UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

MAGISTERSKÉ KOMBINOVANÉ STUDIUM

2011–2013

DIPLOMOVÁ PRÁCE

Danka Biľová

Rizika Internetu a internetové komunikace a jejich dopady na běžného uživatele

Praha 2013

Vedoucí diplomové práce:

doc. RNDr. Dana Procházková, DrSc.

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

MASTER COMBINED-TIME STUDIES

2011–2013

DIPLOMA THESIS

Danka Biľová

Risks of the Internet and Online Communication and Their Impacts on the Common User

Prague 2013

The Diploma Thesis Work Supervisor:

doc. RNDr. Dana Procházková, DrSc.

Prohlášení

Prohlašuji, že předložená diplomová práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpala, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne 23. 2. 2013 Danka Biľová

Poděkování

Zde bych chtěla poděkovat doc. RNDr. Daně Procházkové, DrSc., za její výjimečnou trpělivost při tvorbě předložené práce. V průběhu zpracování mi předala mnoho cenných poznatků a rad, které jsem v práci aplikovala. Velké poděkování patří občanům, kteří byli ochotni podělit se o mnohdy nepříjemné a bolestné zkušenosti s narušením jejich soukromí. Děkuji respondentům, kteří se zúčastnili dotazníkového šetření, i specialistům, kteří mi pomohli zorientovat se v technických oblastech kyberprostoru.

Anotace

Předložená diplomová práce se zabývá analýzou případů, které ovlivnily soukromí, bezpečí a životy běžných uživatelů Internetu. Pojednává o novodobém fenoménu, tj. o extrémním nárůstu komunikace na Internetu, zejména na sociálních sítích. Hodnotí rizika, která existují pro uživatele Internetu, i na reálných příkladech dokumentuje neopatrnost uživatelů samotných při surfování a on-line komunikaci. Diplomová práce identifikuje a analyzuje nejčastější bezpečnostní chyby, které uživatelé činí, a navrhuje opatření k eliminaci nežádoucích jevů ohrožujících bezpečí a další aktiva běžného uživatele Internetu.

Klíčová slova

Anonymita, bezpečí, bezpečnost, Internet, komunikace, kyberprostor, kyberzločin, počítač, rizika, sociální sítě, uživatel.

Annotation

The proposed Diploma Thesis deals with the analysis of cases which affected privacy, security and lives of common users of the Internet. The Thesis deals with the modern phenomenon, i.e. on the extreme increase of the Internet communication, especially on communication by means of social media. The Thesis evaluates the risks that exist for Internet users and on real-life examples documents a carelessness of users themselves during their surfing and online communication. The Thesis identifies and analyses the most common security mistakes that users make, and proposes measures to eliminate unfavourable phenomena that threaten security and other assets of the common Internet user.

Key words

Anonymity, security, safety, Internet, communication, cyberspace, cybercrime, computer, risks, social nets, user.

OBSAH

ÚVOD

Motto: Chování lidí na Internetu a sociálních sítích závisí především na morálce jejich uživatelů.

Internet je fenoménem posledních let, který otevřel dříve netušené možnosti komunikovat a snadno a téměř bezplatně se dostat prakticky k jakýmkoliv informacím. Čas, který lidé tráví u počítače, se neustále prodlužuje. Nejedná se pouze o pracovní činnost. Počítačová technika je nedělitelnou součástí každé průměrné domácnosti. Možnost neomezené komunikace je nespornou výhodou, na straně druhé je Internet nástrojem velmi často zneužívaným. Záleží pouze na úmyslu internetového uživatele. Občané, kteří využívají Internet k práci a k běžné komunikaci se světem, si často neuvědomují, jak obrovská rizika na ně v tomto virtuálním prostoru číhají. Internetoví predátoři, čekají na slabost druhé strany a disponují značnými kybernetickými dovednostmi. Rovněž obrovský rozmach technologií jim v posledních letech umožňuje uplatnit sofistikované způsoby, kterými realizují své úmysly. Internetoví útočníci zneužívají nejen technické nedokonalosti či neaktuálnosti příslušných softwarů, ale čím dále častěji se problematika přesouvá také do roviny psychologické, kde svými aktivitami působí na lidskou psychiku.

Důvodem, proč pro předloženou diplomovou práci bylo vybráno právě téma rizika internetové komunikace, je osobní zkušenost autorky a jejích blízkých se zneužitím Internetu a přímými dopady zneužití na jejich majetek, bezpečí i psychické zdraví.

Cílem práce je identifikovat nejčastější rizika spojená s používáním Internetu a internetové komunikace a identifikovat jejich dopady na běžného uživatele. V závěru práce jsou uvedena doporučení pro běžného uživatele, která by měl používat při používání internetu a zvláště pak při užívání sociálních sítí.

První kapitola pojednává o vzniku Internetu a jeho nyní téměř výsadním postavení mezi elektronickými médii. Popisuje základní služby, které Internet poskytuje, i jeho výhody, charakterizuje nejvyužívanější sociální sítě, prostřednictvím kterých komunikace na Internetu z větší části probíhá. Druhá kapitola definuje kyberzločin a hrozby Internetu z technického i sociologického pohledu. Popisuje typy uživatelů – predátorů, kteří Internet a internetovou komunikaci zneužívají k ilegálním aktivitám.

Rovněž popisuje psychopatologické jevy, jež jsou charakteristickým znakem pro internetovou komunikaci. Třetí kapitola uvádí konkrétní případy, ve kterých byl Internet a internetová komunikace zneužity k neetickým a nelegálním aktivitám. Čtvrtá kapitola popisuje metody, jež byly použity pro zpracování dat. Pátá kapitola obsahuje detailní analýzu a výsledky šetření a zpracování dat včetně tabulek. Následuje interpretace výsledků práce, závěr, přílohy a seznam použité literatury.

Metodika práce spočívá v dodržení všech zásad kladených na odbornou práci, tj. je proveden souhrn dosavadních odborných znalostí o cílech v oblasti internetové komunikace a jejich hrozeb a o schopnosti identifikovat rizika Internetu. Práce dále obsahuje vstupní data, která jsou zpracována písemně i formou dotazníku, grafů a tabulek, charakteristiku metod při zpracování dat, výsledky zpracování dat, jejich vyhodnocení a interpretaci, závěr a seznam použitých zdrojů.

TEORETICKÁ ČÁST

1 GENEZE VZNIKU INTERNETU

Internet způsobil ve světě počítačových a komunikačních technologií doslova revoluci. Vynálezy jako telegraf, telefon, rádio a počítač připravily půdu pro další stupeň komunikační technologie. Internet je technologií, která slouží k šíření informací a která má dnes celosvětové pokrytí. Je rovněž médiem pro spolupráci a interakci mezi jedinci a jejich počítači bez geografických hranic. Je symbolem úspěchu z pohledu vývoje v oblasti informačních technologií a infrastruktur.

Jeho historie sahá do šedesátých let minulého století. Informace, které objasňují důvody vzniku, jsou u jednotlivých zdrojů rozdílné. Některé prameny uvádějí, že se zrodil jako produkt studené války mezi Východem a Západem. Měla to být reakce USA na vypuštění Sputniku, první umělé družice země, ve snaze získat zpět dominantní postavení ve světě technologií.

Stránky www.internetsociety.org v souvislosti s počátky internetu zmiňují J. C. R. Licklidera jeho Galactic Network Concept, ve kterém v srpnu 1962 popsal určité sociální interakce, jež měly být uskutečněny prostřednictvím sítí. Představoval si globálně propojenou síť počítačů, přes kterou by měl kdokoliv rychlý přístup k různým datům a programům.[1] Lidicker byl prvním vedoucím počítačového výzkumného programu pro ARPA.[2]

V roce 1965 se vědcům Lawrence G. Robertsovi a Thomasu Merrillovi podařilo spojit dva počítače, jeden v Massachusetts a druhý v Kalifornii, nízko rychlostním připojením prostřednictvím vytáčené telefonní linky, čímž potvrdili přesvědčení Leonarda Kleinrocka o nutnosti přepojování paketů.

Roberts později, již jako zaměstnanec DARPA, pracoval na vývoji konceptu počítačové sítě a dal dohromady plán pro počítačovou síť Advanced Research Projects Agency Network (dále jen ARPANET), jenž byl publikovaný v roce 1967.

[1] INTERNET SOCIETY. *Brief History of the Internet*. [online]. © 2012 [cit. 2012-05-05]. Dostupné z: http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet/#Origins

[2] *ARPA (The Advanced Research Project Agency)*, v roce 1996 změnila název na DARPA – Defence Advanced Research projects Agency (Agentura pro výzkum pokročilých obranných projektů).

V roce 1969 byla pomocí čtyř hostitelských počítačů vytvořena první experimentální síť ARPANETu. Projekt byl poprvé představen veřejnosti v roce 1972. Ve stejném roce byla představena další novinka – elektronická pošta, která se během dekády stala největší síťovou aplikací.

V těchto souvislostech je třeba zmínit jméno Douglase Engelbarta, amerického vynálezce a průkopníka v počítačové technologii, který vynalezl jako první počítačovou myš.

V současné době je Internet nedílným nástrojem používaným dennodenně v běžném životě. Mezi jeho základní vlastnosti patří globální pokrytí. Celková penetrace Internetu se v jednotlivých oblastech světa liší, ale dopady na společnost jsou celosvětové. Další důležitou vlastností je jeho decentralizovanost, Internet nemá ústřední řízení, žádná centrální autorita o jeho existenci, formě, ani působnosti nerozhoduje. Funguje na bázi dohod provozovatelů a uživatelů.

Každý, kdo splní předepsaná kritéria, se k Internetu může připojit, může se ve vytvořeném virtuálním prostoru volně pohybovat, komunikovat anebo ho i zneužívat.

1.1 Služby a výhody Internetu

Internet nabízí několik standartních služeb, jejichž prostřednictvím fungují jednotlivé uživatelské aplikace. Mezi základní služby patří:

- *WWW (World Wide Web)* – nejvíce využívaná služba internetu, systém webových stránek zobrazovaných pomocí webového prohlížeče. Slouží ke zveřejnění různých informací. Výhodou jsou nízké pořizovací i provozní náklady a možnost jejich pravidelných aktualizací. Stránky jsou vytvořeny v jazyku HTML (Hyper Text Markup Language), jehož hlavní výhodou je využití hypertextu.
- *HTTP, HTTPS (Hyper Text Transfer Protocol*) – služby pro přenos hypertextových stránek. Prostřednictvím předmětného protokolu se data přenášejí do počítače. Běžně se používá protokol HTTP, pro zabezpečený přenos protokol HTTPS (Hyper Text Transfer Protocol Secure).

- *E-mail (Electronic mail)* – elektronická pošta, umožňuje přenos a doručování zpráv po sítí uživatelům do schránek na poštovních serverech. Zprávy můžou obsahovat různé přílohy. Každý uživatel má na poštovním serveru přidělenou schránku. Pro přenos zpráv používá protokol SMTP (Simple Mail Transfer Protocol), pro stahování e-mailových zpráv ze vzdáleného mailu na klienta používá protokoly POP 3 (Post Office Protocol), IMAP (Internet Message Access Protocol). Elektronická pošta vznikla v roce 1965, v roce 1972 byla představena veřejnosti a poprvé byl použit znak @ (čes. zavináč; angl. at) sloužící k oddělení jména uživatele od domény.
- *FTP (File Transfer Protocol)* – služba, která umožňuje obousměrný přenos dat.
- *VoIP (Voice over Internet Protocol)* – telefonování pomocí Internetu, např. Skype – umožňuje provozovat videohovory i chat.
- *DNS (Domaine Name System)* – domény (systém jmen počítačů pro snadnější zapamatování).
- *Skype* – proprietární protokol.
- Další služby a protokoly (např. online hry).

Připojení k Internetu se v současnosti realizuje prostřednictvím: telefonní linky (majitelem je telefonní operátor); pozemní bezdrátové datové sítě; kabelové přípojky; mobilní telefonní sítě; satelitní datové sítě; či elektrické napájecí sítě.

Internet je svou přirozeností ambivalentní médium, které není samo o sobě ani dobré ani špatné. Dobré je, pokud slouží člověku a pomáhá mu. Vše však záleží pouze na chování osoby, jež Internet používá.

Dnes se pracuje s informacemi. Jsou pro byznys klíčové, zejména jejich aktuálnost a možnost rychlého vyhledání. Cena za získání informace, kterou je možné na Internetu najít, je v podstatě nulová, nepočítáme-li poplatek za připojení. Obrovskou výhodou je nejen pravidelná aktualizace a rychlost publikování informací, ale i možnost dohledání souvisejícího materiálu, včetně archivů. Internet je nesmírně efektivní komunikační médium. Vyhledávání informací umožňují internetové vyhledávače, ve světě například Google, Yahoo!, Bing. V České republice se jedná o Seznam.cz, Centrum.cz nebo Atlas.cz.

Nejpoužívanějším vyhledávačem na světě je Google. Byl založen v roce 1998, má 1000 milionů uživatelů a výnos pro společnost Google jen za poslední čtvrtletí roku

2011 představovalo 10,58 miliard amerických dolarů.[3] Název vychází ze slova „googol“ označujícího číslo složené z jedničky a stovky nul.[4] Z názvu se odvodilo často používané sloveso googlovat – hledat.

Z komerční stránky je Internet naprosto nepostradatelnou součástí marketingu a obchodu. E-commerce je na vzestupu především díky dostupnosti, pohodlí pro uživatele a kupující, cenovým zvýhodněním oproti standardním způsobům prodeje i interaktivním formám reklam, podpoře produktů a nižším cenám.

Jednou z nejmarkantnějších výhod Internetu je možnost komunikace. Elektronická komunikace téměř vytlačila dříve standardní komunikační prostředky (dopisy, faxy, dálnopisy). Díky existenci datových schránek se zjednodušila i úřední komunikace v administrativě.

Internet je stále považován za svobodné médium, za prostředek, který nabízí mnoho úhlů pohledu na problém. Už to nejsou pouze vyvolení, již prostřednictvím zpráv, televize, tisku a rozhlasu rozhodují o tom, jak budeme vnímat dění kolem nás, společnost, politiku, morální hodnoty a kulturu. Internet poskytuje způsoby k vyjádření názorů, zprostředkovává názory těch, kteří mají potřebu se vyjádřit i příspěvky osob, jež nemají přístup k tvorbě zpravodajství a publicistiky.

Internet je svobodným médiem i přes tendence o sledování pohybu uživatele v kyberprostoru. Koncem ledna 2012 ohlásil Google nové zásady ochrany osobních údajů. Namísto odlišných pravidel u různých produktů platí nyní pro zaregistrovaného uživatele stejná pravidla pro všechny produkty Google. Předmětný vyhledávač nyní sbírá informace o uživateli, respektive o jeho aktivitách a o jeho surfování po Internetu, s cílem zvýšit bezpečí uživatelů. Nová pravidla vyvolala spoustu negativních ohlasů uživatelů kvůli obavám o intruzi do jejich soukromí. Google na negativní stanoviska reagoval vysvětlením o údajném zlepšení služeb s ohledem na možnosti efektivnějšího vyhledávání a zlepšení péče o své uživatele.

Formy, rychlost, kreativita, snadná dostupnost informací, názorů, diskusí, interaktivní komunikace, to všechno jsou obrovské plusy pro internetový virtuální svět.

---

[3] GOOGLE INVESTOR RELATIONS. *Google Announces Fourth Quarter and Fiscal Year 2011 Results.* [online]. [2012-05-13]. Dostupné z: http://investor.google.com/earnings/2011/Q4_google_earnings.html

[4] GOOGLE COMPANY. *Our history in depth.* [online]. [cit. 2012-05-13]. Dostupné z: http://www.google.com/intl/en/about/company/history/

Internet boří hranice a čas, umožňuje komunikaci v reálném čase (Skype, chat, ICQ[5]) nebo i s jistým časovým zpožděním (vzkazy, e-mail, blogy). Internet neutralizuje etnické, kulturní, sociální i psychologické bariéry.

Každá výhoda má však i své stinné stránky. Možnost komunikovat bez omezení generuje mnoho rizik. Jejich identifikace a vysoce škodlivé dopady (nové hrozby) budou popsány v dalších kapitolách.

1.2 Sociální sítě

Sociální sítě, též společenské sítě či komunity (angl. social networks, social media), bezpochyby revolucionizovaly web. Začaly se rozvíjet v polovině 90. let minulého století v USA. Nejdříve jejich prostřednictvím komunikovali zejména studenti. Objevily se stránky s prvními profily a skupiny přátel. V současné době mezi hlavní sociální sítě řadíme Facebook, Twitter, MySpace, LinkedIn, Google+. V České republice pak např. Ukaž se, Líbím se Ti, Lidé.cz, Spolužáci.cz.

Sociální sítě lze ve zkratce popsat jako virtuální navazování vztahů. Můžeme je definovat jako spojení určitých jednotlivců nebo organizací, které jsou vázány přátelstvím, příbuzenstvím, společným zájmem, profesním zařazením, vztahy, včetně sexuálních, např. "I just made love", vztahy znalostí apod. Uživatelé vycházejí z tradičních sociálních skupin.

Uživatelé vytvářejí v rámci sociální sítě určité „uzly", které si můžeme představit jako páteřní body pro rozvíjení nových vazeb. Je pravdou, že na jedné straně sociální sítě můžou sloužit pro: společný zájem; sdružení členů (např. určitého etnika); zábavu; sdílení obsahu, videí, fotek; komunikaci (chat, nebo přes prohlížeč – ICQ); vytváření nových sociálních vazeb; hraní her; hledání zaměstnání; inzerci; reklamu.[6] Na druhé straně existuje také reálné nebezpečí, že mohou být zneužity proti jednotlivým uživatelům.

[5] *ICQ (I Seek You)* – software pro Internetovou službu, která umožňuje uživatelům sledovat připojení přátel a komunikovat s nimi.
[6] SOCIAL NETWORKING. [online]. © 2006–2012 [cit. 2012-05-15]. Dostupné z: http://www.whatissocialnetworking.com

Sociální sítě mají obrovský potenciál nejen pro komunikaci a obchodní činnost, ale i pro bezpečnostní hrozby, které jsou nezanedbatelné. Lidé na sebe chtějí v jistém smyslu upozornit, publikují větší a větší množství osobních a citlivých informací. Podle provedených šetření například Facebook ví o svém průměrném uživateli mnohem více, než Federal Bureau of Investigation (dále jen FBI) nebo Central Intelligence Agency (dále jen CIA).[7] Z důvodu publikování mnohdy citlivých dat a nízkého zabezpečení uživatelských účtů dochází ve velkém k únikům osobních údajů, ke zneužití soukromých informací, k pronásledování, šikaně, nabouráním se do účtů za účelem zcizení identity apod.

Nežádoucí jevy, které se na sociálních sítích a Internetu obecně čím dál častěji objevují, mnohdy dokážou způsobit uživatelům psychická traumata, sociální diskvalifikaci a ekonomické problémy, v některých případech dochází i k sebevraždám. V politické rovině rovněž dochází k manipulaci s veřejným míněním.

1.3 Druhy sociálních sítí

Facebook (www.facebook.com) – nejrozšířenější sociální síť na světě. Předmětné sociální síti a popisu jejího fungování je – v teoretické i praktické předložené diplomové práce věnována největší pozornost, protože se jedná o nejrozšířenější sociální síť a komunikační prostředek v České republice.

Facebook je uzavřenou sociální sítí, po jejímž vzoru vznikly další obdobné projekty. Původně ji Mark Zuckerberg založil jako komunikační portál pro studenty Harvardovy univerzity. Postupem času byl portál rozšířen i na další univerzity v USA a později i pro schválené zahraniční univerzity. V České republice se jako první připojila Masarykova univerzita v Brně. Pro veřejnost síť funguje od roku 2006.

[7] CAMERON, K. *Kim Cameron´s Identity Webblog.* In: *24 year old student lights match: Europe versus Facebook.* [online]. © 13. 10. 2011 [cit. 2012-05-12]. Dostupné z: http://www.identityblog.com/?p=1201

Měsíčně jej využívá 901 milionů uživatelů (12 % populace),[8] denně přibližně 483 milionů osob, přičemž z 80 % se jedná o uživatele mimo území USA a Kanady. Facebook existuje ve více než 70 jazykových mutacích.[9]

Facebooková adresa je v současné době používána mnohem častěji jako standardní webová adresa, protože pro obchodní společnosti je nyní mnohem snazší kontaktovat klienta prostřednictvím Facebooku.

Facebook byl kompletně lokalizován i do českého prostředí, oficiální kancelář v ČR nemá. Evropská zastupitelství jsou v Amsterdamu, Paříži, Bruselu, Madridu, Miláně a Stockholmu.

Na Facebooku je možné zakládat i oficiální stránky (pages), a proto je aplikace využívána zejména firmami a celebritami, které daným způsobem komunikují se svými příznivci či fanoušky (likers).

Odběry – uživatel Facebooku se může dobrovolně rozhodnout o poskytování informací, které na Facebooku publikuje, i dalším uživatelům, které nemá mezi přáteli. Předmětné příspěvky se automaticky objevují na zdi „odběratelů".

V roce 2011 Facebook představil novou funkci Timeline, jež chronologicky seřadí všechny příspěvky od registrace uživatele na Facebook až po ty naposled publikované.

Právě předmětná funkce byla terčem kritiky z důvodu ochrany osobních údajů. Dle reakcí na on-line fórech funkce Timeline údajně udržuje všechny příspěvky již jednou publikované v archivu a není možné nic smazat trvale. V souvislosti s problematikou Timeline vyšlo na povrch, že v podstatě všechny publikované příspěvky jsou a vždy byly v útrobách Facebooku.

I po zrušení uživatelského účtu si Facebook ponechává data, fotky a příspěvky uživatelů, za co byl již opakovaně kritizován médii i veřejností. Akt požadující vymazání předmětných údajů je právně nevymahatelný, protože uchovávání osobních dat i po zrušení účtu je jednou z podmínek, se kterou musí uživatelé při registraci souhlasit.

Zakladatel Facebooku Mark Zuckerberg tvrdí, že soukromí je mrtvé a není již společenskou normou.[10] Podle Zuckerberga jsou lidé stále otevřenější a nemají žádný

[8] CZECH TECHNICAL UNIVERSITY: *International konference: CyberTerrorism and CrimeConference CYTER 2012*. [CD-ROM]. Praha: CVUT Praha. 2012. [cit. 2012-07-07]. ISBN 978-80-01-05072-9.
[9] FACEBOOK COMPANY. *Newsroom.* [online]. [cit. 2012-05-12]. Dostupné z: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

problém zveřejňovat informace o svém soukromí a životě. Konečně na zmíněném principu je Facebook založen. Na jedné straně je dobré sdílet názory, fotky a zážitky s přáteli, na straně druhé je nutné si uvědomit hranici, za kterou není dobré zajít a že není žádoucí, aby do soukromí viděl kdokoliv, kdo si vzpomene.

Soukromí lze nastavit tak, že uživatel může regulovat vizuál svého profilu pro úplně neznámé lidi. Pokud kdokoliv zadá své jméno do vyhledávače, například Google nebo Seznam, velice rychle najde i konto na Facebooku.

Podle nastavení účtu a soukromí se různým uživatelům zobrazí údaje o tom, s kým se daná osoba přátelí, jaké jsou její zájmy, názory a preference. „Riziku vyhledání" facebookového účtu je možné vyhnout se tak, že se zruší povolení veřejného vyhledávání. Osoby, které již na Facebooku zaregistrované jsou, uvidí pouze data, jež jim uživatel povolí v základních nastaveních.

V praxi se lze setkat s názorem, že člověk, který nemá účet na Facebooku, není normální. Některé firmy údajně získávají informace o žadatelích o práci i prostřednictvím Facebooku. Snaží se tak získat pravý obraz o jejich názorech, zvycích, způsobu jejich standardní komunikace a chování, projevech, které při běžném pohovoru nelze zjistit. V případě, že žadatele pod jeho vlastním jménem na Facebooku nenaleznou, budí to podezření, že se jedná o jakousi osobnostní zvláštnost, protože na Facebooku údajně určitě je, pouze se pohybuje pod skrytou identitou (nickem). Je proto rozšířen i názor, že Facebook se stal fenoménem, jakousi součástí životů většiny populace.

Twitter (https://Twitter.com) – nejpopulárnější mikroblogovací systém na světě umožňující psát, číst a přeposílat texty o 140 znacích. Texty se nazývají *tweety* (angl. tweets) a zobrazují se na stránce uživatele a jeho odběratelů (followers). Sledování určitého uživatele se nazývá *following*. Uživatelé dostávají nebo odesílají tweety přes stránku Twitteru pomocí sms zpráv nebo externích aplikací. Je možné nastavit odesílání tweetů tak, aby je neviděly osoby, kterým to uživatel nedovolí.

Uživatel si své kamarády (followers) nevybírá sám, ale followers si vybírají uživatele podle toho, co píše. Čím jsou příspěvky a informace publikované uživatelem zajímavější, tím více následovníků má. Celebrity velmi často využívají předmětnou

[10] O´BRIEN.T. *Facebook´s Mark Zuckerberg Clamis Privacy is Dead*. [online]. © 11. 1. 2010 [cit. 2011-05-12]. Dostupné z: http://www.switched.com/2010/01/11/facebooks-mark-zuckerberg-claims-privacy-is-dead/

formu komunikace se svými fanoušky – followers, protože obrovskou výhodou Twitteru je komunikace v reálném čase. Uživatel si může složit vlastní sociální síť z popových hvězd, spisovatelů, politiků a nechat je vstoupit do jeho života.

LinkedIn (www.linkedin.com) – sociální síť pro profesionály. Sociální síť orientovaná na obchodní kontakty láká manažery a personalisty více než obecněji zaměřené projekty.

V profilu uživatele se zobrazuje prioritně kariéra, pracovní místo a vzdělání. Profily jsou publikovány výhradně v anglickém jazyce. Uživatelé LinkedIn často již neposílají zaměstnavatelům životopisy, ale link na svůj profil. LinkedIn je častým pomocníkem personalistů a headhunterů, kteří mají možnost hledat mezi obrovským množstvím potenciálních zaměstnanců, a kteří prostřednictvím sítě mohou přímo kontaktovat uživatele za účelem nabídky zaměstnání. V tomto případě hraje důležitou roli zpracování profilu, jeho forma, publikování významných projektů i profesionální historie a dosažených kariérních stupňů. Celosvětově má LinkedIn přes 35 milionů uživatelů, stále častěji jej využívají i Češi. Kromě životopisu nabízí LinkedIn nejrůznější skupiny a aplikace, nebo vyhledávání bývalých i současných kolegů ze sítě. Prostřednictvím dané sítě je velmi snadné (i bez nutnosti registrace) zjistit mnoho informací o uživateli, který má vytvořený profil.

MySpace (www.myspace.com) – populární síť využívaná často ke sdílení hudby a videa. K šíření svého díla ji využívají i profesionální umělci. Před nástupem Facebooku šlo o absolutní jedničku ve stejné kategorii sítí, podle mnohých ve sdílení multimediálního obsahu stále nemá konkurenci. Sloganem sítě je „A place for friends“ (Místo pro přátele). Z důvodu ochrany dětí je síť přístupná pouze uživatelům starším 14let.

Google+(https://plus.google.com) – pátá největší sociální síť, jež je provozována společností Google. Používá ji 170 milionů uživatelů.[11] Její provoz byl zahájen 28. června 2011, prvotní investice představovala 585 milionů amerických dolarů. Původně byla síť zpřístupněna pouze na pozvánky a pro limitovaný počet uživatelů. Nyní je přístupná pro každého.

[11] CZECH TECHNICAL UNIVERSITY: *International konference: CyberTerrorism and CrimeConference CYTER 2012*. [CD-ROM]. Praha: CVUT Praha. 2012. [cit. 2012-07-07]. ISBN 978-80-01-05072-9.

Spolužáci.cz (www.spoluzaci.cz) – sociální síť, provozovaná serverem Seznam.cz. Sdružuje v rámci České republiky spolužáky ze všech typů škol (od základních až po vysoké). Systém je členěn do měst, jednotlivých škol a následně do tříd. Síť slouží ke komunikaci mezi spolužáky a ke sdílení studijní problematiky.

Dead Soci.al (www.deadsoci.al) – bizarní sociální síť byla založena podnikatelem Jamesem Norrisem v roce 2012 a umožňuje posílat zprávy „post mortem“. Uživatelům umožňuje bezplatně publikovat zprávy, fotky, videa a audio nahrávky na Facebook, Twitter, LinkedIn i poté, co zemřou. Uživatel si může pomocí kalendáře naplánovat statusy, které se budou v předem daných časových intervalech objevovat na jeho profilu. Zakladatel sítě se inspiroval facebookovou Timeline, která chronologicky zobrazuje život člověka od narození, tudíž posmrtnou konverzaci považuje za další logický krok. Spuštění dané služby vyvolalo silné kontroverzní reakce ve světě, nicméně sociální síť standardně funguje.

So.cl (www.so.cl) – nejnovější sociální síť byla založena 20. května 2012 Microsoft Fuse Labs. Prozatím se jedná o experimentální výzkumný projekt, jehož vývoj stále probíhá a jehož cílem není konkurovat zavedeným sociálním sítím. Projekt se zaměřuje na studenty a studující, kteří chtějí využívat Internet ke vzdělávání. Účelem je profitovat z „moudrosti mas“ prostřednictvím kombinovaného vyhledávače. To, co uživatel hledá, vidí ostatní uživatelé, kteří pak nabízí způsoby i vlastní výsledky hledání k relevantnímu tématu.

K přihlášení je nutné mít účet na Facebooku nebo Windows live ID. Nevýhodou pro český trh je především skutečnost, že So.cl využívá vyhledávač Bing, který není pro Českou republiku přizpůsoben, proto výsledky nejsou optimální.

S údaji, týkajícími se potřeby a touhy sdělování či prezentace soukromí jednotlivců, které často uvádí zakladatelé a propagátoři sociálních sítí, a které mluví ve prospěch předmětných sítí, není možno bez výhrady souhlasit. Proti jejich výrokům svědčí v praxi mnohokrát potvrzené výsledky výzkumu i poučení získaná důkladnou odbornou analýzou problémů, které řešili záchranáři při velkých katastrofách, např. u mnoha lidí evakuovaných po velkých živelných pohromách (zemětřesení, hurikány apod.) dochází po cca pěti dnech v evakuačních táborech, kde je o ně dobře postaráno, k psychickým

problémům, protože jim chybí soukromí.[12] V dané souvislosti je třeba také zmínit Maslowovou pětiúrovňovou pyramidu lidských potřeb, kde hned po fyziologických potřebách, které jsou logicky hodnoceny jako nejpodstatnější, následuje na druhém místě potřeba bezpečí, jistoty, jak ve smyslu jistoty např. zaměstnání, ale také ochrany před agresory apod.

[12] PROCHÁZKOVÁ, D. *Krizové řízení, havarijní plánování a ochrana obyvatelstva*. České Budějovice: VŠERS, o. p. s., 2009. s. 96. ISBN 978-80-86708-86-7.

2 OCHRANA KYBERPROSTORU A KYBERZLOČIN

Jednou z hlavních charakteristik Internetu je jeho anonymita. Je to znak, který se objevuje v mnoha definicích a popisech kyberprostoru. Anonymita je pro uživatele osvobozující, boří mnoho bariér. Současně však je příčinou nebývalého rozmachu kriminality v kyberprostoru. Útočníci disponují silnými zbraněmi, kromě anonymního jednání i sofistikovanými technickými prostředky. Internet se používá pro sexuální zneužívání dětí a obchodování s lidmi, anonymita podporuje komunikaci mezi nejrůznějšími teroristickými skupinami.

Mladá nastupující generace si práci s technologiemi osvojuje mnohem lépe než starší ročníky, které už mají své místo ve společnosti a Internet spíše využívají jako prostředek k běžné komunikaci a byznysu. Obrovský rozmach technických vymožeností, nastupující tendence neakceptování zažitých etických norem ve spojení s anonymitou naznačují, že lze v souvislosti s nelegálním a nemorálním jednáním v kyberprostoru očekávat zhoršení stavu.

Obtížnost sledování projevů počítačové kriminality spočívá v tom, že se odehrávají v prostředí, které je objektivně velmi obtížně vnímatelné. V současném období krize lze očekávat nárůst kybernetické kriminality, protože se jedná o rychlý, bezpečný a vysoký zisk, právě kvůli důmyslně propracovaným praktikám útočníků a malým možnostem vystopovat a prokázat trestný čin. S kybernetickou kriminalitou nesouvisí pouze jeden specifický druh trestné činnosti, ale různorodé nelegální a zakázané aktivity, jež sdílejí společné unikátní prostředí, kterým je právě kyberprostor.[13]

Možnosti Internetu jsou nyní téměř neomezené a pachatelé mají před vyšetřovacími orgány téměř vždy náskok. V prostředí kyberprostoru, kde je aplikována řada technologií, je nesmírně složité evidovat, dokumentovat, vyšetřovat a dokazovat trestnou činnost, protože všichni používají Internet, tj. síť realizovanou pomocí technologie, která výrazně posunula rozvoj lidské společnosti. Současný problém je

[13] YAR, M. *Cybercrime and society. Crime and punishment in information age*. [online]. 1st edition. London; Thousand Oaks, CA: Sage publications, 2006. [cit. 2012-08-10]. ISBN 1-4129-0753-5. Dostupné z: http://aleph.nkp.cz/F/?func=file&file_name=find-b&local_base=nkck

v tom, že kybernetické sítě, které zajišťují její využití, nejsou dosud konstruovány tak, aby byly bezpečné.[14]

2.1 Kyberprostor a kyberzločin

Kyberprostor lze definovat jako mentálně vytvořené virtuální prostředí, v rámci kterého probíhají propojené počítačové aktivity.[15]

Za tvůrce termínu je považován William Gibson, jenž ho použil ve svém slavném kyberpunkovém románu Neuromancer z roku 1984: *„I když se předmětný termín poprvé objevil v roce 1982 v jeho povídce ‚Burning chrome', do širšího povědomí pronikl právě románem Neuromancer.*"[16]

Autor vytvořil osobitý, fiktivní svět a jazyk (pojmy kyborg, klon, simulakra, matrix apod.). Kyberpunk představuje víru v používání technologií k podpoře a kultivaci individualismu a připouští možnost sebeurčení lidské bytosti. Uvedené znaky se v devadesátých letech minulého století prolínaly se sci-fi literaturou, až se pojetí kyberkultury stalo součástí běžného života.

