Kybernetická kriminalita

Luboš Pernica

Bakalářská práce
2017/2018

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Luboš Pernica**
Osobní číslo:	**L15201**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Kybernetická kriminalita**

Zásady pro vypracování:

1. **Zpracujte analýzu informačních zdrojů.**
2. **Zpracujte současný stav řešení zadané problematiky.**
3. **Systémově vyjádřete model kybernetické kriminality.**
4. **Zpracujte výsledky modelování a navrhněte návrhy pro praxi.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[2] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[3] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-589-0.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**prof. Ing. Jiří Dvořák, DrSc.** Ústav krizového řízení
Datum zadání bakalářské práce:	**3. listopadu 2017**
Termín odevzdání bakalářské práce:	**15. května 2018**

V Uherském Hradišti dne 15. listopadu 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ / ~~DIPLOMOVÉ~~ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/~~diplomové~~ práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1)];
- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou/diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou/diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské/diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské/diplomové práce využít ke komerčním účelům;
- pokud je výstupem bakalářské/diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se bakalářská práce skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské/diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské/diplomová práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti 3.5.2018

podpis studenta

---

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich částí, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou

zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.

2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Moje bakalářská práce se zabývá problematikou týkající se kybernetické kriminality. V teoretické části práce analyzuji informační zdroje, uvádím právní aspekty kybernetické kriminality a tuto rozděluji dle druhů. Závěrem teoretické části se poté zabývám mezinárodními a národními dokumenty, sloužící k boji proti kybernetické kriminalitě. Praktická část je zaměřená na model kybernetické kriminality, statistiku a dotazníkový průzkum včetně analýzy rizika. Závěrečná část praktické části, je věnována konkrétním příkladům kybernetické kriminality, metodám řešení a způsobům prevence.

Klíčová slova: kybernetická kriminalita, oběť, trestný čin, útočník, prevence

ABSTRACT

My bachelor thesis deals with issues related to cyber crime. In the theoretical part of the thesis I analyze information sources, introduce legal aspects of cybercrime and divide them according the types. In the conclusion of the theoretical part, I deal with international and national documents to combat cybercrime. The practical part is focused on the model of cyber crime, statistics and questionnaire survey including risk analysis. The final part of the practical part is devoted to specific examples of cyber crime, methods of solving and means of prevention.

Keywords: cyber crime, victim, crime, attacker, prevention

Tímto děkuji mému vedoucímu bakalářské práce prof. Ing. Jiřímu Dvořákovi, DrSc. za odborné vedení, užitečné připomínky a poznatky při zpracovávání mé bakalářské práce. Dále děkuji kpt. Bc. Jiřímu Sopouškovi za poskytnutí materiálů a odborných konzultací.

OBSAH

ÚVOD

Devatenácté století bývá zcela oprávněně označováno za věk páry. Dvacáté století přineslo další dynamický rozvoj vědomostí a průmyslového potenciálu lidstva. Na sklonku druhé světové války jsme vstoupili do atomového věku a současně došlo k nástupu počítačových technologií. Původně velmi nákladné přístroje výpočetní techniky se začaly masově rozšiřovat. Od sklonku milénia jsme svědky masového rozšíření mobilních telefonů. Přístroje, které byly původně velikosti diplomatického kufříku a byly symbolem vysokého sociálního postavení ve společnosti, jsou v současnosti celosvětově rozšířeny, a to i v oblastech, které jinak pokládáme za rozvojové. Rozšířila se i funkce mobilních telefonů, původně nahrazujících pevné telefonní spojení s bonusem posílání SMS. Obdobně jako u počítačů i u mobilních telefonů způsobil doslova revoluci nástup Internetu. Počítače postupem času, byly dostupnější širší veřejnosti a i mobilní technika se stávala stále dostupnější.

V současné době se dá říci, že kdo není na síti, jako by nebyl. Stačí se podívat po okolí a prakticky každý má v ruce mobilní telefon nebo tablet a komunikuje nebo je alespoň připojen k síti internet. Toto se zdaleka netýká jen mladé generace, dětí a studentů, ale tento trend je patrný napříč celou populací. Vývoj je znát na každém kroku a již si nedovedeme představit práci či studium bez použití výpočetní, komunikační techniky a internetové sítě, protože tyto technologie nám práci velice usnadňují a urychlují.

Právě to, že téměř vše je připojeno a prakticky každý má Internet ať již přes mobilní síť, wifi síť či prostřednictvím kabelu, tak tato realita je živnou půdou pro kybernetické zločince, protože tito mají veliké množství potenciálních obětí. A právě kybernetická kriminalita je v současné době na vzestupu a to díky tomu, že spousta uživatelů si vůbec neuvědomuje rizika, která jsou skryta v kybernetickém prostoru.

I. TEORETICKÁ ČÁST

1 HISTORIE VZNIKU KYBERPROSTORU

K prvnímu síťovému propojení mezi počítači došlo v roce 1968. Jednalo se o propojení mezi čtyřmi univerzitními počítači v různých částech USA. Nikdo ovšem nepředpokládal tak obrovský rozvoj v oblasti síťových technologií. A už vůbec ne síť, která bude propojovat milióny stanic napříč celým světem. Toto byl počátek vzniku sítě Arpanet.

Vzhledem k tomu, že se nepředpokládal tak obrovský rozmach síťové komunikace, tak ani nebyl kladen takový důraz na bezpečnost jako dnes.[1]

1.1 Protokoly TCP/IP

Počátkem 70. let se ovšem do sítě Arpanet v akademickém prostředí začaly připojovat desítky univerzit a dalších úřadů napříč celými Spojenými státy. V roce 1973 se do sítě připojily i dvě evropské instituce: Norský seismologický ústav Norsar a University College London.

Na stejných principech jako síť Arpanet byly založeny např. síť na Havaji Alohanet nebo Cyckaldes ve Francii. Tyto sítě však mezi sebou nemohly komunikovat, byť byly založeny na stejných principech.

V roce 1973 začali Bob Kahn a Vint Cerf pracovat na technologiích, které by sjednotily protokoly v paketových sítích jejich rozhraní s koncovými počítači a datové objekty, jež jsou vyměňované v těchto sítích.

Protokoly TCP/IP umožnily propojení geograficky vzdálených a přitom technologicky různorodých sítí. Díky tomuto propojení sítí vznikla síť sítí Internet.[2]

1.2 Word Wide Web

Počátkem 90. let dvacátého století bránilo masivnímu rozvoji Internetu mezi populaci několik věcí. Internet byl v té době stále oficiálně určen pro akademickou komunitu.

---

[1] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*.

[2] *Jak na internet* [online]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/.

K legislativním změnám, které by umožnily komerční využití Internetu, došlo v roce 1991 v USA a následně i ve zbytku světa.

Druhým problémem byly aplikace. Šlo o programy, které byly pro veřejnost těžko použitelné a přesto, že se v počítačích začala již používat grafická rozhraní, byly tyto programy pouze v textové podobě.

Opravdovou revolucí v rozšíření Internetu, byl vznik WWW (World Wide Web). K jeho vzniku došlo v Ženevském centru jaderného výzkumu a dále byl přidán komunikační protokol HTTP (Hyper-Text Transfer Protocol).

Dalším předpokladem ke globálnímu rozmachu Internetu bylo dokončení vývoje prvního grafického klienta s názvem Mosaic, který nesl znaky dnešních moderních prohlížečů. Mosaic byl volně dostupný pro prakticky všechny počítačové platformy, a proto došlo k masovému rozšíření Internetu mezi uživatele.[3]

1.3 Počátky českého Internetu

K oficiálnímu spuštění Internetu v českém prostředí došlo 13.2.1992 na pražském ČVUT. Jednalo se o jednu mezinárodní linku, která spojovala Prahu a Linz. Již v průběhu roku 1991 byl podán návrh k vybudování celorepublikové sítě. Tato síť měla propojovat všechna tuzemská akademická centra. V červnu roku 1992 uvolnilo na projekt Ministerstvo školství 20 miliónů korun. Původní síť s názvem FESNET se v průběhu roku 1992 přejmenovala na Cesnet.[4]

1.4 Internetový rozvoj v českých zemích

Před rokem 1995 o Internetu v naší zemi věděl jen málokdo. Toto se začíná měnit přelomem let 1995 a 1996, kdy na trh vstupuje celá řada komerčních internetových poskytovatelů. Republika byla v této době již k Internetu připojena třetím rokem, ale vzhledem k monopolu firmy Eurotel, který se vztahoval mimo jiné i na veřejné služby, nebylo umož-

[3] *Jak na internet* [online]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/.
[4] *Historie Internetu v České republice* [online]. Dostupné z:https://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm.

něno dřívější připojení k síti Internet. Po pádu tohoto monopolu na sklonku roku 1995 se naskytla možnost využití Internetu v komerční sféře, kdy následoval jeho rozmach.[5]

1.5 Kybernetický prostor

Abychom mohli hovořit o kybernetické kriminalitě, je velice důležité definovat kybernetický prostor.

V současné době existuje více než 28 definic kyberprostoru, avšak vědci ani vlády se nemohou shodnout na přesném znění.

Dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti se kybernetickým prostorem dle § 2 písm. a) v tomto zákoně rozumí kybernetickým prostorem "*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*"[6]

První úvaha o kyberprostoru se nachází v knize Williama Gibsona - Neuromancer, která vyšla v roce 1984, a zmiňuje se o ní Václav Jirovský ve své knize takto: "*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města ..*"[7]

Člověku by se mohlo by se zdát, že kybernetickým prostorem je pouze svět Internetu, ale toto je poněkud mylná představa. V dnešní době pracuje pomocí různých systémů, kde se používá moderní technika, prakticky vše. Člověk ani nemusí být připojen k internetové síti, a přesto je v nebezpečí. Ovšem zneužití takových systémů je trochu složitější a zůstává otázkou: Vyplatí se to pachateli?

V každém případě je důležité být při práci v kybernetickém prostoru opatrný a nepodlehnout falešné iluzi bezpečí.

---

[5] *Historie Internetu v České republice* [online]. Dostupné z:https://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm.

[6] *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014

[7] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*.

1.6 Psychika jednotlivce v kybernetickém prostoru

S rozvojem různých technologií a zejména pak Internetu je vytvářena spousta prostoru pro vlastní realizaci jedinců a jejich socializaci. V případě, že se tito jedinci pohybují v kybernetickém prostoru, je samozřejmě ovlivňována jejich psychika, sociální zvyklosti a přístup k různým hodnotám. Rozmanitost nových druhů pocitů, které zakouší tito uživatelé po zapnutí počítače a připojení se k síti, je psychology přirovnávána ke známým pocitům a zkušenostem ze skutečného světa např. prohlížení webovských stránek přirovnávají k pocitům, jaké lidé zažívají při cestování. Pokud tráví čas na různých chatových serverech, může jim to nahrazovat pobyt ve společnosti. Zde jim totiž nic nehrozí. Můžou měnit svůj věk, pohlaví a uskutečňovat svoje vlastní představy o sobě. Zde je vidět, že vliv technologií na současnou společnost je nesporný. Nesporný dopad mají i tyto technologie na psychiku jedince. Tyto nové zkušenosti z kybernetického prostoru se potom mohou promítat do reálného života. Moderní sociologie a psychologie se těmito jevy začínají zabývat avšak k uceleným závěrům je ještě daleko. Toto je problém především u dětí, jejichž psychika ještě není dostatečně vyzrálá na to, aby mohla rozlišovat, co je ještě v pořádku a co je už za hranou. Tato dětská psychika je velice ovlivňována různými videi, která jsou prezentována na Internetu. Děti potom mohou mít touhu tyto videa napodobovat a tento způsob zábavy může mít nedozírné následky. [8]

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

2 KYBERNETICKÁ KRIMINALITA

Dle vlastních praktických zkušeností a policejních statistik je kybernetická kriminalita na vzestupu a toto je vidět i na počtu přijatých oznámení na Policii ČR. Tento trend má vzrůstající tendenci zejména proto, že se informační technologie staly dostupnými téměř pro každého. A v současné době si nedovedeme představit bez pomoci informačních technologii běžnou práci, jež se nám díky nim velice usnadnila a zrychlila. Pokud se podíváme kolem sebe, tak velký počet uživatelů je připojených v síti a komunikuje. Díky tomuto trendu roste i četnost zneužívání těchto systémů k páchání trestné činnosti.

2.1 Analýza informačních zdrojů

Kybernetické kriminalitě a bezpečnosti je v současné době věnována veliká pozornost jak u nás, tak i ve světě. Touto problematikou se zabývají vlády i soukromé společnosti. Pořádají se kurzy, semináře, školení. Je prováděna osvěta jak mezi seniory, dospělými, tak i dětmi formou různých besed, sezení, jak na teoretické bázi, tak i formou praktických ukázek a školení.

Kybernetickou kriminalitou a vůbec kyberprostorem se také zabývá velká spousta různých knih, časopisů, periodik a www stránek na tuto problematiku zaměřených. Dále se pořádají různé semináře, na kterých přednáší odborníci na kybernetickou kriminalitu.

Policie např. pořádala seminář na téma "Kyberšikana". Tento proběhl 1. 11. 2017 v Břeclavi ve spolupráci s Břeclavskou městskou policií a Pedagogicko - psychologickou poradnou Břeclav. Hlavním cílem semináře bylo nastínit, jaká nebezpečí mohou na děti číhat v kybernetickém prostoru.[9]

Dále probíhají různé přednášky na vysokých, středních i základních školách. Například v březnu 2017 byla přednáška "Kybernetická bezpečnost vs Kybernetická kriminalita", tato byla uspořádána gymnáziu Příbor.[10]

---

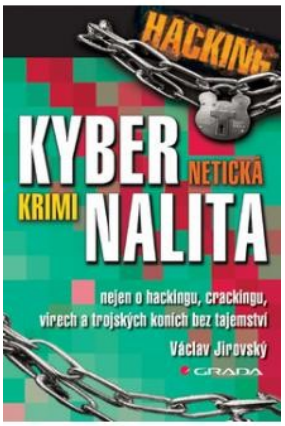
[9] *NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost* [online]. Dostupné z: www.govcert.cz/cs/vzdelavani/skoleni-seminare-a-konference/

[10] *NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost* [online]. Dostupné z: www.govcert.cz/cs/vzdelavani/skoleni-seminare-a-konference/

Další velice zajímavá dvoudenní konference proběhla v Brně ve dnech 20. - 21. 9. 2017 CYBERCON BRNO 2017, kde se probíraly témata jako např. kyberprostor jako nástroj hybridního válčení, pokročilé způsoby detekce kybernetických hrozeb, kybernetická kriminalita a její vyšetřování.[11]

Ve své bakalářské práci jsem použil i zahraniční zdroj Josefa Požára o trendech kybernetické kriminality, který publikoval v časopise Acta Informatica Pragensia.

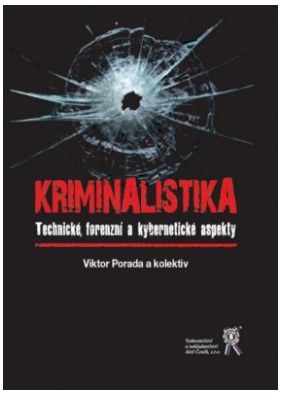
Velice cenným zdrojem jsou informace z knihy Václava Jirovského Kybernetická kriminalita, která čtenáře provede od samého vzniku kybernetického prostoru až po nebezpečí, která na uživatele číhají, kdy publikace je velmi podrobná.



Obrázek 1- Kybernetická kriminalita[12]

[11] *NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost* [online]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2543-cybercon-brno-2017-a-seminar-k-zkb/.
[12] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*.

Další cennou knihou je kniha Viktora Porady Kriminalistika: technické, forenzní a kybernetické aspekty, která se zabývá jak klasickou kriminalistikou, tak metodikou vyšetřování trestných činů, včetně metodiky vyšetřování kybernetických trestných činů.



