jsem si omylem stáhnul do počítače	21,8	23,1
stáhnu si z internetu volně dostupný kód počítačového viru a pošlu ho z legrace kamarádovi	56	54,8
na kamarádovu zeď na facebooku napíši nějakou nadávku	38,7	40,8
použiju volně dostupný program, který mi zjistí heslo do cizí wifi sítě	48	41,6
nahraju na internet program, který umí odemknout zkušební verzi windows, aby šla používat po	36,7	37,9
na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v nějaké trapné situa	47,6	46,8
dám na svůj facebook zprávu, že by měli jít cikáni do plynu	40,7	43
spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat na sociá	59,3	61,4
použiju volně dostupný program, který zablokuje provoz nějaké webové stránky svými stálými d	47,6	43,6
změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni	42,7	39,5
nahraju na wikipedii článek o tom, jak je škola pitomá	23,4	26,4
zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky	33,5	32,2
dám na facebookovou zeď kamaráda zprávu, že by měli být uprchlíci nahnáni zpět do moře	42,7	41,5
náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu jeho zprávy a místo nich dám od	64,1	58,3
použiju volně stažitelný program, který mi ve školní síti zjistí, kdo si co píše na chatu	50	48,3
použiju volně stažitelný program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužá	51,6	46,1
pošlu své kamarádce (14 let) svojí fotku ve spodním prádle	23,4	26,9
na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačová h	52,8	53,1
pošlu spolužákovi zprávu, že si na něj před školou počkáme a že do stane pěstí	39,1	43,9
přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky, místo skutečností	35,1	33,7
píši si na internetu s dospělým člověkem	7,7	8,7
pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý	35,9	38,4
napíšu svá kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslala, zveřejním ve š	60,9	64,1
založím si webové stránky s doménou, která je stejná jako slavná zahraniční značka a umístím si	41,1	38,3
registruji si doménu se jménem nového výrobku dříve, než výrobce a budu mu jí nabízet na prod	43,5	37,8
staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout	18,1	20,8
kamarádka (14 let) mi pošle svo jí fotku ve spodním prádle	21,8	26,6
pošlu email na policii, že na letišti je bomba	66,1	66,4
nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru	36,3	38,2
rodiče mi dají svoje číslo platební karty, abych ji mohl používat, a já si s ní zaplatím počítačovou h	22,2	19,5
založím si webová stránky s doménou, jako je česká firma u zahraničního registrátora (třeba s ko	59,3	49,3
kamarádka (14 let) mi pošle svojí fotku, na které se nahá sprchuje	38,3	38,9


Název grafu
kamarádka (14 let) mi pošle svojí fotku, na které se nahá...
založím si webová stránky s doménou, jako je česká firma u...
rodiče mi dají svoje číslo platební karty, abych ji mohl používat,...
nainstaluji v rozporu se školním řádem do školního počítače...
pošlu email na policii, že na letišti je bomba
kamarádka (14 let) mi pošle svo jí fotku ve spodním prádle
staženou písničku si nahraju na svůj blog, aby si ji ostatní taky...
registruji si doménu se jménem nového výrobku dříve, než...
založím si webové stránky s doménou, která je stejná jako...
napíšu svá kamarádce, že když mi nepošle další fotku, tak tu,...
pošlu své kamarádce (14 let) svojí fotku ze sauny, kde jsem nahý
píši si na internetu s dospělým člověkem
přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím...
pošlu spolužákovi zprávu, že si na něj před školou počkáme a...
na internetu si stáhnu číslo kreditní karty a použiju ho na...
pošlu své kamarádce (14 let) svojí fotku ve spodním prádle
použiju volně stažitelný program, který mi ve školní síti zjistí...
použiju volně stažitelný program, který mi ve školní síti zjistí,...
náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu...
dám na facebookovou zeď kamaráda zprávu, že by měli být...
zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj...
nahraju na wikipedii článek o tom, jak je škola pitomá
změním pomocí cracku zakoupenou počítačovou hru, aby ji...
použiju volně dostupný program, který zablokuje provoz...
spolužák mne naštval, tak se na něj domluvím se spolužáky a...
dám na svůj facebook zprávu, že by měli jít cikáni do plynu
na kamarádovu zeď na facebooku umístím video, na kterém je...
nahraju na internet program, který umí odemknout zkušební...
použiju volně dostupný program, který mi zjistí heslo do cizí...
na kamarádovu zeď na facebooku napíši nějakou nadávku
stáhnu si z internetu volně dostupný kód počítačového viru a...
někdo vytvořil počítačoví vir, který jsem si omylem stáhnul do...
napíšu program, který umí odemknout nelegálně stažené...
udělám si doma sbírku cracků k programům nebo hrám
vytvořím a pošlu někomu email, který vypadá jako zpráva z...
na počítači ve škole uvidím, jaké má učitelka heslo do...
stahuji si z internetu programy pro crackování her
na počítači ve škole uvidím, jaké má učitelka heslo do...
přijdu k počítači, uvidím, že se kamarád neodhlásil z...
dám na svůj facebook zprávu, že učitelka je pitomá
náhodou uvidím, jaké rodiče mají uživatelské jméno a heslo na...
zkusím odhadnout heslo, které má kamarád na facebooku a...
počítačový virus zablokuje počítač a musím někam poslat...
nahrávám na svůj blog odkazy, odkud si mohou stáhnout...
nabízím na internetu za nabití kreditu zaslání staženého filmu...
náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo...
zkusím se připojit jako administrátor do školní sítě, abych viděl,...
stáhnu si písničku z internetu a pouštím si ji
náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo...
nahraju na internet do diskuzního fóra cracky k počítačovým...
použiju heslo a uživatelské jméno jiného uživatele, které mi...
mám hodně stažených filmů, tak je nahraju na server, aby si je...
vytvořím webové stránky, které vypadají jako přihlašovací...
nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat...
nahraju kamarádovi bez jeho vědomí do počítače volně...
přijdu k počítači ve škole, je otevřený prohlížeč, a když dám...
stáhnu si počítačovou hru z internetu
0
10
20
30
40
50
60
70
80
90
Stč.
Praha