Kyberprostor je virtuální realitou, která funguje paralelně se skutečnou realitou. Dle Gibsona je možné jej navštívit po přímém napojení mozku k počítači prostřednictvím elektrod a lze se v něm pohybovat bez rušivých vlivů technologického zprostředkování.

John Barlow, zakladatel Electronic Frontier Foundation, považuje za kyberprostor existující počítačové sítě a vlastně veškeré telekomunikační sítě.[17] Podle Barlowa se v kyberprostoru nalézáme například ve chvílích, když telefonujeme.

Z historie vzniku kybernetiky a informatických oborů víme, že za zakladatele kybernetiky je považován Norbert Wiener, americký matematik, který pro ni v roce 1947 vytvořil název odvozený z řeckého slova „χυβερνητης", jež znamená kormidelník.

Pod pojmem kybernetická kriminalita rozumíme jednání, kterým je porušován zákon nebo které je v rozporu s morálními regulemi společnosti. V anglické literatuře se

[14] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury.* Praha*:* ČVUT, 2012. s. 186–189. ISBN 978-80-01-05103-0.
[15] WALL, D. S. *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge; Malden MA: Polity Press, 2007. s. 221. ISBN 978-0-7456-2735-9.
[16] JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vyd. Praha: Grada, 2007. s. 17. ISBN 978-80-247-1561-2.
[17] Tamtéž, s. 17.

používá termín „cybercrime“ a pojem může – zjednodušeně řečeno – znamenat jakýkoli čin, který směřuje k narušení nebo zneužití počítače nebo počítačového systému a informací, které obsahuje. Hmotné škody způsobené počítačovou trestnou činností se ročně pohybují v desítkách miliard dolarů.[18]

„V případě kybernetických zločinů je nutné rozlišovat, zda se jedná o zločin směřovaný přímo proti počítačům (hardwaru, sítím, softwaru, datům) nebo o zločin vedený pomocí počítačů, tj. případ, kdy je počítač použit jako zbraň.“[19]

Novým trendem je prodej crimeware toolkit, tj. hotového software v podobě produktů sloužících k průniku do počítače a k vykonání specializovaných aktivit (zcizení dat, monitorování psaní na klávesnici daným uživatelem k vystopování hesel k účtům a citlivým datům, tzv. „keylogger“[20] apod.).

Pachatelé pracují v prostředí, ve kterém se mohou velmi sofistikovaně pohybovat, měnit identity a rychle mizet. Výhodou pro útočníky a nevýhodou pro vyšetřovatele je i variabilita existence i výkladu právních předpisů v různých státech.[21]

Existuje více pohledů na kategorizaci pachatelů trestních činů. Motivací je mnoho, například finanční zájem, konkurenční boj, kyberválka, kyberterorismus (špionáž, kritická infrastruktura), hacktivismus[22]. Obecně je lze rozčlenit do čtyř základních motivačních sektorů[23] (model kvadrantové kružnice), kterými jsou: pomsta, výstřednost, publicita a finanční zisk.

Sektory jsou graficky uspořádány tak, aby proti sobě ležely motivační impulsy, které se navzájem vylučují, a naopak vedle sebe jsou umístěny sektory, které se mohou prolínat. V uvedených čtyřech motivačních sektorech je umístěno osm základních skupin pachatelů, u nichž je navíc vyjádřena i úroveň jejich technologických znalostí

[18] BUSINESSIT. *Kybernetická kriminalita III. Nakročeno ke kyberterorismu*. [online]. © 2011–2013 [cit. 2012-8-10]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-nakroceno-ke-kyberterorismu.php

[19] PŘIBYL, T. *Kyberzločin*. [online]. © 5. 6. 2006 [cit. 2012-8-12]. Dostupné z: http://computerworld.cz/securityworld/kyberzlocin-46339

[20] Keylogger program snímá úhozy na klávesnici a současně printuje monitor při každém dotyku klávesy. Tímto způsobem program zjistí potřebná hesla a následně je bezprostředně odešle čekajícímu útočníkovi, který má okamžitý přístup ke kompromitovanému bankovnímu účtu.

[21] WALDEN, I. *Computer crimes and digital investigations*: *the transformation of crime in the information age*. 1st edition. Oxford: Oxford University Press, 2007. s. 127. ISBN 978-0-19-929098-7.

[22] Spojení hackingu, aktivismu, technologií a politiky, hacking k politickým účelům.

[23] KOLEKTIV AUTORŮ. *Sborník příspěvků z konference. Dětská kybernetická kriminalita a sociální sítě*. Jihlava: Vyšší policejní škola MV, 2011. s. 73. ISBN 978-80-260-0723-4.

a dovedností (novic, kybernetický chuligán, vnitřní nepřítel, malý zlodějíček, stará garda, autor virů, profesionální kriminálník, informační válečník).[24]

Před lety byly cílem útoků počítače samotné, nyní je trend zcela jiný, počítače se čím dále častěji stávají „prostředníkem“ pro provádění nelegálních činností. Útočníci našli mnohem atraktivnější cíle, než jsou samotné počítače soukromých uživatelů. Zaměřením útoku lze snadno odhalit profesionalitu útočníka. Pokud se jedná o útok, jehož cílem je zničit počítač, je útočník považován za amatéra. Profesionálové nemají v úmyslu počítač zničit, naopak, potřebují ho jako prostředníka k páchání trestné činnosti. „*Pomocí virtuálních počítačových útoků lze získávat reálné finanční prostředky*.“[25]

U kyberkriminality je zásadním faktem skutečnost, že společnost má k problému obecně laxní postoj z důvodu značné neúspěšnosti při vyšetřování a postihu a jeho vnímání společností je zatíženo jeho nehmotným charakterem.

Jarkovský ve své knize Kybernetová kriminalita srovnává běžnou ozbrojenou bankovní loupež s kybernetickým zločinem obdobného charakteru,[26] viz tabulka 1. Podkladem pro srovnání byly statistiky amerického FBI.

[24] RAK, R., KUMMER, R. *Motivace a znalosti pachatelů kybernetické trestné činnosti*. [online]. © 19. 12. 2006. [cit. 2012-8-26]. Dostupné z: http://computerworld.cz/securityworld/motivace-a-znalosti-pachatelu-kyberneticke-trestne-cinnosti-46254
[25] PŘIBYL, T. *Kyberzločin.* [online]. © 5. 6. 2006 [cit. 2012-8-12]. Dostupné z: http://computerworld.cz/securityworld/kyberzlocin-46339
[26] JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vyd. Praha: Grada, 2007. s. 30. ISBN 978-80-247-1561-2.

Tabulka 1: Základní výsledky srovnání bankovní loupeže s kybernetickým zločinem

Parametr	**Průměrné ozbrojené přepadení**	**Průměrný kybernetický útok**
Nebezpečí	Pachatel riskuje, že bude zraněn nebo zabit	Bez fyzického zranění
Zisk	Průměrně 3 až 5 tisíc amerických dolarů	Od 50 do 500 tisíc amerických dolarů
Pravděpodobnost dopadení	Dopadeno 50 až 60 % pachatelů	Dopadeno cca 10 % útočníků
Pravděpodobnost odsouzení	Odsouzeno 95 % dopadených pachatelů	Z dopadených útočníků dojde k soudnímu pojednávání pouze u 15 % útočníků a z nich je skutečně odsouzeno pouze 50 %
Trest	Průměrně 5 až 6 let, pokud pachatel někoho nezranil	Průměrně 2 až 4 roky

Zdroj: JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

Z tabulky 1 a dalších statistik FBI vyplývá, že pokud je kybernetický útok úspěšný, vede k daleko většímu zisku pro pachatele při mnohem menším předpokladu odhalení a trestu v porovnání se „standardním“ fyzickým přepadením. Za kyberzločin se považuje i nelegální stahování software, což velká část občanů neshledává jako porušení zákona, spíše za chytrost, a proto uvedená problematika je vnímána mnohem benevolentněji než klasická krádež.

Je třeba uvést, že stále ještě exaktní definice kyberzločinu. Mezi jeho základní charakteristiky patří: technická komplexita (naplňující člověka na jedné straně pocitem bezpečí a na druhé straně obavami z „Velkého bratra“), rychlý vývoj (zvyšování zranitelnosti a rozšiřování možnosti porušování práv) a kryptografie (jako prostředek ochrany a překážka odhalení pachatelů).[27]

[27] GŘIVNA T., PONČÁK, R. *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008. s. 34. ISBN 978- 80-903786-7-4.

Definice kyberzločinu, která je v právním diskurzu více méně akceptována, definuje kyberzločin kumulativně jako*:*

a) trestný čin ohrožující informační a komunikační technologie (dále jen ICT), informační a síťovou bezpečnost (trestný čin proti počítačové integritě nebo také trestný čin v úzkém pojetí);

b) trestný čin využívající ICT ke spáchání tradičních trestných činů (trestný čin vztahující se k počítačům);

c) *trestný čin vztahující se k obsahu, jako například dětská pornografie, pomluva a porušení práv k duševnímu vlastnictví (trestný čin vztahující se k obsahu počítačových dat).*“[28]

Samotný koncept kyberzločinu jako vedlejšího efektu informační revoluce a jejího nejslavnějšího produktu – Internetu – je stále velmi neurčitý. Rozsáhlá literatura o povaze počítačové trestné činnosti může být rozdělena do mnoha diskurzů.[29]

Komise expertů na zločin v kyberprostoru (*Committee of Experts on Crime in Cyber-Space*), ustanovená v roce 1997, zpracovala návrh mezinárodní dohody usnadňující spolupráci pro odhalování počítačových zločinů. Sekce 1, Trestní právo hmotné (*Substantive criminal law*) definuje následující oblasti:

Přestupky proti důvěrnosti, integritě, dosažitelnosti počítačových dat a systémů:

- nezákonný přístup *(illegal access),*
- nezákonné odposlouchávání *(illegal interception),*
- narušování dat *(data interference),*
- narušování systémů *(system interference),*
- zneužití prostředků *(disuse of devices).*

Přestupky vztahující se k počítači:

- počítačové padělání *(computer-related forgery),*
- počítačový podvod *(computer fraud).*

Přestupky vztahující se k obsahu počítače a k dětské pornografii *(content related offences, offences related to child pornography).*

[28] GŘIVNA T., PONČÁK, R. *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008. s. 34. ISBN 978- 80-903786-7-4.
[29] Tamtéž, s. 26.

Přestupky vztahující se k autorskému právu a k právům souvisejícím *(offences related to infringements of copyright and related rights).*[30]

2.2 Hrozby na Internetu a ochrana, kterou poskytuje česká legislativa

V české legislativě jsou v oblasti kyberzločinu nejčastěji uplatňovány následující zákony:

- Občanský zákoník, zákon č. 40/1964 Sb., ve kterém je definováno vlastnické právo a entity, proti kterým je kriminální činnost namířena – právnické a fyzické osoby.
- Autorský zákon, zákon č. 121/200 Sb., v České republice i ve světě byl v letech 2011 a 2012 často zmiňován v médiích v souvislosti s kontroverzní dohodou ACTA (Obchodní dohoda proti padělatelství)[31] a jejich protesty a aktivitami po zadržení Kima Dotcoma, provozovatele serveru Megaupload.
- Zákon o elektronických komunikacích, zákon č. 127/2005 Sb., upravující některé důležité aktivity související s případným nezákonným chováním subjektu v prostředí počítačové sítě.
- Obchodní zákoník, zákon č. 513/1991 Sb. (závazkové a podnikatelské vztahy).
- Zákon o ochraně osobních údajů, zákon č. 101/200 Sb., jež souvisí s ochranou telekomunikačního tajemství a má působnost zejména v oblasti databází, které by mohly jednoznačně vést k identifikaci osoby.
- Trestní zákoník, zákon č. 40/2009 Sb., ve své poslední úpravě a s ním související předpisy, by měl sloužit jako donucovací nástroj v případě prokázaného porušení některého zákonného předpisu spadajícího do sféry odpovědnosti.

Mnohdy záleží na výkladu jednotlivých zákonů, některé kriminální delikty v počítačové oblasti se velmi obtížně začleňují do osnov zákonů.

[30] COUNCIL OF EUROPE. *Convention on Cybercrime.* [online]. © 23. 9. 2001 [cit. 2012-7-4]. Dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Překlad textu autorka práce.
[31] *ACTA (Anti Counterfeiting Trade Agreement)* – vícestranná mezinárodní dohoda s trestněprávními prvky, jejímž účelem je vymezení mezinárodního systému pro vynucování duševního vlastnictví.

Hrozby na Internetu

Současné trendy na poli zajištění informačního a síťového bezpečí nejsou povzbudivé. *„Informační bezpečnost chápaná jako soubor opatření a činností zajišťující bezpečí informací a sítí nemá stále jasné principy a účinné nástroje.“*[32]

Informační společnosti po celém světě jsou stále závislejší na informačních a komunikačních technologiích a růst kyberzločinnosti činí předmětné společnosti vysoce zranitelnými. V současné době je možné koupit si na Internetu různé druhy útoků na zakázku. Důvodem může být konkurenční boj, pomsta nebo pouze snaha uškodit.

Proti informačnímu systému může být veden útok, důsledky v případě úspěchu závisí na povaze systému. Výsledným efektem mohou být drobné nepříjemnosti pro napadené uživatele, v horším případě může dojít k obrovským finančním ztrátám nebo výpadkům životně důležitých funkcí systému, a to i lidské společnosti.

Žádný informační systém není stoprocentně bezpečný, záleží i na přístupu uživatele a jeho vnímání možných hrozeb. S tím souvisí uživatelské chování na internetu i postoj ke stahování a otevírání různých souborů. Cena chráněného objektu nemusí být stejná pro vlastníka informace a pro útočníka. V současné době neexistuje univerzální taxonomie škodlivých jevů spojených s lidským úmyslem (hrozeb), protože jejich existence, zaměření i formy se často mění.

Jirovský rozeznává hrozby základní a aktivační.[33] Pro potřeby diplomové práce byla vymezena pouze jedna kategorie.

Základní hrozby – lze rozeznat čtyři skupiny odrážející čtyři hlediska bezpečnosti informačního systému.

Únik informace – informace důvěrného charakteru je úmyslně prozrazena neautorizovanému subjektu nebo je jím odhalena. Únik může vést k přímému útoku s vážným dopadem.

Narušení integrity – porušení konzistence dat, kdy může dojít k vytvoření nových dat či změně nebo vymazání stávajících dat neautorizovaným subjektem.

Potlačení služby – úmyslné bránění přístupu legitimního subjektu k informacím nebo systémovým zdrojům. Příkladem jsou útoky DoS[34], DDoS[35], což jsou síťové útoky,

[32] PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. 1. vyd. Praha: ČVUT, 2011. s. 196. ISBN 978-80-01-04843-6.
[33] JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vyd. Praha: Grada, 2007. s. 30. ISBN 978-80-247-1561-2.

které brání přístup ke službám. Blokují služby sítě zaplavováním spojení, zhroucením serverů, programů běžících na serverech apod. Útokem dochází ke zhroucení či vyřazení serverů z činnosti.

Nelegitimní použití – zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem. Např. průnik do systému a používání placených služeb bez faktického vyúčtování a zaplacení služby.

2.3 Vymezení pojmů, které jsou používané v souvislosti s jevy, které ohrožují počítače a celé informační systémy

V praktické části byly v rámci rozhovorů i dotazníkového šetření některé z hrozeb identifikovány, proto je nutné teoreticky popsat jejich charakteristiku i dopad.

Trojský kůň (trojan) – nejběžnější případ vložené hrozby, kdy software obsahuje neviditelnou nebo při běžném provozu nepozorovatelnou část, která po spuštění naruší bezpečnostní prvky systému. Jedná se např. o program, který podporuje běžnou činnost uživatele a přitom umožňuje uložení záznamu o jeho aktivitách a jejich odesílání útočníkovi, až po zneužití pro útoky DoS.

Zadní vrátka (Backdoor) – část systémového software umožňující obejití bezpečnostních nástrojů systému. Je obvykle obtížně zjistitelný, zvláště tehdy, pokud se často nepoužívá. Při infiltraci je skvěle maskován, a proto není blokován firewally. Má velice dokonalou komunikaci. Lze ho detekovat jen tehdy, když se zrovna používá a když je právě spuštěný scan kvalitního antivirového programu.

Malware (škodlivé kódy a software, včetně virů, červů, trojských koňů, spyware, botů a botnetů) – vyvíjejí se a rychle se šíří, využívají se mimo jiné pro spáchání útoku „odmítnutí služby“, podvodů, krádeže identity, praní špinavých peněz atd.

Spamy a podvodné maily – v současné době představuje spam většinu odeslaných e-mailů. Nejedná se pouze o obtěžování, ale čím dále častěji se jedná o prostředek šíření malware. Spam se nyní objevuje i na mobilních telefonech pracujících na systémech

[34] *DoS (Denial of Service)* – odmítnutí služby. Existuje několik kategorií, může být lokální nebo vzdálený.
[35] *DDoS (Distributed Denial of Service)* – distribuované odmítnutí služby. Sofistikovanější útok, nástroj pro mnoho záplavových útoků, zde se používá určitý počet infikovaných počítačů – zombies.

iOS,[36] android apod. Podvodné maily jsou nevyžádané, ale velmi přesvědčivé falešné maily, ve kterých odesílatel slibuje různé výhry, skvěle placenou práci z domova, převod dědictví (např. velmi rozšířené nigerijské spamy). Záměrem je vylákat z lidí peníze a osobní údaje včetně informací o kreditních kartách či účtech.

Nigerijské dopisy nebo nigerijské spamy se začaly objevovat v malém měřítku v šedesátých letech minulého století a rozšířily se především v letech devadesátých, kdy z Nigérie přicházelo obrovské množství dopisů leteckou poštou. Kolem roku 2002 se podvody přesunuly do roviny elektronické.

Nigerijský spam je podvodný dopis zaslaný prostřednictvím elektronické pošty ze zahraničí, nejčastěji z Nigérie, Senegalu a Ghany. Obvykle řetězová zpráva má neznámého odesílatele, je psaná špatnou a lámanou češtinou, pravděpodobně za pomoci automatického překladače. Účelem pisatele je získání citlivých osobních údajů, čísla účtu a podpisu oběti k provedení nelegální finanční transakce, která obvykle končí vybráním účtu oběti.

Je možné setkat se se dvěma klasickými scénáři. První scénář představuje dojemný příběh, ve kterém pisatel apeluje na city příjemce, popisuje nepříznivou situaci v rodině a žádá o příspěvek na školu, léky, případné minimální životní režii. Druhým scénářem jsou mrtví milionáři a jejich privátní bankéři, kteří za nemalou finanční odměnu žádají o pomoc při převodu peněz do ciziny. Oběť má za příslušnou úplatu poskytnout své bankovní konto k proprání těchto peněz.

Jedinou ochranou je na předmětné maily nereagovat, protože jakmile útočníci zjistí, že e-mailová adresa je aktivní a respondent má zájem komunikovat, zefektivní své podvodné metody, aby od oběti získali potřebné informace za účelem jejich zneužití.

„Botnety – síť unesených zombie počítačů, obsahuje seznam IP adres počítačů zombie, které jsou infikovány nástroji vzdálené správy a které mohou být následně vzdáleně kontrolovány.“[37] Bot je zkratkou slova robot, jedná se o počítač ovládaný útočníkem, který instaluje specializovaný crimeware do počítače oběti, často bez jejího vědomí. Počítač je pro útočníka robotem, který vykonává naplánovanou činnost. Na napadeném počítači nemusí dojít ke škodám, slouží spíše jako prostředník útoků na

[36] *iOS* – mobilní operační systém vytvořený společností Apple Inc.
[37] GŘIVNA, T., PONČÁK R. *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008. s. 27. ISBN 978-80-903786-7-4.

další počítače, který v daném případě figuruje jako hlavní zdroj útoku, takže kryje primární zdroje útoků.

Dle statistik bezpečnostní firmy Dambala – je z celkového počtu 1,6 miliardy počítačů připojených k Internetu 12 – 15 % botů, což představuje 19 až 24 milionů počítačů.[38] Botnety představují jeden z hlavních nástrojů organizovaného kyberzločinu používaného pro DoS útoky, krádeže identity, phishing i pro umísťování adware a spyware. Často jsou pronajímány skupinám organizovaného zločinu.

Indiskrece – autorizovaná osoba prozradí důvěrnou informaci neautorizované osobě z neopatrnosti nebo za úplatu.

Únik informace – získání důvěrné informace neautorizovanou osobou.

Podvržení služby – podvržený systém, který se vůči napadenému uživateli chová jako běžná součást systému, slouží k získávání citlivých informací k nežádoucím účelům.

Krádež – zcizení citlivých informací nebo kritického prvku bezpečnostního systému.

Fyzický průnik – neautorizované získání kontroly nad systémem proniknutím k ovládacím prvkům.

Prolamovače hesel (password crackers) – principem je zkoušení hesel pomocí slovníku hesel anebo útokem hrubou silou (brute-force-attack). Slovník hesel obsahuje vlastní databázi slov, kterou používá při prolamování hesla. Princip hrubé síly spočívá ve zkoušení různých kombinací znaků. Pokud útočník zná oběť, je velká pravděpodobnost, že heslo předmětnou technikou zjistí, protože lidé standardně používají znaky, které přímo souvisí s jejich životem a soukromím, například data narození, křestní jména, příjmení, jméno matky za svobodna, místo bydliště, dále číselnou řadu 12345, slovo „heslo“ apod. Existuje databáze nejčastěji používaných hesel, podle které útočník může najít konkrétní řešení.

Použití nástrojů pro prolamování hesel je legální pouze tehdy, pokud uživatel prolamuje heslo, které si sám nastavil a zapomněl (např. Allrounder: Passware Kit Enterprise nebo Office: Advanced Office Password Breaker, Accent Office Password Recovery atd.). Stažení není žádným problémem, lze je volně získat i z bezpečných

[38] ACOHIDO B. *Are there 6.8 million or 24 million bitted PCs on the Internet?* [online]. © 20. 4. 2010 [cit. 2012-6-13]. Dostupné z: http://lastwatchdog.com/6-8-million-24-million-botted-pcs-internet/

internetových stránek například Slunečnice (www.slunecnice.cz) nebo Softpedia (www.softpedia.com).

Kvalitní prolamovače hesel jsou schopny ověřit od desítek tisíc až v případě velmi sofistikovaných programů, milion hesel za sekundu. Čím je komplikovanější a delší heslo, tím menší je šance pro jeho odhalení. Doporučuje se proto kombinace velkých a malých písmen a čísel.

Specializací v oblasti prolamování hesel jsou multiuživatelské online hry, kdy někdo z hráčů dosáhne výrazného úspěchu ve hře (pokročilý level). Útočníci ukradnou přístupová hesla ke hrám vysoce levelových hráčů, která pak na černém trhu nabízejí k prodeji. Podle odborníků se hodnota přístupových kódů k masovým virtuálním hrám jen ve východní Asii pohybuje v miliardách amerických dolarů.[39] Útoky na hráče nejsou neškodné, protože uživatelé aplikací často používají totožná hesla pro všechny ostatní aplikace. V momentě prolomení vstupů může dojít k přístupům k účtům, číslům kreditních karet i k citlivým informacím.

2.4 Hackeři a crackeři

Oblast hackingu a crackingu je nesmírně kontroverzní téma, protože cokoliv je řečeno, může být dotčenou komunitou oceněno nebo zatraceno. Ověřitelnost jakýchkoliv dat je velmi složitá, jelikož vzhledem k oblasti zájmu se jedná o uzavřenou entitu. Žádné informace nejsou věcné a zaručené, lze se pouze opřít o příběhy, které kolují internetem nebo jsou popsány v literatuře, jež se věnuje předmětnému tématu.

Pojmenování „hacker“ a termín „hacking“ vznikl zhruba v padesátých letech minulého století v komunitě radioamatérů, kde se jím označoval šikovný, technicky nadaný jedinec, schopný hledat nová zapojení a metody ke zlepšení výkonu a dosahu svého vysílače.[40] Vysvětlení užití právě termín „hacking“ existuje několik variant. Jeden z pramenů uvádí, že byl převzat z angloamerického žargonu jezdců na koních, kde se jím označovala nenucená vyjížďka bez nějakého přesného cíle. Další historický

[39] KOLEKTIV AUTORŮ. *Sborník příspěvků z konference. Dětská kybernetická kriminalita a sociální sítě*. Jihlava: Vyšší policejní škola MV, 2011. s. 68. ISBN 978-80-260-0723-4.
[40] JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vyd. Praha: Grada, 2007. s. 47. ISBN 978-80-247-1561-2.

zdroj odkazuje na skupinu železničních modelářů, kteří přizpůsobovali koleje, výhybky a mašinky tak, aby jezdily rychleji, lépe nebo odlišně.

Hacking se v současném pojímání dostává do povědomí na přelomu šedesátých a sedmdesátých let v dálkové komunikační síti American Telephone and Telegraph (dále jen AT&T), kdy skupinka technologických nadšenců využívala nedokonalost telefonní sítě za účelem telefonování bez poplatků. Systém spočíval v napodobení tónu o určitém kmitočtu, kterým se řídilo přepínání dálkových hovorů. Tón byl generován pomocí dětské píšťalky a balení cereálií „Cap´n Crunch“.

Rozvoj hackingu se datuje k osmdesátým létům minulého století. Hackerské skupiny se zaměřovaly na „lámání“ hesel počítačů a přístupových kódů. Hacking se postupně začal měnit s nárůstem počtu a dostupností informací na počítačových sítích. Používají ho lidé bez potřebného vzdělání a vědomostí „script kiddies“, „lammers“ a „loosers“, tj. jedinci, kterými hackerská komunita pohrdá. Vznikají hackerské stránky, na kterých lze volně stáhnout přístupová hesla, klíče i programy, jež využívají bezpečnostní díry v systémech.

Každá generace hackerů vyrůstala v jiných podmínkách: sociálních, politických, technologických a byla jinak vnímána společností. V době raného vývoje existovalo něco, co bylo označováno jako hackerská etika. Jednalo se o určitá pravidla, podle kterých se měl hacker řídit – např. svoboda informací, nedůvěra k autoritám, neomezený přístup k počítačům a čemukoliv, co může pomoci pochopit, jak funguje svět, kategorizace hackerů podle schopností hackovat, možnost na počítači tvořit umění atd.). Osoby, které se chtěly nazývat hackery, pravidla dodržovaly a propagovaly je. Staří hackeři byli opravdovými odborníky, původci originálních myšlenek a nápadů. Jejich úmyslem nebylo škodit, zaměřovali se spíše na výzkum a zlepšování systémů informačních technologií v rámci univerzit a jejich excesy byly v rámci akademické půdy tolerovány. Novodobí hackeři jsou zcela odlišní, disponují důkladnými odbornými znalostmi, ale působí v odlišném prostředí. Aktivity už dávno přesáhly akademickou půdu, nyní se zaměřují na světový kyberprostor a jejich cíle a zájmy jsou zcela jiné. Tak, jako každá výhoda generuje i nevýhodu, i nevýhoda může pomoci vývoji a zdokonalování. Díky praktikám hackerů dnes existují sofistikovanější antivirové programy a lepší ochrana informačních systémů.

Experti zabývající se bezpečnosti sítí se úmyslně nabourávají do systémů, aby zjistili zranitelná bezpečnostní místa a vytvořili protiopatření ke snížení identifikovaných rizik.[41]

Hacker v současné době pro mnoho lidí představuje typ spíše introvertního, nezajímavého, zakomplexovaného, fyzicky neatraktivního umaštěného chlapa.[42] Je to obecně rozšířená představa zlomyslného jedince, který odposlouchává informace, nabourává se do systémů s úmyslem škodit, a tím si zvedat sebevědomí, kriminálníka, který krade informace a prodává je nebo škodí jen pro radost.

Důvodem, proč je dnešní pohled na hackery vysoce negativní, je jejich časté zkreslování a dezinterpretace v médiích. Ta často popisují hackera jako zločince, jehož jediným cílem je páchat zlo, krást software a nabourávat se do počítačů za účelem zcizení a zneužití dat nebo využití počítače pro ilegální aktivity. Dokonce i v internetovém slovníku cizích slov abz.cz je jako význam slova hacker uvedeno: „*Uživatel počítačových systémů snažící se přes počítačové sítě proniknout do cizích systémů.*“[43] Komentáře pod předmětným výrazem původní významový obsah negují. Dle autorů komentářů se jedná o osoby disponující perfektními znalostmi počítačových systémů, které dokážou používat a upravit podle svých potřeb. Uvedená definice je vystihující pro slovo cracker. Hacker neškodí, naopak svými znalostmi spíše pomáhá zdokonalit systém.

Hacker je podle Jargoogle osoba, kterou baví zkoumat detaily programovatelných systémů a hledat metody, jak zvýšit jejich výkonnost. V tom se odlišuje od většiny uživatelů, která upřednostňuje naučit se pouze nutné minimum. Jsou to osoby, pro které je potěšením mít důkladné znalosti vnitřního fungování systému, počítačů, počítačových sítí a všech souvisejících zvláštností.[44]

Crackeři

V diskusích o hackingu se objevuje jako opozitum slova hacker. Jejich cílem je zneužití hackerských metod za účelem finančního obohacení, různých podvodů,

[41] HARPER, A., HARRIS, S., NESS, J., et al. *Grey hat hacking. The ethical hacker´s handbook*. 3rd edition. New York: McGraw Hill, 2011. ISBN 978-0-07-174255-9.
[42] Vlastní průzkum autorky.
[43] ABZ.CZ. SLOVNÍK CIZÍCH SLOV – ON-LINE HLEDÁNÍ. *Hacker* [online]. © 2005–2006 [cit. 2012-8-1]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/hacker-hekr
[44] JARGOOGLE. *Hacker*.[online]. © 27. 10. 2003 [cit. 2012-8-5]. Dostupné z: http://www.catb.org/jargon/html/H/hacker.html

teroristických aktivit, vandalismu a obecně nelegálních, destruktivních a neetických aktivit. Jedná se o skupinu lidí spojenou s kriminální činností. Hacker tvoří, cracker ničí. Cracker je hacker v negativním slova smyslu, v současné době se pro předmětnou činnost obecně, i díky médiím, používá téměř výhradně termín hacker, jak již bylo zmíněno výše.

Slovy Erica S. Raymonda, amerického programátora: *„Je tady určitá skupina lidí, kteří si hlasitě říkají hackeři, ale nejsou jimi. Jsou to lidé (převážně adolescenti mužského pohlaví), kteří zapáleni pro nabourávání se do počítačů a telefonního systému. Skuteční hackeři říkají těmto osobám crackeři a nechtějí mít s nimi nic společného. Opravdoví hackeři je považují za líné, nezodpovědné a nepříliš moudré. Tvrdí, že schopnost narušit bezpečnost systému z nikoho neudělá hackera stejně tak jako dovednost ukrást auto neudělá ze zloděje automechanika.“*[45]

Různí autoři uvádějí několik dělení hackerů do kategorií. Obecně jsou definovány tři základní skupiny hackerů, přičemž se podle motivace hackera uplatňuje takzvané „kloboukové dělení“, (white hats, black hats, grey hats).[46]

Hackeři používají různé techniky k průniku do systému, od hardwarových nástrojů přes softwarové nástroje (velmi často používané) až po sociální inženýrství neboli techniky zneužití lidského činitele.

2.5 Nebezpečné komunikační praktiky

Rizika Internetu spolu s technickou oblastí spočívají i v nevhodném, nebezpečném a nezákonném obsahu a v potencionální patologické komunikaci a vztazích. Mluví se o takzvaných sociopatologických jevech, mezi které řadíme:

- netholizmus (netholism),
- kyberšikanu a tzv. spokojené fackování (cyberbullying and happy slapping),

[45] RAYMOND, E. S. *How to become a hacker*. [online]. © 2001 [cit. 2012-8-15]. Dostupné z: http://www.catb.org/esr/faqs/hacker-howto.html. Překlad textu autorka práce.
[46] HARPER, A., HARRIS, S., EAGLE, CH. et al. *Hacking – manuál hackera*. 1. vyd. Praha: Grada, 2008. s. 54. ISBN 978-80-247-1346-5.

- kybernetové pronásledování a kybernetové obtěžování (cyberstalking and cyberharassment),
- kybergrooming (cyber grooming),
- sexting,
- hoax.

Netholismus

Nadměrné trávení času ve virtuálním světě, závislost na Internetu, neboli patologické užívání Internetu, které se časem projeví na lidské psychice. Anglicky se nazývá „Internet Addiction Disorder“.[47]

Postižení netholismem se vyskytují napříč celým věkovým spektrem. Anonymita a pohyb ve virtuálním světě, který neutralizuje etnické, psychologické a sociální bariéry jsou hlavními motivátory pro extrémní surfování na Internetu. Netholismus závisí zejména na komunikaci a typu informací, které uživatel na Internetu vyhledává. Za příčiny vzniku netholismu se zpravidla označují: sociální vyloučenost, nefunkční rodinné vztahy, nedostatek skutečných přátel, selhávání v reálném světě, absence koníčků, nuda.

Netholici přikládají Internetu nesmírnou důležitost, internetová aktivita se pro ně stává nejdůležitější aktivitou na světě. Veškeré další aktivity, včetně školních i pracovních povinností, jsou u netholiků na pokraji jejich zájmu. Po určité době dochází ke změnám nálad, abstinenčním příznakům, zvyšování prahového efektu i konfliktům s okolím.

Lidé, kteří si z jakýchkoliv důvodů nemůžou najít přátele nebo partnera, hledají substituci prostřednictvím seznamek, sociálních sítí, hledají sex na porno stránkách nebo sexuálních seznamkách, na kterých dokážou surfovat a chatovat celé hodiny. Jedinci postupně ztrácejí kontakt s realitou a společností kolem sebe a vzniká bludný kruh, postupně roste jejich agresivita a nespokojenost v případě nemožnosti připojit se na Internet.

[47] GROHOL, J. *Internet Addiction Guide*. [online]. © 26. 10. 2012 [2012-11-17]. Dostupné z: http://psychcentral.com/netaddiction/

Děti bývají závislé zejména na počítačových hrách, kterým věnují drtivou většinu svého času na úkor školních povinností, koníčků, osobního kontaktu s kamarády a dalších volnočasových aktivit. Závislost následně generuje asociální projevy, kterým je převzetí virtuálních vzorců chování, mnohdy s agresivními a iracionálními prvky, stupňuje se izolace, neschopnost budovat zdravé sociální vztahy.