Obrázek 2 - Kriminalistika[13]

Rovněž jsou pořádány semináře týkajících se kybernetické kriminality. Tyto jsou uskutečňovány za účasti předních odborníků z řad Policie ČR zabývajících se vyšetřováním kybernetických trestných činů, i počítačových odborníků z IT společností zabývajících se zabezpečením systémů.

Dalším velice cenným zdrojem informací je projekt E-Bezpečí. Jedná se o celorepublikový projekt zaměřený na prevenci, vzdělání, výzkum, intervenci a osvětu, která je spojena s rizikovým chováním na internetu a souvisejícími fenomény. Projekt se zaměřuje na nebezpečné internetové praktiky, jež ohrožují jak děti tak i dospělé.

Specializace projektu je zaměřena zejména na:

- kyberšikanu a sexting (jedná se o různé formy vydírání, vyhrožování, poškozování oběti pomocí komunikačních technologií)
- kybergrooming (komunikace s neznámou osobou vedoucí k osobní schůzce)

[13] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*.

- kyberstalking a stalking (nebezpečné pronásledování za použití informačních technologií)
- rizika sociálních sítí, hoax a spam (zejména v síti Facebook)
- zneužívání osobních údajů v prostředí elektronických médií.[14]

Obrázek 3 - E-Bezpečí[15]

2.2 Právní aspekty kybernetické kriminality

Vzhledem k tomu, že v současné době nemá kybernetická kriminalita žádný oficiálně definovaný obsah, kdy existuje více různých pojetí zejména podle toho, z jakého úhlu se na problém díváme, je třeba kybernetickou kriminalitu chápat jako specifickou trestnou činnost, kterou lze páchat pouze za použití výpočetní techniky, kde je tato technika předmětem trestného činu, nebo nástrojem ke spáchání trestného činu.[16]

Dle odborné literatury jde v případě kybernetické kriminality, o taková kriminální jednání, při nichž bylo užito výpočetní techniky, informačních či komunikačních systémů a byly:

a) užity jako nástroj k spáchání trestného činu

b) cílem útoku pachatele, přičemž tento útok musí být trestným činem, za podmínky, že jsou tyto prostředky užity či zneužity v kyberprostoru.

Velice často se kybernetická kriminalita považuje za nový druh kriminality, ale pravda je, že při kybernetické kriminalitě je využíváno známých druhů protiprávních jednání. Rozdíl je jen v tom, že tyto techniky protiprávních činů jsou přeneseny do virtuálního

[14] *Bezpečí* [online]. Dostupné z: https://www.e-bezpeci.cz/index.php/home
[15] *Bezpečí* [online]. Dostupné z: https://www.e-bezpeci.cz/index.php/ home
[16] POŽÁR, Josef. Selected Trends of the Cybercrime.

prostředí, kde tyto činy lze páchat rychleji, s větší efektivitou a pod rouškou anonymity než v reálném světě.[17]

Dále odborná literatura uvádí, že každý pachatel je hmotného původu, a proto ho je možné usvědčit na základě jeho vzájemného působení s okolím. Každý pachatel musí respektovat fyzikální zákony, i když je to proti jeho vůli. Vzájemné působení pachatele s okolím je dáno právě těmito zákony formulovanými pro příslušné podmínky trestného činu. Správným vyložením těchto fyzikálních zákonů lze poté určit velké množství parametrů, které charakterizují pachatele.[18]

2.3 Druhy kybernetické kriminality

Kybernetická kriminalita zahrnuje velké množství různých druhů trestných činů. Některá z nich ani nemusí na první pohled působit, že do této kategorie trestné činnosti patří.

2.3.1 Podvodná jednání

Nejčastějším trestným jednáním je přečin podvodu dle § 209 zák. 40/2009 Sb. trestní zákoník., kdy je i častý souběh s neoprávněným přístupem k počítačovému systému a nosiči informací dle § 230 zák. 40/2009 Sb. trestní zákoník.

Do této kategorie patří podvodné e-shopy. Tyto vznikají pod záminkou vylákaní finančních prostředků a po krátké existenci opět zanikají. Získané finanční prostředky jsou většinou vyvedeny mimo území státu za účelem anonymizace finančních toků, popřípadě je využíváno virtuální měny.

Podobně je používán i postup v rámci podvodných inzerátů (prodej elektroniky, zvířat, automobilů nebo třeba i pronájmy bytů) a také jednání známé jako nigerijské podvody. Do této kategorie lze zařadit i podvody prostřednictvím podvržených emailů nebo

[17] KOLOUCH, Jan. *CyberCrime*

[18] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*.

krádeže z bankovních účtů za pomoci phishingu.[19] Tento termín je vysvětlen v kapitole 8.9.1

2.3.2 Hacking

Neoprávněný přístup k počítačovému systému a nosiči informací je dle § 230 zák. 40/2009 Sb. trestným činem, a toto jednání se označuje se jako hacking. V případě hackingu jde o narušení dat, narušení systému nebo zneužití zařízení. Nejčastějším jednáním pachatele bývá překonání zabezpečení počítačového systému a získání přístupu k informacím oběti, s nimiž může dále nakládat dle vlastního uvážení. Součástí této činnosti často bývá i šíření škodlivých kódů a zavedení tzv. backdoorů do volně přístupných softwarů.

Stále častěji dochází i k napadení emailových účtů, bankovních účtů v internetovém bankovnictví nebo k napadení účtů v sociálních sítích. Všechny tyto činnosti jsou motivovány snahou získat přístup k citlivým informacím s možností jejich zneužití či finančního prospěchu. S touto činností souvisí i další navazující trestná činnost jako např. vydírání, nebezpečné pronásledování, krádeže z účtů, různé podvody atd.).

Dále se může jednat i o porušení tajemství dopravovaných zpráv dle § 182 zák. 40/2009 Sb. Takové jednání bývá označováno jako sniffing. Při této technice pachatel zachytává komunikaci v síti, a získává tak přístup k citlivým údajům nejen o provozu sítě, ale i obsahu. Toto jednání se velice často děje na nezabezpečených wi-fi sítích, na straně zmanipulovaných emailových serverů, a v poslední době dochází i k napadení domácích routerů. Pachatelé se pak mohou dostat k velice citlivým údajům jako např. hesla, platební údaje nebo různé osobní intimní informace. Těchto údajů, potom pachatelé využívají k získání finančního obohacení, různého zneužití nebo alespoň k poškození pověsti oběti.[20]

2.3.3 Blagging

V internetové síti se šíří i velké množství různorodých podvodů, při kterých je využíváno i sociální inženýrství. Určitému nebezpečí jsou zde vystaveny nejenom různé spo-

---

[19] P*olicie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

[20] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

lečnosti, ale také jednotlivci. Typickým příkladem podvodu, který využívá sociálního inženýrství je tzv. CEO – v tomto případě jde o fiktivní příkaz, jež vede k platbě na účet. Tyto podvody jsou ve většině případů prováděny na základě velmi dobrých znalostí trhu, struktury společnosti a jejich zákazníků. Získané informace jsou potom použity k dokonalé a přesvědčivé argumentaci, aby oběti provedly požadované úkony. Velice častým scénářem bývá, kdy se pachatelé vydávají za důvěryhodného partnera společnosti, a pod touto záminkou se zkontaktují s pro ně potřebným zaměstnancem firmy. Tohoto potom pomocí velice přesvědčivých argumentů přimějí k provedení požadované transakce.[21]

2.3.4 Podvodné e-shopy

V současné době velice roste obliba nakupování prostřednictvím Internetu. Jedná se o nakupování v různých slevomatech tykajících se dovolených, víkendových pobytů, různých zážitků, stejným způsobem jsou opatřovány nákupy věcí denní potřeby: jídlo, oblečení, různá elektronika apod.

Takové nákupy přes Internet jsou rychlé, velice často se zboží sežene za výhodnější cenu než v kamenném obchodě i je nabízeno doručení až do místa bydliště nebo možnost vyzvednutí na vybrané pobočce.

I přes tyto nesporné výhody by měli být kupující velice opatrní a to zvláště při nakupování u neověřených e-shopů, při podezřele nízké ceně, mimořádná obezřetnost je na místě především při požadavku e-shopu na platbu předem. U podvodných e-shopů toto bývá zpravidla jediná možnost platby.

Poslední dobou se také objevují nabídky brigád, které spočívají v zakládání inzerátů případně přeposílání plateb, kde figurují naivní oběti. Tito brigádníci pak pro pachatele zakládají bankovní účty, na které se přeposílají platby z podvodných e-shopů a následně se tyto finanční prostředky přeposílají či jiným způsobem předávají pachatelům. Dle § 217

[21] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

zák. 40/2009 Sb. se tímto svým jednáním brigádníci mohou dopouštět trestného činu legalizace výnosů z trestné činnosti. Tohoto činu se lze dopustit i nedbalostním jednáním.[22]

2.3.5 Mravnostní trestné činy

Mravnostní trestné činy, jež mohou být páchány prostřednictvím prostředků výpočetní a komunikační technologie jsou uvedeny v trestním zákoníku č. 40/2009 Sb., kde se dle ustanovení § 191 jedná o šíření pornografie, § 192 se zabývá výrobou a jiném nakládání s dětskou pornografii, § 193 zneužití dítěte k výrobě pornografie, § 193 a) účast na pornografickém představení, § 193 b) navazování nedovolených kontaktů s dítětem a § 201 ohrožování výchovy dítěte.

V těchto případech dochází ke kontaktování dětí mladších 18 let s úmyslem získat jejich intimní videa či fotografie, nebo je vylákat k osobní schůzce. Nejvíce jsou děti takto kontaktovány prostřednictví chatu, sociálních sítí či online her. V případě, že pachatel získá vytoužené materiály, jsou tyto dále šířeny popřípadě směňovány v uzavřených fórech, emailovými zprávami apod. Do této kategorie patří i delikty, které směřují vůči zletilým osobám jako je sexuální nátlak, kuplířství, obchodování s lidmi atd.[23]

2.3.6 Trestné činy proti autorskému právu

Dle § 270 trestního zákoníku jde o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Zde se jedná převážně o sdílení filmů, hudby nebo softwaru v rozporu s autorským právem.[24]

2.3.7 Násilné projevy a hate crime

Do této kategorie patří dle trestního zákoníku § 175 vydírání, § 353 nebezpečné vyhrožování, § 354 nebezpečné pronásledování (stalking), § 357 šíření poplašné zprávy. U těchto trestných činů by se mohlo zdát, že toho moc společného s kybernetickou kriminali-

---

[22] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.
[23] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.
[24] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

tou nemají. Ale opak je pravdou, protože při využití informačních technologií je pachatel schován za vyšší mírou anonymity.

Dále do této kategorie dále patří i různé extremistické projevy např. § 356 podněcování k nenávisti vůči skupině osob nebo omezování jejich práv a svobod, § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob.[25]

2.3.8 Kyberšikana

Kyberšikana sama o sobě není trestným činem. Některé její projevy se však dají klasifikovat jako jiné trestné činy dle Trestního zákoníku např. § 175 Vydírání je trestní sazba až 16 let odnětí svobody, § 184 pomluva až 2 roky, § 354 nebezpečné pronásledování až 3 roky, § 180 neoprávněné nakládání s osobními údaji až 8 let, § 192 výroba a jiné nakládání s dětskou pornografií až 8 let a další.[26]

Jedná se o šikanování postižené oběti s cílem ji nějakým způsobem poškodit nebo ublížit za použití informačních technologií. Nejčastějšími projevy kyberšikany jsou:

- Zasílání různých zastrašujících nebo urážlivých zpráv. Pomlouvání oběti pomocí e-mail, chatu.
- Pořizování videí, fotografii, zvukových záznamů. Tyto materiály potom jsou velice často nějakým způsobem upraveny a poté zveřejněny. Cílem je poškození oběti.
- Zakládání internetových stránek, na nichž dochází k urážení, pomlouvání či ponižování konkrétní osoby.
- Zneužití účtu či profilu (e-mailový, diskusní, facebook apod.).
- Napadání nebo provokování uživatelů na diskusních fórech.
- Vydírání postižené osoby pomocí internetu nebo mobilního telefonu.
- Obtěžováním např. neustálím voláním, psaním sms zpráv.[27]

---

[25] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.
[26] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník*
[27] Policie České republiky [online]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx.

2.3.9 Sexting

Jedná se o rozesílání fotografií, videí či různých zpráv se sexuální tématikou. Při tomto jednání dochází k poškození či vydírání oběti.[28]

2.3.10 Kybergrooming

Jde o jednání pachatele, který s dítětem manipuluje, tak aby ho vylákal na osobní schůzku a následně došlo k sexuálnímu zneužití či ublížení na zdraví. Pachatelé zde oslovují svoje oběti na sociálních sítích a následně se je snaží přemluvit k obnažování před webkamerou, sebeukájení a poté nabízí za úplatu i pohlavní styk.[29] Pachatel zde často vystupuje pod smyšlenou identitou např. dítěte. Toto počínání se poté klasifikuje jako svádění k pohlavnímu styku dle § 202 trestního zákoníku č. 40/2009 Sb.[30]

[28] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.
[29] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx.
[30] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník*.

3 MEZINÁRODNÍ DOKUMENTY V BOJI PROTI KYBERNETICKÉ KRIMINALITĚ

Dva nejvýznamnější dokumenty v boji proti kybernetické kriminalitě jsou Úmluva Rady Evropy č. 185 o kyberkriminalitě a Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě.

Tyto dva dokumenty v současné době přispívají k ochraně společnosti před kybernetickou kriminalitou, tím že stanoví základní rámec trestných kybernetických činů a současně stanoví prostředky pro odhalování a vyšetřování tohoto druhu kriminality.

3.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě

Úmluva o kyberkriminalitě představuje nejvýznamnější právní dokument týkající se kybernetické kriminality a jejím hlavním účelem je sjednocení národních právních úprav kybernetické kriminality. Tato úmluva stanovuje smluvním stranám povinnost zavést do národních právních řádů takové nástroje, pomocí kterých bude možné postihovat definované kybernetické trestné činy. Velice důležitá je právě důkladná definice skutkové podstaty trestného činu. Právě toto je podmínkou k tomu, aby bylo možné užít norem trestního práva v kybernetickém prostoru. Úmluva dále vytváří právní rámec pro jednotný a společný postup proti pachatelům této trestné činnosti bez ohledu na místo spáchání.

Úmluva o kyberkriminalitě, byla schválena Výborem ministrů Rady Evropy 8. 10. 2001. Česká republika tuto úmluvu podepsala 9. 2. 2005.[31]

3.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě

Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě byl přijat 28. 1. 2003. Tento dokument definuje okruh trestných činů, kterým se Úmluva o kyberkriminalitě nevěnuje. V Úmluvě o kyberkriminalitě chybí trestné činy, jež se zabývají šířením

[31] KOLOUCH, Jan. *CyberCrime*

určitého závadného materiálu. Tento protokol vymezuje trestné činy, spočívající především v šíření materiálů s xenofobním, rasistickým, či jinak projevující se nesnášenlivostí.[32]

3.3 Dokumenty EU/ES sloužící k harmonizaci právních úprav

EU se snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možno účinněji postihovat negativní aspekt kyberkriminality spočívající v její neohraničenosti specifičnosti. Proto je potřeba zefektivnění mezinárodní spolupráce, aby bylo možné tento negativní jev co nejúčinněji postihovat. Prostředkem pro sbližování práva jednotlivých členských států jsou především rámcová rozhodnutí, směrnice a další dokumenty EU/ES.

Z hlediska boje s kybernetickou kriminalitou se jeví jako nejvýznamnější dokumenty.:

- Směrnice Rady 91/250/EHS o právní ochraně počítačových programů.
- Rozhodnutí rady 92/242/EHS o bezpečnosti informačních systémů.
- Rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu.
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
- Rámcové rozhodnutí rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi státy.
- Nařízení Evropského parlamentu a Rady (EU) 2016/794, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. 5. 2016.