Příloha 11

Příloha 11 – shrnuté výsledky z části výzkumu Zkušenost s kyberkriminalitou

část s výběrem, odpověď ano vrstevník	Praha	Stč.
Přihlásil ses neoprávněně do cizího internetového bankov	2,4	2,9
Stahoval sis z internetu kódy platebních karet cizí osoby?	2	2,9
Použil jsi internetové bankovnictví cizí osoby bez jejího vě	4,4	3,5
Poslal jsi někdy přes internet zprávu, že je někde bomba?	5,2	5
Zkoušel jsi použít na internetu kódy platebních karet cizí o	6	5
Použil jsi bez svolení cizí platební kartu na internetu?	6	6,4
Zkoušel jsi odposlouchávat provoz v počítačové síti?	5,6	7
Vytvořil jsi někdy webovou stránku, která se snaží vypadat	6,5	8,8
Nahráváš stažená videa na internet, nebo tam nahráváš o	8,9	10
Nahráváš staženou hudbu na internet, nebo tam nahráváš	11,7	10,3
Objednal sis na internetu zboží na jiné údaje než skutečné	10,1	10,3
Zkusil jsi někdy zahltit něčí počítačovou síť nebo webovou	8,5	11,6
Pozměnil jsi bez oprávnění nějaký počítačový program?	13,7	12,8
Požadoval jsi prostřednictvím internetu, nebo sociálních s	8,1	13
Poslal jsi někomu schválně počítačový vir nebo jiný škodliv	12,9	13,2
Přihlásil ses neoprávněně k cizí webové stránce?	11,7	14,3
Rozesílal jsi spamové emailové zprávy, nebo sis nainstalov	14,9	16,3
Šikanoval jsi někoho přes internet nebo na sociálních sítích	23,4	19,4
Psal jsi na internet nějaké nenávistné příspěvky proti nějak	16,1	21,7
Psal sis na internetu nebo sociálních sítích komunikaci s en	25	21,7
Použil jsi někdy program, který ti umožnil se přihlásit do ci	21,4	25,1
Posílal jsi někomu nahé fotografie osoby mladší 15 let (svo	25	27,2
Připojoval ses bez dovolení na facebookový profil někoho	29,4	33
Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, n	48	48,8
Stahuješ si videa z internetu?	58,1	56,1
Stahuješ si hudbu z internetu?	81,5	84,8


zkušenost s daným jednáním
Stahuješ si hudbu z internetu?
Stahuješ si videa z internetu?
Udělal sis registraci na internetu, kde jsi uvedl...
Připojoval ses bez dovolení na facebookový...
Posílal jsi někomu nahé fotografie osoby...
Použil jsi někdy program, který ti umožnil se...
Psal sis na internetu nebo sociálních sítích...
Psal jsi na internet nějaké nenávistné příspěvky...
Šikanoval jsi někoho přes internet nebo na...
Rozesílal jsi spamové emailové zprávy, nebo sis...
Přihlásil ses neoprávněně k cizí webové stránce?
Poslal jsi někomu schválně počítačový vir nebo...
Požadoval jsi prostřednictvím internetu, nebo...
Pozměnil jsi bez oprávnění nějaký počítačový...
Zkusil jsi někdy zahltit něčí počítačovou síť...
Objednal sis na internetu zboží na jiné údaje...
Nahráváš staženou hudbu na internet, nebo...
Nahráváš stažená videa na internet, nebo tam...
Vytvořil jsi někdy webovou stránku, která se...
Zkoušel jsi odposlouchávat provoz v počítačové...
Použil jsi bez svolení cizí platební kartu na...
Zkoušel jsi použít na internetu kódy platebních...
Poslal jsi někdy přes internet zprávu, že je...
Použil jsi internetové bankovnictví cizí osoby...
Stahoval sis z internetu kódy platebních karet...
Přihlásil ses neoprávněně do cizího...
0 10 20 30 40 50 60 70 80 90
Stč.
Praha