„Průměrné využívání počítače neovlivňuje negativně sociální dovednosti a aktivity dětí, ale dle zkušeností se jeví jako zásadní posoudit vliv nadměrného využívání počítačů a Internetu na pocit osamění, sociální vazby a duševní pohody u dětí a adolescentů.“[48]

Publikované případy obětí netholismu, jež lze najít na Internetu, poukazují na dopady, kterými jsou: sociální izolace, negativní změny v chování, narušení vztahů s blízkými osobami, snížení fyzické aktivity, ztráta zaměstnání, problémová finanční situace z důvodu potřeby kupovat si nový hardware i software; v horších případech dochází k zdravotním potížím, k sebevraždám a vraždám z důvodu nárůstu agresivity i neschopností vyrovnat se se závislostí a zejména s běžnou realitou. Netholismus je současně spojován s počítačovou a majetkovou kriminalitou zejména v souvislosti s online hrami.

Kyberšikana

„Kyberšikana je specifický druh násilí, který využívá k ponižování, nadávání, urážení, zastrašování, vyhrožování, vydírání a pronásledování jedinců moderní média – internet, digitální technologie, mobilní telefony.“[49] Spočívá v zasílání obtěžujících, urážejících, ponižujících zpráv a mailů, ve vytváření stránek, blogů, diskusí, které ponižují jednotlivce nebo skupinu lidí. Termín se používá v souvislosti s dětmi a nezletilými, pokud jsou dotčenými dospělí, mluví se o kybernetovém obtěžování (cyber harassment) nebo kybernetovém pronásledování (cyber stalking).

Oproti tradiční šikaně je kybernetová šikana nebezpečnější, a to zejména nepostižitelností pachatele kvůli nízké pravděpodobnosti jeho identifikace a získání přímých důkazů o terorizování oběti. Uvedený fakt poskytuje útočníkům obrovské

[48] ŠMAHEL, D. *Psychologie a internet, děti dospělými a dospělé dětmi*. 1. vyd. Praha: Triton, 2003. s. 74. ISBN 80-7254-360-1.
[49] VAŠUTOVÁ, M. *Proměny šikany ve světě nových médií*. 1. vyd. Ostrava: Filosofická fakulta Ostravské univerzity v Ostravě, 2010. s. 77. ISBN 978-80-7368-858-5.

možnosti seberealizace a uplatnění metod, které jsou limitovány výhradně jejich vynalézavostí a přístupem k technologiím. Pachatel se v určitém momentu může stát i obětí. Děti často mění role z oběti na šikanéra a naopak.

Výše zmíněná skutečnost a současná právní nepostižitelnost nezletilých však dává příležitost k realizaci často velmi krutých a zraňujících dopadů šikany. Jsou evidovány případy, kdy děti, které byly účastníky šikany, se navzájem zabily anebo spáchaly sebevraždu.

Happy slapping

Specifický druh kyberšikany. Objevil se v roce 2005 v jižních předměstích Londýna u hiphopových gangsta teenagerů.[50]

Účelem happy slappingu je nečekaně fyzicky napadnout oběť, přičemž komplic agresora pořizuje nahrávku na mobilní telefon nebo na kameru. Získané video umístí na Internetu (např. You Tube) nebo šíří dál prostřednictvím telefonu.[51]Útočníci svým konáním získávají věhlas a proslulost v určité komunitě lidí. V České republice se happy slapping objevil ve formě šikany učitelů, kdy došlo k záměrnému vyprovokování konfliktní situace mezi žákem a přednášejícím za účelem pořízení videozáznamu a jeho následném zveřejnění.

Kybernetové pronásledování a obtěžování

Čeština používá i termínu kybernetický lov. Zjednodušeně se dá definovat jako nebezpečné pronásledování, zastrašování a obtěžování oběti zneužitím informačních a komunikačních technologií.[52] Může probíhat zasíláním stovek obtěžujících mailů, sms, mnohonásobným zasíláním nevyžádané pošty (spamů), zasíláním virů, publikováním nepřístojných vzkazů v návštěvních knihách atd.

---

[50] AKWAGYIRAM, A. *Does „Happy Slapping“ Exist?* [online]. © 12. 5. 2005 [cit. 2012-9-9]. Dostupné z: http://news.bbc.co.uk/2/hi/4539913.stm

[51] E-BEZPECI.CZ. *Happy Slapping.* [online]. © 2010 [cit. 2012-09-07]. Dostupné z: http://cms.e-bezpeci.cz/content/view/71/39/lang,czech/

[52] BOCIJ, P. *Cyberstalking. Harrassment in the Internet Age and How to Protect your Family*. 1st edition. Westport CT: Praeger Publishers, 2004. s. 3. ISBN 0-275-98118-5.

Cyberstalking nebo cyber harrassment je úmyslné pronásledování a trápení jiné osoby, které snižuje kvalitu jejího života, ohrožuje její bezpečí a narušuje psychickou pohodu.

Pro cyberstalkery je typická vytrvalost, systematičnost, velmi často patří mezi psychopatické osobnosti „deprivanty“[53] či mezi sociálně úspěšné psychopaty, kteří se neodhaleni pohybují mezi normálními lidmi. Jejich cílem je kontrola, manipulace a tyranie. Neznají lítost, ani pocity viny, nemají svědomí, pohrdají lidmi. Rozhodně nepřijímají odpovědnost za vlastní činy. Užívají takzvané nicknames – přezdívky. Obtěžování a znepříjemňování života jiným osobám je jejich koníčkem, svoje potřeby uplatňují bez ohledu na potřeby a city jiných lidí. Jedná se o nejhorší typy lidí, jež se pohybují v prostředí Internetu. Jejich parazitní strategie má destruktivní dopad na okolí, které systematicky obtěžují.

Kybernetové obtěžování není pouze jiným způsobem, který může být spojován se „standardním“ stalkingem. Jedná se o kompletně novou formu deviantního chování, jež může mít mnohem závažnější dopady.[54]

Častými oběťmi kybernetického pronásledování jsou ženy po ukončení partnerského vztahu, zejména pokud ještě nemají nového partnera, osamělé osoby (rovněž spíše ženy) nebo osoby pracující v exponovaných profesích (celebrity, osoby, které mají úzký kontakt s lidmi a velké pravomoci). Evidují se rovněž případy, kdy stalking (i cyberstalking) vyústil v silnou duševní újmu anebo dokonce i ve vraždy[55] nebo v sebevraždy obětí.

Stalking je od ledna 2010 zakotven v Trestním zákoníku (zákon č. 40/2009 Sb.), v hlavě X – Trestné činy proti pořádku ve věcech veřejných, v paragrafu č. 354 – Nebezpečné pronásledování, a je definováno takto:

1) „*Kdo jiného dlouhodobě pronásleduje tím, že*
   a) *vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo osobám blízkým,*
   b) *vyhledává jeho osobní blízkost nebo jej sleduje,*

[53] KOUKOLÍK, F., DRTILOVÁ, J. *Vzpoura deprivantů: nestvůry, nástroje, obrana*. 2. vyd. Praha: Galén, 2006. s. 44. ISBN 978-80-7262-410-2.
[54] BOCIJ, P. *Cyberstalking. Harrassment in the Internet Age and How to Protect your Family*. 1st edition. Westport CT: Praeger Publishers, 2004. s. 16. ISBN 0-275-98118-5.
[55] TYDEN. CZ *Stalking má být trestný, shodli se ministři*. [online]. © 27. 6. 2008 [cit. 2012-09-09]. Dostupné z: http://www.tyden.cz/rubriky/domaci/stalking-ma-byt-trestny-shodli-se-ministri_67942.html

c) *vytrvale jej prostřednictvím prostředků elektronických komunikací písemně nebo jinak kontaktuje,*
d) *omezuje jej v jeho obvyklém způsobu života, nebo*
e) *zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu*

a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.“[56]

Kybergrooming

Jde o velmi nebezpečný a zákeřný způsob, jak získat důvěru oběti, zneužít její naivitu, nezkušenost, touhu po přátelství, případně její špatné psychické rozpoložení. Hlavním cílem kybergroomera je sjednat si osobní schůzku a oběť zneužít. Do češtiny je lze přeložit jako kyberkrášlení, respektive krášlení a změnu identity, za účelem přilákání oběti. „*Nebezpečná internetová manipulace, v rámci které útočník usiluje o osobní schůzku s nezletilou obětí.*“[57] Zasažený se domnívá, že na Internetu potkal někoho opravdu mimořádného, avšak nejpravděpodobnějším cílem je sexuální zneužití.

Útočník nejdříve identifikuje pravděpodobnou oběť, která bude odpovídat jeho preferencím a kterou bude snadné oklamat, poté pozvolna získává její důvěru. Rozhodně se nejedná o krátkodobý proces. Kybergroomeři jsou neobyčejně vynalézaví, trpěliví, přátelští, obratně budují rozvoj vzájemného vztahu, mluví o lásce a o další budoucnosti po společném setkání v reálném světě. V konverzaci se po navázání „bližšího vztahu“ často objevují sexuální témata. Kybergroomer žádá fotky, případně sex přes webkameru. Pravidlem je, že kybergroomer požaduje maximální utajení virtuálního vztahu. Oběťmi bývají nejčastěji děti, nezletilí a ženy.

[56] Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů České republiky*. 2009, s. 436. ISSN 1211-1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy

[57] E-BEZPECI.CZ. *Kybergrooming*. [online]. © 2008–2012 [cit. 2012-9-10]. Dostupné z: http://e-bezpeci.cz/

Sexting

Pod pojmem sexting se rozumí *„akt zaslání sexuálně explicitního materiálu prostřednictvím mobilních telefonů. Slovo je odvozeno z kombinací dvou pojmů: pohlaví a posílání zpráv.“*[58]

Materiál často vzniká ještě v době trvání partnerského vztahu, cílem bývá posílení erotiky mezi partnery. Problém vzniká po rozchodu, zejména pokud je rozchod pro jednoho z partnerů frustrací. Z pomsty pak útočník fotografie či video expřítele zveřejní na Internetu nebo šíří dál pomocí mobilu.

Sexting je velice nebezpečné chování, protože potencionální útočník má k dispozici citlivý materiál, který nezískal neoprávněně a může ho lehce zneužít. Video a fotky můžou být použity i několik let po jejich pořízení. Oběť může být vystavena obtěžování i vydírání, a to může zanechat vážné následky na oběti, například psychické zhroucení i sociální diskvalifikaci.

I přesto, že osoby starší 15 let mohou mít sex (nedopouštějí se trestního činu), nesmí se u daného aktu fotografovat ani natáčet. V opačném případě by se mohlo jednat o výrobu a držení dětské pornografie. Za dítě se podle zákona považuje osoba mladší 18 let,[59] a pokud se prokáže, že došlo k přeposílání materiálu se sexuálním obsahem u osob dotčené věkové kategorie, „odesílatel“ se vystavuje trestnímu postihu za šíření dětské pornografie.

Internetové stránky www.sexting.cz informují, že 10,44 % českých dětí odeslalo další osobě alespoň jednu fotografii nebo video se sexuálním obsahem a 9,15 % má takové vyobrazení volně zveřejněno na Internetu.[60]

Hoax

Falešná a poplašná zpráva, podvod, vtip, šířená pomocí e-mailů. Obsahují šokující, nepravdivá sdělení. Často mají podobu varování před aktuálním nebezpečím (internetová nebezpečí, sociální či ekonomické hrozby), v horších případech se jedná

---

[58] USLEGAL.COM. *Sexting Law and Legal Definition*. [online]. © 2001–2012 [cit. 2012-9-10]. Dostupné z: http://definitions.uslegal.com/s/sexting/. Překlad textu autorka práce.

[59] Zákon 104/1991 Sb. o přijetí Úmluvy o právech dítěte. In: *Sbírka zákonů České republiky*, 1991. s. 503. ISSN 1211–1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=104/1991&typeLaw=zakon&what=Cislo_zakona_smlouvy

[60] SEXTING.CZ. *Sexting v České republice*. [online]. © 2009–2012 [cit. 2012-9-9]. Dostupné z: http://www.sexting.cz/

o snahu vymámit z uživatelů peníze za služby a zboží nebo i o citové vydírání za účelem získat peníze „na pomoc“. Následování nebezpečného doporučení, jak se zbavit domnělého viru, může uživateli nenávratně poškodit počítač. Cílovou skupinou jsou především děti nebo nezkušení uživatelé, kteří výše zmíněné nepravdivé informace šíří dál, například nesmyslným sdílením na Facebooku.

2.6 Sociální inženýrství

„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.“ (Albert Einstein)

Lidský faktor je nejslabším článkem sofistikovaného a vysoce technicky vytvořeného bezpečnostního systému. „*Sociální inženýrství, též manipulativní komunikace, je ovlivňování a přesvědčovaní lidí s cílem oklamat je způsobem, že uvěří, že sociální inženýr je osoba s totožností, kterou předstírá, kterou si ve skutečnosti vytvořil pro potřeby manipulace.*“[61] Pomocí popsané techniky je „sociotechnik“ schopen využít lidi, se kterými hovoří, k získání hledané informace.

Sociální inženýr využívá stejné přesvědčovací techniky, které každý z nás denně používá. Lidé se obvykle snaží budovat důvěryhodnost. „*Sociotechnik využívá přesvědčovací metody manipulativním, klamavým, vysoce neetickým způsobem, často s devastujícím účinkem.*“[62]

Metoda vede k tomu, že legitimní uživatelé poskytnou sociotechnikovi důvěrné informace, které mu pomohou získat přístup do jejich počítačového systému, anebo je zneužít k vlastnímu prospěchu. Klamaný uživatel tak činí bez vědomí, že napomáhá útočníkovi.

Praxe z oblasti jednání lidí ukazuje, že lidé řeknou velmi mnoho detailních informací, když se vhodným způsobem dokáže tazatel zeptat. Sociotechnická metoda v popsaném provedení spočívá v podvádění lidí, jedná se o útok cestou nejmenšího odporu. Využívá psychologické metody a přesvědčivý jazyk, které umožňují získat potřebné údaje o uživateli, firmě, respektive o vybraných cílech.

[61] MITNICK, K., SIMON, W. L. *Umění klamu*. Gliwice: Helion S. A., 2003. s. 3. ISBN 83-7361-210-6.
[62] MITNICK, K., SIMON, W. L. *The Art of Intrusion: the real stories behind the exploits of hackers, intruders.* Indianapolis. In: Wiley Publishing, Inc., 2005. s. 232. ISBN 07-645-6959-7. Překlad autorka.

Dotazovaná osoba nepozná, že mluví s podvodníkem, který určitými indiciemi dokáže vzbudit důvěru a dojem, že dotázaný mluví s kompetentním člověkem, respektive s osobou, za kterou se lživě vydává. Médiem pro sociotechnický útok je kromě klasické pošty také Internet (e-mail, ICQ) a telefon.

Sociotechnici využívají lenosti lidí, jejich důvěru, přehlížení drobných odlišností, ochotu pomoci jiným a také strach z autorit. Často se vydávají za nadřízené osoby z managementu, které zaměstnanec osobně nezná.

Se sociálním inženýrstvím je spojeno jméno Kevin Mitnick. Causa Mitnick zahýbala světem počítačů v 90. letech minulého století. Mitnicka již na střední škole zaujalo nabourávání se do systémů, hledání bezpečnostních děr, zjišťování cizích hesel. Aktivity mu poskytovaly zdroj zábavy, proto se postupně se v hackování začal zdokonalovat. Později se mu opakovaně podařilo nabourat se do systémů, které byly považovány za neproniknutelné. Kontaktoval zaměstnance a sdělil jim předem získané důvěrné informace, čímž v nich vyvolal dojem oprávněné osoby. Zaměstnanci mu následně poskytli informace, na základě kterých pronikl do vysoce zabezpečených systémů bez jakéhokoliv poškození software nebo hardware.[63]
Mitnick byl za nelegální aktivity odsouzen, dostal i zákaz přístupu k Internetu. Nyní pracuje jako vysoce uznávaný bezpečnostní konzultant, založil firmu Mitnick Security Consulting LLC, vydal dvě knihy, The Art of Deception (Umění klamu) a The Art of Intrusion (Umění nežádoucího pronikání). Sociotechnika je kromě nabourání se do počítačového systému za účelem osobního prospěchu hmotného i nehmotného často využívána ke kybergroomingu, k trestním činům krádeží, k vydírání druhých osob nebo ke zcizení identity.

Úroveň poznání a platforma znalostí byly získány syntézou údajů z oblastí psychologie a sociologie na universitě, z referátů na odborné konferenci CyberTerrorism and CyberCrime CYTER2012, diskusemi s pracovníky zabývajícími se problematikou informačních technologií a studiem relevantních publikací.

[63] KULHAVÝ, P. *Kevin Mitnick – slavný podvodník nebo obávaný hacker?* [online]. © 26. 9. 2003 [cit. 2012-9-11]. Dostupné z: http://www.root.cz/clanky/kevin-mitnick-podvodnik-hacker/

PRAKTICKÁ ČÁST

3 PŘÍPADY ZNEUŽITÍ INTERNETU A JEJICH DOPADY

V předložené kapitole jsou popsány vybrané případy a kauzy z České republiky i ze světa, ve kterých došlo ke zneužití Internetu a internetové komunikace. Důsledkem pak bylo poškození konkrétních lidí a dalších chráněných aktiv. Je vytvořen datový soubor, na jehož základě byla analyzována a vyhodnocena rizika spojená s Internetem.

3.1 Popis případů z ČR, získaných obsahovou analýzou dat z Internetu

Případ 1. Jana Berkusová, psychoterapeutické centrum Hukvaldy

Jana Berkusová založila v Hukvaldech speciální psychoterapeuticko-vzdělávací centrum pro děti a dospělé, které bez problémů fungovalo asi dva měsíce. Po uvedené době jí při pokusu o přihlášení se do e-mailu začal systém hlásit nefunkční heslo nebo špatné přihlašovací údaje. Uživatelka netušila, co se stalo, až jí klienti kontaktovali s tvrzením, že obdrželi sms, ve které bylo uvedeno, že paní Berkusová je podvodnice, která tahá z lidí peníze, využívá své děti a je alkoholička.

Stejné vyjádření jejím jménem s doznáním a omluvou se objevilo i na internetových stránkách jejího psychoterapeutického centra. Klienti i investoři přestali komunikovat. Pro paní Berkusovou bylo nařčení doslova likvidační. Webové stránky stále běžely a na svůj mail se kvůli změněnému heslu nemohla dostat, takže ho nemohla nechat zablokovat. Seznam.cz byl nucen čekat na rozhodnutí soudu k zablokování e-mailového účtu, protože neměl k dispozici žádný nástroj, jak zjistit, že e-mailová stránka paní

Berkusové skutečně patří. Podezřelým z narušení soukromí a poškození práv paní Berkusové byl čtyřiceti čtyřletý muž.[64]

Na internetové stránce www.podvody.net je publikováno následující oznámení: „*Chci tímto upozornit všechny, že Jana Berkusová je neplatič a podvodník vysokých kvalit. Pokud jste také naletěli, ozvěte se na tel. 777 324 240.*“[65] Autorka na uvedené číslo opakovaně volala, bylo vždy nedostupné. Zkoušela najít internetové stránky psychoterapeutického centra v Hukvaldech (www.domecek-hukvaldy.webnode.cz). Po zadání předmětné adresy se objevuje oznámení, že požadovaná stránka nebyla nalezena, pravděpodobně byla zrušena nebo byla špatně zadána její adresa.

Na písemnou žádost odeslanou osobně autorce reportáže ČT Ostrava, přišla odpověď, která obsahovala informaci o tom, že ještě v květnu 2012 byl případ na mrtvém bodě. Policie pokračovala ve výsleších svědků. Autorka reportáže sdělila, že k zablokování stránek došlo pár týdnů po jejím odvysílání. Jednalo se o nesmírně složitý proces vzhledem k tomu, že stránky byly spravovány jménem paní Berkusové, stejně jako její e-mailový účet. Bylo nutné dokazovat, že ona není osobou, která stránky a e-mail zneužívá. Paní Berkusovou se z důvodu jejího pobytu v zahraničí nepodařilo osobně zkontaktovat.

Případ 2. Tomáš Kadlec, podvodné vylákání peněz, klamavá reklama na Internetu

Zlínský podnikatel Tomáš Kadlec je obviněn z podvodu při zajišťování práce v zahraničí. Za vstupní poplatek dva tisíce korun nabízel lidem prostřednictvím webových stránek dobře placenou práci v cizině.[66]

Systém fungoval na základě registrace zájemců na internetových stánkách a následné úhradě poplatku za „balíček“, který představoval zprostředkování práce a zajištění administrativních úkonů. Klientům byly poslány pouze propagační materiály. Když

[64] CESKATELEVIZE.CZ. *Události v regionech.* [online] © 18. 1. 2012 [cit. 2012-07-09]. Dostupné z: http://www.ceskatelevize.cz/ivysilani/10122978233-udalosti-v-regionech-ostrava/412231100030118-udalosti-v-regionech/obsah/186726-policie-stale-casteji-resi-pripady-internetove-kriminality/

[65] PODVODY.NET. *Jana Berkusová Hukvaldy 21 Domeček her a zábavy*. [online] [cit. 2012-07-09]. Dostupné z: http://www.podvody.net/Jana-Berkusov%C3%A1-Hukvaldy-21-Dome%C4%8Dek-her-a-z%C3%A1bavy

[66] CESKATELEVIZE.CZ. *Zlínský soud otevřel nejrozsáhlejší kauzu ve své historii*. [online]. © 7. 2. 2012 [cit. 2012-07-09]. Dostupné z: http://www.ceskatelevize.cz/ct24/regiony/166032-zlinsky-soud-otevrel-nejrozsahlejsi-kauzu-ve-sve-historii/

chtěli klienti služby reklamovat, jak jim bylo na příslušných webových stránkách doporučeno, komunikace se ze strany agentury přerušila.

K datu 13. březen 2012 je evidováno 4246 poškozených a škoda přesahující třináct milionů korun. Od dalších 275 lidí se Tomáš Kadlec peníze pokoušel vylákat, šlo o 806.000 korun.[67] Podle policie byly internetové stránky profesionálně zpracované, zobrazení bylo ošetřené tak, že při zadání příslušných klíčových slov se stránky ukazovaly na prvních místech, takže uchazeči o zaměstnání v zahraničí se jim nemohli vyhnout. Jednalo se například o nabídky práce na internetových stránkách např. pracevzahranici.eu, aupair.cz, brigady.net, práce-anglie.cz. Tomáš Kadlec vinu popírá, odmítá stanovisko o zajištění práce s tvrzením, že agentura zajišťovala výhradně cestovatelský a překladatelský servis. Kauza není uzavřena, vzhledem k vysokému počtu poškozených a požadavku obhajoby, která trvá na osobním výslechu všech poškozených.

Případ 3. Pavel Hovorka, kybergrooming

Třiceti pětiletý Pavel Hovorka, zaměstnanec tiskáren, vyhledával prostřednictvím služebního mailu chlapce především ze slabšího sociálního prostředí, slibujíc jim peníze nebo splnění jejich přání výměnou za jejich nahé fotografie.

Jeho údajně první oběť vyhrála jím vypsanou soutěž VIP dítě, jednalo se o chlapce z dětského domova, který Hovorka, jako bývalý chovanec dětského domova, sponzoroval. Výhrou měly být dva týdny strávené v Praze. Hovorka s chlapcem údajně strávil několik dnů na vrátnici, kde jej zneužíval.[68]

Další oběti hledal na seznamovacích serverech. S chlapci si nejdříve psal a telefonoval. Poté, co si získal jejich důvěru, žádal jejich nahé fotografie. Po získání fotek svým obětím vyhrožoval vyzrazením jejich homosexuální orientace a zveřejněním fotek, které mu za úplatu poslali. Oběti si rovněž zval k sobě do práce, kde několik

[67] IDNES.CZ. *Soud rozplétá podvody s nabídkami práce, chce vyslechnout tisíce svědků*. [online]. © 27. 2. 2012 [cit. 2012-07-09]. Dostupné z: http://zpravy.idnes.cz/soud-rozpleta-podvody-s-nabidkami-prace-chce-vyslechnout-tisice-svedku-1nn-/krimi.aspx?c=A120227_161747_zlin-zpravy_jog

[68] BUBLANOVÁ A. *Za zneužití dvaceti chlapců půjde Hovorka na osm let do vězení.* [online]. © 5. 2. 2009 [cit. 2012-07-11]. Dostupné z: http://www.mediafax.cz/krimi/2814724-Za-zneuziti-dvaceti-chlapcu-pujde-Hovorka-na-osm-let-do-vezeni

z nich údajně donutil k pohlavnímu styku, podle obžaloby některé z nich i znásilnil.[69] Soud uznal Hovorku vinným ze sedmi případů pohlavního zneužívání a třinácti případů vydírání. Byl odsouzen k šesti a půl letům vězení, rovněž mu byla nařízena sexuologická léčba.[70]

Případ 4. Nigerijské spamy v České republice

a) Nejznámějším a nejtragičtějším případem v České republice je kauza mělnického lékaře Jiřího Pasovského.[71] Zmíněný konkrétní případ takzvaného nigerijského dopisu, který lékař obdržel poštou, je předchůdcem současných nigerijských spamů. Pasovský na základě oficiální nabídky z Nigérie nakoupil v roce 1995 akcie společnosti Nacional Nigeria Petroleum Company, do které v průběhu několika let postupně investoval téměř patnáct milionů, z nichž značnou část si půjčil z různých zdrojů, včetně lichvářů. Nabídka vypadala důvěryhodně, mělo jít o vládní kontrakt, na který se vztahovaly vládní záruky.

Navzdory slibům a zárukám Pasovský o všechny investované peníze přišel. Ve snaze získat své investice zpět, pravidelně navštěvoval Pasovský nigerijskou ambasádu, kde se žádného odškodnění se nedočkal. Z důvodu ztráty životních úspor a obrovskému zadlužení Pacovský v roce 2003 zastřelil nigerijského konzula v Praze, Michaela Lekaru Wayidu, a postřelil recepčního.

b) Mladé ženě z Jindřichova Hradce dorazila v květnu 2009 prostřednictvím Internetu lákavá nabídka zaručeného dědictví.[72] Zpráva byla poslána neznámým pachatelem z e-mailového účtu u patchanprivacy004@yahoo.com. Útočník se v ní představil jako Patrik Chan a uvedl, že je zaměstnancem banky v Hongkongu. Oběť informoval o tom, že měl bohatého klienta, Musa Omaru Numana, který zemřel v Iráku

[69] NEBUĎ OBĚŤ. *Kybergrooming*. [online]. © 2010–2012 [cit. 2012-07-11]. Dostupné z: http://www.nebudobet.cz/?page=kybergrooming

[70] IDNES.CZ. *Deviant Hovorka se dočkal za zneužití dvaceti chlapců mírnějšího trestu*. [online]. © 26. 5. 2009 [cit. 2012-7-11]. Dostupné z: http://zpravy.idnes.cz/deviant-hovorka-se-dockal-za-zneuziti-dvaceti-chlapcu-mirnejsiho-trestu-14o-/krimi.aspx?c=A090526_073207_krimi_cen

[71] JOHN, R. *Tajemství nigerijských dopisů: Stále existují lidé, kteří se snadno nechají připravit o peníze.* [online]. © 24. 7. 2012 [cit. 2012-8-24]. Dostupné z: http://www.reflex.cz/clanek/zpravy/47196/tajemstvi-nigerijskych-dopisu-stale-existuji-lide-kteri-se-nechaji-snadno-pripravit-o-penize.html

[72] MILLEROVÁ, H. *Chtěla být fiktivní dědičkou a přišla o 617.571 korun.* [online]. © 12. 1. 2010 [cit. 2012-8-24]. Dostupné z: http://www.policie.cz/clanek/chtela-byt-fiktivni-dedickou-a-prisla-o-617-571-korun.aspx

při výbuchu bomby, a na jeho účtu po něm zůstala finanční částka 22.500.000 amerických dolarů. Bance se údajně nepodařilo zjistit žádnou osobu v příbuzenském vztahu k zemřelému Musa Omaru Numarovi, proto Patrik Chan požádal oběť, zda by se nevydávala za jeho příbuznou. Garantoval vyřízení veškerých formalit spojených s dědickým řízením a převedení uvedených finančních prostředků na účet s požadavkem, že mu oběť následně zašle 70 % z této částky. Oběť odkázal na Pietera Rodolfa, jenž měl pracovat v bankovním ústavu v Nizozemí a který jí měl zajistit založení účtu u této banky za účelem převodu peněz. Mladá žena kontaktovala Pietera Rodolfa, jenž ji zařídil fiktivní účet u neexistující banky v Nizozemí a prostřednictví za tímto účelem úmyslně založených webových stránek, navodil u poškozené dojem, že má skutečně zřízený účet u banky.

Z oběti bylo vylákáno nejdříve 3900 amerických dolarů, následně v červenci 2009 z údajného důvodu osvobození od daně, oběť uhradila částku ve výši 29.250 amerických dolarů. Transakce byly potvrzeny Pieterem Rodolfem, který oběti následně poslal číselný kód. Ten byl potřebný pro zadání příkazu k převodu peněz z účtu banky v Nizozemí na účet v České republice. Po zadání číselného kódu byla oběť požádána o další autorizační kód. Oběť opětovně kontaktovala Pietera Rodolfa, který ji sdělil, že je potřebné uhradit tzv. antiteroristický kód nutný k převodu tak vysoké částky do jiné banky. Za tento kód požadoval po oběti finanční částku ve výši 49.550,60 amerických dolarů. Požadovanou částku oběť již neodeslala. Oběti vznikla škoda ve výši 617.571 korun českých. Policie dne 6. ledna 2010 zahájila trestní řízení a požádala o spolupráci Europol.

Případ 5. Výhružné e-maily na Masarykově univerzitě v Brně

V březnu 2009 podal profesor Jaroslav Hroch z Filosofické fakulty brněnské Masarykovy univerzity trestní oznámení na neznámého pachatele, který mu od prosince 2008 zaslal devět anonymních e-mailů. Vzkazy obsahovaly výhrůžky smrtí, konkrétně: aby si dal pozor na přechodech pro chodce, nechodil ven mezi lidi, protože jej může potkat něco zlého, nechal se zavřít na psychiatrii, v trolejbusu si nesedal, protože na sedačce může být na něj nastražená infikovaná jehla z injekční stříkačky apod.

V rámci policejního šetření byly ověřovány čtyři IP adresy[73] počítačů a následně bylo zjištěno, že dvě z nich postupně patřily počítači, který byl umístěn v pracovně profesora Horyny a docenta Brázdy. V dané době, kdy byly ze serveru seznam.cz odeslány některé anonymní e-maily, byl na fakultním serveru otevřen z téhož počítače i fakultní poštovní účet profesora Břetislava Horyny. Vyšetřování bylo dvakrát pozastaveno, protože nebyly nalezeny dostatečné důkazy, které by vedly k odhalení pachatele. O rok později, na podzim roku 2010, bylo zahájeno zrychlené soudní řízení s B. Horynou, který byl obviněn z autorství anonymních výhružných e-mailů. V reportáži Petra Albrechta z ČT1[74] odvysílané 4. listopadu 2010 byl profesor Horyna označen za odesílatele e-mailů a viníka. Kauza rozdělila členy i studenty katedry. Jedna skupina odsoudila přístup ČT za porušení principu presumpce neviny a vytýkala profesoru Hrochovi aktivitu na medializaci případu. Druhá skupina fakultní veřejnosti žádala okamžité propuštění profesora Horyny.

V únoru 2012 byl vynesen prvoinstanční rozsudek, jímž byl profesor Horyna uznán vinným a odsouzen k zaplacení peněžité pokuty ve výši 50.000 korun českých. Po dalších odvoláních a soudních jednáních byl koncem května 2012 rozsudek potvrzen v nezměněné podobě a nabyl právní moci. Motiv činu se doposud nepodařilo zjistit. Břetislav Horyna vinu odmítá s tvrzením, že k vyhrožování neměl důvod. Tvrdí, že někdo zkopíroval jeho IP adresu a tu přidal do výhrůžných e-mailů, aby tak vzniklo podezření, že pisatelem je právě on.[75] Na tom, kdo e-maily skutečně posílal, se neshodli ani odborníci na počítačové technologie. Proti Horynovi tedy neexistuje žádný přímý důkaz. Řetězec těch nepřímých však dle soudu jasně svědčí o jeho vině.

J. Hrochovi nebyly z „finančních důvodů“ pro akademický rok 2012/2013 vypsány žádné termíny kurzů. B. Horyna byl v roce 2012 uvolněn ze všech funkcí, do nichž byl jmenován děkanem, tj. z členství v Ediční radě a ve Vědecké radě, a byla mu

[73] *IP adresa* – číslo, které identifikuje internetové rozhraní v počítačové síti, která používá IP (internetový protokol)

[74] CESKATELEVIZE.CZ. *Profesor filozofie vyhrožoval kolegovi smrtí*. [online]. © 4. 11. 2010 [cit. 2012-8-30]. Dostupné z: http://www.ceskatelevize.cz/ct24/regiony/jihomoravsky-kraj/106264-profesor-filozofie-vyhrozoval-kolegovi-smrti-pujde-pred-soud/

[75] IHNED.CZ. *Pokuta nebo vězení. Profesor odsouzen za vulgární maily kolegovi*. [online]. © 21. 2. 2011 [cit. 2012-8-30]. Dostupné z: http://mam.ihned.cz/cesko/c1-50699500-pokuta-nebo-vezeni-profesor-odsouzen-za-vulgarni-maily-kolegovi

pozastavena výuka v povinných kurzech.[76] Od vynesení rozsudku je v pracovní neschopnosti.