Existuje celá řada dalších směrnic a nařízení zabývajících se kybernetickou kriminalitou.[33]

[32] KOLOUCH, Jan. *CyberCrime*
[33] KOLOUCH, Jan. *CyberCrime*

3.4 Bezpečnostní strategie ČR

I přesto, že na Českou republiku dopadla zhoršená bezpečnostní situace zatím jen okrajově, je potřeba se věnovat celé škále možného nebezpečí.

Bezpečnostní strategie ČR je základním dokumentem bezpečnostní politiky ČR, který definuje bezpečnostní hrozby a způsoby, jak těmto hrozbám čelit. Na tuto strategii navazují další strategie a koncepce. Tento dokument se zabývá celkovou bezpečností strategií ČR včetně možností kybernetických útoků.

Právě v souvislosti s hrozbou kybernetických útoků patří k vládním prioritám zajištění bezpečnosti kritické informační infrastruktury a významných informačních systémů pomocí vládního koordinačního místa pro okamžitou reakci na kybernetické bezpečnostní incidenty. Vláda prosazuje tyto opatření tak, aby byla v souladu s principy vývoje informační společnosti a národní strategií kybernetické bezpečnosti na období let 2015-2020.[34]

3.5 Bezpečnostní hrozby

Bezpečnostní strategie ČR se zabývá bezpečnostními problémy republiky celkově a řeší zde např.

- *Hrozba v podobě nestability a konfliktů v evropském uspořádání* - *N*evyřešené konflikty mohou mít přímý i nepřímý vliv na bezpečnost ČR i se svými negativními důsledky.
- *Terorismus* - Hrozba terorismu je trvale vysoká. Významným a narůstajícím bezpečnostním rizikem je fenomén tzv. zahraničních bojovníků.
- *Šíření zbraní hromadného ničení* - Určité státní i nestátní organizace usilují otevřeně či skrytě o získání zbraní hromadného ničení včetně jejich nosičů.
- *Kybernetické útoky* - *V*zhledem k tomu, že kybernetický prostor je velice nespecifický právě díky neexistujícím geografickým hranicím a možnosti učinit útok z jakékoli části planety, umožňuje tak útočníkům poškodit strategické a významné zájmy ČR bez využití konvečních prostředků. Kybernetické útoky se neustále zvyšují jak proti veřejné tak i proti soukromé sféře. Tyto útoky mohou způsobit selhání

[34] Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR. *Bezpečnostní strategie České republiky 2015: Schváleno Vládou České republiky v únoru 2015*

zejména komunikačních, energických, dopravních sítí dále selhání průmyslových, finančních nebo vojenských systémů.

- *Negativní aspekty mezinárodní migrace* - Zvyšující se počet lokálních ozbrojených konfliktů, vyvolává zvýšení míry nelegální migrace, která následně může být zdrojem řady bezpečnostních problémů.
- *Extremismus a nárůst interetnického a sociálního napětí* - Jde především o problém existence sociálně vyloučených lokalit a sociálních skupin, které se spolupodílí na vytváření kriminogenního prostředí.
- *Organizovaný zločin, zejména závažná hospodářská a finanční kriminalita, korupce, obchodování s lidmi a drogová kriminalita* - Narůstá zde schopnost kriminálních sítí narušovat instituce a hodnoty právního státu, infiltrovat orgány státní správy a ohrožovat bezpečnost občanů. Často se toto děje prostřednictvím korupce.
- *Pohromy přírodního a antropogenního původu a jiné mimořádné události* - Zde dochází důsledkem extrémních projevů počasí k pohromám přírodního a antropogenního původu, které mohou mít kromě ohrožení bezpečnosti, životů a zdraví obyvatel, jejich majetku a životního prostředí dopad také na ekonomiku země, zásobování surovinami, vodou či poškození kritické infrastruktury. [35]

3.6 Národní strategie kybernetické bezpečnosti České republiky na období let 2015 - 2020

Národní strategie kybernetické bezpečnosti navazuje na Bezpečnostní strategii ČR. Jejím hlavním cílem je:

- Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti.
- Aktivní mezinárodní spolupráce.
- Spolupráce se soukromým sektorem.
- Výzkum a vývoj / Spotřebitelská důvěra.
- Podpora vzdělávání, osvěta a rozvoj informační společnosti.

[35] Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR. *Bezpečnostní strategie České republiky 2015: Schváleno Vládou České republiky v únoru 2015*

- Podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu.
- Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce). Účast na tvorbě a implementaci evropských a mezinárodních pravidel.[36]

3.7 Audit národní bezpečnosti

Česká republika má také vypracovaný Audit národní bezpečnosti, který vyhodnocuje případné hrozby. Hodnocení rizik musí pracovat nejen s jejich přímým vlivem, ale i se všemi sekundárními dopady, které hrozba vyvolává.

Audit národní bezpečnosti analyzuje celou škálu možných nebezpečí pro Českou republiku včetně vyhodnocení nebezpečnosti. Analyzuje např. terorismus, extremismus, organizovaný zločin, bezpečnostní aspekty migrace, přírodní hrozby. Organizovaný zločin atd.

Řeší také hrozby v kybernetickém prostoru dle analýzy je zhodnocení relevance hrozby pro ČR jako střední a vysoké riziko dle typu možného útoku. [37] Tato analýza hrozeb je vypracovaná pomocí SWAT analýzy.

3.8 Odpovědné instituce a orgány

Národní bezpečnostní úřad NBÚ - je v ČR zodpovědným vládním tělesem za kybernetickou bezpečnost. Od roku 2011 působí jako gestor kybernetické bezpečnosti a národní autorita v této oblasti.

Ministerstvo vnitra - plní úkoly v oblasti vnitřní bezpečnosti a veřejného pořádku. Z hlediska kybernetické bezpečnosti má klíčovou roli především jako hlavní gestor elektronizace výkonu veřejné správy.

Policie ČR - jako největší bezpečnostní sbor je jedním ze základních pilířů vnitřní bezpečnosti ČR. V boji s hrozbami v kyberprostoru jí patří nezastupitelná role orgánu činného v

[36] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 - 2020* [online]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf.

[37] *AUDIT NÁRODNÍ BEZPEČNOSTI*

trestním řízení, jehož úkolem je vyhledávat, odhalovat a vyšetřovat kybernetickou trestnou činnost.

Ministerstvo obrany - Odpovídá za zajištění kybernetické bezpečnosti rezortních komunikačních a informačních systémů a vojenských sítí.

Ministerstvo zahraničních věcí - se v součinnosti a spolupráci s NBÚ a některými dalšími rezorty podílí na realizaci či úspěšném naplňování konkrétních úkolů stanovených v Akčním Plánu a k Strategii především ve vztahu k mezinárodním organizacím a vybraným státům.

Zpravodajské služby ČR - mají za úkol získávání informací a jejich vyhodnocování s cílem odhalit ohrožení zájmů a bezpečnosti státu a obyvatelstva ČR.[38]

[38] *AUDIT NÁRODNÍ BEZPEČNOSTI*

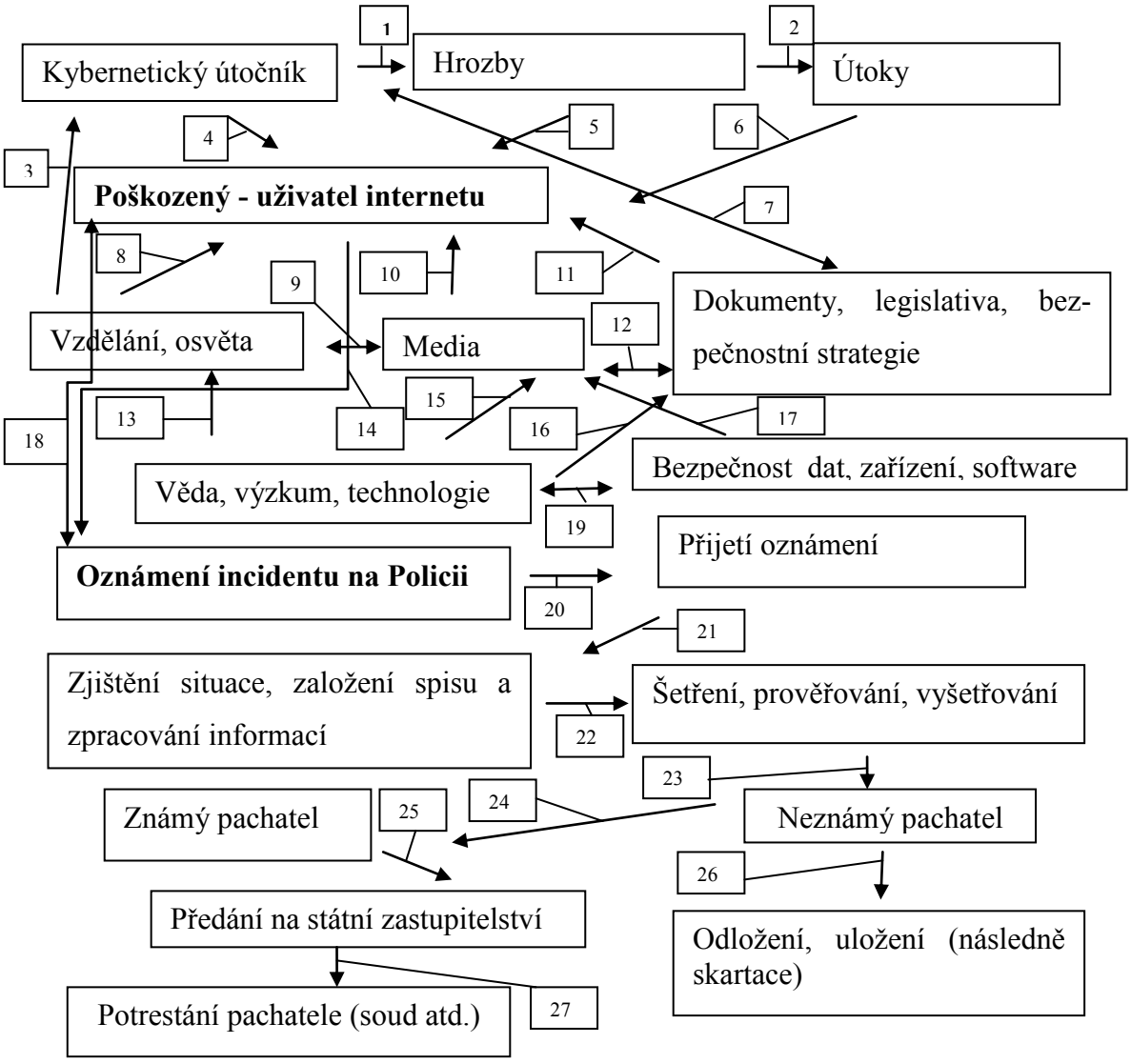
4 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI BAKALÁŘSKÉ PRÁCE

V teoretické části jsem využil zdrojů jak z odborné literatury, tak i z odborných webovských stránek a tyto zdroje jsou uplatitelné pro praxi. Na základě analýzy těchto zdrojů jsem zpracoval teoretickou část své bakalářské práce, která se zabývá historií vzniku kybernetického prostoru přes rozdělení kybernetické kriminality až po mezinárodní dokumenty zabývající se problematikou kybernetické bezpečnosti.

Veškeré tyto skutečnosti byly přípravou pro zpracování praktické části bakalářské práce.

II. PRAKTICKÁ ČÁST

5 MODEL KYBERNETICKÉ KRIMINALITY



Obrázek 4 - Model kybernetické kriminality[39]

[39] Vlastní zpracování autora

5.1 Prvky kybernetického modelu

- **Poškozený, uživatel internetu** - jedná se o všechny uživatele internetu, kybernetického prostoru (firmu, dospělou osobu či dítě). Všichni, ti kteří se připojí do sítě, se stanou potenciální oběti nějakého kybernetického útoku.
- **Kybernetický útočník, hrozby, útoky** - osoba, která má na svědomí vývoj škodlivých programů, kybernetických podvodů a veškeré bezpečnostní incidenty a kybernetické trestné činy. Z tohoto potom vyplívají veškeré možné hrozby a útoky z kybernetického prostředí. Útočník se neustále vzdělává a zkouší jak obejít bezpečnostní opatření a dalo by se říci, že je neustále o krok napřed. Protože útočník najde nějakou bezpečnostní chybu, vytvoří nový škodlivý program, a tento distribuuje po síti. A teprve poté je vyvíjena ochrana a zabezpečení.
- **Vzdělání, osvěta** - jedná se o veškeré vzdělávací aktivity ve školách, zaměstnáních, školeních a seminářích.
- **Média** - jde o tisk, televizi, rozhlas, internet apod., kterými lze šířit osvětu a vzdělání. Nejvíce odborných informací poskytuje internet a tematicky zaměřené časopisy či jiná literatura.
- **Dokumenty, legislativa, bezpečnostní strategie** - patří sem zákony, vyhlášky, úmluvy, bezpečnostní strategie, dále sem patří různá bezpečností pravidla a vnitřní řády např. na školách, institutech apod.
- **Věda, výzkum, technologie** - zde jde o různé aktivity v oblasti výzkumu a vývoje nových technologii a bezpečnostních prvků, bezpečnostního softwaru, vývoj aktualizací apod.
- **Bezpečnost dat, zařízení, software -** zde jde o zabezpečení softwaru, hardwaru a dat. Je nutné, aby se systémem pracoval poučený uživatel, který má zájem o zabezpečení svých dat.
- **Oznámení incidentu na policii, šetření** - okamžiku, kdy dojde k incidentu a uživatel internetu se stane poškozeným (obětí), tak v případě, že celý incident nahlásí, nastane proces vyšetřování. Na základě výsledků potom dojde k potrestání pachatele, nebo se celá věc odloží.

5.2 Popis vztahů kybernetického modelu

Zde se jedná o vzájemný vztah mezi uživatelem (poškozeným) kybernetického prostoru, útočníkem a dalšími prvky. Tento popis se vztahuje k obr. 4.

1. útočník vytváří hrozby
2. hrozby jsou zdrojem možných útoků
3. útočník, aby byl neustále v obraze, se musí také vzdělávat, ale také může útočit
4. útočník působí na uživatele
5. hrozby působí na uživatele
6. samotný útok na uživatele
7. útočník studuje dokumenty, legislativy apod.
8. uživatel (poškozený) se případně vzdělává, působí na něho osvěta
9. vzdělání, osvěta a dokumenty s legislativou jsou ve vzájemné symbióze
10. na uživatele působí media
11. dokumenty, legislativa apod. pro ochranu uživatele
12. dokumenty, legislativa a vzděláni s osvětou jsou ve vzájemné symbióze
13. věda, výzkum má vliv na osvětu a vzdělání
14. oznámení incidentu poškozeným na policii
15. působení na média
16. určité vzájemné působení mezi výzkumem a legislativou
17. v případě nového vyvinutí zabezpečení dat, softwaru je toto medializováno
18. vzájemná následná komunikace mezi poškozeným a policií při vyšetřování incidentu
19. věda, výzkum a bezpečnost dat, zařízení software jsou ve vzájemné symbióze
20. - 27. samotný proces vyšetřování

5.3 Výsledky modelování a návrh pro praxi

Model kybernetické kriminality demonstruje vzájemný vztah mezi jednotlivými prvky. Toto propojení vzájemného působení jednotlivých vztahů modelu bylo konzultováno s odborníky z kybernetické kriminality, a na základě těchto skutečností je zcela nutné uživatele seznámit v co největším měřítku se všemi riziky, která v kybernetickém prostoru hrozí. Z praxe je zcela zřejmé, že u pachatelů se zvyšuje jejich odbornost v oblasti krytí identity, což znesnadňuje jejich vypátrání. Proto je velice důležitá preventivní činnost a

osvěta uživatelů, aby tito byli schopni rozpoznat hrozící riziko a včas reagovat. U dětí je třeba, aby rodiče kontrolovali jejich činnost v kybernetickém prostoru a hovořili s nimi o jejich aktivitách v kybernetickém prostoru, protože jen takto je možné případné nebezpečí včas odhalit a učinit případně potřebná opatření.

5.4 Současný stav řešení dané problematiky

V současné době, při zvyšujícím se náporu kybernetické kriminality, je boj s tímto fenoménem velice složitý. Velikým problémem je skutečnost, že v případě realizovaného kybernetického trestného činu není zcela jasné odkud k útoku došlo. V tomto okamžiku pracovníci kybernetické kriminality s nadsázkou říkají, že rázem jsou pro ně všichni uživatelé kybernetického prostoru možní pachatelé. Na vyšetřování tohoto druhu kriminality se používají odlišné metody vyšetřování, protože skutečné místo činu může být kdekoli. Vyšetřovatelé jsou vděční, když pachatel svoji trestnou činnost provádí na území republiky či v zemích EU. Zjištění pachatele v ostatních evropských zemích bývá již o něco složitější, ale jakmile pachatel svoji činnost provádí mimo Evropu, tak je jeho dopadení sice možné, ale zdlouhavé. Nejhorší situace nastane, když pachatel svojí trestnou činnost provádí v zemi, se kterou nemáme žádné dohody o spolupráci. V tomto případě je potom jeho dopadení takřka nemožné.

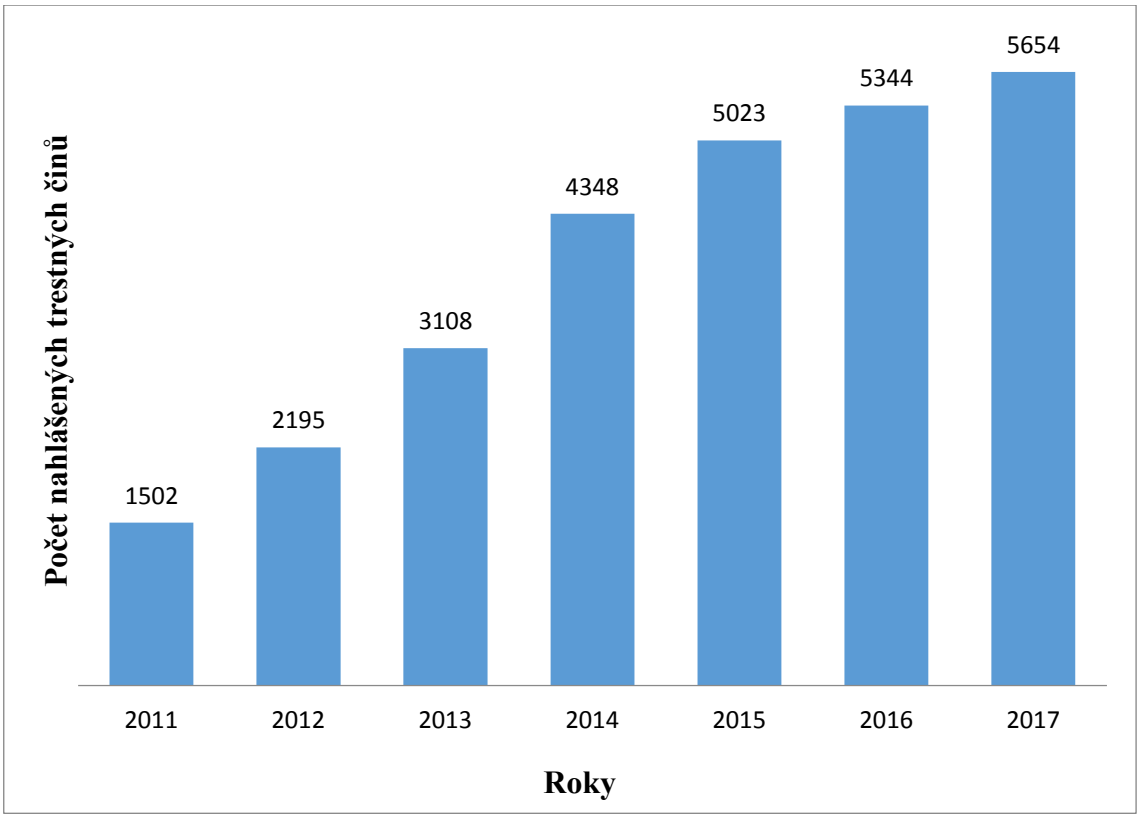
V okamžiku, kdy se příjme oznámení o kybernetickém trestném činu, tak tento se začne vyšetřovat dle vyšetřovacích metod. Jakmile se zjistí skutečné místo, kde k útoku došlo např. v případě dětské pornografie apod., tak poté si celou věc většinou přebírá mravnostní oddělení a dále postupuje dle svých postupů. Ve velkém množství šetřených případů se stává, že během vyšetřování je nutná mezinárodní spolupráce zejména proto, že pachatelé svoji trestnou činnost provádějí z různých míst na světě. Proto je docela možné si myslet, že komunikujeme s člověkem, který je z vedlejšího města a následným šetřením se zjistí, že tato osoba s námi komunikovala z Jihoafrické republiky.

Zde je proto velice důležitá vzájemná mezinárodní spolupráce napříč všemi zeměmi, ale to je ideál, ke kterému má současné fungování světa značně daleko.

6 STATISTIKA KYBERNETICKÝCH TRESTNÝCH ČINŮ

Dle celorepublikových statistik má obecná kriminalita sestupnou tendenci, ovšem kybernetická kriminalita neustále vzrůstá, což dokazují následujících statistiky.

6.1 Statistika kybernetických trestných činů v ČR



Graf 1 - Počet oznámených kybernetických trestných činů v celé republice[40]

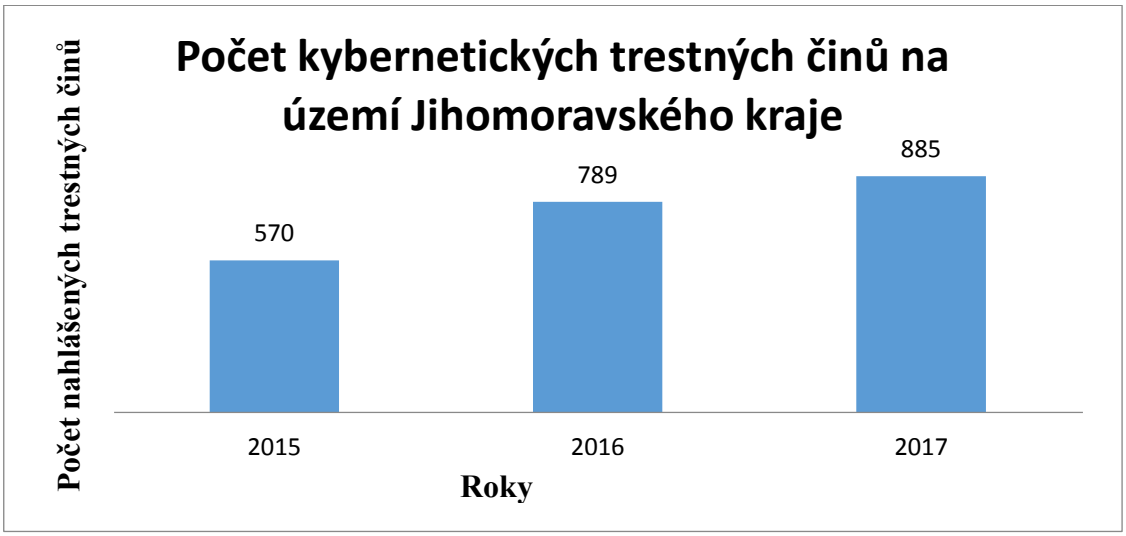
Graf 1 jednoznačně dokládá, že kybernetická kriminalita stoupá opravdu strmě vzhůru a tento trend je potřeba potlačit. Následující tabulka 1 rozděluje kybernetickou trestnou činnost dle druhů a počtů v jednotlivých letech.

[40] Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx.

Tabulka 1 - Druhy oznámených trestných činů v celé republice[41]

Druhy oznámených trest-ných činů v jednotlivých letech	2011	2012	2013	2014	2015	2016	2017
podvodná jednání	917	1303	1863	2478	2932	3235	3140
Hacking	66	112	220	555	578	534	608
mravnostní delikty	132	161	261	314	351	344	561
autorskoprávní delikty	155	241	181	262	315	237	296
násilné projevy + hate crime	86	111	155	202	230	265	318
Ostatní	146	267	428	537	617	729	731
Celkový počet šetřených činů	**1502**	**2195**	**3108**	**4348**	**5023**	**5344**	**5654**

6.2 Statistika kybernetických trestných činů na území Jihomoravského kraje



Graf 2 - Počet oznámených trestných činů na území Jihomoravského kraje[42]

[41] Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx.
[42] Interní zdroj PČR

Tabulka 2 - Druhy oznámených trestných činů na území Jihomoravského kraje[43]

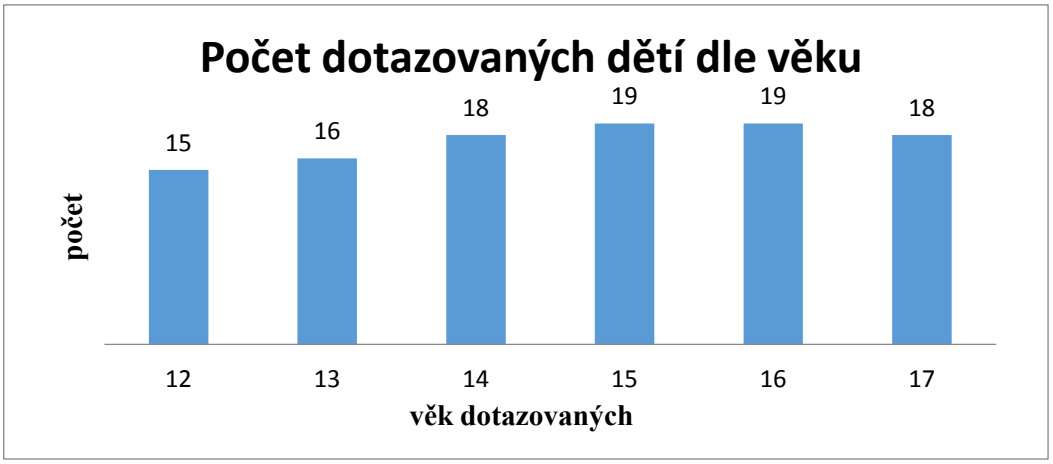
Druhy oznámených trestných činů v jednotlivých letech v JMK	2015	2016	2017
Podvodná jednání	348	591	712
Dětská pornografie	25	34	31
Specifické útoky	158	109	118
Vyhrožování	11	16	21
Pronásledování	12	12	7
Pomluva	11	13	15
Celkem	**565**	**775**	**904**

Vzhledem k stoupajícímu trendu je zapotřebí mezi uživatele, kteří se pohybují v kybernetickém prostoru, šířit náležitou osvětu a poučit je o číhajících nebezpečích. Protože v případě, že se my uživatelé budeme chovat zodpovědně a budeme vědět, jaká nebezpečí na nás číhají a mohou číhat, tak budeme připraveni čelit možným hrozbám, a tím kybernetickým zločincům jejich nekalé aktivity velice ztížíme. Samozřejmě toto se týká kybernetické kriminality, která se zabývá různým vniknutím do systému za účelem získání dat a informací. Popřípadě napadení nějakého bezpečnostního systému, podvodu, zneužití dítěte apod. V případě pomluvy, kyberšikany, stalkingu apod. nám samozřejmě jakékoli zabezpečení nepomůže. Proto je velice důležité vědět co v takových případech dělat.

[43] Interní zdroj PČR

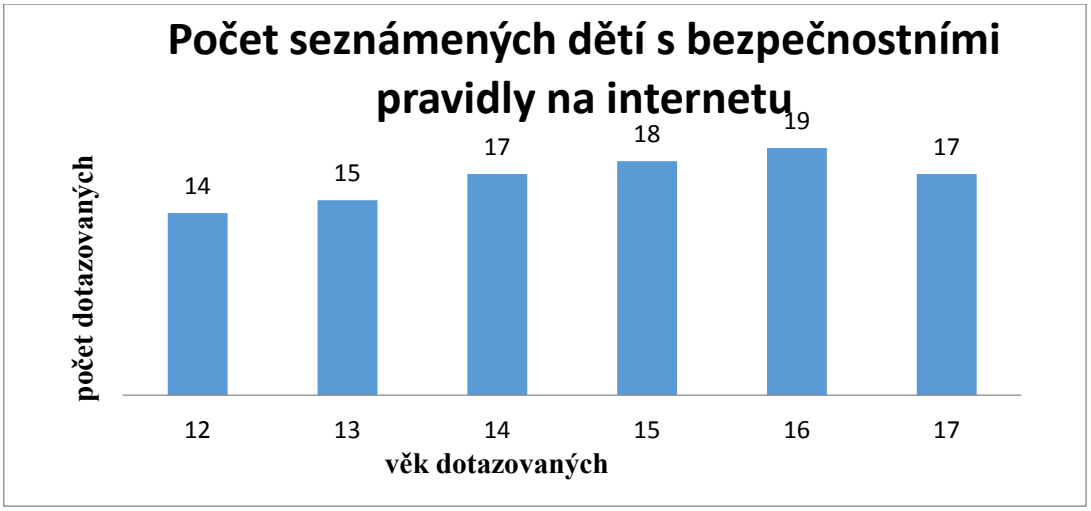
7 DOTAZNÍKOVÝ PRŮZKUM A ANALÝZA RIZIK

Cílem dotazníkového průzkumu, bylo zjistit, kolik dětí pohybujících se na Internetu je seznámeno s bezpečným chováním a kolik dětí se tímto řídí ve škole a doma. Celkový počet dotazovaných byl 105 dětí ve věku 12 až 17 let.