Případ 6. Šíření počítačového viru v České republice

Na podzim roku 2012 upozornila Policie České republiky na stoupající počet případů, ve kterých docházelo k šíření počítačového viru, konkrétně k infikování počítačů trojským koněm. Po aktivaci kódu se dotčenému uživateli na monitoru zobrazilo fiktivní hlášení psané krkolomnou češtinou, ve kterém byl uživatel s odvoláním na různé paragrafy upozorněn na skutečnost, že jeho počítač byl *„zablokován Policií ČR z důvodu porušování autorských práv, nakládáním s materiály obsahující dětskou pornografii či šířením spamů.“*[77] Jednání spočívalo v šíření počítačového škodlivého kódu spolu s neoprávněným podvodným lákáním finančních prostředků. Útok se skládal částečně z technického útoku, při kterém se dostala informace k poškozenému, a dále ze sociálního inženýrství, jehož prostřednictvím byly po dotčených uživatelích požadovány peníze, tzv. složení kauce, po jejímž zaplacení měl být počítač opětovně odblokován. Policie upozornila veřejnost, aby na podobné výzvy nereagovala. Vyloučila, že by uvedeným způsobem realizovala zákonná opatření směřující k případným pachatelům trestních činů. Policie identifikovala více zdrojů šířících inkriminovaný škodlivý kód, který se objevoval zejména na erotických stránkách nebo při instalaci nelegálních software. *„Po aktivaci virus stahoval citlivá data, zároveň mohl spustit i webkameru, pomocí které bylo možné pořídit snímek dotčeného uživatele, který útočníci umístili do horní části zprávy, včetně uvedené města, ve kterém se IP počítače nachází.“*[78] Poškozených byly desítky, někteří z nich požadovanou částku skutečně zaplatili. Pokud byl počítač off-line, bylo možné na něm

[76] PHIL. MUNI. CZ. *Vyjádření Filosofické fakulty k případu výhružných e-mailů*. [online]. © 17. 7. 2012 [cit. 2012-8-30]. Dostupné z: http://www.phil.muni.cz/wff/home/vyveska/vyjadreni-vedeni-filozoficke-fakulty-k-pripadu-vyhruznych-e-mailu

[77] VIRY. CZ. *Policie ČR Vás sleduje.* [online]. © 5. 10. 2012 [cit. 2012-11-21]. Dostupné z: http://www.viry.cz/policie-cr-vas-sleduje/

[78] TOPINKOVÁ, M. *Policie varuje před počítačovým virem, který se šíří Internetem v Česku*. [online]. © 8. 10. 2012 [cit. 2012-11-22]. Dostupné z: http://zpravy.idnes.cz/sireni-pocitacoveho-viru-0yf-/krimi.aspx?c=A121008_144459_domaci_maq

normálně pracovat. „*Závadná stránka se automaticky spustila po připojení počítače k Internetu, čímž se kompletně zablokoval*.“[79]

Případ 7. Phishingový útok na klienty České spořitelny

Dne 10. října 2006 se v e-mailových schránkách mnoha uživatelů českého Internetu objevil na první pohled legitimní e-mail, který vyzýval uživatele k přechodu na nový bezpečnostní systém České spořitelny.[80] Důvodem byly údajné množící se případy podvodů. E-mail byl napsán specifickou češtinou bez diakritiky a nebyl doručován pouze klientům České spořitelny, ale obecně na velké množství českých schránek. E-mail v závěru uživateli jasně sděloval, že v případě ignorace přechodu na nový bezpečnostní standard bude bankovní účet zablokován do okamžiku prokazatelné a komplexní identifikace uživatele. Odkaz, který byl součástí zprávy a na první pohled ukazoval na regulérní stránky České spořitelny, v sobě skrýval odkaz na úplně jiný server s falešnou webovou stránkou, která se tvářila jako přihlašovací stránka České spořitelny, včetně virtuální klávesnice s pomocí které bylo možné zadat heslo. V e-mailu se dokonce uváděla možnost potenciálních nesrovnalostí, které byly zdůvodněny zkušebním provozem systému. Desítky klientů nátlaku podlehlo a identifikační údaje k internetovému bankovnictví prostřednictvím falešné webové stránky vyplnilo. Případ se opakoval v roce 2008 rafinovanějším způsobem, jenž představoval anglicky psané maily s předmětem „anketa spokojenosti klienta“. I přes neobvyklost komunikace s klientem v cizím jazyce měl i tento případ své oběti. V souvislosti Českou spořitelnou se objevily i další podvodné maily, které měly charakter varovné zprávy z banky proti phishingu.[81]

[79] CESKATELEVIZE.CZ *Počítačový virus se tváří jako zpráva od policie*. [online]. © 7. 11. 2012 [cit. 2012-11-22]. Dostupné z: http://www.ceskatelevize.cz/zpravodajstvi-brno/zpravy/202531-pocitacovy-virus-se-tvari-jako-zprava-od-policie-pozaduje-zaplaceni-pokuty/

[80] KRČMÁŘ, P. *Český phishing v akci*! [online]. © 13. 10. 2006 [cit. 2012-11-30]. Dostupné z: http://www.root.cz/clanky/cesky-phishing-v-akci/

[81] HOVORKA, M. *Další podvodný e-mail proti České spořitelně, tváří se jako varovná zp*ráva z banky. [online]. © 12. 3. 2008 [cit. 2012-12-02]. Dostupné z: http://www.podnikatel.cz/clanky/dalsi-podvodny-e-mail-proti-ceske-sporitelne/

Případ 8. Falešná identita na Facebooku, pohlavní zneužití nezletilého chlapce

Dva muži ve věku dvacet a dvaadvacet let si založili fiktivní dívčí profil na Facebooku za účelem navázat kontakt s nezletilým třináctiletým chlapcem, kterého si předem vyhlédli. Pod falešnou identitou vylákali z chlapce jeho nahou fotografii, kterou ho posléze rovněž pod stejnou identitou vydírali. „Dívka" hrozila rozesláním fotografie jeho kamarádům a spolužákům, v případě, že nebude mít sex s vedoucími skautského oddílu.[82] Původně se chlapec domníval, že skautští vedoucí mu pomáhají vyhnout se veřejné ostudě.

Dle informací matky týraného chlapce, které sdělila televizi Nova, docházelo k análnímu a orálnímu styku, točení videa a fotografování nahého těla. Útočníci měli rozpis, který den chlapce zneužíval bratr Piškot a který den bratr Meluzín a který den chlapce zneužívali oba najednou.[83] Matka na událost přišla poté, co objevila v synově počítači celou komunikaci na Facebooku. Podle ní byl hoch na pokraji sebevraždy. Psycholožka vzhledem k síle emočního vypětí hocha deklarovala bezpodmínečnou nutnost odborné psychoterapie s cílem bezodkladně řešit několikaměsíční traumatický zážitek a eliminovat psychické dopady do budoucna.

3.2 Popis případů ze zahraničí získaných obsahovou analýzou dat z Internetu

Případ 9. Operace Trident Breach

Jedná se o případ ohromné sofistikovanosti a ukázku perfektně organizovaného zločinu skupiny hackerů, kteří vymysleli nový a propracovaný systém obohacování se přes Internet. Skvěle organizovaný a strukturovaný systém, který vyžadoval mnoho spolupracujících lidí. V kauze, která je vedena pod názvem „Operation Trident

[82] IDNES.CZ. *Mladí skautští vedoucí vydírali svého svěřence a nutili ho k sexu*. [online]. © 26. 3. 2012 [cit. 2012-12-04]. Dostupné z: http://zpravy.idnes.cz/skautsti-vedouci-vydirali-sveho-sverence-a-nutili-ho-k-sexu-pqw-/krimi.aspx?c=A120326_202533_krimi_js

[83] TV NOVA. *Chlapce z Ústí sexuálně zneužívali vedoucí ve skautu! Vymysleli na něj léčku na Internetu.* [online]. © 28. 3. 2012 [cit. 2012-12-06]. Dostupné z: http://tn.nova.cz/zpravy/cernakronika/chlapce-sexualne-zneuzivali-vedouci-ve-skautu-vymysleli-na-nej-lecku-na-internetu.html

Breach“[84], útočníci ukradli 70 milionů dolarů z výplatních účtů 390 amerických společností a organizací i z privátních bankovních účtů.

Prvním krokem bylo napadení stovky tisíc domácích počítačů v USA počátkem roku 2008, a to použitím zákeřného trojana pod názvem Zeus. Když uživatel klikl na přílohu anebo e-mailový odkaz, Zeus okamžitě infikoval počítač. Trojan byl vytvořen za účelem vykrást bankovní účty napadených uživatelů. Vykradení proběhlo po zjištění vstupních dat přihlášením se do elektronického bankovnictví prostřednictvím software keylogger, který byl do počítače nainstalován automaticky otevřením infikovaného souboru společně se stažením trojana.

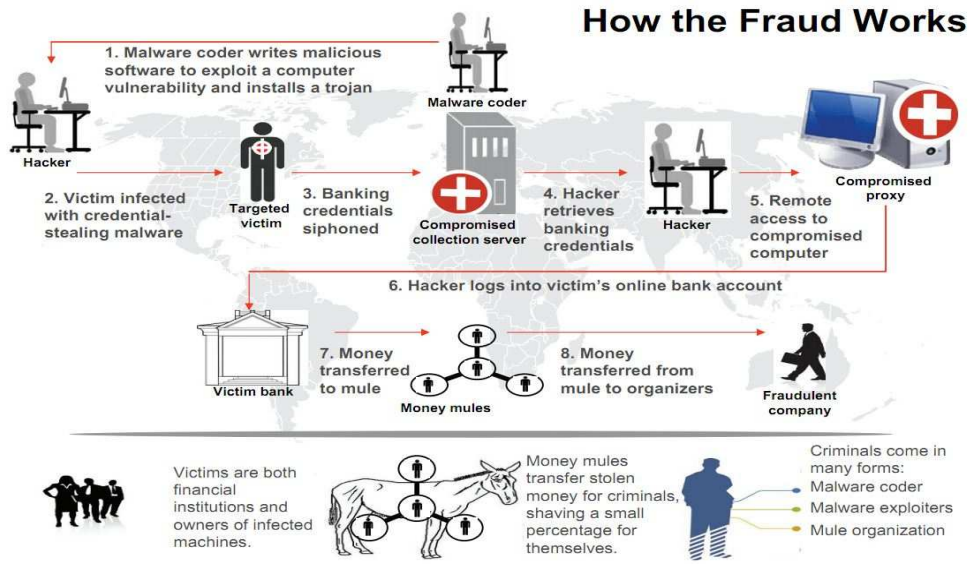
Kauza Trident Breach je specifická tím, že útočníci jako druhý krok vytvořili síť takzvaných „money mules“[85], peněžních mezků, původně mnohdy nic netušících Američanů, kterým posílali e-maily s lákavými nabídkami na velice výhodnou práci z domova. Název pracovní pozice byl „Manažer transakcí pro mezinárodní společnost“ (schéma organizace podvodu viz obrázek 1).

Podmínkou bylo, aby si „zaměstnanci“ otevřeli nový vlastní účet v bance. Útočníci převáděli peníze z firemních účtů typu Automatic Clearing House (dále jen ACH) na účty money mules, kteří následně za desetiprocentní provizi převáděli finanční částky přes Western Union a MoneyGram do východní Evropy. Banky po čase pojaly podezření a nastavily nová bezpečnostní opatření. Transakce přes určité účty začaly blokovat.

[84] WILLIAMS, B. *University professor helps FBI crack $ 70 million cybercrime ring*. [online]. © 21. 3. 2012 [cit. 2012-10-25]. Dostupné z: http://rockcenter.msnbc.msn.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring#comments

[85] *Money mule* – osoba najata podvodníky, nejčastěji formou podvodných mailů nabízejících práci z domova, za účelem praní peněz. Osoba často nemá povědomí o pravém účelu finančních transakcí.

Obrázek 1: Schéma podvodu případu Trident Breach



Zdroj: KREBSONSECURITY. *Ukraine Detains 5 Individuals Tied to $ 70 Million in U. S. eBanking Heists*. [online]. © 10. 9. 2012 [cit. 2012-10-25]. Dostupné z: http://krebsonsecurity.com/tag/operation-trident-breach/

Útočníci reagovali najmutím studentů z Ruska, jimž zařídili falešné pasy, studentská víza a pomohli s přesunem do USA, konkrétně do lokality New York. Mimo USA byla síť money mules rozhozena i na Ukrajině a v Holandsku.

Do dnešního dne není jasné, zda všichni studenti věděli o tom, že jsou najmutí na zločineckou činnost. Opět se opakoval stejný model: studenti si otevřeli několik vlastních bankovních účtů, přes které převáděli peníze svým šéfům. Organizace byla tak funkční a sofistikovaná, že nikdo ze zainteresovaných zúčastněných nepočítal s odhalením.

K odhalení ve velké míře pomohl profesor Warner, který pomocí techniky dolování dat a hledáním skrytých souvislostí sestavil linii mezi počítači infikovanými trojanem Zeus. Stopy ho přivedly až na Ukrajinu, čímž bylo mnoho hackerů a jejich money mules identifikováno.

Osmnáct money mules zůstalo v USA na svobodě. Opět pomohl profesor Warner se svými studenty, kteří použili speciální techniky pro stopování internetových zločinců. Začali surfovat po sociálních sítích Facebook a VKontakte (ruská obdoba Facebooku) a byli velice rychle schopni z profilových stránek identifikovat téměř všechny money mules, kteří zůstali na svobodě v USA. Money mules detekovali podle fotek, na kterých byla například jedna dívka vyfocena se svazkem stodolarových bankovek, jiný chlapec

zveřejnil svoji fotografii, na které popíjel se svými přáteli v baru a byl oblečen v tričku I love New York, další hoch prezentoval sebe a nové auto, které si právě zakoupil.

Na operaci spolupracovali FBI, Sluzhba Bezpeky Ukrajiny (dále jen SBU) a The Netherland´s Police Agencies Hit Tech Crime Unit. Vůči devadesáti dvěma lidem bylo vzneseno obvinění, třicet devět lidí bylo zatčeno.[86] Důvodem, proč byl případ úspěšně vyřešen, byla i skutečnost, že zločinci, kteří měli své profily na Facebooku, neměli profily s ohledem na soukromí nijak zabezpečené.

Případ 10. Bullying Trial, Tyler Clementi Case

Případ byl mediální bombou, vyvolal vlnu protestů vůči kyberšikaně a ostré diskuse o sexuální předpojatosti a mezikulturních rozdílech. Případ doposud není jednoznačně posuzován. Podle *Abc.news*, které se předmětné kauze s ohledem na jednotlivé body obžaloby detailně věnovaly, existují bipolární úhly pohledu na události i spouštěcí mechanismy.[87] Případ se odehrál se v září 2010 a týká se studentů Rutgersovy University v Piscataway v New Jersey. Student Tyler Clementi byl prostřednictvím webkamery špehován svým spolubydlícím Dharunem Ravi v čase, kdy se svým intimním přítelem trávil čas ve studentském pokoji.

Clementi požádal Raviho o uvolnění pokoje na večer kvůli očekávané návštěvě. Ravi pokoj uvolnil, ale v mezičase aktivoval webkameru na notebooku. Následně sledoval aktivity Clementiho i jeho přítele a předmětnou informaci publikoval a komentoval na Twitteru. Zpráva se tak dostala ke všem Raviho „followers“, včetně Tylera. Druhý den proběhla konfrontace obou studentů a i přesto Tyler opětovně požádal Raviho o soukromí pro další večer. Student Ravi pokoj uvolnil, opět aktivoval webkameru a informaci o pravděpodobném intimním kontaktu zveřejnil na Twitteru.

Ke druhému špehování již nedošlo, protože přítel studenta Tylera kameru zakryl. Tyler druhý den požádal o změnu pokoje a jako důvody uvedl šikanu a narušování soukromí. Dne 22. září Tyler Clementi spáchal sebevraždu skokem z Washingtonova

[86] KREBSONSECURITY. *Ukraine Detains 5 Individuals Tied to $ 70 Million in U. S. eBanking Heists*. [online]. © 10. 9. 2012 [cit. 2012-10-25]. Dostupné z: http://krebsonsecurity.com/tag/operation-trident-breach/

[87] ABCNEWS. *Tyler Clementi Suicide*. [online]. © 2010–2012 [cit. 2012-10-27]. Dostupné z: http://abcnews.go.com/topics/news/tyler-clementi-suicide.htm

mostu v New Yorku. Svůj úmysl před skokem zveřejnil na Facebooku. Případ vyvolal obrovské genderové protesty i striktní odsouzení kyberšikany. Student Dharun Ravi čelil 35 bodům obžaloby, které mimo jiné obsahovaly kyberšikanu, narušování soukromí, sexuální předpojatost, zastrašování z předpojatosti, neoprávněné zasahování do soukromí a nelegální pořizování důkazného materiálu, ovlivňování svědků, křivé výpovědi a jiné delikty.[88]

Po dlouhém procesu, ve kterém vyplavalo na povrch mnoho dalších detailů týkajících se vzájemných vztahů mezi Ravim a Clementim, byl Ravi uznán vinným z dvaceti čtyř bodů obžaloby. Šetření kauzy odhalilo špatné vzájemné vztahy mezi Ravim a Clementim, který Raviho diskriminoval a osočoval kvůli indickému původu. Zjistilo se, že špehování a zveřejnění Clementiho orientace nebylo jediným důvodem Clementiho sebevraždy. Z tohoto důvodu nebyl Ravi odsouzen k přísnému trestu odnětí svobody a rovněž nebyl deportován z USA.

Raviho jednání nebylo shledáno úmyslem spáchat trestní čin a rovněž se neprokázaly nejzávažnější body obžaloby, konkrétně úmysl způsobit újmu z důvodu sexuální předpojatosti, narušení soukromí za účelem vyhrožování a vydírání kvůli sexuální orientaci. Ravi si současně nebyl vědom faktu, že svým počínáním páchá trestní čin.

Případ 11. Happy slapping

- Velká Británie, srpen 2009: dva teenageři Leon Elcock a Hamza Lyzai, členové gangu „happy slapping“, napadli a před očima jeho tříleté vnučky brutálně ubili důchodce Ekrama Haquea.[89] Důchodce následkům zranění podlehl. Jeho smrt byla vyústěním série happy slapping útoků, které byly nahrávány na mobilní

[88] DEMARCO, M. *Live coverage: Dharun Ravi found guilty on most counts in webcam spyimg trial verdict*. [online]. © 16. 3. 2012 [cit. 2012-09-10]. Dostupné z: http://www.nj.com/news/index.ssf/2012/03/ravi_webcam_trial_verdict.html

[89] YOUTUBE. *The Happy Slapping Killing of Ekram Haque*. [online]. © 26. 7. 2010 [cit. 2012-09-11]. Dostupné z: http://www.youtube.com/watch?v=sP37aSPTHWg&oref=http%3A%2F%2Fwww.google.cz%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D2%26ved%3D0CC0QFjAB%26url%3Dhttp%253A%252F%252Fwww.youtube.com%252Fwatch%253Fv%253DsP37aSPTHWg%26ei%3DcGw-UNCXEszItAbn9oFQ%26usg%3DAFQjCNFsrSYTgXvbQOvUM--hRzb086jIKw

telefony, a později publikované na Internetu.[90] V průběhu vyšetřování bylo u členů gangu nalezeno šest nahraných videí útoků.

- Velká Británie, 9. červen 2005: dva dospívající mladíci napadli 17letou studentku Kerry Sevillovou. Jeden z nich ji střelil do nohy vzduchovkou, zatímco druhý celý čin nahrával na svůj mobil. Video bylo následně umístěno na Internet.
- Velká Británie, 18. červen 2005: policie zatkla tři 14leté chlapce, kteří byli podezřelí ze znásilnění 11leté dívky. Vedení školy bylo na tento čin upozorněno poté, co jeden ze školních zaměstnanců našel záznam tohoto činu na mobilu jednoho ze studentů.
- Velká Británie, prosinec 2005: byl zavražděn David Morley. Z jeho neúmyslného zabití byli shledáni vinnými 15letá dívka Chelsea O'Mahoneyová a spoluobžalovaní Reece Saergant (21 let), Darren Case, (18 let), a David Blenman,(17 let). Dle hlášení O'Mahoneyová udělala dokument o tom, jak parta jejích kamarádů ukopala Davida k smrti.
- Austrálie, 23. říjen 2006: policie zahájila vyšetřování ve věci DVD, které mimo jiné obsahovalo záznam, kdy pár dospívajících mladíků pohlavně zneužilo jednu dívku a poté jí zapálilo vlasy. Kopie nahrávky byly údajně prodány.
- Velká Británie, červenec 2007: Anthony Anderson (27 let) močil na umírající ženu, zatímco jeho kamarád vše natáčel na mobilní telefon. Celou dobu přitom křičel: „Toto je materiál pro YouTube!"[91]

Případ 12. Megan Meier, MySpace hoax

Případ kyberšikany americké teenagerky, do kterého byly zapletené dospělé osoby ze sousedství oběti. Třináctiletá dívka Megan Taylor Meier se přes sociální síť MySpace seznámila s šestnáctiletým pohledným chlapcem Joshem Evansem.

Matka Tina Meier měla prvních šest týdnů internetové přátelství své dcery pod dohledem včetně přihlašovacích údajů do předmětné sociální sítě. Důvodů bylo několik.

[90] BBC. *Happy slapping youths detained for grandfather death*. [online]. © 16. 6. 2010 [cit. 2012-09-10]. Dostupné z: http://www.bbc.co.uk/news/10331547
[91] NEBUĎ OBĚŤ. *Happy slapping (spokojené fackování)*. [online]. © 2010–2012 [cit. 2012-09-10]. Dostupné z: http://www.nebudobet.cz/?page=happy-slapping

Dcera Megan ještě nedosáhla věku čtrnácti let, který je oficiálně požadován jako minimální věk pro vstup do sociální síť MySpace. Sociální síť MySpace požaduje pouze potvrzení, že žadatel o vstup dosáhl věku čtrnácti let, ale tuto skutečnost již dále neověřuje.

Dívka užívala léky proti depresi a trpěla nízkým sebevědomím kvůli nadváze, se kterou od malička bojovala. Matka v obavách, aby nedošlo k eskalaci psychických problémů dcery, dohlížela na veškerou komunikaci dívky na MySpace. Dcera postupně začala s Joshem Evansem komunikovat intenzivněji i proto, že jí dal najevo, že se mu líbí. Joshův zájem Megan velmi povzbudil, stavy deprese začaly u dívky postupně mizet.

Dne 15. října 2006 Megan najednou obdržela od Joshe znepokojivé obvinění týkající se jejího špatného přístupu k přátelům. Pro Megan byla předmětná zpráva naprosto nepochopitelná, proto se dožadovala dalšího vysvětlení. Joshova komunikace se radikálně změnila, začal trefně útočit na slabá místa Megan. Některé zprávy byly sdíleny i s dalšími kamarády Megan, následně se po sociální síti začaly šířit nelichotivé statusy o dívce. Matka tuto skutečnost zjistila další den a zakázala Megan dále na sociální síti komunikovat. Ještě téhož byla Megan, tři týdny před jejími čtrnáctými narozeninami, nalezena v šatně oběšena.

V rámci vyšetřování bylo následně zjištěno, že Josh Evans je ve skutečnosti žena jménem Lori Drew, matka bývalé kamarádky Megan, se kterou se dívka přestala přátelit. Lori Drew společně se svojí osmnáctiletou zaměstnankyní a dcerou Ashley Grills založily imaginární profil na MySpace, jehož účelem bylo pomstít se Megan za ukončení přátelství s Ashley a šíření pomluv. Tři ženy prostřednictvím chatu postupně zjišťovaly důvěrné informace o Megan, aby je posléze mohly využít k ponižování a šikanování.

Případ byl vyšetřován jako internetová šikana, ale kvůli nedostatečným důkazům byla Lori Drew v roce 2009 zproštěna viny. Kauza byla v USA medializovaná, případ se v některých státech v USA zasloužil o změnu legislativy. Za internetové obtěžování a šikanu, v případě jejich prokázání, se stanovily tresty odnětí svobody a vysoké pokuty.

Ve snaze pomoci dalším obětem kybernetové šikany a zabránit dalším tragickým koncům byla v Chesterfield Missouri založena nadace Megan Taylor Meier Foundation, jejíž specializovaní lektoři formou seminářů a interaktivních prezentací šíří ve školách

osvětu a povědomí nejen o hrozbách na Internetu, ale i o dalších negativních jevech, které ohrožují zranitelnou duši dětí v problémovém věku puberty. Manželé Meierovi se po smrti své dcery pod nepříznivým vlivem událostí rozvedli.[92]

Případ 13. Jessica Logan, sexting case

Jessica Logan, osmnáctiletá studentka z Ohia, poslala přes mobilní telefon několik fotek svého nahého těla svému příteli. Po rozchodu rozeslal přítel e-mailem citlivé fotky mnoha spolužákům. Vzhledem k obsahu se elektronická zpráva obrovskou rychlostí rozšířila po celé škole. Jessica byla nucena čelit posměchu, nadávkám, vyloučení z kolektivu a dokonce i fyzickým útokům od spolužaček.[93] Situace byla pro Jessicu tak skličující, že odmítala chodit do školy. Z veselé a společenské dívky se stala psychická troska. Matka se o situaci dozvěděla poté, co od školy obdržela informaci o absencích své dcery.

Jak se později prokázalo, vedení školy o obtěžování Jessicy vědělo, nepodniklo však žádná opatření vedoucí k odstranění nežádoucího stavu. Matka chtěla mluvit s rodiči dívek, které se na šikaně aktivně podílely, ale její dcera, která se v dané situaci projevila jako typická oběť šikany, ji přemluvila, aby ustoupila od záměru a problém zbytečně neeskalovala. Jessica se dva měsíce po rozeslání fotek doma oběsila. Poté, co se vrátila domů z pohřbu své kamarádky, která spáchala sebevraždu.

Matka dívky se po tragické smrti dcery nejdříve psychicky zhroutila, pak podala šest neúspěšných žalob na vedení školy za nečinnost v případě šikany její dcery.[94]

---

[92] MEGANMEIERFOUNDATION.ORG. *Megan Meier´s Story*. [online]. © 13. 11. 2007 [cit. 2012-09-12]. Dostupné z: http://www.meganmeierfoundation.org/megansStory.php

[93] SAMEER. *Sexting, the Jessica Logan case, and what schools can do*. [online]. © 10. 3. 2009 [cit. 2012-09-14]. Dostupné z: http://cyberbullying.us/blog/sexting-the-jesse-logan-case-and-what-schools-can-do.html

[94] GERHARDSTEIN AND BRANCH. *Parents of Jessica Logan resolve case against Sycamoree school district*. [online]. © 2012 [cit. 2012-09-14]. Dostupné z: http://www.gbfirm.com/parents-of-jessica-logan-resolve-case-against-sycamore-school-district/

Případ 14. Star Wars kid

V květnu 2003 se Ghyslain Raza stal celosvětově známým pod přezdívkou „Star Wars kid“ (Kluk ze Star Wars) díky amatérské videonahrávce z roku 2002, na níž se nepříliš zdařile pokouší ztvárnit svou oblíbenou postavu z Hvězdných válek, Dartha Maula. Jeho spolužáci nahrávku nalezli a zveřejnili na Internetu pod jménem „Jackas starwars funny“.[95] Nahrávka se stala nesmírně populární, během následujících dvou týdnů zaznamenal server několik miliónů stažení této nahrávky a byly k ní přidávány různé zvukové a světelné efekty. Jen do roku 2010 bylo virální video shlédnuto více než miliardou lidí.[96] Časem vznikly různě upravené a sestřihané nahrávky využívající zároveň scény z filmů jako Pán prstenů, Matrix Reloaded, Kill Bill a jiné. V roce 2008 byl Raza parodován v seriálu South Park v epizodě Canada on Strike.

Chlapec následkem zesměšňování a ponižování utrpěl těžký psychický otřes a musel se podrobit dlouhodobému léčení. Nahrávka velmi okatě demonstrovala jeho nadváhu a neohrabanost, což řada diváků z internetového světa komentovala na svých stránkách a blozích. Vzhledem ke svým důsledkům je publikování této nahrávky často udáváno jako první celosvětově známý příklad kyberšikany se závažnými důsledky. Zveřejnění mělo i soudní dohru ve formě žaloby spolužáků.[97]

Případ 15. Sebevražda Ryana Halligana

Ryan Halligan, třináctiletý kluk z Vermontu v USA, spáchal v roce 2003 sebevraždu následkem dlouhodobé šikany od spolužáků, kteří o něm na Internetu rozšířili pomluvu o jeho údajné homosexualitě. Ryan dostával přes Internet mnoho výhrůžných a posměšných vzkazů. Ve stejné době Ashley, ve škole oblíbená spolužačka, která s Ryanem chatovala a předstírala, že se jí líbí, zveřejnila celou vzájemnou korespondenci, aby Ryana před spolužáky ponížila.

---

[95] YOUTUBE. *jackass_starwars_funny*. [online]. © 26. 1. 2006 [cit. 2012-09-22]. Dostupné z: http://www.youtube.com/watch?v=o0IuErI3CV0

[96] PASTERNACK, A. *After Lawsuits and Therapy Star Wars Kid is Back*. [online]. © 2011 [cit. 2012-09-23]. Dostupné z: http://motherboard.vice.com/2010/6/1/after-lawsuits-and-therapy-star-wars-kid-is-back

[97] NNDB. *Ghyslain Raza*. [online]. © 2012 [cit. 2012-09-23]. Dostupné z: http://www.nndb.com/people/441/000031348/

Kamarád, se kterým si Ryan v té době dopisoval, měl na něj velice negativní vliv. Utvrzoval Ryana v tom, že pokud se zabije, lidé, kteří mu ubližují, se budou cítit provinile. V říjnu 2003 spáchal Ryan sebevraždu oběšením. Otec se dozvěděl veškerá fakta o šikaně až ve chvíli, kdy po Ryanově smrti společně s policií prozkoumali jeho počítač. Spolužačka Ashley poté, co se dozvěděla o Ryanově sebevraždě včetně důvodů, chtěla sama spáchat sebevraždu, protože se cítila vinna za to, že k Ryanově tragické smrti částečně přispěla. V kauze nebyl nikdo obviněn, protože dle stanoviska policie neexistoval zákon, na základě kterého by mohli viníky obvinit z trestného činu.[98]

Případ 16. Sebevražda Amandy Todd

Patnáctiletá Amanda Todd spáchala sebevraždu kvůli kyberšikaně, ponižování a vydírání. Dne 7. září 2012 Amanda umístila na YouTube vlastní video „My Story: Struggling, bullying, suicide and self harm“[99], ve kterém se pomocí popsaných kartiček snažila sdělit svoje trápení a negativní zkušenosti s vydíráním, šikanou a fyzickým napadením. Na videu informuje veřejnost o využívání video chatu s úmyslem seznámit se s novými lidmi. Jeden z nových přátel ji přesvědčil, aby na kameru obnažila své poprsí. Později dívku vydíral zveřejněním pořízené fotky, pokud se mu na kameru opět neobnaží. Předmětné fotky i další materiál byly na Internetu později zveřejněny, což u Amandy způsobilo deprese a panickou poruchu. I přes změnu bydliště se psychický stav dívky zhoršoval, až nebyla schopna opustit byt. Později se vyděrač znovu objevil na scéně, založením facebookového účtu s profilovou fotkou obnažené Amandy, která se po tomto zjištění neúspěšně pokusila o sebevraždu. Po návratu z nemocnice dívka zjistila, že na facebookovém účtu se objevilo mnoho vulgárních komentářů. Rodina se opět přestěhovala, ale minulost Amandu dohánělа dalšími urážlivými komentáři na jejím skutečném facebookovém profilu. Následoval další neúspěšný pokus o sebevraždu. Poté 7. září 2012 Amanda publikovala zmíněné video. Dne 10. října 2012 byla doma nalezena mrtvá.

[98] RYANPATRICKHALLIGAN.ORG. *Ryan´s story*. [online]. © 2010 [cit. 2012-09-17]. Dostupné z: http://www.ryanpatrickhalligan.org/

[99] YOUTUBE. *My story: Struggling, Bullying, Suicide, Self Harm, #RIPAmanda Todd*. [online]. © 7. 9. 2012 [cit. 2012-09-17]. Dostupné z: http://www.youtube.com/watch?v=vOHXGNx-E7E

Aktivistická skupina Anonymous identifikovala jako Amandina údajného vyděrače a trýznitele muže ve věku 32 let. Zveřejnila jeho jméno a adresu na sociálních sítích. Policie po prozkoumání tipu informovala veřejnost, že veškerá obvinění jsou nepodložená. Zveřejnění identity nařčené osoby vyústilo v tisíce facebookových výhrůžek smrtí.[100]Případ se v době zpracování předložené diplomové práce vyšetřuje jako sebevražda, investigace se zaměřuje na monitorování obsahu sociálních sítí.[101]

Případ 17. Chris Chaney, Operace Hackerazzi

Pětatřicetiletému Američanovi Christopheru Chaneymu se podařilo neoprávněně vniknout do zabezpečených počítačů a ukrást identitu a přihlašovací údaje k e-mailovým účtům asi padesáti hollywoodských celebrit.[102] K privátním e-mailovým adresám celebrit se dostal různými kombinacemi jmen a příjmení a jejich přiřazováním k Gmailu. Když detekoval funkčnost adresy, zajišťoval si přístup k e-mailovému účtu prostřednictvím funkce zapomenutého hesla. V případě zapomenutého hesla je nutné odpovědět na bezpečnostní otázky, které obvykle představují dotazy typu jména zvířete, jména matky za svobodna, jméno manžela, jméno uživatele za svobodna, oblíbený film apod.

U celebrit jsou odpovědi na podobné dotazy velmi snadné vzhledem k pravidelnému zveřejňování jejich osobních informací a soukromého života v médiích. Chaney hledal potřebné informace na blozích, v bulváru, na sociálních sítích Classmates.com, Twitteru, Facebooku apod. Nejdříve se mu podařilo dostat se k několika málo účtům celebrit, ze kterých následně získal další funkční e-mailové kontakty. Poté, co nelegálně pronikl k účtům, nastavil v nich odesílání kopií zpráv na svůj účet, který měl vytvořený speciálně pro daný účel. Během jednoho roku monitoroval e-mailovou komunikaci nejznámějších hollywoodských celebrit. V několika případech psal jménem celebrit,

[100]SHAW, G., SINOSKI, K. *B. C. man denies harrassing Amanda Todd; RCMP say allegations are „unfounded“*. [online]. © 17. 10. 2012 [cit. 2012-11-20]. Dostupné z: http://www.ottawacitizen.com/news/denies+harassing+Amanda+Todd+RCMP+allegations+unfounded/7400309/story.html

[101] ABC. NEWS. *Bullied Teeen Leaves Behind Chilling You Tube Video*. [online]. © 12. 10. 2012 [cit. 2012-11-20]. Dostupné z: http://abcnews.go.com/International/bullied-teen-amanda-todd-leaves-chilling-youtube-video/story?id=17463266#.UMPAp3dXsms

[102] FBI. LOS ANGELES. *Florida Man Arrested in „Operation Hackerazzi“ for Targeting celebrities with Computer Intrusion, Wiretapping, and Identity Theft*. [online]. © 12. 10. 2011 [cit. 2012-11-05]. Dostupné z: http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft

kterým se neoprávněně dostal k účtu, maily dalším známým osobám se žádostmi o fotky pod různými záminkami. Poté, co se mu prostřednictvím e-mailu a Twitteru podařilo proniknout do mobilního telefonu herečky Scarlett Johansson,[103] ukradl a vypustil na Internet její nahé fotky. Chaney zpočátku nedisponoval žádnými speciálními počítačovými dovednostmi. Původní zvědavost přerostla v závislost, která následně generovala potřebu zdokonalit se počítačové oblasti. Christopher Chaney byl v březnu 2012 uznán vinným z devíti zločinů včetně krádeže identity, krádeží a zneužití dat a nelegálnímu nabourání se do zabezpečených počítačů.