Graf 3 - Počet dotazovaných dětí dle věku[44]

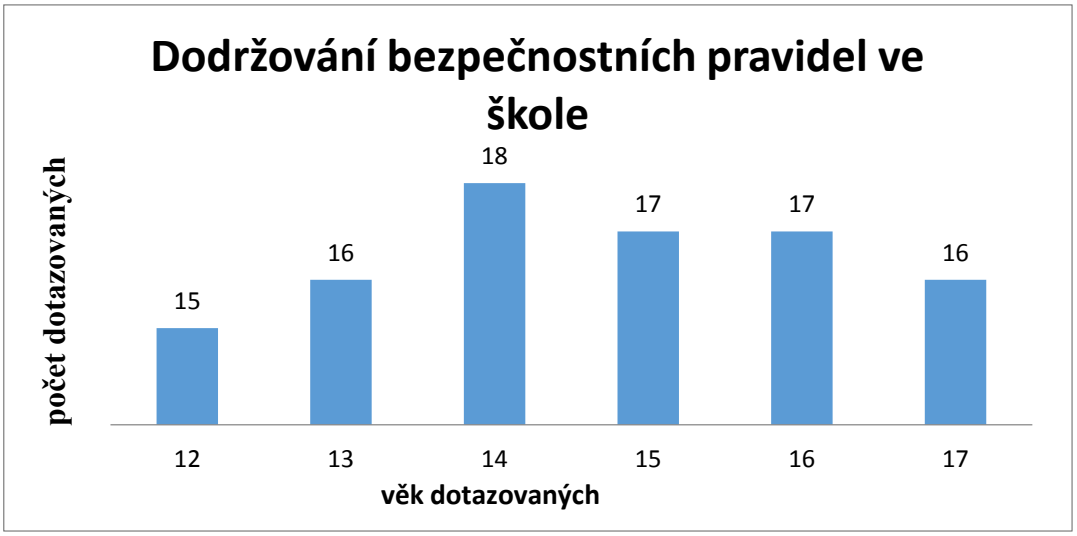
Tabulka 2 - Počet poučených dětí ohledně bezpečného chování na internetu



Graf 4 - Počet seznámených dětí s bezpečnostními pravidly chovaní na internetu[45]

[44] Vlastní zpracování autora
[45] Vlastní zpracování autora

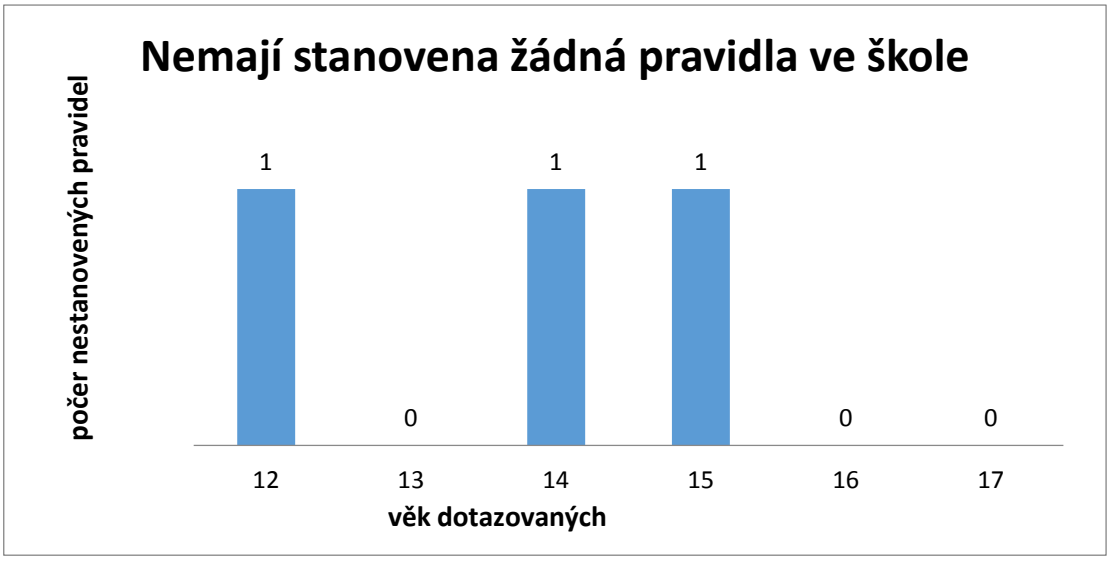
Z celkového počtu 105 dotazovaných dětí v dotazníku 5 z nich odpovědělo, že nebyly nikterak poučeny ohledně bezpečného chování na internetu. Tato hodnota odpovídá 4,76 % nepoučených dětí z celkového počtu dotazovaných.



Graf 5 - Dodržování bezpečnostních pravidel na internetu[46]

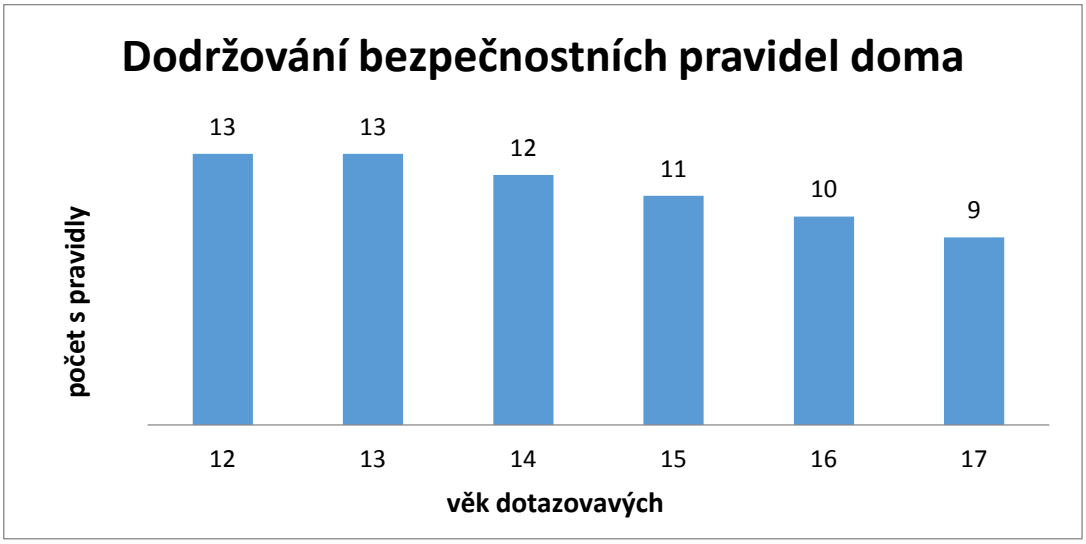
Bezpečnostní pravidla ve škole dodržuje celkem 99 dětí ze 105 dotazovaných. Celkem se tedy ve škole pravidly neřídí 5,7% dotazovaných dětí.

[46] Vlastní zpracování autora



Graf 6 - Počet dětí ve škole bez pravidel[47]

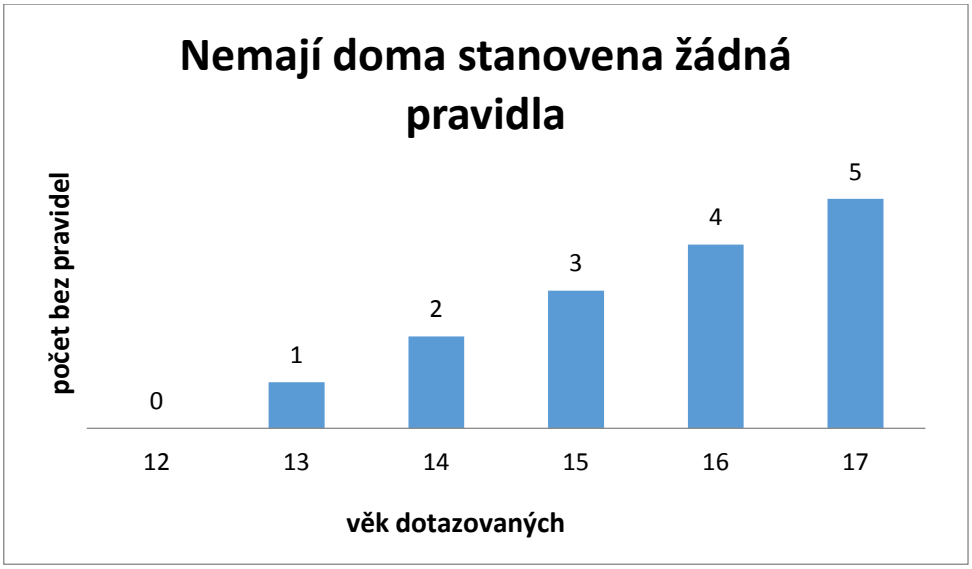
Tři děti uvedly, že ve škole nemají stanovena žádná pravidla.



Graf 7 - Dodržování bezpečnostních pravidel doma[48]

[47] Vlastní zpracování autora
[48] Vlastní zpracování autora

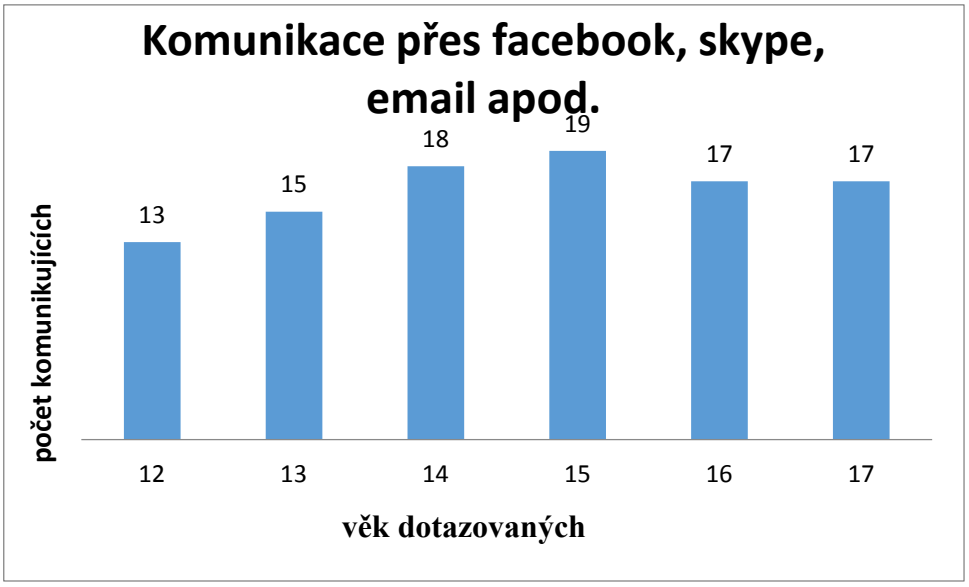
Celkem 68 dětí uvedlo, že bezpečnostní pravidla doma dodržuje, což odpovídá 64,5 % dotazovaných dětí. Zde bylo dále zjištěno, že se stoupajícím věkem klesá počet dětí, která pravidla dodržují.



Graf 8 - Děti doma bez pravidel[49]

Z celkového počtu 105 dotazovaných dětí uvedlo 15 z nich, že nemá stanovena žádná pravidla. Tento počet odpovídá 14 % dotazovaných.

[49] Vlastní zpracování autora



Graf 9 - Komunikace dětí[50]

Ze 105 dotazovaných dětí 99 uvedlo, že komunikují přes facebook, skype, email atd., což odpovídá 94,3 % dotazovaných dětí, které komunikují prostřednictvím sítě.

7.1 Shrnutí dotazníkového průzkumu

V průzkumu bylo dotázáno celkem 105 dětí z volnočasových aktivit Sokol Brno. Cílem průzkumu bylo zjistit, kolik dětí má stanovena bezpečnostní pravidla a kolik dětí tato pravidla nerespektuje. Z celkového počtu dotázaných dětí bylo zjištěno, že 36 % z nich bezpečnostní pravidla nedodržuje a že cca 94 % dotazovaných dětí komunikuje pomocí sociálních sítí, mailů apod. Poučení dětí ohledně bezpečného chování je obdobné napříč všemi věkovými kategoriemi. 14 % dětí uvedlo, že doma nemá stanovena žádná. Dětí, které nemají stanovena žádná pravidla, s přibývajícím věkem přibývá.

7.2 Analýza rizik metodou PNH

Jedná se o jednoduchou polokvantitativní metodu, při které se vyhodnocují příslušná rizika ve třech složkách s ohledem na:

- pravděpodobnost vzniku rizika (P)

[50]Vlastní zpracování autora

- pravděpodobnost následků rizika (N)
- názor hodnotitelů na riziko (H)

Tabulka 3 - (P) - Pravděpodobnost vzniku a existence nebezpečí[51]

P - pravděpodobnost vniku a existence nebezpečí	
1	nahodilá
2	nepravděpodobná
3	pravděpodobná
4	velmi pravděpodobná
5	trvalá

Tabulka 4 - (N) - Možné následky ohrožení[52]

N - možné následky ohrožení	
1	malé ohrožení pachatelem
2	lehká ohrožení pachatelem
3	vážnější ohrožení pachatelem
4	velké ohrožení pachatelem
5	neustálé ohrožení pachatelem

Tabulka 5 - (H) - Názor hodnotitelů[53]

H - názor hodnotitelů	
1	zanedbatelný vliv na míru ohrožení a nebezpečí
2	malý vliv na míru ohrožení a nebezpečí
3	větší, nezanedbatelný vliv na míru ohrožení a nebezpečí
4	velký a významný vliv na míru ohrožení a nebezpečí
5	více významných vlivů na míru ohrožení a nebezpečí

Celkové zhodnocení rizik získáme součinem jednotlivých činitelů. Výsledkem je potom ukazatel míry rizika (R).

R=PxNxH

[51] Vlastní zpracování autora
[52] Vlastní zpracování autora
[53] Vlastní zpracování autora

Tabulka 6 - Ohodnocení míry rizika[54]

Rizikový stupeň	R	Míra rizika
I.	> 100	nepřijatené riziko
II.	51 - 100	nežádoucí riziko
III.	11 - 50	mírné riziko
IV.	3 - 10	akceptovatené riziko
V.	< 3	bezvýznamné riziko

Při této analýze, jsem se zaměřil na rizikovost děti do 18 let, které tráví čas v kybernetickém prostoru prostřednictvím Facebooku a různých chatovacích serverech.

Tabulka 7 - Nepoučené dítě bez dozoru rodičů[55]

Druh činnosti	Rizikový faktor	Identifikace rizika	Vyhodnocení závažnosti rizika				Bezpečnostní opatření k omezení rizika
			P	N	H	R	
Činnost v kybernetickém prostředí	Nepoučené dítě trávící čas bez dozoru rodičů např. na Facebooku, různých chateh apod.	Možný kontakt s pachatelem	5	4	4	80	Zde jde o nežádoucí riziko, protože nepoučené dítě, které nemá občas dozor rodičů, může komunikovat s možným pachatelem, tato komunikace může být bez povšimnutí.

U nepoučených dětí, které tráví svůj volný čas na Internetu, prostřednictvím Facebooku a různých chatovacích či seznamovacích serverů jde o riziko II. stupně. V případě, že takováto komunikace není kontrolovaná a dítě není řádně poučené o možných nebezpečích, tak může dojít k samotnému ohrožení dítěte. Protože takový jedinec ani nemusí vědět, že mu hrozí nějaké nebezpečí, a může souhlasit např. s osobní schůzkou.

[54]Vlastní zpracování autora
[55] Vlastní zpracování autora

Tabulka 8 - Poučené dítě bez dozoru rodičů[56]

Druh činnosti	Rizikový faktor	Identifikace rizika	Vyhodnocení závažnosti rizika				Bezpečnostní opatření k omezení rizika
			P	N	H	R	
Činnost v kybernetickém prostředí	Poučené dítě trávící čas bez dozoru rodičů např. na Facebooku, různých chateh apod.	Možný kontakt s pachatelem	4	3	3	36	Mírné riziko, poučené dítě zpravidla ví, jaké riziko může z komunikace hrozit. V případě kontaktu s pachatelem se zpravidla někomu svěří.

U poučených dětí, které tráví čas na Facebooku, chatech a různých seznamovacích serverech, jde o riziko III. stupně a jedná se o mírné riziko. I zde hrozí, že pachatel se pokusí s dítětem navázat kontakt, avšak takovéto dítě může odhalit možné nebezpečí a svěřit se rodičům.

Tabulka 9 - Poučené dítě pod dozorem rodičů[57]

Druh činnosti	Rizikový faktor	Identifikace rizika	Vyhodnocení závažnosti rizika				Bezpečnostní opatření k omezení rizika
			P	N	H	R	
Činnost v kybernetickém prostředí	Poučené dítě trávící čas pod dozorem rodičů např. na Facebooku, různých chateh apod.	Možný kontakt s pachatelem	3	2	2	12	Mírné riziko, ale i zde je určitá pravděpodobnost napadení stanice. Proto je důležité zabezpečení systémů a jejich aktualizací.

U dětí, které jsou poučené, a rodiče kontrolují jejich činnost, je riziko na samé hranici III. a IV. stupně. I zde může dojít ke kontaktu s pachatelem, ale tento může být včas odhalen díky kontrole.

Děti, které tráví čas u počítačů připojených k Internetu, je třeba, řádně poučit o bezpečnostních pravidlech a dbát na jejich dodržování.

[56] Vlastní zpracování autora
[57] Vlastní zpracování autora

8 KYBERNETICKÁ KRIMINALITA V PRAXI

Ve svém zaměstnání se setkávám s různými druhy kriminality. Zatímco běžná kriminalita rok od roku mírně klesá, tak naopak kybernetická kriminalita je na vzestupu. V této části své bakalářské práce uvádím několik typů kybernetické kriminality, která se týká dětí a následně nejčastěji se vyskytující trestné činy včetně rad, jak se těmto činům bránit.

8.1 Zneužívání dětí na internetu

Sexuální zneužívání dětí je velice závažným problémem v současném internetovém světě, zejména proto, že internet poskytuje anonymitu a je možné se v něm vydávat za kohokoliv. Dále tomu dopomáhají byť nevědomky i sami děti a rodiče a to zejména tím, že různě publikují na sociálních sítích vše ze svého života, nejrůznější fotografie včetně intimních. Proto k vyhledávání i kontaktování obětí z velké většiny dětí dochází nejčastěji na sociálních sítích, chatech a seznamkách. Pachatel se většinou vydává za jejich vrstevníka a děti ztrácejí zábrany a neuvědomují si rizika. Tyto děti nedokáží rozpoznat nebezpečí a často se nechají snadno přesvědčit k zasílání svých erotických fotografií. Toto počínání se potom označuje za sexting.

8.2 Sexting

Jsou to především právě děti, které sami dobrovolně poskytují citlivý materiál a tento může pachatel proti nim použít např. k vydírání. Děti se nafotí či natočí v sexuálních pozicích a tento materiál potom posílají pachateli, který ho dále distribuuje po Internetu. Následné odstranění je potom prakticky nemožné. Děti šířící své vlastní intimní fotografie či videa se sami stávají pachateli. Zde si je třeba uvědomit, že i osoba ve věku mezi 15 a 18 lety, může mít legální pohlavní styk, avšak výroba či distribuce pornografie u jedinců v tomto věkovém rozpětí je trestná.[58] Jedná se zejména o výrobu a jiné nakládání s dětskou pornografií dle § 192, zneužití dítěte k výrobě pornografie § 193, ohrožování výchovy dítěte § 201 vše podle trestního zákoníku č. 40/2009 Sb.[59]

---

[58] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx.
[59] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník*.

8.3 Kybergrooming

Jedná se o velmi nebezpečné chování. Jde o takové aktivity, které se snaží vyhlédnutou oběť donutit k osobní schůzce. Ke kontaktu dochází nejčastěji prostřednictvím různých chatu, SMS zpráv, Facebboku, Skypu apod.

Výsledkem takovéto schůzky může být potom sexuální zneužití, fyzické týrání, únos apod.

Tímto jednáním jsou nejvíce ohroženy děti a skládá se z několika kroků.

1. Vzbuzení důvěry a pocitu bezpečí, následně nenápadné izolování oběti od okolí (pachatel bývá velice trpělivý, nikam nespěchá).
2. Podplácení různými dárky a budování kamarádského vztahu.
3. Získání emoční závislosti obětí na pachateli.
4. Osobní schůzka.
5. Sexuální obtěžování, únos, týrání, zneužití (velice ohroženy jsou právě děti).

Toto je jen malý výčet toho, jaká nebezpečí číhají na uživatele v kybernetickém prostoru. Právě proto, že kybernetičtí zločinci nikdy nespí a neustále vymýšlejí nové způsoby páchání trestných činů, je zapotřebí se mít neustále na pozoru a při práci v síti se chovat obezřetně.[60]

Dalším velkým problémem dnešní doby je kybernetická šikana.

8.4 Kybernetická šikana

Kybernetická šikana je fenoménem 21. století. Existuje několik druhů kybernetické šikany. Tyto druhy mohou být realizovány pomocí mobilního telefonu např. šikanujícími telefonáty, tichými telefonáty, zasíláním SMS nebo MMS zpráv. Pomocí internetu prostřednictvím šikanujících emailů, přes založené www stránky, chatovací místnosti, sociální sítě apod.

---

[60] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

Kybernetická šikana je závažným společenským problémem. Ještě před osmi roky bylo velice málo materiálů, které by se této problematice věnovaly. V současné době se jejich počet rapidně zvýšil. Problém kybernetické šikany je natolik závažný, že vznikla prví nadnárodní síť výzkumníků z různých oborů "COST Action ISO801", která zahrnuje 28 evropských zemí a Austrálii.

Závažnost kybernetické šikany se projevuje i v České republice. Dalším nebezpečím je to, že obětí nemusí být pouze žáci či studenti, ale také např. učitelé nebo zaměstnanci. [61]

Ve většině případů kybernetické šikany se jedná o přestupky nebo jiné správní delikty.[62] Ovšem v důsledku tohoto počínání může dojít i ke spáchání trestného činu ,např. Účast na sebevraždě § 114, Vydírání § 175, Nebezpečné vyhrožování § 353, Útisk § 117 nebo také Hanobení národa, rasy, etnické nebo jiné skupiny osob § 355 vše dle trestního zákoníku č. 40/2009 Sb.[63]

8.4.1 Příklady kybernetické šikany v České republice

- Martin, byl dlouhodobě šikanován spolužáky. Tito ho svlékali do spodního prádla, zesměšňovali ho. Jejich útoky se neustále stupňovaly a vyvrcholení všeho bylo, když ho natočili na toaletě z hora kabinky v okamžiku, když měl průjem. Video kolovalo poté třídou, všichni se mu smáli. Martin se zhroutil, byla mu diagnostikována školní fobie a byl tři měsíce hospitalizován v léčebně. Učitelé měli sice důkaz na videonahrávce, ale věc skončila tak, že se jednalo o ojedinělý incident.[64]
- Na střední průmyslové škole, byla šikanovaná 55 letá učitelka. Žáci ji bránily v odchodu ze třídy, mlátili ji a různě ji vyhrožovali. Učitelka nakonec byla hospitalizovaná v psychiatrické léčebně a nakonec zemřela. Mladíci skončili u soudu.[65]

A mnoho dalších případů je řešeno každoročně po celé republice.

---

[61] ŠMAHAJ, Jan. *Kyberšikana jako společenský problém: Cyberbullying as a social problem*.
[62] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx
[63] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník*.
[64] *Kyberšikana a její prevence: příručka pro učitele*.
[65] *Idnes* [online]. Dostupné z: https://zpravy.idnes.cz/

8.4.2 Prevence kybernetické šikany

Jedna z možností prevence kybernetické šikany je zřízení určitých pravidel na školách.

Mezi tyto pravidla patří například:

- První hodiny školního roku jsou věnovány vyložení pravidel školy a tato jsou vyvěšena ve třídách.
- Zákaz používání mobilních telefonů během vyučování. Toto opatření slouží jako prevence natáčení nebo fotografování žáků i učitelů. V případě napomenutí a neuposlechnutí smí vyučující učitel telefon zabavit uložit ho do trezoru a vydat pouze rodičům.
- Blokování přístupu na Internet, pokud je potřeba žáky cíleně přimět k potřebné činnosti.
- Využívání softwaru, který umožní vyučujícímu se informovat o činnosti žáka na počítači. O tomto zavedeném opatření by měli být žáci informováni.
- Při hodinách je zamezen přístup na stránky s hrami, chaty, sociálními sítěmi apod.
- Žáci mají zřízeny své školní emailové schránky, kam mají přístup jen oni a to odkudkoliv.
- Žáci mají velice omezené uživatelská práva, na to, co mohou v počítačích nastavovat.
- Zákaz vstupu na stránky s pornografickou a násilnickou tématikou
- Zákaz přístupu na proxy, servery pomocí kterých se dají omezení obcházet.
- Veškerý online provoz je sledován a zaznamenáván.[66]

Ovšem zavedení a dodržování pravidel neznamená, že kybernetická šikana nebude, protože velká část této aktivity probíhá mimo školní prostředí, anebo pokud ve škole, tak potom k distribuci materiálů se dochází mimo školu. A toto velice ztěžuje možné vypátrání pachatelů.[67]

---

[66] *Kyberšikana a její prevence: příručka pro učitele*.
[67] ŠMAHAJ, Jan. *Kyberšikana jako společenský problém: Cyberbullying as a social problem*

8.4.3 Obrana před kybernetickou šikanou

V případě, že se staneme obětí kybernetické šikany, je potřeba dodržet určité kroky, které nám pomůžou odrazit případné další útoky, popřípadě snížit jejich intenzitu a následný dopad.

- Ukončit komunikaci - přestat s útočníkem jakkoli komunikovat, nesnažit se ho žádným způsobem odradit od jeho počínání, nemstít se mu, nevyhrožovat.
- Zablokovat útočníka - zamezit útočníkovi přístup k účtu, telefonnímu číslu, změnit si virtuální identitu. Vzhledem k tomu, že útočník si může také měnit svoji virtuální identitu, blokací nelze definitivně zamezit, kontaktu s pachatelem ale jde o to znesnadnit mu jeho počínání.
- Oznámit útok, a konzultace s někým, kdo může pomoci - i když se člověk může v důsledku útoku cítit ponížený a zranitelný či pociťovat obavy z reakcí okolí, tak je důležité o problému říci někomu v okolí. V případě, že se toto týká dítěte, je důležité, aby se svěřilo rodičům nebo učiteli, aby se mohla učinit potřebná opatření.
- Uchovat důkazy - pro oběť je velmi důležité uchovat si důkazy. Na základě důkazů může být proti útočníkovi později zahájeno vyšetřování.[68]

Problém kybernetické šikany se týká dětí i dospělých a v současné době moderních technologií je tento problém stále palčivější.

Velký rozdíl mezi kybernetickou šikanou a běžnou je v tom, že při klasické šikaně dítě přijde domů a zde je v bezpečí, má klid. Ale pokud je dítě šikanované pomocí Internetu, tak před touto formou šikany jen velmi těžko unikne, protože fotografie či video je k vidění neustále, kdy takové materiály mohou vidět tisíce lidí. I když může vypnout počítač, či odpojit se ze sítě, tak stejně kompromitující podklady jsou neustále sdíleny a vše probíhá dál. Právě toto má na dětskou psychiku ničivé účinky a velice často se potom stává, že taková osoba si následky nese až do dospělosti a někdy i celý život.[69]

[68] *Kyberšikana a její prevence: příručka pro učitele*
[69] ŠMAHAJ, Jan. *Kyberšikana jako společenský problém: Cyberbullying as a social problem*.

8.5 Desatero bezpečného Internetu pro děti

1- Nedávej nikomu telefon ani adresu.
2- Neposílej nikomu cizímu svou fotografii a už vůbec ne intimní, tuto neposílej ani svému kamarádovi – nikdy nevíš, co s ní může udělat.
3- Udržuj své hesla v tajnosti, nesděluj je ani kamarádovi.
4- Nikdy nereaguj na neslušné nebo vulgární emaily. Nejlépe je ignorovat.
5- Nedomlouvej si schůzky přes internet, aniž by o tom někdo věděl.
6- Pokud najdeš obrázek, video nebo email, který tě šokuje, opusť stránku.
7- Řekni dospělému, pokud tě nějaké stránky nebo něčí vzkazy uvedou do rozpaků či dokonce vyděsí.
8- Neotvírej přílohy emailů, které přišly z neznámé adresy, mohou obsahovat viry.
9- Nevěř každé informaci, kterou získáš z Internetu.
10- Pokud se nechceš s někým bavit, tak se nebav.[70]

Pokud se děti budou chovat podle těchto rad, budou lépe chráněny. I přesto je potřeba na ně dohlížet a zbytečně neriskovat.

Dále je přínosné, aby doba strávená u počítače byla pro děti omezená. Dobré je s dětmi uzavřít dohodu, kdy a jak budou internet používat, popřípadě jaké stránky budou navštěvovat. Je také možné vytvořit osobní prostředí dítěte, ve kterém je přístup k internetu omezen na určité stránky. Toto řešení je nejbezpečnější.

8.6 Pachatel kybernetické kriminality

Kybernetická kriminalita má dle policejních statistik rok o roku stoupající tendenci. Reakcí na tuto situaci je rozšiřování řad odborníků a vyšetřovatelů v oblasti kybernetické kriminality. Dle vlastních zkušeností z policejní praxe se dají osoby, které páchají kybernetické trestné činy rozdělit, na dvě skupiny - amatéry a profesionály.

- **Amatéři** - jedná se o pachatele, kteří se zabývají nejběžnějšími trestnými činy. Tyto potom aplikují pomocí sítě Internet. Zpravidla se jedná o různé

[70] *Bezpečný internet* [online]. Dostupné z: http://www.bezpecnyinternet.cz/deti/rady-pro-tebe/desatero-bezpecneho-internetu.aspx.

podvody při prodávání zboží, žádosti o půjčky. Případně se může jednat i o kybernetickou šikanu apod. D této kategorie spadají začínající hackeři, kteří ještě nejsou na dostatečné úrovni. U tohoto typu útočníků je zpravidla jejich dopadení jednodušší, protože nejsou dostatečně vzdělaní a jsou opojeni pocitem bezpečí v kybernetickém prostoru.

- **Profesionálové** - jedná se převážně o zkušené hackery, organizované skupiny apod. Tito pachatelé sledují a studují nejnovější trendy v oblasti kybernetické bezpečnosti a vyvíjí svoje vlastní škodlivé programy, které jsou schopné obejít ochranný software. Vymýšlí nové druhy podvodů apod.

Na základě těchto skutečností vzniká široká paleta možných útoků, jež se týkají nás všech uživatelů Internetu. V dalších kapitolách představuji alespoň některé typické útoky.

8.7 Neoprávněné vniknutí do počítače, systémů a databází

Pachatel takovéto trestné činnosti se pokusí vniknout do vyhlédnutého počítače či systému a to obvykle prostřednictvím Internetu. V takovém případě musí pachatel překonat ochranná opatření, jako jsou hesla, přístupové kódy, certifikáty apod. Jakmile pachatel získá přístup k informacím, tak zpravidla tyto informace dále neoprávněně využívá pro svoje potřeby. Případně s nimi obchoduje či je používá k jiné trestné činnosti.[71]

8.8 Napadení cizího počítače

Pachatel této trestné činnosti napadá počítače, systémy a databáze pomocí počítačových virů nebo jiných škodlivých programů (tzv. malware). Někdy se jedná o tzv. spící programy (např. trojský kůň). Spící programy za určitých předem stanovených podmínek jsou aktivovány a jejich cílem je zablokování počítače, vymazání dat apod.[72]

[71] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*
[72] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*

8.9 Kybernetické podvody

Jde zde z velké části o podvodné jednání osob využívajících internetové sítě jako nástroje k páchání běžných podvodů. Pohybem na internetové síti je možno oslovit velké množství potenciálních obětí a současně zůstat skrytý v anonymitě v rámci provedeného podvodu.

Podvody, které jsou páchány pomocí Internetu, bývají detailně promyšlené a velice často také zahrnují psychosociální aspekt neboli snahu o vyvolání důvěry. Využívá se zde velice často například výhodné a časově omezené nabídky.

Poškozená oběť v prvních okamžicích nemusí ani tušit, že se stala obětí trestného činu. Tuto skutečnost zjistí až v okamžiku, když se jí zablokuje počítač, dojde k neoprávněnému čerpání finančních prostředků z účtu a podobně.[73]

8.9.1 Phishing

Typickým příkladem internetových podvodů je phishing, kdy se za pomoci Internetu pachatel pokouší získat citlivé údaje. Tento druh kriminality nevyužívá slabin počítačových technologií, ale slabin samotného uživatele. Útočník odešle email vydávající se za známou firmu a snaží se získat citlivá data s přesměrováním na falešnou internetovou stránku. Často jde o získání hesel k internetovému bankovnictví nebo údaje o platební kartě, PIN apod.

Phishing lze provádět i mimo internetové prostředí a to v reálném světě, ovšem ve virtuálním světě útočník rozešle obrovské množství zpráv potenciálním obětem s minimální námahou.