Případ 18. Kauza Justina Berryho, internetové porno

Justin Berry byl chlapec z rozvrácené rodiny, který byl v dětství fyzicky napadán svým otcem. Byl osamělý, realizoval se ve světě počítačů, ve svých třinácti letech si vytvořil vlastní webové stránky. Jeden z jeho přátel mu ukázal webkameru, již získal za registraci u internetového poskytovatele Earthlink. Justin ve snaze získat pomocí kamery více přátel na Internetu se u předmětného poskytovatele zaregistroval a po instalování kamery si nahrál potřebný software. Jeho fotografie i s kontaktními údaji byla automaticky vyvěšena na spotlife.com, internetový seznam uživatelů webových kamer.

Justina během pár minut kontaktoval první predátor, poté se v rychlém sledu začali objevovat další zájemci. Někteří z nich okamžitě přiznali svůj aktuální věk, další se vydávali za mladé dívky, ale po určitém čase odhalili své pohlaví i skutečný věk. Justin nepovažoval jejich chování za ohrožující, naopak se ve své virtuální komunitě cítil velmi příjemně. Jeho noví přátele byli štědří, nabídli mu možnost otevření tzv. „seznamu přání“ a doručování dárků prostřednictvím Amazon.com. Štědří a milí muži, vzhledem k Justinově problematickému vztahu s otcem, u něj hráli velmi významnou a pozitivní roli.

Predátoři hocha postupně zmanipulovali k tomu, aby se jim před kamerou ukázal bez tílka nebo jen v boxerkách. Nátlak se postupně zvyšoval, oběti byly nabídnuty peníze za nahé pózování před kamerou. Matka u chlapce nemonitorovala žádnou změnu chování,

[103] GREGG, M. *How are Celebrity Cellphones Hacked?* [online] © 16. 3. 2012 [cit. 2012-09-10]. Dostupné z: http://www.huffingtonpost.com/michael-gregg/how-are-celebrity-cell-ph_b_1353780.html

pouze častější nemoci, kvůli kterým zůstával doma. Justin časem pronikl do internetového podsvětí a zjistil existenci mnoha dalších teenagerů provozujících stejný byznys prostřednictvím speciálních webových stránek. Situace eskalovala, když Justina kontaktoval jeden z přátel s pozváním do kempu v Michiganu, kde ho sexuálně zneužil.

Justinovy sexuální aktivity se zintenzivnily, hoch vytvořil novou webovou stránku, prostřednictvím které provozoval soukromé sexuální show za vysoké poplatky. Stal se závislým na drogách, na které si musel vydělávat pornografií. Na jedné ze schůzek byl opět sexuálně zneužit jedním ze svých „fanoušků".

V roce 2003 se o problematiku začal zajímat reportér Kurt Eichenwald z New York Times, který Justina kontaktoval pod změněnou identitou. Reportérovi se i vzhledem k zhoršujícímu se psychickému stavu Justina Berryho, který nutně potřeboval léčení i psychologickou pomoc, podařilo přesvědčit ke spolupráci s FBI a odhalit tak síť internetových predátorů zainteresovaných v dětské pornografii.[104]

Případ 19. Zcizení osobních dat za účelem nelegálního výběru peněz z bankovního účtu

Uživatelka z Miami na Floridě slyšela o nebezpečí, jež se vyskytovalo speciálně u internetového prohlížeče, který používala. Chtěla se ujistit, že její domácí počítač je v pořádku. Když došla domů, vyhledala si na Internetu informace o zranitelnosti počítače, aby zjistila, zda je chráněný. S pomocí často používaného vyhledávače nalezla webové stránky, které nabízely nejen informace o zranitelnosti systému, ale měly i možnost automatického stažení ochranného patche[105] na její počítač.

Uživatelka si informace přečetla, ale rozhodla se nepřijmout stažení souborů, protože se dřív naučila stahovat informace pouze ze schválených zdrojů. Pak šla na oficiální stránky webového prohlížeče ke stažení opravy. Zatímco si uživatelka četla informace o zranitelnosti na prvních stránkách, útočníci, kteří stránky vytvořili, využili toho, že její počítač byl v danou dobu napadnutelný. Ve skutečnosti, když klikla na „ne" (k zamítnutí stažení souborů, které byly nabízeny), došlo k instalaci programu

[104] EICHENWALD, K. *Through his Webcam a Boy Joins a Sordid Online World*. [online]. © 2005 [cit. 2012-11-15]. Dostupné z: http://www.nytimes.com/2005/12/19/national/19kids.ready.html?pagewanted=1

[105] *Patch* – část software určená pro opravu problémů a aktualizaci počítačových programů.

crimeware.[106] Program od tohoto okamžiku zaznamenával stisky kláves (keylogger), všechno, co psala, a veškeré informace zároveň odesílal majiteli webových stránek.

Po přihlášení na bankovní účet uživatelky program zaznamenal i tyto úhozy včetně důvěrných informací, jména banky, uživatelského jména, hesla, posledních čtyř cifer identifikačního čísla pojištěnce a jména matky za svobodna. Systém banky byl zabezpečený, všechny údaje byly zakódovány, takže nikdo podél celé trasy nemohl náhodou objevit tyto informace. Keylogger však zaznamenával informace v reálném čase tak, jak je uživatelka zadávala, než došlo ke kódování, proto mohl obejít stávající zabezpečení. Veškeré údaje byly následně prodány útočníkům specializujícím se na používání kradených bankovních informací k nelegálním výběrům. Když uživatelka o několik měsíců později ukládala peníze na svůj účet a vyžádala si výpis, byla v šoku, když zjistila, že její účet je téměř prázdný.[107]

Případ 20. Internetové obtěžování, Seattle

James Robert Murphy po dobu šesti let posílal stovky nevyžádaných a obtěžujících e-mailů své bývalé přítelkyni Joelle Ligon a jejím kolegům v Seattle. Svoji identitu schoval speciálním programem a vytvořil „Anti Joelle Fanclub“, který využíval jako fiktivního odesílatele výhrůžných e-mailů. Murphy původně posílal nepravdivé informace o soukromém životě Joelle Ligon jejím kolegům, včetně nařčení o falešném vysokoškolském diplomu, údajnému neserióznímu postupu, kterým získala místo u nového zaměstnavatele, údajné sexuální deviaci i závislosti na drogách. Samotná Joelle Ligon dostávala výhrůžné e-maily obsahující důvěrné informace z jejího soukromého života. Obtěžování vyústilo v rozeslání pornografického materiálu i žádostmi o sex, a to takovým způsobem, jako kdyby Joelle Ligon sama odeslala e-maily ze své adresy vlastním kolegům.[108] Joelle Ligon identifikovala pachatele, ale nebyla schopna mu to nijak prokázat. Případ začaly vyšetřovat tajné služby, FBI, policie

[106] *Crimeware* – škodlivý software, tajně nainstalován do počítačů speciálně pro usnadnění počítačové trestné činnosti.
[107] NORTON. *Příběhy o počítačové kriminalitě: Sandra.* [online]. © 1995–2013 [cit. 2012-11-20]. Dostupné z: http://cz.norton.com/cybercrime-stories-sandra/article
[108] FBI. *Crime /Punishment. Man Sentenced for Internet Harassment.* [online]. © 2012 [cit. 2012-10-13]. Dostupné z: http://crime.about.com/od/online/a/web_harass.htm

a Federální telekomunikace.[109] V roce 2004, po patnácti měsících vyšetřování, se jim podařilo pachatele usvědčit a následně obvinit z 26 zločinů. Bylo to první federální trestní stíhání na internetové obtěžování.[110]

3.3 Popis případů získaných rozhovory s postiženými uživateli Internetu

Informace byly získány vlastním kvalitativním průzkumem, formou rozhovorů s uživateli Internetu. Jedná se o sedm autentických případů v souvislosti s počítačovou kriminalitou i se zneužitím údajů prostřednictvím Internetu.

Případ 1. Koobface

Nejdříve je nutné objasnit, co je Koobface. Jedná se o nebezpečný počítačový červ napadající sociální sítě. Název Koobface je anagramem ke slovu Facebook. Virus je vytvořen za účelem infikování zejména operačních programů Microsoft Windows. Poprvé se objevil v roce 2008. Původně se zaměřoval na krádeže přihlašovacích údajů do sítě Facebook, následně využíval infikované počítače jako „zombie" – prostředníky pro další nelegální aktivity, tzv. botnet. Na přelomu let 2011 a 2012 byli odhaleni tvůrci červa Koobface, jednalo se o pětičlenný tým ruských hackerů z Petrohradu.[111]

Virus se do počítače se dostává prostřednictvím soukromých zpráv (chatů) mezi jednotlivými uživateli, šíří se rozposíláním zpráv uživatelům sociální sítě, kteří jsou v seznamu přátel někoho, jehož počítač byl už infikovaný. Aby se virus dostal do operačního systému oběti, vyžaduje spolupráci koncového uživatele. Nejčastěji láká uživatele ke stažení falešné aktualizace přehrávače Flash Adobe, zprávou s odkazem na nastražený web (YouTube), kde Koobface čeká na reakci oběti. Kliknutím na

[109] HO, V. *Cyberstalker enters guily plea*. [online]. © 29. 7. 2004 [cit. 2012-10-13]. Dostupné z: http://www.seattlepi.com/local/article/Cyberstalker-enters-guilty-plea-1150519.php
[110] FISCHER, K. *First US Cyberstalking case taking shape*. [online]. © 24. 4. 2004 [cit. 2012-10-13]. Dostupné z: http://arstechnica.com/uncategorized/2004/04/3694-2/
[111] NAKED SECURITY. *The Koobface malware gang – exposed!* [online]. © 1997–2012 [cit. 2012-03-05]. Dostupné z: http://nakedsecurity.sophos.com/koobface/

aktualizaci přehrávače, virus detekuje druh operačního programu a okamžitě se začíná infiltrovat do počítače.

Konkrétní uživatelská zkušenost s Koobface

Šlo o neobvyklou shodu okolností a kumulaci nestandardních, ale do sebe zapadajících, událostí. Uživatelka požádala o přátelství na Facebooku bývalou profesorku angličtiny, která se odstěhovala do USA. Potvrzení přátelství dorazilo, a protože profesorka byla online, uživatelka jí napsala pár slov. Dorazila odpověď v angličtině, respektive krátký pozdrav „hi" a odkaz na internetovou stránku „You look funny in this video" (Vypadáš na tom videu legračně). Vzhledem k aktuálnímu místu pobytu angličtinářky uživatelku anglická komunikace nijak nepřekvapila a na odkaz klikla. Otevřela se stránka YouTube, na které byl odkaz se jménem uživatelky a popisem videa. Uživatelka posléze sdělila, že stránka již na první pohled jevila méně profesionální prvky grafiky než standardní YouTube, přesto ji tato skutečnost nevarovala. Pod standardním oknem YouTube byly odkazy přátel z Facebooku a doporučení, že se jedná o skvělé video, ale je bezpodmínečně nutné aktualizovat novou verzi přehrávače Flash.

Aktualizace se automaticky nabídla. Uživatelka i přesto, že si byla vědoma, že v notebooku má poslední verzi Adobe Flash, klikla na uvedený odkaz. Během několika vteřin si uvědomila, že stahování aktualizace do notebooku probíhá nestandardně jak s ohledem na grafiku, tak i průběh stahování dat. Na monitoru počítače se po několika vteřinách objevila grafika v podobě „modré obrazovky smrti"[112], následně harddisk začal vydávat nestandardní zvuky evokující kolaps systému. Notebook se po chvíli samovolně restartoval.

Bylo zjevné, že notebook byl napaden. Po restartování se v pravém dolním rohu objevila hláška s logem „nového" antivirového programu Mc Affee „*Počítač byl napaden, ale je plně chráněn, není nutné provádět dodatečné žádné akce k zajištění ochrany. Problém se řeší.*"

Hláška zůstala na monitoru i po vypnutí a opětovném zapnutí notebooku. Antivirový program Microsoft Security Essentials, který byl v notebooku před

[112] *Modrá obrazovka smrti (BSoD, Blue screen of death)* – slangové označení chybového hlášení, které operační systém Microsoft Windows zobrazí v situaci, kdy došlo k závažné systémové chybě, ze které není systém schopen se zotavit. Toto chybové hlášení se zobrazí přes celou obrazovku, bílým písmem na modrém pozadí.

restartováním nainstalován, byl z notebooku odstraněn bez zadání příkazu uživatelky. Notebook byl následně zkontrolován programem Malwarebytes Antimalware. Ten v průběhu kontroly našel a odstranil 36 trojanů, které se během stahování nebezpečného software tvářícího se jako Adobe Flash infiltrovaly do notebooku. Hláška Mc Affee po odstranění trojanů z notebooku zmizela.

Bylo však zřejmé, že notebook je stále infikován, indikovala to zcela odlišná grafika dolní lišty na ploše. Domněnku potvrdila i skutečnost, že jakákoliv snaha o stažení antivirového programu z Internetu byla neúspěšná. Notebook se „bránil“ varováním o zdvojení antivirových programů. Opakované pokusy o odstranění falešného Mc Afee z programů byly neúspěšné. Současně proběhlo několik nezdařilých pokusů o přeinstalování do posledního bodu obnovení podle původně nastavených parametrů.

Notebook byl předán osobě, která se problematice informačních technologií věnuje. Falešný Mc Afee blokující instalaci antivirového programu byl odinstalován a následně byl nainstalován jiný antivirový program, který další přítomné hrozby detekoval a odstranil je. V tu chvíli začalo centrum akcí hlásit blokování aktualizací operačního systému. Při hloubkové kontrole bylo zjištěno, že z registrů se funkce aktualizací ztratila a nebylo možné tuto funkci obnovit ani prostřednictvím příkazů. Přistoupilo se k poslednímu možnému řešení, a to k reinstalaci celého operačního systému. Po nové instalaci byl zakoupen antivirus Eset Smart Security 5, který zkontroloval případné zbytky viru na disku C i D.

Notebook po reinstalaci pracuje bez problémů se software. Eviduje se ale možný dopad viru na hardware. Přibližně 3 týdny po události na notebooku přestala fungovat baterka, objevila se i nefunkčnost harddisku. Důvodem bylo pravděpodobně obrovské zatížení systému při instalaci viru do útrob notebooku anebo opakované pokusy zbavit se viru. Jedná se pouze o spekulaci, která je ale vzhledem k časové linii celé události dost pravděpodobným následkem infiltrace viru do systému.

Důležitým faktem je i skutečnost, že přibližně tři měsíce po napadení virem Koobface detekoval antivirový program přítomnost škodlivého kódu Bot, který byl s největší pravděpodobností do notebooku instalován v průběhu infiltrace Koobface. Antivirový program detekoval Bot v momentu, kdy byl vzdáleným příkazem spuštěn k akci.

Případ 2. AceTools.biz

Uživatel si instaloval bezplatnou zkušební verzi překladače AceTools.biz slibující překlady z 35 jazyků. Odkaz na stránky, ze kterých je možné překladač stáhnout, jsou k nalezení standardně na google.com. K datu 2. dubna 2012 byl ke stažení na www.instaluj. cz za 2518 korun českých.

Uživatel během dne zjistil, že se jedná o neprofesionální a nekvalitní program, proto zkušební verzi programu odinstaloval.

Za měsíc uživatel obdržel osobní e-mail od zástupce společnosti AceTools.biz v angličtině. E-mail informoval uživatele o tom, že používá nelegální verzi programu, obsahoval i sdělení o zaprotokolování IP adresy. Závěrem mailu odesílatel vyhrožoval iniciováním trestního řízení, informoval uživatele o následných postizích s vyčíslením pokuty odpovídající legislativě České republiky ve výši 100.000 korun českých a možností trestního stíhání a odsouzení „počítačového piráta“ až na dva roky.

Uživateli byla nabídnuta poslední šance k zakoupení „legální“ verze za cenu 85 euro v časovém horizontu sedmi dnů. V případě neuhrazení poplatku za „legální“ verzi společnost hrozila podáním trestního oznámení a vymáháním vysokého penále. Uživatel si byl vědom, že žádnou nelegální verzi programu nepoužívá, současně tak ho zarazila skutečnost, že společnost poslala vyhrůžku na jeho e-mailovou adresu, kterou při instalaci neuváděl. Uvedený fakt ho inspiroval k surfování po Internetu, aby našel bližší informace o firmě AceTools.biz.

Byly zjištěny zajímavé skutečnosti. Desítky klientů stěžujících si na obtěžování, vydírání a zastrašování zástupci předmětné pochybné společnosti. Bylo zřejmé, že někteří klienti, si software „zakoupili“ pomocí nelegálního klíče vygenerovaného k tomu určeným software. Zcela zásadním problémem byla ale skutečnost, jakým způsobem se firma AceTools.biz dostala k e-mailovým adresám.

Odpověď byla ve spolupráci s autorkou diplomové práce nalezena na internetu. Firma se k e-mailové adrese dostává nabouráním se do počítače právě prostřednictvím instalace software – překladače, který z Microsoft Office Outlook dekóduje e-mailovou adresu uživatele a odešle předmětný údaj firmě AceTools.biz.

Na internetu bylo zjištěno, že obětí jsou desítky. Předmětná problematika zkoumající tak zaujala, že začali společně pátrat, odkud mail dorazil. Každý e-mail zanechává unikátní elektronickou stopu. Stopu a IP adresu, odkud byl jakýkoliv e-mail odeslán

(pokud zpráva není odeslaná z veřejné Wi-Fi sítě, případně prostřednictvím webhostingu), lze zjistit na serveru i v Microsoft Office Outlook ve vlastnostech konkrétního e-mailu. V případě, že se jedná o veřejnou síť, je možné alespoň lokalizovat poskytovatele.

Konkrétní IP adresu odesílatele e-mailu, který se podepsal jako Dan Smith, autorka diplomové práce alokovala v USA v Dallasu. Odesílatelem byl dallas.simonliu.net, avšak původní e-mail byl poslán z IP adresy lokalizované v Číně.[113] Do vyhledávače byly zadány klíčová slova Dallas a Simon Liu, protože se předpokládalo, že to bude pravděpodobně jméno člena společnosti AceTools.biz. Google nabídl osobu jménem Simon Liu žijící v Dallasu s otevřeným profilem na síti LinkedIn. Z profilu sociální sítě bylo zjištěno, že osoba jménem Simon Liu skutečně žije v Dallasu, má čínský původ, bakalářský titul z počítačových věd a specializaci na Microsoft Office.

Lze se domnívat, že se jedná o bílého koně čínských podvodníků snažící se daným způsobem získávat peníze od uživatelů, kteří si jejich software stáhnou do počítače. Jelikož jsou aktivity společnosti AceTools.biz nelegální, zvolili jsme jako nejvhodnější metodu ignorování vyhrůžek a komunikace zástupců společnosti AceTools.biz.

Nejpravděpodobnějším důvodem, proč firma produkt nabízí, je vydírání a podvodné získávání finančních prostředků od obětí, které uvěří vyděračským, ale profesionálně se tvářícím e-mailům. Textace mailu má právnickou formu, uživatelé neznalí věci raději zaplatí, než aby měli riskovat případné postihy.

Společnost AceTools.biz nemůže na uživatele podat žádné trestní oznámení, protože se k e-mailovým adresám dostává protiprávním způsobem, a to nabouráním se do počítače a neoprávněným stažením dat, které následně přeposílá do vlastní databáze. Skupina organizovaného zločinu terorizuje uživatele zastrašováním, kyberšikanou, vydíráním, obtěžováním a psychickým nátlakem. Dotčený uživatel, se kterým bylo společně pátráno po detailech, e-mail od AceTools.biz ignoroval a nikdo ze společnosti ho již nekontaktoval.

Po nahlédnutí na stránku AceTools.biz lze konstatovat, že stránka se již na první pohled jeví jako neprofesionální jak grafickým zpracováním, tak i poskytováním potřebných údajů, jakými jsou například kontakty. Po konzultaci s dotčeným uživatelem bylo zjištěno, že software neobsahoval žádné jiné licenční ujednání.

[113] Viz příloha A – Detekování IP adresy.

V počítači byl nainstalován kvalitní legální antivirový program, který nedetekoval přítomnost viru, protože se jednalo o standardní software, jehož účelem nebylo poškodit počítač, ale pouze zjistit e-mailovou adresu oběti a přeposlat ji do databáze. I neškodný a poctivý software je běžně schopen detekovat různá nastavení v počítači, která na rozdíl od společnosti AceTools.biz nezneužívá k ilegálním aktivitám. Důvodem detekování e-mailové adresy firmou AceTools.biz je rozesílání vyděračských a obtěžujících e-mailů za účelem vymáhání peněz.

Zajímavostí je, že překladač firmy AceTools.biz není originálním produktem. Dle uživatelských zkušeností publikovaných v diskusích program údajně ilegálně stahuje data z Google Translator a Babel Fish, které své služby na Internetu poskytují zdarma.

Případ 3. Nabourání se do účtu na Facebooku

Uživatelka při přihlašování se ke svému účtu na Facebooku zjistila, že zadané heslo ani při opakovaných pokusech není akceptováno. Zkontrolovala e-mailovou poštu, ve které našla oznámení od společnosti Facebook o tom, že byla vyžádaná změna hesla. Uživatelka o změnu nežádala, jednalo se o provedení změny hesla cizím uživatelem. Z časových důvodů problém v danou chvíli neřešila, požádala Facebook o nové heslo prostřednictvím odkazu, který byl součástí e-mailu. Během dne se opět přihlásila ke svému účtu, ale bez úspěchu. Heslo bylo opětovně změněno.

V e-mailové schránce bylo další upozornění o změně hesla. Prostřednictvím odkazu v e-mailové zprávě od Facebooku si vyžádala nové heslo a zkontrolovala nastavení. Při podrobné kontrole položek nastavení účtu zjistila, že účet má dvě e-mailové adresy pro odesílání informací, jedna z nich byla adresa bývalého přítele, který svůj vlastní e-mail bez jejího vědomí přidal do kontaktů, pravděpodobně při prvním neautorizovaném vstupu do facebookového účtu uživatelky. Bylo zjevné, že se jedná o mstu, expřítel měl v úmyslu uživatelku tímto způsobem terorizovat a šikanovat. Otázkou bylo, jakým způsobem heslo dekódoval, protože uživatelka nikomu nikdy nesdělila hesla k žádnému ze svých účtů.

Uživatelka si uvědomila, že expřítel věděl její standardní e-mailovou adresu, pod kterou se přihlašovala i na Facebook. Oběť se původně domnívala, že bývalý přítel při

pokusu o změnu hesla správně odpověděl na kontrolní otázku, která byla pro útočníka jednoduchá, sdělit jméno matky uživatelky za svobodna. Agresor, protože měl informace o blízké rodině uživatelky, odpověď znal, takže měl volnou ruku pro přístup do účtu a provádění změn nastavení.

Později si uživatelka uvědomila, že heslo bylo pravděpodobně dekódováno ještě v době jejich soužití. V počítači měla nastavené automatické přihlašování se k účtu. V daném případě se při přihlášení objeví e-mailová adresa i „neviditelné" heslo ve formě teček, které je možné dekódovat prostřednictvím zadání příkazu „zkontrolovat prvek – password – edit-text". Existují i postupy pro jednotlivé prohlížeče, které po zadání specifických příkazů umožňují uživateli zjistit uložená hesla ve formuláři.[114] S největší pravděpodobností se expřítel dostal k heslu výše popsaným způsobem, protože společně používali stejný notebook s jedním uživatelským účtem.

Jediným způsobem, jak se vyhnout dalšímu nabourávání do sledovaného Facebookového účtu, bylo vytvoření nového e-mailového účtu, který bude používán výhradně pro Facebook. Uživatelka změnila původní přihlašovací e-mail na nový a změnila i heslo. Zrušila propojené e-mailové adresy a expřítele na sociální síti zablokovala. Viditelnost kontaktních údajů na Facebooku nastavila do režimu „pouze já". Daným nastavením nikdo z jejích přátel nyní nevidí žádné kontaktní údaje, včetně e-mailových adres.

Změnou přihlašovacího mailu uživatelka znemožnila agresorovi další přístup ke svému účtu. Současně tak u nastavení zabezpečení a schválení přihlášení nastavila zadávání bezpečnostního kódu při každém pokusu o přihlášení k účtu z nerozpoznaného zařízení. Bezpečnostní kód zasílá společnost Facebook na mobilní telefon uživatele, který je nutné sdělit při aktivaci služby.

Případ 4. Zcizení identity, neoprávněný přístup k účtu na Facebook

Uživatelka zjistila, že jeden z jejích dobrých přátel na Facebooku ji bezdůvodně odebral z přátel. Kontaktovala ho s dotazem o vysvětlení. Sdělený důvod byl pro ni

[114] HERVYHO ZÁPISNÍK. *Jak jsem „hacknul" účty Facebooku a zůstal nepovšimnut*. [online]. © 15. 6. 2011 [cit. 2012-04-14]. Dostupné z: http://hervyho-zapisnik.blogspot.cz/2011/06/jak-jsem-hacknul-ucty-facebooku-zustal.html

velmi překvapující a šokující. Změna chování, neadekvátní reakce a útoky dotčené uživatelky při chatování.

Uživatelka si byla vědoma, že k žádnému podobnému chování z její strany nedošlo, současně si byla jista, že s kamarádem již dlouhou dobu nechatovala, proto chtěla znát další detaily. V rámci diskuse zjistila, že k chatování mělo dojít v čase, kdy byla v práci a vůbec neměla přístup k Facebooku. Přítel z Facebooku si původní chat uložil a poslal ho uživatelce mailem. Obsah a forma sdělení vůbec neodpovídala způsobu komunikace uživatelky, navíc se v počátku diskuse objevila žádost o poskytnutí finančních prostředků ze strany uživatelky.

Uživatelka si byla jista, že v inkriminované době byl doma její druh, se kterým používá stejný počítač. Uvědomila si, že přístup ke svému uživatelskému účtu v počítači neměla zajištěný heslem, současně tak heslo k Facebooku bylo automaticky uložené v počítači. Pro dalšího uživatele jejího počítače nebyl problém se k účtu na Facebooku bez jakýchkoliv problémů připojit. Podezření se potvrdilo, druh chatoval jejím jménem i s jinými uživateli Facebooku.

Případ 5. Falešná žádost o přátelství na Facebooku

Uživatelka obdržela žádost o přátelství od osoby, která se představila jménem bývalého spolužáka ze střední školy. Na profilové fotce byla zobrazena její oblíbená hudební skupina, žádné další informace vedoucí k identifikaci osoby žádost neobsahovala.

Po bezprostředním potvrzení žádosti iniciovala druhá strana chatování. Uživatelku po chvíli zarazily dotazy, které směřovaly ke zjištění detailů jejího osobního života a soukromí. „Spolužák“ jí sdělil, že je na Facebooku nový, proto nemá kompletní profil, ani přidané žádné přátele.

Po několika trefně mířených dotazech uživatelka zjistila, že pravděpodobně chatuje se svým kolegou, který si již delší dobu psychopaticky vynucoval její přízeň a pronásledoval ji. Kolega si na Facebooku vytvořil falešnou identitu se jménem bývalého spolužáka uživatelky. Jméno bylo údajně zjištěno prostřednictvím známých uživatelky s dokonalým využitím metod sociálního inženýrství.

V průběhu chatu došlo ke stažení několika fotek uživatelky publikovaných na Facebooku. Fotografie kolega druhý den vytiskl a vystavil v rámečku na svém pracovním stole.

Případ 6. Sexting, zneužití intimních fotek rozesláním řetězového e-mailu

Uživatelka poslala partnerovi e-mailem – ve snaze eliminovat dopad dočasného partnerského odloučení v době jeho služební cesty mimo republiku – intimní fotky. Je nutné uvést, že uživatelka se svým přítelem sdílela společný počítač, který byl v jejím vlastnictví. Přístup ke všem aplikacím a k e-mailovým účtům obou uživatelů byl veden prostřednictvím uživatelského účtu poškozené. Bylo nutné zadat heslo pouze při přihlášení se do počítače.

Po rozchodu a vynuceném odchodu přítele z bytu začala poškozená dostávat obtěžující sms, které vystupňovaly ve vyhrožování rozesláním intimních fotek do zaměstnání, přátelům a rodině.

Expřítel uživatelky si ještě v době přístupu k počítači bez jejího vědomí stáhl veškeré uložené kontakty. Po rozchodu začal vyhrožovat již výše zmíněným rozesláním diskreditujícího fotografického materiálu, a to z anonymní e-mailové adresy. Fotky byly skutečně odeslány na adresy přátel, kolegů, známých a rodiny uživatelky.

Nebylo možné prokazatelně detekovat IP adresu odesílatele. Při pokusu o identifikování adresy podle elektronické stopy e-mailu bylo zjištěno, že e-mail s fotkami byl odeslán z veřejné Wi-Fi sítě v obchodním centru, současně tak byl dle zkušeností specialistů počítačových technologií s největší pravděpodobností změněn MAC,[115] takže nebylo možné identifikovat odesílatele. Pachateli nemohlo být nic prokázáno, protože výhrůžné sms nebyly odesílány z čísla mobilního telefonu, ale přes sms bránu z veřejné Wi-Fi sítě.

[115] *MAC (Media Access Control)* – unikátní číslo každého zařízení, které má schopnost přihlásit se na Wi-Fi.

Případ 7. Zneužití soukromé fotky na Facebooku pro komerční účely bulvárního média

Pozůstalí i letecká společnost čelili smutné události, kterou bylo neobvyklé úmrtí pilota za letu. Jednalo se o člověka, kterého si vzhledem k jeho loajalitě, profesionálním dovednostem i nadstandardně lidskému přístupu a vstřícnému projevu kolegové nesmírně vážili. Na počest uctění jeho památky jeden z kolegů publikoval fotku na své facebookové zdi. U příspěvku se okamžitě začaly objevovat desítky soustrastných a děkovných komentářů. Fotku začali sdílet další facebookoví přátelé, celkem došlo ke sto čtyřiceti osmi sdílením.

Během tří hodin od původního publikování se fotka objevila na internetových stánkách jednoho bulvárního deníku se šokujícím nadpisem a bombasticky zformulovaným článkem. V následujících dnech byl článek postupně doplňován o další spekulace a domněnky.

Rodina, blízcí a kolegové zemřelého byli šokováni skutečností, že fotka člověka, kterého náhle ztratili za velmi nestandardních okolností, se zničehonic objevila v elektronických i tištěných médiích, které byly zaplaveny spekulacemi z profesionálního i osobního života zemřelého.

V diskusích pod zveřejněnými články se objevily nelichotivé poznámky a invektivy komentující chování pilota. Osobnosti, která by vzhledem ke svému přínosu společnosti zasloužila pietu a úctu, se tak dostalo skandalózního jednání a negativních komentářů od osob, které dotčeného osobně neznaly.

Anonymita internetu, absence morálky a bezbřehá snaha bulvárních sdělovacích prostředků doslova vytvořit emočně silnou, bombastickou kauzu tam, kde je namístě úcta, korektnost a respekt, způsobila pozůstalým trauma a zhoršila jejich duševní rozpoložení v těžké životní situaci.

Případ 8. Funmoods

Uživatelka stahovala bezplatný software ovladače webkamery. Po stažení zkontrolovala programy v notebooku a zjistila, že se v průběhu instalace bez jejího

vědomí samovolně nainstalovala i aplikace Funmoods.[116] Rozhodla se ji okamžitě odinstalovat, ale před potvrzením operace systém uživatelku informoval, že odinstalováním se resetuje nastavení prohlížečů v notebooku. Uživatelka nevěnovala varování žádnou pozornost i proto, že nechtěla mít nevyžádanou aplikaci v notebooku, a program odinstalovala. Při otevření prohlížeče Mozilla se na předmětné stránce objevila úplně jiná grafika, na prohlížeči byla neoprávněně nastavena nástrojová lišta Funmoods i přesto, že předmětná aplikace byla z notebooku odstraněna. Uživatelka otevřela prohlížeč Explorer, kde detekovala totožný problém. Pomocí vyhledávání se bez úspěchu snažila najít způsob, kterým by Funmoods odstranila. Aplikace sloužila i jako vyhledávač, a proto klíčová slova v souvislosti s odstraněním a názvem aplikace ignorovala. Veškeré internetové odkazy, které uživatelka měla k dispozici, souvisely pouze s využitím předmětné aplikace. Současně se také na stránce začala objevovat spousta reklam a žádostí o vstupy do různých aplikací a her. Bylo nutné použít jiný notebook k vyhledání možnosti odstranění nežádoucího doplňku. Neinfikovaný prohlížeč Mozilla a vyhledávač Google poskytly několik odkazů na způsoby odstranění, které ale byly pro běžného uživatele nesmírně komplikované. Nebylo možné vyhledat pokyny v českém jazyce. Po pečlivém surfování na Internetu se podařilo najít na stránce YouTube názorný návod na odstranění pro oba instalované prohlížeče.[117] Bez uvedené názorné instruktáže by uživatelka jako standardní uživatel počítačových technologií nebyla schopna se nežádoucího a obtěžujícího přídavného software (adware) zbavit. Uživatelka odinstalovala i software webkamery. Po detailním zkoumání zjistila, že stránka, ze které stahovala předmětný software, byla ve Web of Trust[118] (dále jen WOT) označena jako podvodná.

[116] *Toolbar* – nástrojová lišta, prohlížeč, aplikace přidávající emotikony do sociálních sítí a e-mailů. Po instalaci do počítačů automaticky změní přednastavení prohlížečů, uživatele zahlcuje reklamami, průzkumy a nabádá k odebírání zpoplatněných a drahých mobilních služeb.
MESKAUSAS, *T. Funmoods toolbar*.[online]. © 10. 7. 2012 [cit. 2012-11-17]. Dostupné z: http://www.pcrisk.com/removal-guides/6756-remove-funmoods-toolbar
[117] YOUTUBE. *Funmoods – Firefox Uninstall Tutorial*. [online]. © 30. 1. 2012 [cit. 2012-11-17]. Dostupné z: http://www.youtube.com/watch?v=RgvN9D07FGA
[118] *WOT (Web of Trust)* – bezplatný nástroj pro bezpečné surfování na Internetu založený na hodnocení registrovaných uživatelů. Varuje před rizikovými webovými stránkami. Doplněk aplikace Firefox.

3.4 Dotazník

Pro posouzení chování uživatelů na Internetu byl pro sběr dat použit dotazník – příloha B. Před tvorbou a distribucí dotazníku k předložené diplomové práci byl nejdříve formulován výzkumný problém a definován cíl, kterým bylo získání informací o chování běžných uživatelů internetu s ohledem na vnímání internetových rizik. Dotazník vyplnilo 90 respondentů, kteří se považovali za průměrné až zkušené uživatele Internetu a počítačových technologií, vyjma otázek č. 12, 13, 14, na které odpovědělo dalších 20 respondentů, celkem 110 respondentů. Dotazník obsahuje celkem čtrnáct otázek z následujících oblastí:

- chování uživatelů elektronické pošty,
- chování uživatelů při stahování dat z Internetu,
- pozornost uživatelů s ohledem na detekované hrozby v počítači,
- realizované způsoby zneužití Internetu a internetové komunikace,
- využití sociálních sítí.

4 METODY POUŽITÉ PRO ZPRACOVÁNÍ DAT

V praktické části jsou použity metody, které jsou dále popsány. Definice metod jsou převzaty z Všeobecné encyklopedie a z publikací Metody, nástroje a techniky pro rizikové inženýrství a Kapitoly metodologie sociálních výzkumů.

Analogie – úsudek zjišťující shodu porovnávaných předmětů či jevů shody jejich některých vlastností. Je důležitá při vytyčování nových hypotéz v mnohých vědách, zejména společenských.[119]

Analýza – základní myšlenkový postup rozkládající vymezený celek na jeho prvky; obecně každá metoda, která se snaží předmět nebo jev vysvětlit myšlenkovým, faktickým rozborem jeho složek.[120]

Dedukce – odvození tvrzení (důsledků) z jednoho nebo několika jiných tvrzení pomocí odvozovacích pravidel. Je zpravidla přechodem od obecného ke zvláštnímu, důsledek však může být stejně obecný jako jeho výchozí tvrzení.[121]

Diskuse – v pojetí metody je určitá techniky výměny názorů zaměřená na určitý cíl.[122]

Dotazník – psychologická metoda ke zjišťování psychologicky významných údajů o jedinci, jeho osobnosti, vlastnostech, postojích, zájmech. Zadává se individuálně nebo ve skupině, zpravidla písemnou formou.[123] Dotazník v předložené diplomové práci byl anonymní a byl distribuován prostřednictvím systému Survio.com/cs. Obsahoval uzavřené a polouzavřené otázky. Polouzavřené otázky umožnily respondentům vyjádřit svůj názor v případech, kdy existovala možnost, že se neztotožní ani s jednou z nabízených možností. Současně otevřely prostor pro publikování obšírnějšího stanoviska k předmětnému problému.

[119] KOLEKTIV AUTORŮ. *Všeobecná encyklopedie v osmi svazcích*. Praha: Diderot, 1999. s. 468. ISBN 80-902555-2-3.
[120] Tamtéž, s. 468.
[121] Tamtéž, s. 468.
[122] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství.* 1. vyd. Praha: ČVUT, 2011. s. 46. ISBN 978-80-01-04842-9.
[123] Tamtéž, s. 468.

Graf – symbolické kresebné znázornění vztahů či statistických údajů.[124] V předložené diplomové práci byl pro interpretaci dat použit výsečový graf.

Indukce – usuzování od jednotlivého k obecnému, myšlenkový postup umožňující z pozorování jednotlivých faktů vyvodit existenci obecných zákonitostí. Závěr vyvozený indukcí není jednoznačnou hodnotou pravdivostní, platí pouze s určitou pravděpodobností, která závisí především na rozsahu pozorování.[125]

Rozhovor – nestrukturovaný rozhovor – metoda výzkumu, při které nejsou otázky předem dané, ale vznikají při přirozené komunikaci mezi tazatelem a respondentem, kdy respondent nemusí zjistit, že je objektem výzkumného zájmu (skrytý rozhovor, který není inzerovaný jako výzkumný).[126] Pro výzkum a vlastní šetření byla použita forma nestrukturovaného volného rozhovoru, ve kterém nebyla předem určena struktura rozhovoru ani pořadí otázek. Cílem bylo získat informace různého druhu od různých respondentů. Výběr osob byl cílený na základě doporučení pracovníků ze zaměstnání. Osloveny byly konkrétní osoby, které byly na základě informace v souvislosti se zneužitím Internetu označeny jako poškozené. Věkové rozpětí dotazovaných se pohybuje od 33 do 45 let. V demografické kategorii muž/žena představuje poměr osmi šetřených případů, jednoho k sedmi. Vyjma jednoho případu, kterým byl velmi zkušený uživatel Internetu a počítačových technologií, se jednalo o standardní uživatele.

Scénář – metoda scénářů spočívá v simulaci možných příčin nebo možných procesů, které vedly k výsledku. Uspořádává události v čase a zachovává jejich logickou vzájemnou návaznost. Scénář je obecně historicko-systémový model. Při jeho aplikaci je úkolem popsat budoucí nebo minulý vývoj v jeho různých podobách závislých na určitých rozhodnutích.[127]

Syntéza – spojování částí do celku, myšlenkový sled postupující od nejjednodušších pojmů nebo faktů ke složitějším; navazování, nacházení souvislostí.[128]

What if Analysis (analýza toho, co se stane, když) – postup založený na hledání možných dopadů vybraných pohrom nebo provozních situací. Technika „co se stane,

[124] KOLEKTIV AUTORŮ. *Všeobecná encyklopedie v osmi svazcích*. Praha: Diderot, 1999. s. 468. ISBN 80-902555-2-3.
[125] Tamtéž, s. 468.
[126] REICHEL, J. *Kapitoly metodologie sociálních výzkumů*. 1. vyd. Praha: Grada, 2009. s. 110. ISBN 978-80-247-1428-8.
[127] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. 1. vyd. Praha: ČVUT, 2011. s. 135. ISBN 978-80-01-04842-9.
[128] KOLEKTIV AUTORŮ. *Všeobecná encyklopedie v osmi svazcích*. Praha: Diderot, 1999. s. 468. ISBN 80-902555-2-3.

když…“ je přístup spontánní diskuse a hledání nápadů, ve které skupina zkušených a s procesem dobře obeznámených lidí klade otázky nebo vyslovuje úvahy o možných nežádoucích událostech.[129] Nejedná se o vnitřně strukturovanou techniku, namísto toho po analytikovi požaduje, aby přizpůsobil základní koncept určitému účelu.

Dana Procházková v rámci analýzy What If uvádí různé možné dopady:[130]

1. Možné dopady na životy a zdraví lidí: ztráty na životech a poškození zdraví z důvodu selhání zdravotní péče, škody na zdraví způsobené snížením úrovně hygieny, nemožnost uspokojení základních lidských potřeb atd.
2. Možné dopady na bezpečí lidí: psychická újma, ohrožení bezpečnosti státu, selhání bezpečnostních zařízení – zvýšení kriminality, informační kolaps, pocit bezmoci, vznik paniky, ztráta spojení s okolním světem atd.
3. Možné dopady na majetek: škody na objektech, zařízeních, infrastrukturách a technologiích vyvolané dopravními a technologickými haváriemi vzniklými v důsledku selhání počítačových systémů atd.
4. Možné dopady na veřejné blaho: nefunkčnost správy věcí veřejných, neplnění nároků občanů, omezení dopravy atd.
5. Možné dopady na životní prostředí.
6. Možné dopady na infrastruktury a technologie, mimo jiné na kybernetickou infrastrukturu samotnou (komunikační a informační sítě); kaskádový efekt v systémech a sítích – zničení databází informací, nemožnost kontroly a řízení přes kybernetickou síť, ztráta spojení a druhu informací atd.

[129] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*, 1. vyd. ČVUT Praha, 2011. s. 211. ISBN 978-80-01-04842-9
[130] Tamtéž, s. 223–227.

5 VYHODNOCENÍ DAT

Shromážděná data byla vyhodnocena z několika aspektů. Nejprve byla použita metoda „What if“ (co se stane, když) s cílem posoudit dopady sledovaných škodlivých jevů a v druhém případě bylo provedeno celkové vyhodnocení původců dopadů na osobu postiženou kybernetickým útokem.

5.1 Výsledky analýzy rizik

V prvním případě sledujeme dopady na chráněná aktiva. Jsou sledována veřejná aktiva: životy, zdraví a bezpečí lidí; reputace osobnosti; majetek; veřejné blaho; životní prostředí; infrastruktury a technologie, a též aktivum spojené s osobou, proti níž byl zaměřen útok, které v analogii k reputaci organizace[131] označíme jako reputaci příslušné osoby. Výsledky provedeného hodnocení metodami, které byly specifikovány v předchozí kapitole, jsou uvedeny v tabulkách 2 a 3.

Tabulka 2: Seznam dopadů jednotlivých případů na chráněná veřejná aktiva – vyhodnocení případů z Internetu

Případ	**Nástroj použitý ke zneužití**	**Způsob zneužití**	**Klasifikace jednání útočníka**	**Seznam dopadů na chráněná aktiva**
1	E-mail – prolomení hesla. Webové stránky postižené osoby – prolomení hesla.	Umístění nepravdivých informací na webovou stránku. Neoprávněný vstup k e-mailovému účtu a rozesílání nepravdivých informací.	Protiprávní jednání – neoprávněný přístup k počítačovému systému a nosiči informací.	Psychická újma postižené osoby, stres, bezmoc, strach. Poškození reputace poškozené osoby. Narušení bezpečí oběti. Narušení bezpečí klientů, ztráta jejich důvěry a narušení místní sociální

[131] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. 1. vyd. Praha: ČVUT, 2011. s. 234. ISBN 978-80-01-04841-2.

				infrastruktury. Ztráta výdělku oběti a existenční problémy. Veřejné blaho – zrušení sociálního objektu, který poskytoval péči lidem.
2	Webové stránky nabízející zaměstnání umístěné na několika serverech.	Klamavá reklama na webových stránkách serverů pracevzahranici. eu, aupair.cz, brigady.net, práce-anglie.cz	Protiprávní jednání – podvod za účelem osobního obohacení se.	Psychická újma poškozených osob – stres, bezmoc. Ztráta jistot obětí – dlouho hledaná práce i přes uhrazení poplatků za zprostředkování nebyla zajištěna. Celkový počet obětí 4246. Celková vyčíslitelná škoda: více než 13 milionů korun českých. Narušení společenského klimatu. Poškození reputace serverů pracevzahranici.eu , aupair.cz, brigady.net, práce-anglie.cz.
3	Použití serveru zaměstnavatele pro posílání e-mailu – komunikace s obětmi. Seznamovací servery, inzertní portály zaměřené na nezletilé uživatele internetu.	Sociální inženýrství, úmyslné zneužití služebního e-mailu k manipulaci, vylákání citlivých fotek za účelem vydírání. Sexuální zneužití.	Protiprávní jednání – pohlavní zneužití, poškození cizích práv. Týrání svěřené osoby. Ohrožování mravní výchovy mládeže. Svádění k pohlavnímu	Psychická újma obětí – obavy, stres, trvalé psychické následky ze sexuálního zneužití. Fyzická újma obětí důsledkem sexuálního zneužití a použitím násilí. Ztráta jistoty obětí, obavy z prozrazení

			styku. Zneužití dítěte k výrobě pornografie.	sexuální orientace. Vzájemné nepatřičné chování jednotlivce.
4. a	Pošta. E-mail s nepravdivým obsahem.	Obelhání oběti – zasíláním podvodných zpráv a e-mailů za účelem obohacení se. Zneužití neinformovanosti a důvěry oběti.	Protiprávní jednání – poškození cizích práv, podvod a osobní obohacení se.	Psychická újma – poškození psychického zdraví oběti – stres, bezmoc, nervový kolaps oběti. Postupné snížení životního standardu oběti z důvodu zadlužení, které vyústilo v existenční problémy. Ztráta životních jistot následkem obrovského zadlužení. Oběť byla pod vlivem událostí a špatného psychického stavu dohnána ke kriminálnímu činu. Újma na zdraví – oběť postřelila recepčního. Ztráta na životě – oběť zastřelila nigerijského konzula. Celková vyčíslitelná škoda: více než 15 milionů korun českých. Narušení mezinárodního klimatu – problematika byla řešena na úrovni ambasád ČR a Nigérie.

4. b	Podvodné e-maily. Falešné webové stránky.	Sociální inženýrství. Oklamání oběti zasláním podvodného e-mailu se žádostí o pomoc s nelegální finanční transakcí za účelem obohacení se. Zneužití osobních dat oběti.	Protiprávní jednání – podvod za účelem obohacení se. Protiprávní jednání oběti – napomáhání podvodnému jednání	Psychická újma poškozené osoby stres, bezmoc. Ztráta jistoty oběti z důvodu obavy z trestněprávních důsledků za napomáhání ilegálního převodu peněz. Finanční ztráta, celková vyčíslitelná škoda: 617.571 korun českých.
5	Výhrůžné e-maily rozeslané ze serveru zaměstnavatele.	Odeslání anonymních e-mailů vyhrožujících smrtí. Možné, ale nepotvrzené, zneužití/zkopírování IP adresy s cílem diskreditace „údajného“ odesílatele.	Teror vůči jednotlivci. Možné protiprávní jednání neoprávněný přístup k počítačovému systému a nosiči informací (nebylo potvrzeno).	Psychická újma poškozené osoby, stres a obava o vlastní život. Obava oběti o bezpečí rodiny. Ztráta zaměstnání poškozené osoby – pozastavení výuky oficiálně z „finančních“ důvodů a důchodovému věku oběti, neoficiálně – reakce školy na zveřejnění kauzy v médiích. Sociální a profesní diskvalifikace údajného útočníka – ztráta pracovní pozice, pozastavení výuky, zrušení členství v akademických radách. Narušení pracovního klimatu – stres a negativní pracovní atmosféra na

				katedře. Mediální diskreditace katedry filosofie.
6	Internet. Webové stránky.	Odeslání škodlivého kódu do počítačů a zneužití sociálního inženýrství k podvodnému vylákání peněz.	Protiprávní jednání – podvod za účelem obohacení se, neoprávněný přístup k počítačovém u systému a nosiči informací.	Psychická újma poškozených osob. Finanční ztráty. Narušení společenského klimatu. Poškození reputace Policie ČR.
7	Podvodný e-mail. Podvodné webové stránky.	Zneužití sociálního inženýrství za účelem získání přístupových dat k bankovním účtům obětí.	Protiprávní jednání – neoprávněný přístup k nosiči informací, zneužití záznamu na nosiči informací, Podvod za účelem obohacení se.	Psychická újma poškozených osob. Finanční ztráty následkem zneužití přístupových dat k bankovním účtům. Narušení společenského klimatu. Poškození reputace České spořitelny.
8	Facebook.	Vytvoření falešné identity. Zneužití sociálního inženýrství pro získání důvěry dítěte za účelem pohlavního zneužití.	Protiprávní jednání – pohlavní zneužívání, vydírání, výroba a nakládání s dětskou pornografií, trestní zneužití dítěte.	Psychická újma oběti a jeho rodiny. Fyzická újma oběti následkem znásilnění. Narušení společenského klimatu ve skautském klubu, po medializaci případu i v celé ČR. Poškození reputace skautského klubu.
9	Internet. Infikované e-maily.	Infikování domácích počítačů trojanem Zeus	Protiprávní jednání - podvod	Psychická újma obětí – stres, obava

	Domácí počítače – botnety.	prostřednictvím zavirovaných e-mailů, krádež a zneužití dat, vykradení bankovních účtů uživatelů. Zneužití e-mailů nabízející práci k sofistikovanému podvodu ilegálních převodů peněz.	a obohacení druhého. Neoprávněný přístup k počítačové-mu systému a nosiči informací, poškození a zneužití záznamu na nosiči informací, podvod za účelem vlastního obohacení se.	z narušení soukromí, obava ze zneužití dat, šok po zjištění, že došlo k vykradení bankovního účtu. Ztráta přístupu k peněžním prostředkům. Existenční problémy obětí. Ztráta pocitu bezpečí, strach z celkového vývoje situace. Vyčíslitelné finanční ztráty ve výši 70 milionů amerických dolarů. Vznik „ finanční mafie.“ Narušení společenského klimatu. Nežádoucí ilegální imigrace do USA, zločincům byly zajištěny falešné pasy a víza. Nárůst kriminality. Vysoké finanční náklady na vyšetřování (globální rozptyl zločinecké organizace).
10	Webkamera – neautorizované použití. Sociální síť Twitter.	Špehování, zveřejnění nelegálně získaných, citlivých dat na sociální síti Twitter.	Teror vůči jednotlivci. Neoprávněný zásah do práva na ochranu osobnosti.	Psychická újma oběti, která vyústila v sebevraždu oběti. Psychická újma šikanisty údajně netušícího, že se dopouští protiprávního jednání.

				Psychická újma rodičů oběti i rodičů šikanisty Negativní dopad na studentské klima. Narušení společenského klimatu v krajině z důvodu protestů vůči kyberšikaně a diskusím o mezikulturních rozdílech i sexuální intoleranci. Sociální diskvalifikace útočníka i jeho rodiny. Trestněprávní důsledky pro útočníka. Hrozba nucené deportace útočníka ze země.
11	Mobilní telefony, na které byl natáčen závadný materiál. Internetový server YouTube, na který byl umístěn závadný materiál.	Pořizování a distribuce materiálu s ponižujícím obsahem.	Šikana. Neetické jednání osob, pořizování a publikování videa s ponižujícím obsahem. Teror vůči jednotlivci. Protiprávní jednání útočníka – vražda, ublížení na zdraví, nelidské a hrubé zacházení.	Psychické újmy obětí – pocit ponížení, strach, úlek. Fyzické újmy obětí – znásilnění, vážná zranění. Smrt obětí jako následek fyzického napadení. Ztráta pocitu bezpečí, obava o vlastní život, obava o život napadeného. Poškození reputace osob zveřejněním ponižujících scén na Internetu. Narušení

				společenského klimatu.
12	Sociální síť MySpace – falešná identita.	Sociální inženýrství. Podvodné získání důvěry a citlivých informací oběti, které bylo zneužito k šikaně psychicky labilní teenagerky.	Teror vůči jednotlivci. Protiprávní jednání – Účast na sebevraždě, úmyslné ublížení na zdraví (psychickém).	Psychická újma oběti, zhoršení psychického stavu labilní oběti, prohloubení depresí. Sebevražda oběti jako vyústění těžké deprese. Ztráta pocitu bezpečí a jistoty rodinného zázemí – rozvod rodičů oběti jako následek událostí spojených se sebevraždou dcery. Sociální izolace šikanující rodiny, případ byl silně medializován. Narušení společenského klimatu medializací případu, ve kterém dospělá žena šikanovala nezletilé psychicky labilní dítě.
13	Mobilní telefon obsahující fotky se sexuálním obsahem. Řetězový e-mail prostřednictvím kterého došlo k odeslání kompromitujícího materiálu.	Rozeslání, respektive zveřejnění cizích soukromých fotek se sexuálním obsahem.	Šikana. Teror vůči jednotlivci. Protiprávní jednání – vydírání, útisk. Neoprávněný zásah do práva na ochranu osobnosti.	Psychická újma oběti, ponížení. Šok ze zneužití intimních fotek, trauma ze zveřejnění intimity, ztráta sebedůvěry. Přerušení přátelství se spolužačkami. Fyzická újma – zranění, fyzické útoky spolužaček.

				Sebevražda jako následek ponižování, šikany a vyloučení oběti z kolektivu. Ztráta pocitu bezpečí, nucená izolace, ztráta důvěry v blízké osoby. Psychické zhroucení matky oběti po spáchání sebevraždy její dcery. Narušení školního klimatu.
14	Internet – stránky YouTube, na kterých byla neoprávněně zveřejněná cizí nahrávka.	Neautorizované zveřejnění cizí video nahrávky.	Teror vůči jednotlivci. Neoprávněný zásah do práva na ochranu osobnosti.	Psychické zhroucení postižené osoby. Nutnost podrobit se psychiatrické léčbě. Dočasná sociální izolace postižené osoby. Nežádoucí medializace. Finanční ztráty rodin pachatelů – mimosoudní vyrovnání s rodinou oběti.
15	Internet – zveřejnění pomluvy a soukromé korespondence.	Publikování nepravdivých, soukromých a citlivých informací.	Teror vůči jednotlivci. Protiprávní jednání – účast na sebevraždě. Neoprávněný zásah do práva na ochranu osobnosti.	Psychická újma oběti. Sebevražda postižené osoby. Pokus o sebevraždu osoby zainteresované v šikanování. Narušení rodinných jistot blízkých oběti. Narušení společenského klimatu následkem

				medializace kauzy.
16	Internet a Facebook – zveřejnění intimní fotky.	Sociální inženýrství. Vylákání fotografie se sexuální tematikou a její zneužití zveřejněním na Internetu i použitím pro fiktivní profil na Facebooku.	Teror vůči jednotlivci. Protiprávní jednání – vydírání, útisk. Neoprávněný zásah do práva na ochranu osobnosti. Zneužití záznamu na nosiči.	Psychická újma – silné psychické trauma oběti. Ztráta pocitu bezpečí, pocity strachu, deprese, panická porucha postižené osoby. Sociální izolace postižené osoby. Sebevražda postižené osoby. Finanční dopad na rodinný rozpočet z důvodu nutnosti změny pobytu. Narušení rodinného klimatu Psychická újma a sociální dopad na rodinu neprávem obviněné osoby. Narušení společenského klimatu následkem medializace.
17	E-mail – prolomení hesla. Mobilní telefon. Intruze do obsahu složky s fotkami prvotním prolomením totožného hesla na sociální síti.	Neoprávněný vstup k e-mailovému účtu. Neoprávněné přesměrování soukromé komunikace na neautorizovaný účet. Neoprávněný vstup do mobilního telefonu. Publikování fotek s citlivým obsahem.	Protiprávní jednání – neoprávněný přístup k počítačovém u systému a nosiči informací. Zneužití záznamu na nosiči informací. Krádež identity. Teror vůči jednotlivci. Neoprávněný zásah do práva na ochranu osobnosti.	Psychická újma postižených osob. Ztráta pocitu bezpečí postižených osob. Poškození reputace osob zveřejněním fotografií s intimním obsahem.

18	Internet. Webové stránky poskytující erotický obsah.	Sociální inženýrství. Manipulativní přesvědčování, nabádání mladistvého k pornografickým aktivitám před webkamerou.	Protiprávní jednání – pohlavní zneužití; zneužití dítěte k výrobě pornografie; šíření pornografie; ohrožování mravní výchovy mládeže; svádění k pohlavnímu styku.	Psychická destrukce oběti. Sociální izolace oběti. Ohrožení fyzického zdraví oběti – vytvoření drogové závislosti. Fyzická újma oběti opakovaným znásilněním.
19	Infikované webové stránky.	Odeslání škodlivého kódu do počítače.	Protiprávní jednání – neoprávněný přístup k počítačovém u systému a nosiči informací; zneužití záznamu na nosiči informací. Podvod za účelem obohacení se.	Psychická újma oběti. Ztráta pocitu bezpečí. Finanční ztráta.
20	E-mail	Odeslání obtěžujících a výhrůžných e-mailů pod falešnou identitou.	Teror vůči jednotlivci. Protiprávní jednání – vydírání, vyhrožování, Šíření nepravdivých informací.	Psychická újma postižené osoby. Poškození reputace oběti. Narušení pracovního klimatu.

Možné scénáře událostí vyvolané zneužitím Internetu, které byly zpracovány metodou diskuse s osobu profesně se zabývající problematikou počítačových věd, jsou popsány v příloze C.

Tabulka 3: Seznam dopadů jednotlivých případů na chráněná veřejná aktiva – vyhodnocení případů z vlastního šetření

Případ	**Nástroj použitý ke zneužití**	**Způsob zneužití**	**Klasifikace jednání útočníka**	**Seznam dopadů na chráněná aktiva**
1	Uživatelský účet na sociální síti Facebook.	Napadení uživatelského účtu odesláním škodlivého kódu Koobface.	Protiprávní jednání – neoprávněný přístup k počítačovému systému a nosiči informací.	Psychická újma postižené osoby. Obava ze zneužití dat uložených v počítači. Obava z intruze do soukromí. Obava z nefunkčnosti počítače a softwarových aplikací. Nedůvěra v „čistotu“ počítače i po odstranění viru a instalaci nového antiviru. Nemožnost komunikovat a pracovat, dočasná blokace notebooku z důvodu jeho zavirování kvůli eliminaci hrozby dalšího šíření viru. Finanční výdaje na reinstalaci operačního systému a aplikací. Časová investice do zálohování a reinstalace systémů. Finanční investice do zakoupení nového antivirového programu, nového harddisku a baterie, které následkem vniknutí viru přestaly fungovat. Ztráta části dat. Ohrožení

				notebooku infiltrací škodlivého kódu „Bot“.
2	Podvodné webové stránky AceTools.biz, které obsahují umístěn škodlivý software.	Vniknutí škodlivého kódu do počítače a MS Office za účelem dekódování e-mailové adresy uživatele a její odeslání firmě AceTools.biz pro účely vydírání a obohacení se.	Protiprávní jednání – neoprávněný přístup k počítačovému systému a nosiči informací, vydírání, podvod za účelem obohacení se.	Psychická újma postižené osoby po obdržení výhružného e-mailu. Obava uživatele z intruze do soukromí. Obava ze zcizení a zneužití dat uložených v počítači. Strach uživatele z dalšího vyhrožování. Desítky napadených a podvedených uživatelů Internetu. Finanční ztráty uživatelů, kteří podlehli vydírání a za neoriginální produkt zaplatili cca 85 euro. Časová investice do investigace. Ztráta důvěry ve webové stránky Instaluj.cz nabízející podvodný software, který není originálním produktem.
3	Počítač, uložené přístupové heslo k uživatelskému účtu Faceebooku. Sociální síť Facebook.	Neautorizované dekódování přihlašovacích údajů, uložených v počítači, v době simultánního používání jednoho počítače prostřednictvím společného uživatelského	Protiprávní jednání – neoprávněný přístup k počítačovému systému a nosiči informací, zneužití záznamu na nosiči,	Psychická újma postižené osoby šok po zjištění, že došlo k neautorizovanému vstupu do profilu na sociální síti. Strach, nejistota, trauma uživatelky z opakovaných anonymních útoků na uživatelský účet

		účtu.	neoprávněný zásah do práva na ochranu osobnosti. Teror vůči jednotlivci.	Obava ze zcizení a zneužití dat z uživatelského účtu. Obava ze zneužití a zcizení dat z počítače. Trauma z poškození dobrého jména následkem zneužití dat, případně krádeží identity. Ztráta jistoty. Intruze do soukromí. Časová investice do provedení změn dat i zabezpečení uživatelského účtu.
4	Počítač, uložené přístupové heslo k uživatelskému účtu na Facebooku. Sociální síť Facebook.	Neautorizovaný vstup do profilu na sociální síti Facebook.	Krádež identity. Protiprávní jednání – neoprávněný přístup k počítačovému systému a nosiči informací, zneužití záznamu na nosiči, neoprávněný zásah do práva na ochranu osobnosti.	Psychická újma postižené osoby (šok, bezmoc, hněv). Sociální dopad – narušení vztahů s přáteli, rozchod s partnerem. Poškození reputace postižené osoby. Ztráta jistot, ztráta důvěry v partnera.
5	Sociální síť Facebook.	Vytvoření falešné identity na sociální síti. Zneužití sociálního inženýrství za účelem získat přístup k oběti a k jejím fotkám.	Krádež identity. Teror vůči jednotlivci. Protiprávní jednání – neoprávněný zásah do práva na ochranu osobnosti.	Psychická újma oběti. Obava z narušení soukromí. Ztráta jistoty a pocitu bezpečí. Narušení pracovního klimatu.
6	E-mail, kterým byly rozeslány	Zneužití fotek se sexuálním	Teror vůči jednotlivci.	Psychická újma postižené osoby -

	intimní fotky. Domácí počítač, ze kterého byly získány e-mailové adresy.	obsahem, rozeslání fotek z anonymní e-mailové adresy na pracovní i soukromé kontakty oběti.	Protiprávní jednání – neoprávněný zásah do práva na ochranu osobnosti, zneužití záznamu na nosiči, šíření pornograf. materiálu.	zhroucení postižené osoby, nutná psychiatrická léčba. Poškození reputace postižené osoby. Sociální diskvalifikace oběti. Dočasná sociální izolace oběti. Vážné narušení rodinných vztahů. Narušení pracovních vztahů. Ztráta pocitu bezpečí. Ztráta důvěry ve společnost. Finanční ztráty, snížená mzda po dobu psychiatrické léčby. Trvalé psychické následky, trauma z veřejného odhalení intimity, celoživotní nedůvěra ve funkční mezilidské vztahy.
7	Sociální síť Facebook, kde byla publikovaná fotka zemřelého.	Zcizení a zneužití fotky zveřejněné na Facebookovém soukromém profilu uživatele.	Neetické jednání. Protiprávní jednání – neoprávněný zásah do práva na ochranu osobnosti.	Psychická újma – emocionální otřes rodiny poté, co zjistila, že fotka zemřelého je zveřejněna v bulváru i po přečtení hanlivých komentářů v diskusi pod článkem. Zneuctění památky a poškození reputace zesnulého. Psychická újma osob, které fotku s respektem vůči zemřelému komentovaly. Ztráta důvěry

				v „přátele“ kvůli anonymnímu předání fotky ke komerčním účelům. Narušení společenského klimatu kvůli porušení novinářské etiky a piety. Nežádoucí medializace, narušení soukromí pozůstalých.
8	Webové stránky se škodlivým Adware.	Připojení nežádoucí aplikace k bezplatnému software, prostřednictvím kterého se aplikace stáhla do počítače.	Protiprávní jednání – neoprávněný přístup k počítačovému systému a nosiči informací.	Psychická újma – šok oběti z napadení počítačového systému. Časová investice do odstraňování nežádoucí, nevyžádané a nepříliš známé aplikace.

Možné scénáře způsobu provedení zneužití Internetu, které byly zpracovány metodou diskuse s osobu profesně se zabývající problematikou počítačových věd, jsou popsány v příloze D.

5.2 Výsledky vyhodnocení dotazníkového šetření

Celkové statistické vyhodnocení původců dopadů, tj. použitých kybernetických nástrojů, na osobu postiženou kybernetickým útokem provedené na základě údajů získaných z dotazníků, jež je charakterizován v kapitole 4, je v tabulce 4. Podrobné výsledky jsou v příloze E.

Tabulka 4: Vyhodnocení dat dotazníkového šetření

Otázka	Ano	Ne	Použité nástroje kybernetického útoku přes Internet				
1	60	30					
2	43	17					
3			Virus	Vydírání	Spam	Hoax	Jiné
			15	2	30	20	13
4	43	47					
5	28	15					
6	66	24					
7			Trojský kůň	Backdoor	Bot	Spyware	Adware	Jiné
			52	3	4	28	11	5
8			Problémy s operačním systémem	Krádež citlivých dat	Krádež identity	Neuvědomuji si		Jiné
			42	1	0	30		7
9	22	68					
10			Sociální sítě	Podvodné stránky	Podvodná transakce	Nigerijský spam		Jiná
			15	5	3	11		10
11			Útok ponižování v rámci sociálních sítí	E-mailové obtěžování	Vydírání zveřejněním citlivých fotek	Nevím		Jiná
			5	18	4	58		3

Konkrétní odpovědi „jiné“ k otázce č. 8:

- problém postižené osoby s policií,
- manipulace s účtem postižené osoby na Facebooku,
- žádné, hrozba byla odstraněna antivirovým programem,
- kompletní nefunkčnost počítače.

Konkrétní odpovědi „jiné“ k otázce č. 10:

- Wi-Fi,
- nevyžádaná nabídka bankovních služeb od banky, která je dcerou hypoteční banky postižené osoby,
- podvodníci se dostali k e-mailové adrese postižené osoby pravděpodobně prostřednictvím procházení webových stránek, zasílali postižené osobě pak různé nabídky „výhodných“ finančních produktů,
- známý, kterému postižená osoba půjčila notebook, „ukradl“ e-mailovou adresu i hesla, které postižená osoba měla uložené v notebooku pro vstupy na webové stránky,
- postižená osoby řekla nevědomky útočníkovi sám/sama po sofistikovaných dotazech ze strany partnera/partnerky, známého, který byl útočníkem (7 krát),
- postižená osoba měla hesla pro vstupy uložená v mobilu, který jí byl ukraden, došlo k pokusu o vstup na internetové bankovnictví,
- postižené osobě byl odcizen notebook, který nebyl zaheslován a ve kterém postižená osoba měla uložena hesla pro vstupy k e-mailovým účtům, z jednoho účtu došlo k odeslání řetězového spamu.

Konkrétní odpovědi „jiné“ k otázce č. 11:

- Policie ČR.

K otázkám dotazníku označeným pořadovými čísly 12–14 bylo dodatečně dotázáno dalších dvacet osob metodou rozhovoru. Celkový počet respondentů v daných případech vzrostl na sto deset osob. Výsledky statistického hodnocení předmětných otázek jsou v tabulce 5. Na základě údajů v uvedené tabulce lze usuzovat, že nejvíce je používán Facebook, a to standardními uživateli internetu, tj. lidmi, kteří by měli mít určité znalosti a zkušenosti s kyberprostorem.

Tabulka 5: Využití sociálních sítí

Otázka	Ano	Ne				
12	89	21				
13			Druhy využívaných sociálních sítí			
			Facebook	75		
			Twitter	4		
			LinkedIn	13		
			Libimseti	4		
			Lide.cz	5		
			MySpace	2		
			Spolužáci.cz	36		
			Jiné	9		
14					Zkušenost uživatele Internetu	
					Velmi zkušený	19
					Standardní	86
					Nezkušený	5

Výsledky shrnuté v tabulce 5 jsou jistým způsobem překvapivé, protože ukazují, že oběťmi kybernetických útoků jsou i lidé se standardními znalostmi.

Na základě údajů z dotazníku i rozhovorů byly u jednotlivých případů identifikovány dva typy zranitelností, a to: technická a sociální, viz tabulka 6.