Phishingový útok probíhá v několika krocích:

- **Plánování útoku** - v první fázi dochází k výběru cíle a metody útoku, která bude použita. V této fázi dále dochází k vyhodnocování technického zabezpečení cíle a rizika odhalení pachtele.
- **Vytváření podmínek pro phishingový útok** - ve druhé fázi je řešena technická stránka útoku. Útočník získá seznam e-mailových adres uživatelů,

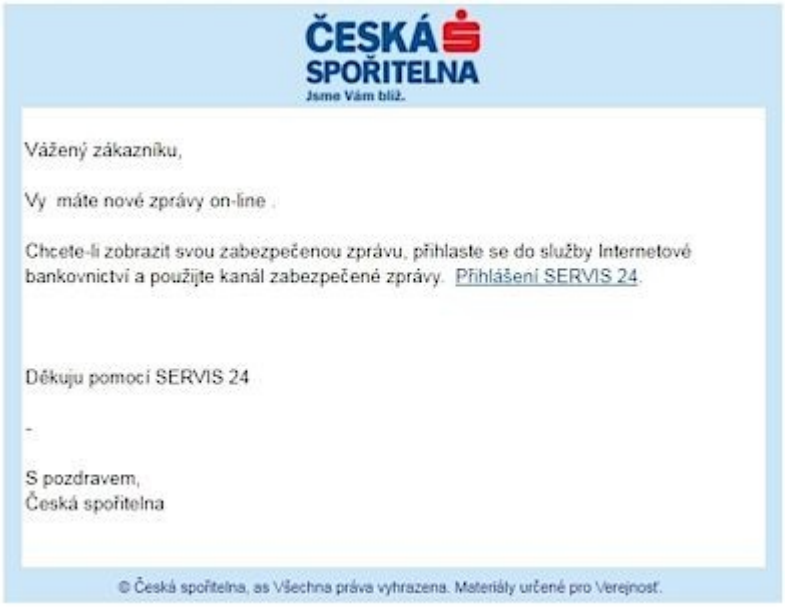
[73] Policie České republiky. Dostupné z: http://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx.

proti kterým je útok směřován a poté dojde k vytvoření důvěryhodného sdělení. Toto sdělení je následně distribuováno uživatelům.

- **Phishingový útok -** jakmile je phishingový email doručen uživatelům, potom dle kvality provedení emailové zprávy, zkušenosti uživatelů, jejich informovanosti o problematice phishingových útoků apod., jsou poté případná získaná data zasílána do datové schránky útočníka. Až teprve v této fázi se uživatel setkává s phishingovým emailem. Velice často je ve zprávě jako záminka uvedena informace o nějaké bezpečnostní chybě společnosti či jiné varování. Tato informace má vzbudit u uživatele pocit autentičnosti zprávy. Jakmile uživatel aktivuje odkaz, je přesměrován na webovou stránku vytvořenou útočníkem, která věrně kopíruje stránku např. bankovní instituce. Uživatel je po přesměrování na tuto stránku vyzván k zadání svých přihlašovacích údajů vč. čísla platební karty a PIN kódu. Následuje sběr dat - zde se útočníkovy v jeho datové schránce shromažďují data od jednotlivých uživatelů, která byla zadána prostřednictvím falešné stránky.
- **Sběr dat -** zde útočník získává data, které mu uživatelé zaslaly prostřednictvím falešné stránky.
- **Odčerpání prostředků z phishingového útoku** - v této konečné fázi útočník vstupuje na skutečná bankovní konta uživatelů, a poté dojde k odčerpání finančních prostředků. Tyto finanční prostředky jsou poté nejčastěji rozmělněny a převedeny na zahraniční konta, kde jsou prakticky nevystopovatelná.[74]

[74] KOLOUCH, Jan. *CyberCrime*.

Jako příklad je zde uvedena ukázka podvodného emailu, pravé a podvodné stránky České spořitelny, a.s.



Obrázek 5 - Podvodný email České spořitelny. a.s.[75]

Obrázek 6 - Pravá přihlašovací stránka České spořitelny a.s.[76]

[75] *Česká spořitelna* [online]. Dostupné z: https://www.csas.cz.

Obrázek 7 - Podvodná stránka České spořitelny a.s.[77]

8.9.2 Pravidla bezpečného chování v případě phishingového podvodu

Zde je důležité vědět, že pokud se klient přihlašuje do internetového bankovnictví, je potřeba nejprve zkontrolovat adresní řádek, kde musí být zabezpečená internetová adresa např. https://www.servis24.cz a vedle ní ikona zámku. Dále je potřeba kliknout na ikonu zámku, kde se poté zobrazí certifikát potvrzující platnost a ověřující identitu stránky. Toto se u podvodných stránek nestane.[78]

8.9.3 Podvodné jednání na internetovém portálu

Dalším typickým příkladem kybernetické kriminality je podvodné jednání na internetových prodejních portálech, které probíhá následujícím způsobem. Pachatel inzeruje nějaké zboží např. televizory. Toto je nabízeno oběti. Oběť si vyhlédnuté zboží objedná a toto je možné zaslat pouze poštou, kde musí být platba za zboží provedena předem. Oběť

[76] KOLOUCH, Jan. *CyberCrime*.
[77] KOLOUCH, Jan. *CyberCrime*.
[78] *Česká spořitelna* [online]. Dostupné z: https://www.csas.cz.

zboží zaplatí předem přes internetové bankovnictví. Objednané zboží však nedorazí a prodávající v roli pachatele současně přeruší veškerou komunikaci.[79]

8.9.4 Jak se nestát obětí podvodného jednání na internetovém portálu

Zde je velice důležité před nákupem na Internetu dodržovat určitá pravidla:

- Nakupovat pouze u ověřených prodejců.
- Pokud je prodejce neznámý, předem si o něm zjistit potřebné informace.
- Uchovat si záznam o internetových transakcích, komunikacích včetně webových stránek prodávajícího.
- Před nákupem si přečíst zásady o platbě a dodání zboží.

Zboží se dá zaplatit několika způsoby: dobírkou, platba v hotovosti, nákupem na splátky. Možná platba pouze předem je velice podezřelá.[80]

8.10 Bezpečné chování při připojení do internetu

V současné době je vývoj programů i operačních systémů vyvíjen tak, aby počítače mohl používat i naprostý laik s minimálními znalostmi. Toto je problém velké většiny operačních systémů, jejichž instalace je stále jednodušší. Také připojení na síť je stále snažší a pro uživatele transparentnější. Zastánci tohoto přístupu argumentují, že použití počítače musí být dostupné každému, ne pouze odborníkům. Důsledkem tohoto je, že na síti jsou potom počítače, které nikdo neudržuje, nebo neví, jak je má udržovat, a programové vybavení není řádně aktualizované. Potom se stane, že jednotlivé služby nebo dokonce celý počítač je přístupný každému, kdo se o přístup pokusí. [81]

Proto je velice důležité, aby bylo co nejvíce uživatelů poučeno o tom, jak se po připojení na Internet chovat a hlavně, aby se podle toho chovali.

---

[79] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/podvodne-jednani-na-internetovem-portalu.aspx.
[80] *Policie České republiky* [online]. Dostupné z: http://www.policie.cz/clanek/podvodne-jednani-na-internetovem-portalu.aspx.
[81] MATYSKA, Luděk. *Zpravodaj ÚVT MU* [online].

8.10.1 Ochrana proti podvodům a útokům na Internetu

Při používání Internetu je nutné si uvědomit, že existuje velké množství způsobů, jakými mohou podvodníci získat přístup k osobním údajům, financím nebo samotnému počítači. Podvodníci, aby dosáhli svého cíle, jsou bohužel velice vynalézaví, a proto opatrnosti není nikdy dost. Už jenom proto, že vpádu do našeho soukromí si mnohdy nemusíme ani všimnout nebo to zjistíme, až když je pozdě.[82]

8.10.2 Ochrana firewallem, antivirovým programem a bezpečné chování na Internetu

Způsobů, jak nakazit počítač škodlivým programem, je mnoho, proto je velmi důležité dbát na vysokou úroveň ochrany. Firewall je základ, který by neměl chybět na žádném počítači. Toto platí i o antivirovém programu, nejlépe takový, který snímá činnost v reálném čase, a je schopný zablokovat škodlivý software ještě před jeho nainstalováním do počítače.

Na co se potom nesmí zapomínat, jsou nejen pravidelné aktualizace antivirových programů, firewallů, ale i operačního systému. Vývojáři jsou totiž neustále pozadu za hackery a podvodníky, proto musí mít každý antivirový program aktuální údaje o hrozbách, aby je dokázal rozpoznat a vypořádat se s nimi. Při prevenci může pomoci i internetový prohlížeč. Dle provedených testů v časopisem Dtest dokázaly internetové prohlížeče Google Chrome a Internet Explorer zabránit přístupu na necelou polovinu phishingových stránek. Google Chrome dále zablokoval přístup i na zhruba čtvrtinu stránek nakažených malwarem. Internet Explorer pak zablokoval jen asi desetinu nakažených stránek.[83]

Samozřejmě i v případě, že je počítač plně zabezpečen, tak vždy záleží zejména na jeho uživateli, jak se na Internetu chová. Pokud například při návštěvě nějaké stránky, nebo při pokusu o stažení nějakého programu vyskočí nabídka stahovat, je velice důležité posoudit, zda se jedná opravdu o to, co bylo v úmyslu stáhnout či nikoliv. Nebezpečí může totiž číhat i na zdánlivě důvěryhodných stránkách, které mohly být napadeny. Administrá-

---

[82] *Dtest* [online]. Dostupné z: https://www.dtest.cz/clanek-4539/ochrana-proti-podvodum-a-utokum-na-internetu?pdf=1

[83] *Dtest* [online]. Dostupné z: https://www.dtest.cz/clanek-4539/ochrana-proti-podvodum-a-utokum-na-internetu?pdf=1

torům totiž nějakou dobu trvá, než hrozbu odhalí, a proto trvá nějaký čas, než jsou tyto stránky opět bezpečné. Šíření různých škodlivých programů není jen otázkou stahování. K nakažení může dojít i při běžném surfování na Internetu, právě jenom návštěvou nakažené stránky. Ale tomuto zpravidla zabrání právě antivirový program, který nám o tomto podá hlášení. Potom je už vždy na uživateli, jak se zachová. Dále je velice důležité v případě doručeného emailu od neznámého adresáta nestahovat přílohy, pokud si uživatel není naprosto jistý, že jde o něco pro mě zájmového a žádaného. Protože i zde se jedná z velké většiny o škodlivé programy.[84]

Ovšem toto jsou všechno věci a postupy, kterým se dá zabránit nebo předcházet. V případě ztráty dat či peněz jsou tyto škody nahraditelné. Daleko větším problémem jsou trestné činy, které jsou páchány na dětech. Jedná se o činy, jež probíhaly a probíhají i v normálním světě mimo kybernetický prostor, ale v současné době se přesouvají právě do kybernetického prostředí, a jsou o to víc nebezpečnější, protože jsou schopny oslovit velké množství obětí, kdy tyto mohou být následně zneužívány.

8.11 Řešení kybernetické problematiky

Základním problémem v oblasti kybernetické problematiky je v současné době nedostatečné podvědomí o možných rizicích, a proto je potřeba uživatele s těmito riziky dostatečně obeznámit a seznámit je s pravidly bezpečného chování v kybernetickém prostoru. Jak bylo uvedeno v kapitole 2.1, jsou pořádány nejrůznější semináře, besedy a různá sezení na téma týkající se kybernetické bezpečnosti, kriminality atd. Na toto téma vychází celá řada odborných publikací a časopisů. Je provozováno velké množství odborných www stránek, které se tímto problémem zabývají. Tyto všechny činnosti jsou přínosem v boji s kybernetickým nebezpečím. Ve školách jsou taktéž děti s tímto nebezpečím seznamovány ať již ve výuce či prostřednictvím různých besed. Otázkou je, jestli toto vše je dostatečné, protože dle policejních statistik kybernetická kriminalita rok od roku stoupá a z tohoto potom vyplývá jediné: Je činnost všech zúčastněných organizací, spolků apod. dostatečná?

Já osobně vidím jako velký problém samotného uživatele, který se pohybuje v kybernetickém prostoru. Uživatelé jsou velice důvěřiví a jsou to především oni, kdo umožní

[84] *Dtest* [online]. Dostupné z: https://www.dtest.cz/clanek-4539/ochrana-proti-podvodum-a-utokum-na-internetu?pdf=1

útok i na zabezpečené platformy, ať již svojí neznalostí či ztrátou ostražitosti. Proto je opravdu velice důležité dodržovat určitá pravidla bezpečného chování a tato pravidla dále šířit a to nejen mezi nejmladšími uživateli, ale napříč všemi uživateli. Tato činnost je ovšem velice složitá a časově náročná. Proto je nutno osvětu zintenzivnit, a to zejména ve školách a na pracovištích. Dále potom i mezi seniory. Protože pokud nebudeme dostatečně seznámeni se všemi riziky a možnými nebezpečími, tak kybernetický zločin bude neustále narůstat. Všechny uživatele samozřejmě nelze dostatečně obeznámit s rizikem a nebezpečím, ale cílem musí být zabezpečit a obeznámit s riziky co možná největší množství uživatelů. Jestli se toto podaří, snad časem ano, ale určitě se tento druh kriminality nepodaří zcela vymýtit. Protože kriminalita byla odjakživa. A navěky nás i bude doprovázet. Tato se bude pouze měnit a různě transformovat, dle vyvíjející se situace. Proto jedním z velice důležitých faktorů je prevence.

8.12 Prevence kybernetické kriminality

Podle mého názoru je prevence důležitější než následné represivní postihy, protože vyšetřování kybernetické kriminality je velice náročné jak finančně, tak i časově a velmi často končí neúspěchem. Prevenci je tedy třeba zaměřit zejména na uživatele, kteří jsou ve styku s výpočetní technikou a kyberprostorem. U těchto uživatelů je třeba zvyšovat jejich právní vědomí. Velice důležitou úlohu zde má právě vzdělávání, které musí být započato nejlépe již od raného období mládeže a dětí, protože právě zde jsou největší nedostatky ve znalostech možného nebezpečí a právního vědomí, vzhledem k jejich mentální vyspělosti. Je důležité děti seznamovat s číhajícím nebezpečím v kybernetickém prostoru a věnovat se i právní výchově. Děti je nutné seznámit se skutečností, že právní normy jsou závazné v kybernetickém prostoru stejně tak, jako v reálném světě. Výuka, která se týká bezpečného užívání internetu, by neměla být zaměřena pouze jednorázovými projekty či na nedostatečnou výuku ve škole, ale musí být ve větší intenzitě a kvalitě zaměřena právě na číhající nebezpečí. Důležité je tyto vzdělávací aktivity provádět i u zaměstnanců, kteří pracují s výpočetní technikou, protože právě tito nedostatečně proškolení zaměstnanci jsou často příčinou kybernetických útoků, protože umožní pachateli přístup do jejich systémů. Tento trend je třeba změnit a napravit právě vzděláváním a osvětou uživatelů Internetu.

Dle vlastních zkušeností, mohu zcela svědomitě říci, že část populace je nepoučitelná, i když je na ni působeno medii, Internetem a různými dalšími zdroji ohledně ohrožení, které se skrývá v kybernetickém prostoru. Tyto osoby, i když vědí, že se např. kradou

věci z vozidel, tak tyto tam stejně nechávají i viditelně umístěné. Nechávají tam dokonce i cennosti a peníze. Stejně se to týká i obětí kybernetické kriminality. Zde ve velké většině převažuje zvědavost či důvěřivost nad selským rozumem.

Zde uvádím konkrétní přiklad z praxe (názvy jsou pozměněny):

- Na obvodním oddělení bylo přijato oznámení, kdy na portále *bardan.am,* působil zástupce firmy Sanka, který prodával její zboží. Tento zástupce vystupoval pod jménem *Petr* a komunikoval pomocí emailu *lucavara @ aaasa.am*. Tento při objednání zboží, inkasoval částku 2000,- Kč, předem a objednané zboží nezaslal a ani nevrátil zaslanou hotovost. Pachatel dohledán a potrestán.
- Na Internetu se objevil prodejce značkových traktorů, tento je nabízel za čtvrtinové ceny. Kupující platili statisícové částky jako zálohy, po té čekali. Několik týdnů, měsíců než celý podvod nahlásili. Šetřením bylo zjištěno, že stopy vedou až za hranice Evropy a pachatelé jsou již nedohledatelní.
- Třináctiletá dívka komunikovala přes Facebook s údajně stejně starým hochem. Komunikace dospěla do stádia, že dívka začala chlapci posílat své intimní fotografie a následně i videa. Ukázalo se, že chlapec je dospělý muž, který videa a fotografie dále šířil po internetu. Jednalo se o muže z Prahy.

Na základě mnoha dalších rozličných spáchaných trestných činech, se dá říci, že pachatelé v kybernetickém prostoru kriminalitu provádějí ve všech možných variantách a je skutečně možné, že ti opravdu velice zdatní kybernetičtí zločinci nám unikají bez povšimnutí.

9 DÍLČÍ ZÁVĚR PRAKTICKÉ ČÁSTI BAKALÁŘSKÉ PRÁCE

V praktické části své bakalářské práce jsem představil model kybernetické kriminality a jeho vzájemné vazby mezi kybernetickými zločinci a poškozenými. Poté jsem zpracoval statistiku kybernetické kriminality v České republice a Jihomoravském kraji. V praktické části bakalářské práce je také proveden dotazníkový průzkum ohledně dodržování bezpečnostních pravidel v kybernetickém prostoru dětmi a analýza rizik. Závěrem se v praktické časti, věnuji kybernetickým trestným činům tykajících se dětí a nejběžněji se vyskytujícím trestným činům.

ZÁVĚR

Vzhledem ke skutečnosti, že v současné době je rozmach komunikační a výpočetní techniky na vzestupu a kybernetický prostor nás všechny obklopuje, si tento fakt ani nemusíme uvědomovat. Pravda je, že již de facto vše je připojeno do kybernetického prostoru, což se týká prakticky všeho např. energie, výrobní podniky, statní podniky, nemocnice, domácnosti, vše je napojeno na počítače, různé sítě a systémy. Toto všechno je v potenciálním nebezpečí, pokud se tímto směrem kybernetičtí zločinci zaměří. Tyto všechny hodnoty je důležité chránit. Kybernetická kriminalita je poměrně novým odvětvím zločinu, kdy lze předpokládat její rozmach a to díky neustálému vývoji různých technologií.

Ve své bakalářské práci jsem se zaměřil, z důvodů velice širokého spektra kybernetické kriminality alespoň na nejběžnější trestné činy, které jsou páchány v kybernetickém prostoru. Zde jsem popsal způsoby páchání a možnou ochranou před touto trestnou činností. Dále jsem zde uvedl konkrétní příklady z praxe vč. statistiky a analýzy rizika.

.

SEZNAM POUŽITÉ LITERATURY

[1] *AUDIT NÁRODNÍ BEZPEČNOSTI*. Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality. Praha, 2016.

[3] *Bezpečný internet* [online]. In: . [cit. 2018-04-13]. Dostupné z: http://www.bezpecnyinternet.cz/deti/rady-pro-tebe/desatero-bezpecneho- interne tu.aspx

[2] *Česká spořitelna* [online]. In: . [cit. 2018-02-27]. Dostupné z: https://www.csas.cz

[3] *Dtest* [online]. In: . 2015 [cit. 2018-02-28]. Dostupné z: htt ps://www.dtest.cz/clanek-4539/ochrana-proti-podvodum-a-utokum-na- interne tu?pdf=1

[4] *E-Bezpečí* [online]. In: . [cit. 2018-03-07]. Dostupné z: https://www.e-bezpeci.cz/index.php/home

[5] *Historie Internetu v České republice* [online]. In: . [cit. 2017-11-21]. Do stupné z: z:https://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm.

[6] *Idnes* [online]. In: . 2016 [cit. 2018-03-03]. Dostupné z: https://zpravy.idnes.cz/

[7] *Jak na internet* [online]. In: . [cit. 2017-11-20]. Dostupné z: htt ps://www.jaknainternet.cz/page/1205/historie-internetu/

[8] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackin gu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[9] KAVALÍR, Aleš, ed. *Kyberšikana a její prevence: příručka pro učitele*. Plzeň: Pro město Plzeň zpracovala společnost Člověk v tísni, pobočka Plzeň, 2009. ISBN 978-80-86961-78-1

[10] Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR. *Bezpečnostní strategie České republiky 2015: Schváleno Vládou České republiky v únoru 2015*. Praha: Ministerstvo zahraničních věcí České republiky, 2015. ISBN ISBN 978-80-7441-005-5

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

[12] MATYSKA, Luděk. *Zpravodaj ÚVT MU* [online]. Roč. XII. Brno: Ústav výpočetní techniky Masarykovy univerzity, 2002 [cit. 2018-02-28]. ISSN 1212-0901. Do stupné z: http://webserver.ics.muni.cz/bulletin/articles/242.html

[13] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 - 2020* [online]. In: . [cit. 2018-02-22]. Dostupné z: htt ps://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[14] *NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost* [online]. In: . [cit. 2017-11-28]. Dostupné z: htt ps://www.govcert.cz/cs/vzdelavani/skoleni-seminare-a-konference/

[15] *NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost* [online]. In: . [cit. 2017-12-12]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2543-cybercon-brno-2017-a-seminar-k-zkb/

[16] *Policie České republiky* [online]. In: . Policie České republiky [cit. 2017-11-25]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[17] *Policie České republiky*. In: . [online]. [cit. 2018-02-16]. Dostupné z: http://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

[18] *Policie České republiky* [online]. In: . Policie České republiky [cit. 2017-11-27]. Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx

[19] *Policie České republiky* [online]. In: . 22.6.2017 [cit. 2018-02-27]. Dostupné z: http://www.policie.cz/clanek/podvodne-jednani-na-internetovem-portalu.aspx

[20] *Policie České republiky* [online]. In: . [cit. 2018-03-21]. Dostupné z: http://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx

[21] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Pl zeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-589-0

[22] POŽÁR, Josef. Selected Trends of the Cybercrime. *Acta Informatica Pragensia*. **2015**(4), 336-348. ISSN 1805-4951.

[23] ŠMAHAJ, Jan. *Kyberšikana jako společenský problém: Cyberbullying as a social problem*. Olomouc: Univerzita Palackého v Olomouci, 2014. ISBN 978-80-244-4227-3

[24] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník*. Vydání: osmé. Praha: Armex Publishing, 2017. Edice kapesních zákonů. ISBN 978-80-87451-47-2

[25] *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) č. 181/2014 Sb.* [online]. In: . Poslanecká sně movna Parlamentu České republiky [cit. 2017-11-21]. Dostupné z: z: htt ps://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

www world wide web (webová stránka)

např. například

apod. a podobně

atd. a tak dále

PIN osobní identifikační číslo např. platební karta

EU Evropská unie

ES Evropská směrnice

tzv. Takzvaně

SMS Short message service (služba krátkých textových zpráv)

MMS Multimedia Messaging Service (multimediální zprávy)

SEZNAM OBRÁZKŮ

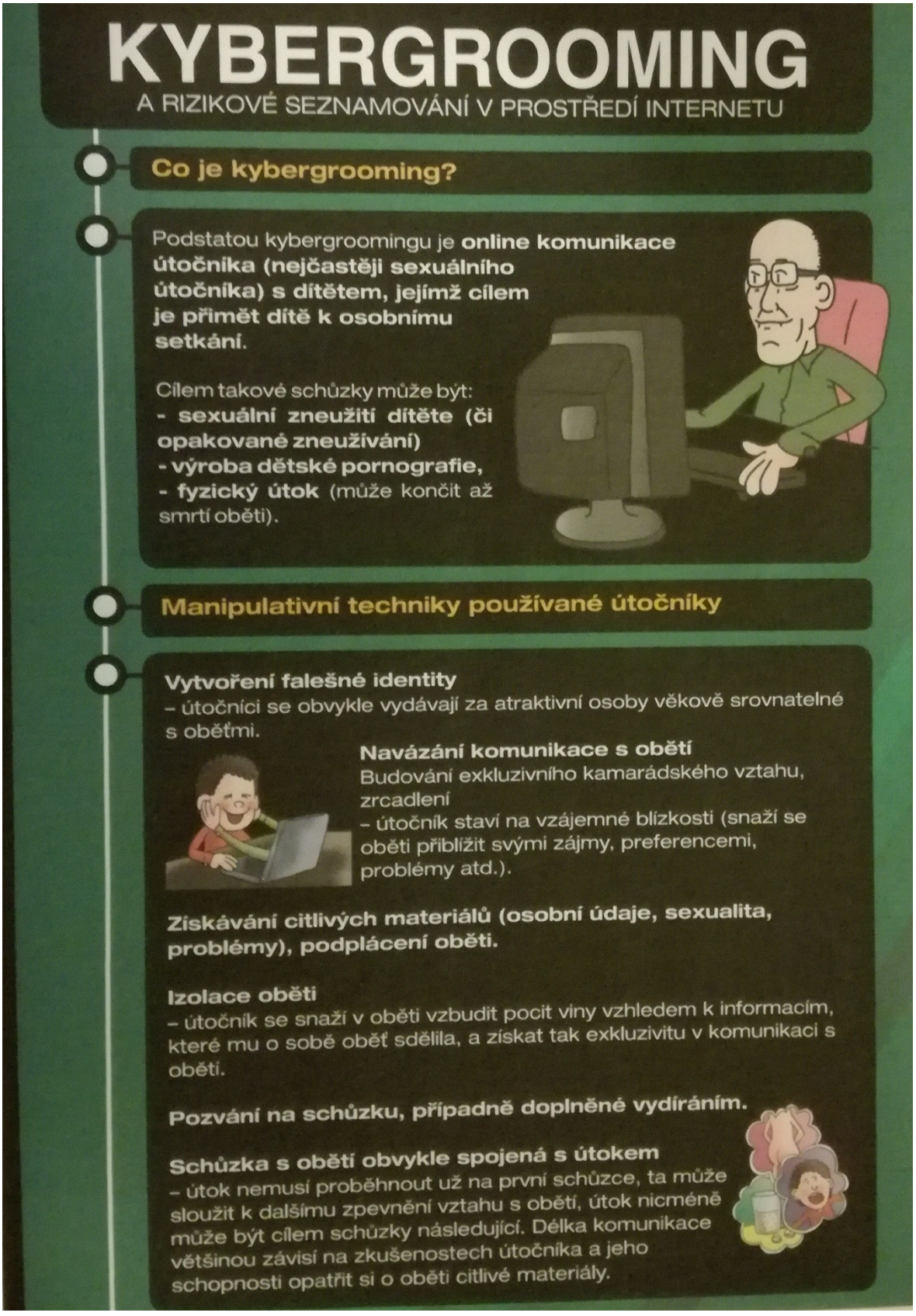
SEZNAM TABULEK

SEZNAM GRAFŮ

REJSTŘÍK

SEZNAM PŘÍLOH

PŘÍLOHA P I: LETÁK KYBERGROOMING



KYBERGROOMING

A RIZIKOVÉ SEZNAMOVÁNÍ V PROSTŘEDÍ INTERNETU

Jak se chránit před kybergroomingem?

Základem je být obezřetný v komunikaci s cizími osobami, zejména pokud nás taková osoba sama kontaktuje a komunikaci se snaží navázat pod různými záminkami. Ideální je do takové komunikace vůbec nevstupovat.

Nepřidávat si neznámé osoby ke svým přátelům v rámci online komunikačních služeb, důsledkem je pak zpřístupnění chráněných informací a vstup neznámého člověka do soukromí oběti. I u známých osob, které online žádají o přátelství, se raději přesvědčit, že se jedná skutečně o onu osobu.

Nebýt přehnaně důvěřivý, výzkumy ukazují, že většina lidí ve virtuální komunikaci lže.

Nesdělovat citlivé informace, které mohou být zneužitelné (např. osobní údaje, přístupová hesla), nesvěřovat se se svými problémy, neřešit svou sexualitu, být velmi opatrný v případě zveřejňování fotek.

Nechodit na osobní schůzku s osobou, kterou známe jen z internetu.

Kdo poradí, co udělat?

V těchto situacích je dobré poradit se s rodičem nebo učitelem. Lze použít i následující odkazy na instituce, které ti mohou pomoci:

Linka bezpečí
www.linkabezpeci.cz
bezplatná telefonní linka: 116 111

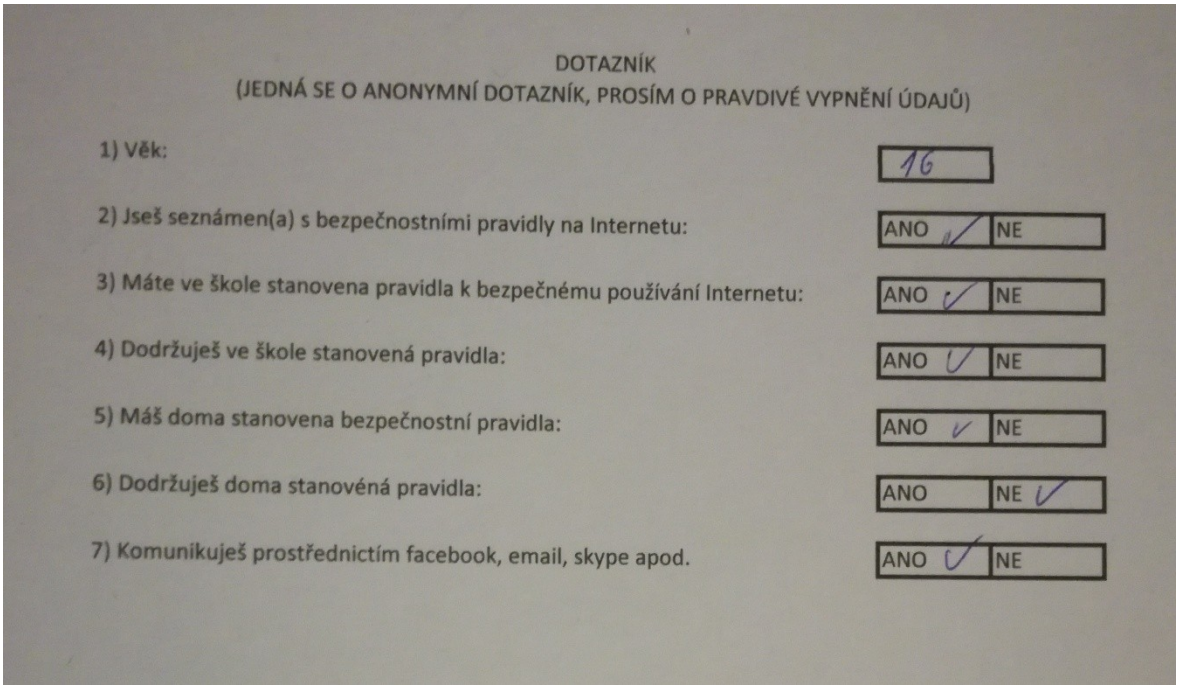
Online poradna E-Bezpečí
www.napisnam.cz

Policie ČR
http://aplikace.policie.cz/hotline/
telefon: 158

Seznam se bezpečně!
www.seznamsebezpecne.cz

Tento materiál vznikl v rámci projektu **Buď v bezpečí**,
realizovaného Policejním prezidiem ČR a projektem E-Bezpečí.

PŘÍLOHA P II: DOTAZNÍK



DOTAZNÍK
(JEDNÁ SE O ANONYMNÍ DOTAZNÍK, PROSÍM O PRAVDIVÉ VYPNĚNÍ ÚDAJŮ)

1) Věk:	16	
2) Jseš seznámen(a) s bezpečnostními pravidly na Internetu:	ANO ✓	NE
3) Máte ve škole stanovena pravidla k bezpečnému používání Internetu:	ANO ✓	NE
4) Dodržuješ ve škole stanovená pravidla:	ANO ✓	NE
5) Máš doma stanovena bezpečnostní pravidla:	ANO ✓	NE
6) Dodržuješ doma stanovéná pravidla:	ANO	NE ✓
7) Komunikuješ prostřednictím facebook, email, skype apod.	ANO ✓	NE