Tabulka 6: Výsledky průzkumu zranitelnosti osob z pohledu jejich technického a sociálního chování (rozhovor a dotazník)

Zranitelnosti osob vyplývající z jejich sociálního chování	**Zranitelnosti osob vyplývající z jejich technického chování**
Důvěra ve společného uživatele počítače. Nepozornost při instalaci, respektive ignorování následujících varovných signálů: - komunikace přítele v cizím jazyce, - stahování z dat a potvrzování údajů prostřednictvím podezřele vypadajících a neprofesionálně graficky zpracovaných webových stránek, - bezmyšlenkovité stahování dat ze stránek, které neobsahují standardní licenční ujednání. Naivita uživatelů při publikování citlivého materiálu v rámci sociálních sítí. Spontánní a bezmyšlenkovité sdílení materiálu na sociálních sítích. Snaha o publikování nestandardního příspěvku, který bude mít na sociální síti obrovskou odezvu. Nízká povědomost hrozby zneužití informací na sociálních sítích. Surfování po podezřelých nebo nebezpečných stránkách. Neznalost „přátel“ na sociálních sítích. Důvěra v neznámé lidi žádající o potvrzení „přátelství“ na sociální síti. Potvrzování neznámých osob na sociálních sítích do okruhu přátel, sdílejících soukromí uživatelů.	Nízká znalost počítačových technologií a principů fungování Internetu. Nedostatečné zabezpečení systému. Stahování dat z nevěrohodných/neznámých zdrojů. Nízké povědomí o rizikách na internetu. Bezmyšlenkovité klikání myší. Nekvalitní „freeware“ antivirový program. Umožnění automatického přihlašování se k účtům. Hesla uložená v počítači. Totožná hesla pro vstupy do všech aplikací. Jeden uživatelský účet pro více uživatelů. Volný přístup ke složkám s citlivými údaji. Nezaheslovaný počítač. Nedostatečné zajištění soukromí na sociálních sítích. Bezpečnostně slabé kontrolní otázky. Slabá hesla. Bezmyšlenkovité otevírání nevyžádané pošty. Otevírání potenciálně nebezpečných příloh nevyžádané pošty, resp. pošty od neznámých odesílatelů. Ukládání hesel do mobilů. Půjčování notebooků známým. Zadávání e-mailových adres pro volné vstupy na internetové stránky. Sdělování e-mailových adres neznámým osobám.

Z uvedených skutečností je zřejmé, že kyberprostor, tak jako jiné oblasti, potřebuje standardy a normy, které zaručí jeho bezpečnost. Aby se zvýšila bezpečnost internetu, je třeba předmětné zranitelnosti snížit, což znamená zavést jistou kulturu bezpečnosti,

která je běžná jak v životě lidí (morální a etická pravidla, legislativa), tak v technologiích (normy, standardy, legislativa).[132]

5.3 Celkové vyhodnocení šetření

Na základě statistiky a srovnání dat se jako nejvyužívanější nástroj ve spojitosti se zneužíváním internetové komunikace jeví e-mail. Z dotazníkového šetření vyplývá, že čtyřicet tři respondentů (téměř polovina dotázaných) identifikovalo problém po otevření nevyžádaných e-mailů, jejichž prostřednictvím jim do počítačů vnikly viry (patnáct případů), spamy a hoaxy. Rovněž byli prostřednictvím e-mailů různým způsobem obtěžováni a vydíraní. V případě spamů a hoaxů se nejedná o závažný problém, ale v případě intruzí různých virů, v případech, kdy došlo ke zneužití e-mailu k vydírání, vyhrožování anebo v případech, kdy jsou maily využity k odeslání kompromitujícího materiálu, se jedná o závažný zásah do bezpečí, soukromí a života uživatelů. Zajímavým poznáním je skutečnost, že šedesát respondentů, což představuje dvě třetiny dotázaných, z nichž většina jsou standardní uživatelé Internetu, kteří se denně v kyberprostoru pohybují, nevyžádaný mail otevřelo.

V rámci šetření, které bylo provedeno osobními rozhovory s uživateli Internetu i analýzou dat z Internetu se e-mail jako nástroj zneužití objevil celkem jedenáctkrát z dvaceti osmi popsaných případů. Jednalo se o závažné případy, kdy byl e-mail zneužit pro vydírání, anonymní komunikaci s nezletilými obětmi za účelem získání jejich důvěry a následného zneužití, k rozesílání nepravdivých údajů i fotek s erotickým obsahem. Dopady byly katastrofální, došlo k poškození reputace osob, jejich bezpečí i zdravotního stavu. Rovněž byly e-maily zneužity k rozeslání škodlivého softwaru, který svou činností globálně finančně poškodil tisíce uživatelů. Velké finanční ztráty se evidují i u podvodných e-mailů, takzvaných nigerijských spamů.

Sociální sítě jsou dle srovnání dat v pořadí druhým nejčastěji zneužívaným nástrojem (v rámci předmětného šetření celkem dvacet čtyři krát). Následky dopadů na psychické zdraví a bezpečí lidí jsou mnohem závažnější, než je tomu u e-mailů. Ze

[132] PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. Praha: ČVUT, 2011. ISBN 978-80-01-04843-6.

šetření lze usuzovat, že vyjma jediné výjimky se jednalo o snahu narušit bezpečí lidí, pod falešnou identitou zlákat a zneužít důvěřivé uživatele, vylákat, odcizit a zneužít publikované informace nebo terorizovat a šikanovat oběť.

Webové stránky se dle výsledků šetření jeví v pořadí třetím nejčastějším nástrojem pro zneužívání. Do uvedené kategorie je třeba zařadit jak podvodné webové stránky, tak i stránky, na kterých byl umístěn závadný materiál. Současně se webové stránky můžou stát jakýmsi „prostředníkem“ pro realizaci nehumánních aktivit, jak tomu ve třech případech posloužily stránky YouTube. Nelze vynechat různé nedůvěryhodné zdroje poskytující například nelegální software, ze kterých se společně se softwarem do počítače často stáhnou i různé škodlivé kódy. Z dotazníkového šetření vyplývá, že téměř polovina respondentů (čtyřicet tři dotázaných) stahovala data z neznámých/neověřených zdrojů, z toho dvacet osm dotázaných (jedna třetina) evidovala následné problémy.

V rámci předmětného šetření se jako nástroj zneužití dost často objevoval i počítač. Došlo zejména k neoprávněným přístupům k heslům v nich uložených, k uloženému citlivému materiálu a následnému zneužití uložených hesel i dat. V případě Trident Breach posloužily tisíce počítačů jako botnety využívané gangem finančních podvodníků.

Sociální inženýrství, i když se nejedná o internetovou aplikaci, bylo jako „podpůrná metoda“ v případech uvedených v předložené diplomové práci zneužito celkem patnáctkrát.

Z technického pohledu nejčastějšími hrozbami, které byly v rámci šetření identifikovány, jsou „trojský kůň“ (celkem padesát dva případů) a Spyware (dvacet osm případů). Hrozby generovaly časté problémy s operačním systémem (nemožnost aktualizací, zpomalení systému – celkem čtyřicet dva případů v rámci dotazníkového šetření). Fakt, že část dotazovaných respondentů neevidovala žádný problém s činností počítače, ani antivirový program nedetekoval žádnou hrozbu v počítači, rozhodně neznamená, že počítač není napaden.

Ve všech případech bez výjimky, ať se jednalo jakýkoliv použitý nástroj, byl ve větší či menší míře přímý dopad na psychické i fyzické zdraví uživatele. Počínaje leknutím, prvotním šokem, obavami o průnik do soukromí nebo zcizením či zneužitím dat na nosiči informaci, psychickým diskomfortem, nejistotou. Psychické zhroucení, nutnost

psychiatrické léčby, fyzické zneužití, případně ultimativní eventualita – smrt (sebevražda oběti a zabití) byly nejzávažnějšími dopady na postižené. Ke krajním situacím představujícím sebevraždy a zabití, došlo v rámci šetření sedmkrát z dvaceti osmi sledovaných případů. Je nutné zmínit i fakt, že psychická nestabilita obětí a případné sebevraždy výrazně negativně ovlivňují psychiku osob blízkých. Psychické trauma poškozených osob má přímý vliv na rodinné i pracovní vztahy, takže poškozených je v daných případech mnohem více.

Druhým v pořadí ohroženým aktivem je majetek a finanční oblast. Napadení počítače způsobuje finanční ztráty uživatelů zcizením a zneužitím dat (přístupem k bankovním účtům, ztrátou a zneužitím cenných dat potřebných k práci), nutností investic do reinstalace systému a zakoupení nového hardwaru a softwaru. Nemalé finanční ztráty se evidují v případech, kdy byl Internet (online komunikace, podvodné webové stránky) zneužit k vlastnímu obohacení se útočníka (nigerijské spamy, falešné nabídky práce, vydírání a žádosti o zaplacení software), dále i finanční ztráty z důvodu nutnosti přerušení zaměstnání kvůli psychiatrické léčbě, nemožnosti vykonávat práci kvůli nefunkčnímu zařízení. V rámci šetření bylo identifikováno čtrnáct případů; obecně lze soudit, že většina pokusů o napadení systému, je provedena s úmyslem získat peníze. V případech, kdy je škodlivým kódem „pouze“ poškozen systém, je nutná investice do jeho opravy. Obecně řečeno, téměř jakékoliv zneužití online komunikace v jakémkoli ohledu nebo technické poškození generuje finanční ztráty poškozených.

Reputace osobnosti je dalším ohroženým aktivem. Zejména v případech, kdy není možné díky anonymitě Internetu vystopovat útočníka a bránit se. Současně tak je časově velmi náročné získat důkazy a obhájit dobré jméno poškozeného. Nemluvě o případech, kdy vzhledem k rozeslání kompromitujícího materiálu poškozených lze již jejich reputaci jen stěží napravit.

Ze sociálního i psychologického hlediska představují kyberzločiny vážné narušení společenského klimatu, počínaje narušením rodinných, školních a pracovních vztahů, konče negativními dopady na celospolečenské klima.

ZÁVĚR

Kyberprostor nabízí obrovské možnosti pro rozvoj technologií a pro řešení mnoha problémů (rychlé spojení, dálkově ovládané dané technologie apod.). Záleží pouze na záměru uživatele, jakým způsobem příležitosti tohoto virtuálního světa využije. V předložené práci jsou uvedena úskalí, která na běžného uživatele čekají při každém kliknutí myší. Přestože se mnoho lidí domnívá, že jejich standardní znalosti jim umožní vyhnout se případným hrozbám, z průzkumu vyplývá, že je nutné být obezřetným již při zapnutí samotného počítače.

Každý člověk má potřebu chránit si svou osobní identitu (tj. soukromí a bezpečí), bohužel zapomíná na internetovou identitu a podceňuje kyber hrozby, které mohou velmi destruktivním způsobem ovlivnit jeho život i život lidí kolem. Lidé často přes Internet sdělí informace, které by nikdy nenapsali na kus papíru a nenechali volně ležet na stole. Svoje soukromí prezentují prostřednictvím sociálních sítí, publikují statusy obsahující informace, které by z hlediska ochrany soukromí měly být před cizími zraky skryty. Data, která by měla být chráněna, se stanou snadno přístupná i zcela neznámým osobám. Slabinu v kybernetickém prostoru vykazuje zejména sociální síť Facebook, nejen v případě veřejných profilů, ale i umožněním falešné identity, možnostmi pro stažení publikovaných soukromých fotek uživatelů a umožněním jejich následného zneužití. Problém není jenom v samotné technologii, která má řadu bezpečnostních mezer, úmyslných i neúmyslných, ale zejména v chování uživatelů, kteří dobrovolně publikují osobní informace.

Ze šetření vyplynulo, že primární hrozbou pro běžného uživatele je uživatel samotný: uživatelé si často neuvědomují následky bezmyšlenkovitého surfování po Internetu bez použití adekvátní technické ochrany a dodržování základních pravidel pro osobní bezpečnost. Do počítačů si stahují aplikace a programy z neověřených zdrojů. Otevírají poštu od neznámých odesílatelů. Na Internetu dobrovolně sdělují citlivé informace. Nezabezpečují si svá citlivá data a přístupy. Přístupy k různým aplikacím si usnadňují uložením hesel v počítači. Používají bezpečnostně slabá hesla. V domnění, že jsou anonymní, se na Internetu často chovají zcela odlišně (tj. velmi nebezpečně), než v běžném životě, kde chrání své bezpečí a soukromí. Při internetové komunikaci ignorují varovné signály. Naivně důvěřují osobám kolem sebe.

Zásady kultury bezpečnosti

Z technického pohledu je pro bezpečnost uživatele bezpodmínečně nutné, aby byl počítač zaheslován a aby v případě, že jeden počítač užívá více uživatelů, byly i přístupy k jednotlivým uživatelským účtům vždy zaheslovány. Nedoporučuje se ukládat hesla k různým aplikacím do počítače, aby nemohla být útočníkem dekódována. Pod žádnou záminkou je třeba nesdělovat hesla ani nejbližším osobám. V případě, že je heslo vyzrazeno, doporučuje se ho ihned změnit. Zvolit si bezpečnostně silná hesla, která nijak nesouvisí s aktivitami a údaji uživatele. Pokud je to možné, notebook nikomu nepůjčovat a ani bez dohledu neumožnit přístup k počítači jinému uživateli. V případě nečinnosti na notebooku nebo počítači, je doporučováno zmíněné kybernetické prvky uzamknout.

Dále je vhodné instalovat spolehlivý antivirový program, nejlépe placený. Bezplatné verze nejsou tak technicky dokonalé, aby byly schopny odhalit každým dnem vznikající a zdokonalující se škodlivé kódy. Nestahovat soubory z neznámých zdrojů a nestahovat nelegální software, který často obsahuje přidané škodlivé kódy. Neotevírat e-maily, zejména jejich přílohy, jejichž odesílatel je neznámý. Neotevírat přílohy, jejichž data nejsou přímo v e-mailu, ale na externím webovém serveru.

Pro přihlašování se k sociálním sítím je doporučováno používat jiný e-mailový účet, než ten, který uživatel standardně používá. Nepublikovat na sociálních sítích žádný materiál, jenž by uživatel veřejně jiným způsobem nepublikoval. Přístupy ke svému profilu na sociální síti Facebook nastavit pouze pro přátele. Zveřejňování příspěvků nastavit pouze pro přátele. Neakceptovat žádosti o přátelství bez ověření identity žadatele (např. vyměnit několik zpráv, zadat kontrolní otázky). Neakceptovat žádosti o přátelství od neznámých uživatelů. Selektovat lidi, se kterými uživatel sdílí osobní informace. Není vhodné mít na sociálních sítích, kde se sdílí osobní informace, stovky přátel – s nárůstem počtu přátel se zvyšuje riziko úniku a zneužití publikovaných informací. V případě podezření zneužití informace nebo obtěžování konkrétního uživatele odebrat z přátel a zablokovat. Umožnění vyhledání profilu nastavit pouze pro registrované uživatele sociální sítě, neumožnit vyhledání profilu přes vyhledávače Google, Bing apod.

Nechovat se na Internetu s pocitem anonymity. I falešná identita, ačkoliv není využívána k nelegálním činnostem, může být kdykoliv odhalena a kompromitující

aktivity zneužity. Co se týče osobní a internetové identity, je třeba být ostražitý a nedůvěřovat nikomu. Neposkytovat žádný materiál, který by mohl být zneužit.

Neignorovat varovné signály, v případě sebemenší nesrovnalosti či pochybnosti okamžitě opustit stránku nebo vypnout počítač. Je lepší chvíli počkat, případně ověřit poskytovatele služeb nebo komunikátora na druhé straně a věnovat verifikaci více času, než ztratit čas, peníze a duševní klid následkem poškození chráněných aktiv.

Hlídat aktivity dětí na Internetu a všímat si odchylek od jejich standardního chování.

Průběžně se alespoň zběžně informovat o novinkách a měnící se situaci v souvislosti s internetovými riziky. Být opatrný je v daném případě namístě. Je lepší problémům předcházet, než je řešit.

Nepoučitelnost, nedisciplinovanost a naivita uživatelů, kteří i přes teoretické znalosti o internetových hrozbách navštěvují pochybné webové stránky, stahují soubory z neověřených zdrojů, podceňují nutnost potřeby instalace kvalitních antivirových programů a nezabezpečí si svá vlastní data před ostatními, symbolizují doslova otevřenou náruč pro veškeré druhy rizik kyberprostoru.

Největší hrozbou pro uživatele samotného je jeho „klikání myší“ a naivní plná důvěra v osoby, se kterými přichází do kontaktu v kyberprostoru. Svět se mění a lidé se mění s ním. I zde se potvrdilo, že z blízkého člověka se obratem může stát predátor.

Lidé si musí chránit své bezpečí a soukromí prioritně sami. Platná legislativa i technická ochrana jsou pouze přidanými hodnotami, nástroji, které pomůžou řešit případný problém, ale rozhodně nezabrání jeho vzniku, pokud sám člověk jde riziku vstříc.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

GŘIVNA, T., PONČÁK, R. *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008. ISBN 978- 80-903786-7-4.

HARPER, A., HARRIS, S., EAGLE, CH. et al. *Hacking – manuál hackera*. 1. vyd. Praha: Grada, 2008. ISBN 978-80-247-1346-5.

JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KOLEKTIV AUTORŮ. *Sborník příspěvků z konference. Dětská kybernetická kriminalita a sociální sítě*. 1. vyd. Jihlava: Vyšší policejní škola MV, 2011. ISBN 978-80-260-0723-4.

KOUKOLÍK, F., DRTILOVÁ, J. *Vzpoura deprivantů: nestvůry, nástroje, obrana*. 2. vyd. Praha: Galén, 2006. ISBN 978-80-7262-410-2.

MITNICK, K. D., SIMON, W. L. *Umění klamu*. 1. vyd. Gliwice: Helion S. A., 2003. ISBN 83-7361-210-6.

PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. 1. vyd. Praha: ČVUT, 2011. ISBN 978-80-01-04841-2.

PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. Praha: ČVUT, 2012. ISBN 978-80-01-05103-0.

PROCHÁZKOVÁ, D. *Krizové řízení, havarijní plánování a ochrana obyvatelstva*. České Budějovice: VŠERS, o. p. s., 2009. ISBN 978-80-86708-86-7.

PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. 1. vyd. ČVUT Praha, 2011. ISBN 978-80-01-04842-9.

PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. 1. vyd. Praha: ČVUT, 2011. ISBN 978-80-01-04843-6.

ŠMAHEL, D. *Psychologie a internet, děti dospělými a dospělé dětmi*. 1. vyd. Praha: Triton, 2003. ISBN 80-7254-360-1.

VAŠUTOVÁ, M. *Proměny šikany ve světě nových médií*. 1. vyd. Ostrava: Filosofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5.

Seznam použitých zahraničních zdrojů

BOCIJ, P. *Cyberstalking. Harassment in the Internet Age and How to Protect your Family*. 1st edition. Westport CT: Praeger Publishers, 2004. ISBN 0-275-98118-5.

HARPER, A., HARRIS, S., NESS, J., et al. *Grey hat hacking. The ethical hacker´s handbook*. 3rd edition. New York: McGraw Hill, 2011. ISBN 978-0-07-174255-9.

KYŠKA, R. *Všetci sme nahí na Facebooku*. 1. vyd. Bratislava: Forza Music, 2010. ISBN 978-80-89359-24-0.

MITNICK, K.D, SIMON, W. L. *The Art of Intrusion: the real stories behind the exploits of hackers, intruders.* Indianapolis. In: Wiley Publishing, Inc., 2005. ISBN 07-645-6959-7.

WALDEN, I. *Computer crimes and digital investigations*: *the transformation of crime in the information age*. 1st edition. Oxford: Oxford University Press, 2007. ISBN 978-0-19-929098-7.

WALL, D. S. *Cybercrime. The Transformation of Crime in the Information Age.* 1st edition. Cambridge; Malden MA: Polity Press, 2007. ISBN 978-0-7456-2735-9.

Seznam použitých internetových zdrojů

ABZ.CZ. SLOVNÍK CIZÍCH SLOV – ON-LINE HLEDÁNÍ. *Hacker*. [online]. © 2005–2006 [cit. 2012-8-1]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/hacker-hekr

ABCNEWS. *Bullied Teeen Leaves Behind Chilling You Tube Video*. [online]. © 12. 10. 2012 [cit. 2012-11-20]. Dostupné z: http://abcnews.go.com/International/bullied-teen-amanda-todd-leaves-chilling-youtube-video/story?id=17463266#.UMPAp3dXsms

ABCNEWS. *Tyler Clementi Suicide*. [online]. © 2010–2012 [cit. 2012-10-27]. Dostupné z: http://abcnews.go.com/topics/news/tyler-clementi-suicide.htm

ACOHIDO B. *Are there 6.8 million or 24 million bitted PCs on the Internet?* [online]. © 20. 4. 2010 [cit. 2012-6-13]. Dostupné z: http://lastwatchdog.com/6-8-million-24-million-botted-pcs-internet/

AKWAGYIRAM, A. *Does „Happy Slapping" Exist?* [online]. © 12. 5. 2005 [cit. 2012-9-9]. Dostupné z: http://news.bbc.co.uk/2/hi/4539913.stm

BBC. *Happy slapping youths detained for grandfather death*. [online]. © 16. 6. 2010 [cit. 2012- 09-10]. Dostupné z: http://www.bbc.co.uk/news/10331547

BUBLANOVÁ A. *Za zneužití dvaceti chlapců půjde Hovorka na osm let do vězení*. [online]. © 5. 2. 2009 [cit. 2012-07-11]. Dostupné z: http://www.mediafax.cz/krimi/2814724-Za-zneuziti-dvaceti-chlapcu-pujde-Hovorka-na-osm-let-do-vezeni

BUSINESSIT. *Kybernetická kriminalita III. Nakročeno ke kyberterorismu.* [online]. © 2011–2013 [cit. 2012-8-10]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-nakroceno-ke-kyberterorismu.php

CAMERON, K. *24 year old student lights match: Europe versus Facebook*. [online]. © 13. 10. 2011[cit. 2012-05-12]. Dostupné z: http://www.identityblog.com/?p=1201

CLOUD, J. *The 'Bullying Trial': The Unsettling Verdicts in the Tyler Clementi Case*. [online]. © 16. 3. 2012 [cit. 2012-09-10]. Dostupné z: http://www.time.com/time/nation/article/0,8599,2109293,00.html

CESKATELEVIZE.CZ. *Události v regionech.* [online] © 18. 1. 2012 [cit. 2012-07-09]. Dostupné z: http://www.ceskatelevize.cz/ivysilani/10122978233-udalosti-v-regionech-ostrava/412231100030118-udalosti-v-regionech/obsah/186726-policie-stale-casteji-resi-pripady-internetove-kriminality/

CESKATELEVIZE.CZ. *Zlínský soud otevřel nejrozsáhlejší kauzu ve své historii*. [online]. © 27. 2. 2012 [cit. 2012-07-09]. Dostupné z: http://www.ceskatelevize.cz/ct24/regiony/166032-zlinsky-soud-otevrel-nejrozsahlejsi-kauzu-ve-sve-historii/

CESKATELEVIZE.CZ. *Profesor filozofie vyhrožoval kolegovi smrtí*. [online]. © 4. 11. 2010 [cit. 2012-8-30]. Dostupné z: http://www.ceskatelevize.cz/ct24/regiony/jihomoravsky-kraj/106264-profesor-filozofie-vyhrozoval-kolegovi-smrti-pujde-pred-soud/

CESKATELEVIZE.CZ *Počítačový virus se tváří jako zpráva od policie*. [online]. © 7. 11. 2012 [cit. 2012-11-22]. Dostupné z: http://www.ceskatelevize.cz/zpravodajstvi-brno/zpravy/202531-pocitacovy-virus-se-tvari-jako-zprava-od-policie-pozaduje-zaplaceni-pokuty/

COUNCIL OF EUROPE. *Convention on Cybercrime.* [online]. © 23. 9. 2001 [cit. 2012-7-4]. Dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

DEMARCO, M. *Live coverage: Dharun Ravi found guilty on most counts in webcam spyimg trial verdict*. In NJ.com [online]. © 16. 3. 2012 [cit. 2012- 09-10]. Dostupné z: http://www.nj.com/news/index.ssf/2012/03/ravi_webcam_trial_verdict.html

E-BEZPECI.CZ. *Kybergrooming*. [online]. © 2008–2012 [cit. 2012-9-10]. Dostupné z: http://e-bezpeci.cz/

E-BEZPECI.CZ. Happy Slapping. [online]. © 2010 [cit. 2012-09-07]. Dostupné z: http://cms.e-bezpeci.cz/content/view/71/39/lang,czech/

EICHENWALD, K. *Through his Webcam a Boy Joins a Sordid Online World*. [online]. © 2005 [cit. 2012-11-15]. Dostupné z: http://www.nytimes.com/2005/12/19/national/19kids.ready.html?pagewanted=1

FACEBOOK COMPANY. *Newsroom.* [online]. [cit. 2012-05-12]. Dostupné z: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

FBI. *Crime /Punishment. Man Sentenced for Internet Harassment.* In: *About.com* [online]. © 2012 [cit. 2012-10-13]. Dostupné z: http://crime.about.com/od/online/a/web_harass.htm

FBI. LOS ANGELES. *Florida Man Arrested in „Operation Hackerazzi" for Targeting celebrities with Computer Intrusion, Wiretapping, and Identity Theft*. [online] © 12. 10. 2011 [cit. 2012-11-05]. Dostupné z: http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft

FISCHER, K. *First US Cyberstalking case taking shape*. [online]. © 24. 4. 2004 [cit. 2012-10-13]. Dostupné z: http://arstechnica.com/uncategorized/2004/04/3694-2/

GERHARDSTEIN AND BRANCH. *Parents of Jessica Logan resolve case against Sycamoree school district*. [online]. © 2012 [cit. 2012-09-14]. Dostupné z: http://www.gbfirm.com/parents-of-jessica-logan-resolve-case-against-sycamore-school-district

GOOGLE COMPANY. *Accounts. Google.com*. [online]. [cit. 2012-8-8]. Dostupné z: https://accounts.google.com/ServiceLogin?service=oz&continue=https://plus.google.com/?hl%3Dcs%26gpsrc%3Dgplp0&hl=cs

GOOGLE COMPANY. *Our history in depth*. [online]. [cit. 2012-05-13]. Dostupné z: http://www.google.com/intl/en/about/company/history/

GOOGLE INVESTOR RELATIONS. *Google Announces Fourth Quarter and Fiscal Year 2011 Results*. [online]. [cit. 2012-05-13]. Dostupné z: http://investor.google.com/earnings/2011/Q4_google_earnings.html

GREGG, M. *How are Celebrity Cellphones Hacked?* In: *Huffingtonpost.com* [online]. © 16. 3. 2012 [cit. 2012-09-10]. Dostupné z: http://www.huffingtonpost.com/michael-gregg/how-are-celebrity-cell-ph_b_1353780.html

GROHOL, J. *Internet Addiction Guide*. [online]. © 26. 10. 2012 [2012-11-17]. Dostupné z: http://psychcentral.com/netaddiction/

HERVYHO ZÁPISNÍK. *Jak jsem „hacknul" účty Facebooku a zůstal nepovšimnut*. [online]. © 15. 6. 2011. [cit. 2012-04-14]. Dostupné z: http://hervyho-zapisnik.blogspot.cz/2011/06/jak-jsem-hacknul-ucty-facebooku-zustal.html

HO, V. *Cyberstalker enters guily plea*. [online]. © 29. 7. 2004 [cit. 2012-10-13]. Dostupné z: http://www.seattlepi.com/local/article/Cyberstalker-enters-guilty-plea-1150519.php

HOVORKA, M. *Další podvodný e-mail proti České spořitelně, tváří se jako varovná zpráva z banky*. [online]. © 12. 3. 2008 [cit. 2012-12-02]. Dostupné z: http://www.podnikatel.cz/clanky/dalsi-podvodny-e-mail-proti-ceske-sporitelne/

IDNES.CZ. *Mladí skautští vedoucí vydírali svého svěřence a nutili ho k sexu*. [online]. © 26. 3. 2012 [cit. 2012-12-04]. Dostupné z: http://zpravy.idnes.cz/skautsti-vedouci-vydirali-sveho-sverence-a-nutili-ho-k-sexu-pqw-/krimi.aspx?c=A120326_202533_krimi_js

IDNES.CZ. *Soud rozplétá podvody s nabídkami práce, chce vyslechnout tisíce svědků*. [online]. © 27. 2. 2012 [cit. 2012-07-09]. Dostupné z: http://zpravy.idnes.cz/soud-rozpleta-podvody-s-nabidkami-prace-chce-vyslechnout-tisice-svedku-1nn-/krimi.aspx?c=A120227_161747_zlin-zpravy_jog

INES.CZ. *Deviant Hovorka se dočkal za zneužití dvaceti chlapců mírnějšího trestu*. [online]. © 26. 5. 2009 [cit. 2012-7-11]. Dostupné z: http://zpravy.idnes.cz/deviant-hovorka-se-dockal-za-zneuziti-dvaceti-chlapcu-mirnejsiho-trestu-14o-/krimi.aspx?c=A090526_073207_krimi_cen

INTERNET SOCIETY. *Brief History of the Internet*. [online]. © 2012 [cit. 2012-05-05]. Dostupné z: http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet/#Origins

JARGOOGLE. *Hacker*. [online]. © 27. 10. 2003 [cit. 2012-8-5]. Dostupné z: http://www.catb.org/jargon/html/H/hacker.html

JOHN. R. *Tajemství nigerijských dopisů: Stále existují lidé, kteří se snadno nechají připravit o peníze*. [online]. © 24. 7. 2012 [cit. 2012-8-24]. Dostupné z: http://www.reflex.cz/clanek/zpravy/47196/tajemstvi-nigerijskych-dopisu-stale-existuji-lide-kteri-se-nechaji-snadno-pripravit-o-penize.html

KOPECKÝ, K. *Kybergrooming nebezpečí kyberprostoru*. [online]. Olomouc: Net University, s. r. o., 2010 [cit. 2012-10-21]. ISBN 978-80-254-7573-7. Dostupné z: http://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.e-nebezpeci.cz%2Findex.php%2Fke-stazeni%2Fmaterialy-pro-studium-studie-atd%3Fdownload%3D5%253Akybergrooming-studie&ei=QTKEUPz2FOr74QTL4IGgDQ&usg=AFQjCNGoVXS1tyLbY1g-pTXD9QIBr7sW9Q

KRČMÁŘ, P. *Český phishing v akci*! [online]. © 13. 10. 2006 [cit. 2012-11-30]. Dostupné z: http://www.root.cz/clanky/cesky-phishing-v-akci/

KREBSONSECURITY. *Ukraine Detains 5 Individuals Tied to $ 70 Million in U. S. eBanking Heists*. [online]. © 10. 9. 2012 [cit. 2012-10-25]. Dostupné z: http://krebsonsecurity.com/tag/operation-trident-breach/

KULHAVÝ, P. *Kevin Mitnick – slavný podvodník nebo obávaný hacker?* [online]. © 26. 9. 2003 [cit. 2012-9-11]. Dostupné z: http://www.root.cz/clanky/kevin-mitnick-podvodnik-hacker/

MEGANMEIERFOUNDATION.ORG. *Megan Meier´s Story*. [online]. © 13. 11. 2007 [cit. 2012-09-12]. Dostupné z: http://www.meganmeierfoundation.org/megansStory.php

MESKAUSAS, *T. Funmoods toolbar*. [online]. © 10. 7. 2012 [cit. 2012-11-17]. Dostupné z: http://www.pcrisk.com/removal-guides/6756-remove-funmoods-toolbar

MILLEROVÁ, H. *Chtěla být fiktivní dědičkou a přišla o 617.571 korun*. [online]. © 12. 1. 2010 [cit. 2012-8-24]. Dostupné z: http://www.policie.cz/clanek/chtela-byt-fiktivni-dedickou-a-prisla-o-617-571-korun.aspx

NAKED SECURITY. *The Koobface malware gang – exposed!* [online]. © 1997–2012 [cit. 2012- 03- 05]. Dostupné z: http://nakedsecurity.sophos.com/koobface/

NNDB. *Ghyslain Raza*. [online]. © 2012 [cit. 2012-09-23]. Dostupné z: http://www.nndb.com/people/441/000031348/

NEBUĎ OBĚŤ. *Happy slapping. (spokojené fackování)*. [online]. © 210–2012 [cit. 2012-09-10]. Dostupné z: http://www.nebudobet.cz/?page=happy-slapping

NORTON. *Příběhy o počítačové kriminalitě: Sandra*. [online]. ©1995–2013 [cit. 2012-11-20]. Dostupné z: http://cz.norton.com/cybercrime-stories-sandra/article

PASTERNACK, A. *After Lawsuits and Therapy Star Wars Kid is Back*. [online]. © 2011 [cit. 2012-09-23]. Dostupné z: http://motherboard.vice.com/2010/6/1/after-lawsuits-and-therapy-star-wars-kid-is-back

PHIL.MUNI.CZ. *Vyjádření Filosofické fakulty k případu výhružných e-mailů*. [online]. © 17. 7. 2012 [cit. 2012-8-30]. Dostupné z: http://www.phil.muni.cz/wff/home/vyveska/vyjadreni-vedeni-filozoficke-fakulty-k-pripadu-vyhruznych-e-mailu

PODVODY. NET. *Jana Berkusová Hukvaldy 21 Domeček her a zábavy*. [online] [cit. 2012-07-09]. Dostupné z: http://www.podvody.net/Jana-Berkusov%C3%A1-Hukvaldy-21-Dome%C4%8Dek-her-a-z%C3%A1bavy

VIRY.CZ. *Policie ČR Vás sleduje*. [online]. © 5. 10. 2012 [cit. 2012-11-21]. Dostupné z: http://www.viry.cz/policie-cr-vas-sleduje

O´BRIEN.T. *Facebook´s Mark Zuckerberg Clamis Privacy is Dead*. [online]. © 11. 1. 2010 [cit. 2011-05-12]. Dostupné z: http://www.switched.com/2010/01/11/facebooks-mark-zuckerberg-claims-privacy-is-dead/

PŘIBYL, T. *Kyberzločin*. [online]. © 5. 6. 2006 [cit. 2012-8-12]. Dostupné z: http://computerworld.cz/securityworld/kyberzlocin-46339

RAK, R., KUMMER, R. *Motivace a znalosti pachatelů kybernetické trestné činnosti*. [online]. © 19. 12. 2006 [cit. 2012-8-26]. Dostupné z: http://computerworld.cz/securityworld/motivace-a-znalosti-pachatelu-kyberneticke-trestne-cinnosti-46254

RAYMOND, E. S. *How to become a hacker*. [online]. © 2001 [cit. 2012-8-15]. Dostupné z: http://www.catb.org/esr/faqs/hacker-howto.html

RYANPATRICKHALLIGAN.ORG. *Ryan´s story*. [online]. © 2010 [cit. 2012-09-17]. Dostupné z: http://www.ryanpatrickhalligan.org/

SAMEER. *Sexting, the Jessica Logan case, and what schools can do*. [online]. © 10. 3. 2009 [cit. 2012-09-14]. Dostupné z: http://cyberbullying.us/blog/sexting-the-jesse-logan-case-and-what-schools-can-do.html

SEXTING.CZ. *Sexting v České republice*. [online]. © 2009–2012 [cit. 2012-9-10]. Dostupné z: http://www.sexting.cz/

SHAW, G., SINOSKI, K. *B. C. man denies harrassing Amanda Todd; RCMP say allegations are „unfounded"*. [online]. © 17. 10. 2012 [cit. 2012-11-20]. Dostupné z: http://www.ottawacitizen.com/news/denies+harassing+Amanda+Todd+RCMP+allegations+unfounded/7400309/story.html

TOPINKOVÁ, M. *Policie varuje před počítačovým virem, který se šíří Internetem v Česku*. [online]. © 8. 10. 2012 [cit. 2012-11-22]. Dostupné z: http://zpravy.idnes.cz/sireni-pocitacoveho-viru-0yf-/krimi.aspx?c=A121008_144459_domaci_maq

TV NOVA. *Chlapce z Ústí sexuálně zneužívali vedoucí ve skautu! Vymysleli na něj léčku na Internetu.* [online]. © 28. 3. 2012 [cit. 2012-12-06]. Dostupné z: http://tn.nova.cz/zpravy/cernakronika/chlapce-sexualne-zneuzivali-vedouci-ve-skautu-vymysleli-na-nej-lecku-na-internetu.html

TYDEN. CZ *Stalking má být trestný, shodli se ministři*. [online]. © 27. 6. 2008 [cit. 2012-9-9]. Dostupné z: http://www.tyden.cz/rubriky/domaci/stalking-ma-byt-trestny-shodli-se-ministri_67942.htmlUSLEGAL.COM. *Sexting Law and Legal Definition*. [online]. © 2001–2012 [cit. 2012-9-10]. Dostupné z: http://definitions.uslegal.com/s/sexting/

WILLIAMS, B. *University professor helps FBI crack $ 70 million cybercrime ring*. [online]. © 21. 3. 2012 [cit. 2012-10-25]. Dostupné z:

http://rockcenter.msnbc.msn.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring#comments

YAR, M. *Cybercrime and society. Crime and punishment in information age*. [online]. 1st edition. London; Thousand Oaks, CA: Sage publications, 2006 [cit. 2012-08-10]. ISBN 1-4129-0753-5. Dostupné z: http://aleph.nkp.cz/F/?func=file&file_name=find-b&local_base=nkck

YOUTUBE. *The Happy Slapping Killing of Ekram Haque*. [online]. © 26. 7. 2010 [cit. 2012-09-11]. Dostupné z: http://www.youtube.com/watch?v=sP37aSPTHWg&oref=http%3A%2F%2Fwww.google.cz%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D2%26ved%3D0CC0QFjAB%26url%3Dhttp%253A%252F%252Fwww.youtube.com%252Fwatch%253Fv%253DsP37aSPTHWg%26ei%3DcGw-UNCXEszItAbn9oFQ%26usg%3DAFQjCNFsrSYTgXvbQOvUM--hRzb086jIKw

YOUTUBE. *jackass_starwars_funny*. [online]. © 26. 1. 2006 [cit. 2012-09-22]. Dostupné z: http://www.youtube.com/watch?v=o0IuErI3CV0

YOUTUBE. *My story: Struggling, Bullying, Suicide, Self Harm, #RIPAmanda Todd.* [online]. © 7. 9. 2012 [cit. 2012-09-17]. Dostupné z: http://www.youtube.com/watch?v=vOHXGNx-E7E

YOUTUBE. *Funmoods – Firefox Uninstall Tutorial*. [online]. © 30. 1. 2012 [cit. 2012-11-17]. Dostupné z: http://www.youtube.com/watch?v=RgvN9D07FGA

Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů České republiky*. 2009, s. 436. ISSN 1211-1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy

Zákon 104/1991 Sb., o přijetí Úmluvy o právech dítěte. In: *Sbírka zákonů České republiky*. 1991, s. 503. ISSN 1211–1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=104/1991&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ostatní zdroje

CZECH TECHNICAL UNIVERSITY: *International konference: CyberTerrorism and CrimeConference CYTER 2012.* [CD-ROM]. Praha: CVUT Praha, 2012. [cit. 2012-07-07]. ISBN 978-80-01-05072-9.

INTERNATIONAL KONFERENCE: CYBERTERRORISM AND CRIMECONFERENCE CYTER 2012. PRAGUE.

SEZNAM OBRÁZKŮ, GRAFŮ A TABULEK

Seznam obrázků

Seznam tabulek

SEZNAM PŘÍLOH

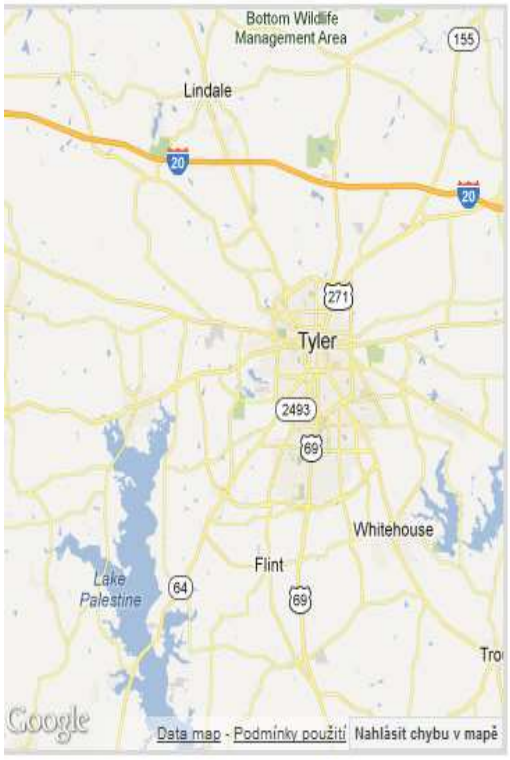
PŘÍLOHY

Příloha A – Detekování IP adresy

Relevantní část hlavičky e-mailu

Received: from dallas.simonliu.net (dallas.simonliu.net **[69.164.199.250]** by e-mail-smtpd1.go.seznam.cz (Seznam SMTPD 1.2.15-6@18976) with ESMTP; Fri, 30 Dec 2011 21:21:30 +0100 (CET) Received: from **[183.39.132.233**] (helo=win7.applib.com)by dallas.simonliu.net with esmtpa (Exim 4.69) (envelope-from <support@acetools.biz>) id 1RgiT1-0003vn-IZ.

Obrázek 1: Informace o IP 69.164.199.250



69.164.199.250 Lookup

Try 212.67.75.188 (your IP address)

IP	‹ 69.164.199.250 ›
Hostname	dallas.applib.com
ISP	Linode
Organization	Linode
Country	United States
Region	Texas
City	Dallas
Local time	2013/11/02 10:29 (Central Standard Time)
Location	32.7831, -96.8067
JSON data	69.164.199.250.json

— Updated by 108.59.11.73

Zdroj: Dazzlepod.com. [online]. © 2012 [cit. 2012-03-15]. Dostupné z: https://dazzlepod.com/ip/?ip_address=69.164.199.250

Obrázek 2: Informace o IP 183.39.132.233

183.39.132.233 Lookup

Try 212.67.75.188 (your IP address)

IP	❮ 183.39.132.233 ❯
Hostname	183.39.132.233
ISP	ChinaNet Guangdong Province Network
Organization	ChinaNet Guangdong Province Network
Country	China
Region	Guangdong
City	Shenzhen
Local time	2013/11/03 00:40 (Hong Kong Standard Time)
Location	22.5333, 114.1333
JSON data	183.39.132.233.json

— Updated by 212.67.75.188

Zdroj: Dazzlepod.com. [online]. © 2012 [cit. 2012-03-15]. Dostupné z: https://dazzlepod.com/ip/?ip_address=183.39.132.233

Příloha B – Dotazník

1. **Otevřel/a jste někdy nevyžádaný e-mail? (E-mail od neznámého odesílatele.)**

   - Ano
   - Ne

2. **Mělo pro Vás otevření nevyžádaného e-mailu nějaké nepříjemné následky? (Obtěžování nebo jiné nebezpečí.)**

   - Ano
   - Ne

3. **Pokud byla odpověď na předchozí otázku ano, napište, o jaké následky se jednalo. (Lze označit více možností.)**

   - Virus
   - Vydírání
   - Spam
   - Hoax – falešná zpráva, smyšlené nebezpečí, žádost o další rozeslání
   - Jiné

4. **Stahoval/a jste někdy soubory z neznámých/neověřených zdrojů?**

   - Ano
   - Ne

5. **Pokud došlo ke stahování souborů z neznámých/neověřených zdrojů, detekoval Váš antivirus nějakou hrozbu?**

   - Ano
   - Ne

6. **Detekoval někdy Váš antivirový program jakoukoliv hrozbu ve Vašem počítači, která byla následně odstraněna, případně odeslána do antivirové karantény?**

- Ano
- Ne

7. **V případě detekování hrozby ve Vašem počítači, o jaký druh hrozby se jednalo? Pokud si vzpomenete dle historie v registru. (Lze označit více možností.)**

   - Trojský kůň
   - Backdoor
   - Bot
   - Spyware
   - Adware
   - Jiné, prosím uveďte

8. **Pokud byl Váš počítač někdy napaden, jaké byly následky? (Lze označit více možností.)**

   - Problémy s operačním systémem, narušení výkonu počítače, nemožnost aktualizací apod.
   - Krádež citlivých dat
   - Krádež identity
   - Neuvědomuji si
   - Jiné, prosím uveďte

9. **Byly někdy Vaše údaje nebo údaje Vašich blízkých, které používáte prostřednictvím Internetu, nějakým způsobem zneužity?**

   - Ano
   - Ne

10. **V případě, že byly údaje zneužity, jak se to stalo? (Lze označit více možností.)**

    - Sociální sítě

- Podvodné stránky
- Podvodná transakce při nákupu/prodeji zboží
- Nigerijský spam – žádost o pomoc při převodu dědictví ze vzdálené země, zaplacení „úhrady“ za převod
- Jiné, prosím uveďte

11. Byl někdo z Vašich známých jakýmkoliv způsobem šikanován prostřednictvím Internetu? (lze označit více možností)

- Útok/ponižování v rámci sociálních sítí
- E-mailové obtěžování
- Vydírání zveřejněním citlivých fotek
- Nevím
- Jiné, prosím uveďte

12. Využíváte sociální sítě?

- Ano
- Ne

13. Které sociální sítě využíváte? (Lze označit více možností.)

- Facebook
- Twitter
- LinkedIn
- Libimseti.cz
- Lide.cz
- MySpace
- Spoluzaci.cz
- Jiné

14. Do které kategorie uživatelů Internetu byste se zařadil/a?

- Velmi zkušený uživatel
- Standardní uživatel
- Nezkušený/začínající uživatel

Příloha C – Možné scénáře událostí, které vyvolalo zneužití Internetu

Příčiny problémů a negativních konsekvencí, které vznikly uživatelům osloveným v rámci kvantitativního průzkumu, lze kvalifikovat na základě analogie s vyšetřenými případy následovně.

Jana Berkusová, psychoterapeutické centrum Hukvaldy – Ke kauze došlo prolomením hesla uživatele, vykradení a zneužití e-mailového účtu a nelegální spravování cizích webových stránek. Do dnešního dne se nezjistilo, co bylo důvodem útoku a jakým způsobem k prolomení hesla došlo, protože nebylo možné prokázat vinu a úmysl podezřelého. Podle charakteru útoku lze vyvodit, že se jednalo o osobní mstu útočníka, který do dnešního dne nebyl potrestán. Pro oběť znamenala kauza existenční kolaps.

Tomáš Kadlec, podvodné vylákání peněz, klamavá reklama na Internetu – Typickým rysem předmětné kauzy je buď požadavek finanční částky za zprostředkování služby, která zprostředkovaná není, anebo prvotní požadavek jedné konkrétní, spíše menší, částky s tím, že žádná další požadována nebude. Jakmile však poškozený vyhoví a peníze pošle, vyskytnou se náhle komplikace, na jejichž řešení je třeba vynaložit další a další (samozřejmě vždy již konečné) finanční prostředky.

Pavel Hovorka, kybergrooming – Útočník využil neznalost obětí, jejich sociální status, vyvolal falešnou důvěru, aby je přiměl k poskytnutí citlivého materiálu, který následně využil k vydírání a poté k sexuálnímu zneužití. Ke komunikaci a sbližování s oběťmi využil sociální sítě – seznamovací servery, na kterých cíleně kontaktoval určité předem selektované typy. Vzhledem k nárůstu uživatelů sociálních sítí a seznamovacích serverů lze usuzovat, že předmětné nežádoucí a nepřijatelné jevy budou eskalovat. Internetoví útočníci, kromě uvedených komunikačních kanálů, využívají také inzertní portály, na kterých nabízejí dětem různé možnosti výdělku či kariéry. Kamil Kopecký ve své studii Kybergrooming nebezpečí kyberprostoru uvádí: „*Internetoví predátoři využívají inzertní portály zaměřené přímo na nezletilé uživatele internetu, na dětské a herní portály i portály zaměřené na různé volnočasové*

aktivity.“[133] Proto se všude kde je možné komunikovat zcela anonymně a kde je možné vytvářet neověřenou falešnou identitu s kybergroomingem budeme potkávat.

Nigerijské spamy v České republice – Příčinou kauzy je důvěřivost, neznalost, neinformovanost a snaha získat téměř bezpracně obrovský finanční obnos. Extrémně velký obnos peněz a snadný přístup k němu jsou neslučitelnými jevy. Autoři nigerijských dopisů zneužili hlouposti, naivity a touhy po rychlém obohacení se. Použili sofistikovaný způsob obelhání oběti primárně formou manipulativně napsaného dopisu, následně účelově vytvořenými webovými stránkami a imaginárním personálním obsazením i takzvaně profesionální a zdánlivě důvěryhodnou komunikací s obětí.

Jedinou účinnou obranou proti nigerijským spamům je jejich vymazání bez toho, aby zpráva byla přečtena. Pokud recipient zprávu otevře, existuje možnost, že odesílatel bude o dané aktivitě informován a získá jistotu, že e-mailová adresa je aktivní. V uvedeném případě lze očekávat další spamy, které je nutné již odstraňovat bez přečtení. Obecně platí, že jakýkoliv mail od neznámého odesílatele, zejména s cizokrajným jménem, se doporučuje okamžitě bez přečtení smazat. V popsaných případech došlo k obrovským finančním ztrátám. Oběť z Jindřichova Hradce se navíc vystavila riziku možného trestního stíhání z důvodu napomáhání ilegálního převodu peněz.

Výhrůžné maily na Masarykově univerzitě v Brně – Počin se dá klasifikovat jako cyber harrassment neboli kybernetové obtěžování, případně cyberstalking. V uvedeném případě došlo k vyhrožování smrtí. Podle indicií a informací, které jsou na Internetu dostupné, lze vyvodit, že oběť znala svého údajného pronásledovatele, rovněž tak byly okolí údajně známy i případné důvody tohoto počinu, kterými měly být rozdílné názory zainteresovaných na tématiku profesní aprobace. I přesto, že soud uznal viníka vinným, přímé důkazy o vině do dnešního dne neexistují. Na předmětném případě lze demonstrovat fakt, že informační technologie společně s Internetem lze zneužít rafinovaným způsobem, který je velice těžko prokazatelný. Dopadem je v daném případě sociální diskreditace oběti i údajného pachatele i finanční pokuta.

---

[133] KOPECKÝ, K. *Kybergrooming nebezpečí kyberprostoru*. [online]. Olomouc: Net University, s. r. o., 2010 [cit. 2012-10-21]. ISBN 978-80-254-7573-7. Dostupné z: http://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.e-nebezpeci.cz%2Findex.php%2Fke-stazeni%2Fmaterialy-pro-studium-studie-atd%3Fdownload%3D5%253Akybergrooming-studie&ei=QTKEUPz2FOr74QTL4IGgDQ&usg=AFQjCNGoVXS1tyLbY1g-pTXD9QIBr7sW9Q

Šíření počítačového viru v ČR – Intruze škodlivého kódu, který, dle sdělení Policie ČR, infikoval počítače zejména při surfování na erotických stránkách nebo při stahování nelegálního software. Zásadní chyba uživatelů, která primárně demonstruje zranitelnost počítačů při stahování jakéhokoli obsahu z neověřených, respektive z nelegálních zdrojů, a rovněž při vstupech na pochybné webové stránky s největší pravděpodobností bez legálního, aktualizovaného a placeného antivirového programu, který je schopen škodlivé viry typu „trojan" detekovat. Sekundárním pochybením byla nedostatečná ostražitost uživatelů, již i přes neprofesionálně zformulovaný text sdělení uvěřili a požadovanou finanční částku útočníkům odeslali.

Phishingový útok na klienty České spořitelny – Neopatrnost a nízká ostražitost uživatelů při komunikaci se serverem internetového bankovnictví, kteří i přes určité nesrovnalosti, jež jsou v dané oblasti zcela vyloučené, vyplnili své identifikační údaje a umožnily tak útočníkům neoprávněný přístup k bankovním účtům.

Falešná identita na Facebooku – Pohlavní zneužití nezletilého chlapce – Falešná identita na sociální síti, zneužití důvěry dítěte, které vyústilo v sexuální zneužívání. Obava dítěte svěřit se rodičům s problémem, rodiče zpočátku neměli informace týkající se internetové komunikace svého syna. Případ je v současné době[134] ve stavu vyšetřování, protože se objevily důkazy o zneužívání dalších nezletilých osob.

Operace Trident Breach – Případ představuje jeden z největších kyberzločinů v souvislosti s nesmírně sofistikovaným způsobem zneužití počítačů, do detailů zvládnutou organizací i výší zpronevěry peněz, včetně globálního pokrytí působnosti zločinecké skupiny. Investigativní techniky a taktiky, zejména kombinace Facebookových a Google aplikací, společně s informacemi dostupnými v databázích, které byly využity v průběhu vyšetřování, byly do dané doby nestandardní a výrazně napomohly úspěšnému vyřešení problému.

Tyler Clementi Case, Bullying Trial – Popsaný příběh demonstruje zneužití informačních technologií, konkrétně webkamery, za účelem sledování osob a následné zveřejnění získaných citlivých a intimních informací na sociální síti, které měly oběť vyvést z rovnováhy a zesměšnit jí. I přesto, že si pachatel údajně neuvědomoval závažnost a trestní odpovědnost svého počínání, svým jednáním přispěl k psychickému traumatu, k pocitu ohrožení a následně ke spáchání sebevraždy oběti.

[134] Platné ke dni 29. 12. 2012.

Happy Slapping – Byly využity informační technologie k pořizování a distribuci materiálu s ponižujícím a nelegálním obsahem. Agresivní chování se mění s vývojem společnosti a jako každá jiná aktivita, těží z výdobytků dané doby. V daném konkrétním případě agresivita a násilí využívají nejmodernější a nejrychlejší komunikační média. Jedná se o realizaci násilných činů uskutečněných primárně za účelem dalšího šíření. Informační technologie v tomto případě plní funkci motivátora. Stimulem je získání určitého postavení ve skupině, kterého lze dosáhnout pouze zveřejněním násilného činu. Dopady jsou nepřijatelné – počínaje fyzickou i psychickou újmou a konče smrtí oběti.

Megan Meier, My Space Hoax – Učebnicový příklad, jak falešná a neověřená identita na sociální síti, založena za účelem šikany a ponižování, může mít destruktivní dopad na osobnost a život oběti. Alarmujícím faktem je, že tak hrozný zločin provedla na dítěti dospělá osoba, která si byla plně vědoma veškerých následků svého počínání. Útoky byly prováděny promyšleně, se záměrem co nejvíce uškodit labilní nezletilé osobě. Důsledkem byla sebevražda. Jedná se o další z mnoha kyberzločinů, kdy útočník z důvodu nedostatku přímých důkazů a prokázání zločinu nebyl potrestán. Internetová anonymita opět napomohla provést útok s ničivým dopadem na lidský život a negativními dopady na lidské soužití

Jessica Logan, sexting case – Zamilovaná mladá dívka bez rozmyslu a dobrovolně předala citlivý fotografický materiál osobě, která ho z pomsty zneužila. Případ byl posuzován i jako šíření pornografie. Nečinnost odpovědných autorit v souvislosti s nežádoucí situací, se kterou byli obeznámeni, demonstruje laxnost a podceňování následků sextingu a rizikového chování na Internetu, kterým bylo rozeslání řetězové zprávy s nahými fotkami dívky. Situace přes veřejnou šikanu vyústila v sebevraždu dívky. Problém by pravděpodobně bylo možné vyřešit zásahem ze strany vedení školy, formou pohovorů se šikanéry a jejich rodiči, případně doporučením pro změnu školního zařízení.

Star Wars Kid – Primární úmysl natočení videa, kterým se jeho nezletilý autor chtěl vžít do role filmového hrdiny, se obrátil proti chlapci samotnému. Materiál byl zneužit neoprávněným zveřejněním na populárních webových stránkách. Údajně nevinný záměr spolužáků, kterým mělo být pouze pobavení, skončil psychickým kolapsem oběti i finančními náklady rodin spolužáků, již materiál zveřejnili. Z určitého pohledu

„neškodná“ zábava, u které na počátku bylo zapomenuté video, způsobila celosvětový rozruch.

Sebevražda Ryana Halligana – Úmyslné šikanování formou online šíření nepravdivých informací o oběti, zveřejnění soukromé korespondence prostřednictvím Internetu, navádění k sebevraždě nakonec skončilo sebevraždou oběti. Případ je důkazem nejen toho, že mnoho dětí se dospělým nesvěří se svými problémy, které by s jejich pomocí mohly bez větších problémů řešit, ale i faktu, že rodiče často nemají přehled o internetových aktivitách svých potomků, což stěžuje možnost adekvátního zásahu ve prospěch šikanovaného dítěte.

Sebevražda Amandy Todd – Jeden z nejdiskutovanějších a nejhorších případů v posledních letech demonstruje jak neadekvátní a rizikové chování oběti na Internetu, tak nezájem okolí, respektive podcenění varovných signálů. Případ je ukázkou, jak anonymita Internetu napomáhá psychopatickým útočníkům realizovat neetické, ilegální a nehumánní aktivity. Lhostejnost okolí a pravděpodobně nedůsledný přístup a vnímavost rodiny vůči psychickému stavu oběti umožnily útočníkovi dosáhnout svého cíle. V kauze se objevuje hned několik internetových sociopatologických jevů, konkrétně kyber krášlení, kyberšikana, sexting, kybernetové vydírání, kybernetové obtěžování, doplněno o sociální inženýrství.

Chris Chaney, Operace Hackerazzi – I z původně nezkušeného uživatele Internetu se může stát sofistikovaný útočník. Kombinace faktorů, kterými jsou anonymita Internetu, díry v zabezpečení internetové identity a soukromé informace o osobách publikované v médiích umožnily útočníkovi přístup k soukromým e-mailovým účtům i k citlivým datům, která pak byla následně zneužita jejich zveřejněním.

Kauza Justina Berryho – internetové porno – Klasický případ nabádání dítěte k pornografii ve spojení s rizikovým chováním oběti – sextingem. Aktivita byla prokázaná na obou stranách, nelze ignorovat úmyslné rizikové chování oběti za účelem obohacení se. V daném případě byla oběť opakovaně fyzicky zneužita. Sekundárním následkem byla drogová závislost, která oběť „nutila“ k provozování sexuálních aktivit. Případ díky zainteresovanosti reportéra New York Times dopadl dobře. Oběť poté, co se dostala z vlivu pedofilů, pomohla policii odhalit obrovskou síť distributorů dětského porna.

Zcizení osobních dat za účelem nelegálního výběru peněz – Technický útok na počítač, neoprávněná a samočinná instalace škodlivého kódu z náhodně prohlížených webových stránek. Důvodem byl nespolehlivý a málo účinný antivirový program, který neodhalil škodlivý kód ani při intruzi, ani jeho dlouhodobější přítomnost v počítači.

Internetové obtěžování Seattle – Prostřednictvím falešné identity byla dlouhodobě prováděna šikana a poškozena reputace uživatelky. Vzhledem k vysoké kybernetické zdatnosti útočníka, který sofistikovaně měnil svou identitu, nebylo možné ho identifikovat bez spolupráce s FBI a s Federálními Telekomunikacemi.

Příloha D – Možné scénáře způsobů provedení zneužití Internetu

Další charakteristické rysy sledovaných případů jsou, že postižené osoby podcenily a nevěnovaly pozornost podstatným znalostem o škodlivých jevech na internetu. Zranitelným sociálním chováním postižené osoby umožnily výskyt osmi dále analyzovaných situací.

1. Využití nástroje „Koobface“, které se projevilo jako:
    - kumulace neobvyklých událostí ve stejném sociálním kontextu, jejichž individuální přítomnost by jinak uživatelku varovala. Konkrétně komunikace v angličtině u profesorky žijící v USA nebyla varovným signálem, odkaz na video byl považován za jakýsi vítající prvek či snahu vždy kreativní a svérázné profesorky o uvítací pozdrav,
    - neopodstatněná důvěra v internetovou stránku, která na první pohled vypadala podezřele,
    - stahování software, který již byl v notebooku instalován a o jehož přítomnosti v notebooku uživatelka věděla,
    - stahování software z neznámého zdroje. Adobe Flash Player nebyl stažen z originálního zdroje, což si uživatelka primárně neuvědomila,
    - neznalost a nízké povědomí o možných hrozbách (Koobface byl v danou dobu virusem známým po celém světě, včetně způsobu jeho instalace),
    - bezplatný a nekvalitní antivirový program, který nezajistil adekvátní ochranu a bez jakéhokoliv varování povolil uživatelce stažení souboru obsahující nebezpečný virus.
2. Využití nástroje „AceTools.biz“, které se projevilo jako:
    - stahování neznámého software od neznámého poskytovatele, na který uživatel neměl k dispozici standardní reference. Uživatel si po zkušenosti s AceTools.biz instaloval do prohlížeče Mozilla Firefox doplněk WOT Safe Search,
    - uživatele nevarovala skutečnost, že software neobsahuje licenční podmínky a instalaci přesto dokončil,

- uživatele nevarovala skutečnost, že grafika stránky poskytující software za poplatek byla velmi amatérsky zpracovaná.

3. Využití nástroje „nabourání se do účtu na Facebooku“, které se projevilo jako:
   - agresor znal jeden z přihlašovacích údajů uživatele,
   - byla vybrána bezpečnostně slabá kontrolní otázka,
   - společné užívání počítače bez zabezpečení jejího uživatelského účtu umožnilo agresorovi bez problémů zjistit přihlašovací hesla uživatelky,
   - v případě agresora se jednalo o velmi zkušeného internetového uživatele a odborníka v ICT technologiích.

4. Využití nástroje „zcizení identity – neoprávněný přístup k účtu na Facebooku“, které se projevilo jako:
   - nulové zajištění účtu jednoho z více uživatelů počítače,
   - uložení přihlašovacích údajů do paměti počítače,
   - bezohlednost, nerespektování soukromí, snaha o kontrolu a získání moci nad partnerem.

5. Využití nástroje „falešná žádost o přátelství na Facebooku“, které se projevilo jako:
   - lehkovážné potvrzení přátelství bez ověření totožnosti neznámého uživatele žádajícího o vstup do soukromí facebookového účtu.

6. Využití nástroje „Sexting, zneužití intimních foteček rozesláním na desítky e-mailových adres“, které se projevilo jako:
   - nebezpečné chování na Internetu, odeslání fotek se sexuálním obsahem s identifikovatelným znaky dotčené osoby,
   - naivní důvěra,
   - nulové zabezpečení uživatelského účtu v notebooku při užívání notebooku více uživateli.

7. Využití nástroje „zneužití fotky publikované na internet“, které se projevilo jako:
   - primárně dobrý úmysl o informovanost „přátel“ a naivní domněnka, že se publikováním fotky uctí památka kolegy, který byl následně zneužit,

- neuvědomění si, že se jedná o vysoce citlivou, emocionálně vděčnou, atraktivní a nestandardní událost, jež bude „mediální bombou“, pro kterou budou média i veřejnost získávat informace jakýmkoliv způsobem, z jakýchkoliv dostupných zdrojů,
- sdílení a zobrazování fotky nebylo nastaveno pouze pro přátele, fotka se mnohonásobným sdílením dostala mimo okruh zainteresovaných osob, včetně komentářů a dalších podrobností. Bylo jen otázkou času, kdy se tento unikátní materiál objeví v médiích,
- snaha bulváru za každou cenu publikovat informace šokujícím způsobem za účelem zvýšení návštěvnosti internetových stránek i zisků z prodeje tiskovin bez ohledu na emoce pozůstalých.

8. Využití nástroje „Funmoods“, které se projevilo jako:
   - stahování software z neověřeného zdroje,
   - nespolehlivý antivirový program (v konkrétním případě bezplatná verze).

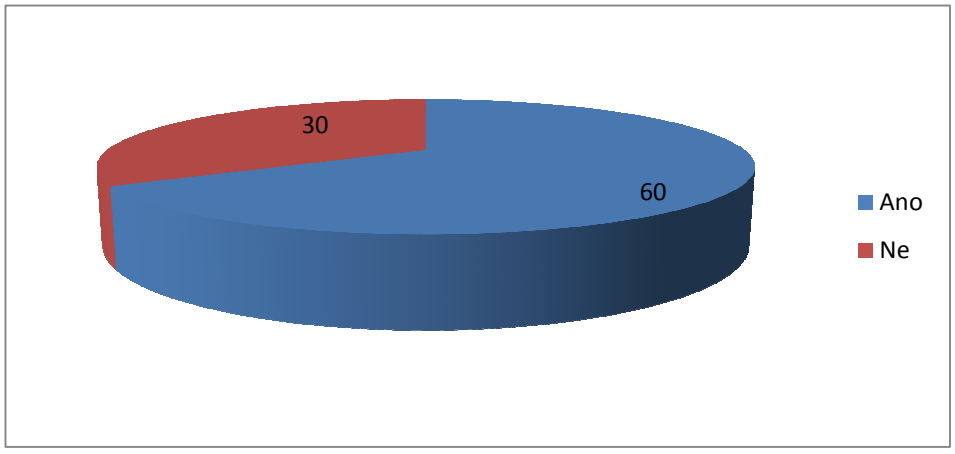
Příloha E – Vyhodnocení dotazníkového šetření

Vyhodnocení odpovědí na otázku „*Otevřel/a jste někdy nevyžádaný mail? (mail od neznámého odesílatele)*“ je v tabulce 1 a znázorněno v grafu 1 (zodpovězeno 90krát).

Tabulka 1: Statistika otevření nevyžádaných e-mailů

Odpověď	**Odpovědi**	**Podíl**
Ano	60	66,66 %
Ne	30	33,33 %

Graf 1: Statistika otevření nevyžádaných e-mailů

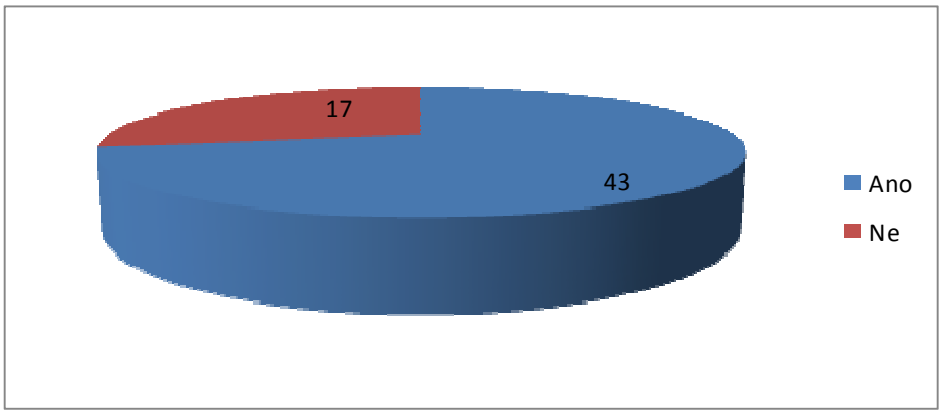


Vyhodnocení odpovědí na otázku „*Mělo pro vás otevření nevyžádaného mailu nějaké nepříjemné následky? (obtěžování nebo jiné nebezpečí)*“ je v tabulce 2 a znázorněno v grafu 2 (zodpovězeno 60krát).

Tabulka 2: Případné následky po otevření nevyžádaného e-mailu

Odpověď	**Odpovědi**	**Podíl**
Ano	43	71,66 %
Ne	17	28,33 %

Graf 2: Případné následky po otevření nevyžádaného e-mailu

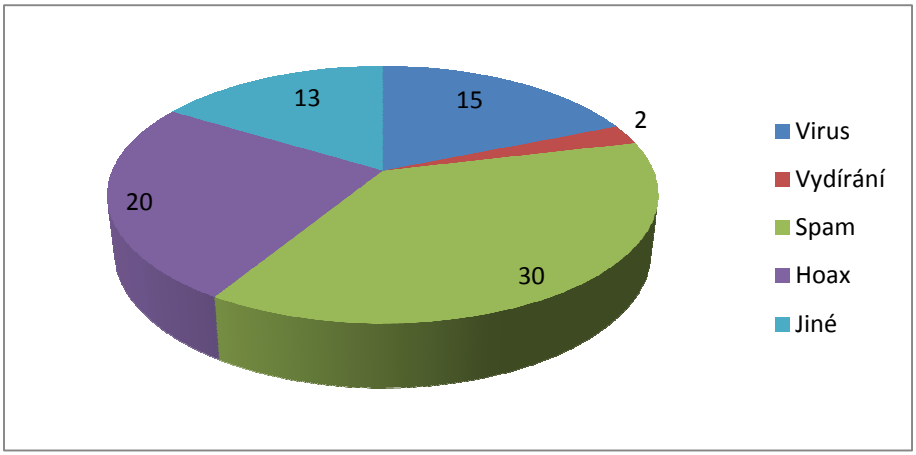


Vyhodnocení odpovědí na otázku „*Pokud byla odpověď na předchozí otázku ano, napište, o jaké následky se jednalo? (lze označit více možností)*“ je v tabulce 3 a znázorněno v grafu 3 (zodpovězeno 43krát).

Tabulka 3: Druhy následků po otevření nevyžádaného e-mailu

Odpověď	**Odpovědi**	**Podíl**
Virus	15	34,88 %
Vydírání	2	4,65 %
Spam	30	69,76 %
Hoax	20	46,51 %
Jiné	13	30,23 %

Graf 3: Druhy následků po otevření nevyžádaného e-mailu

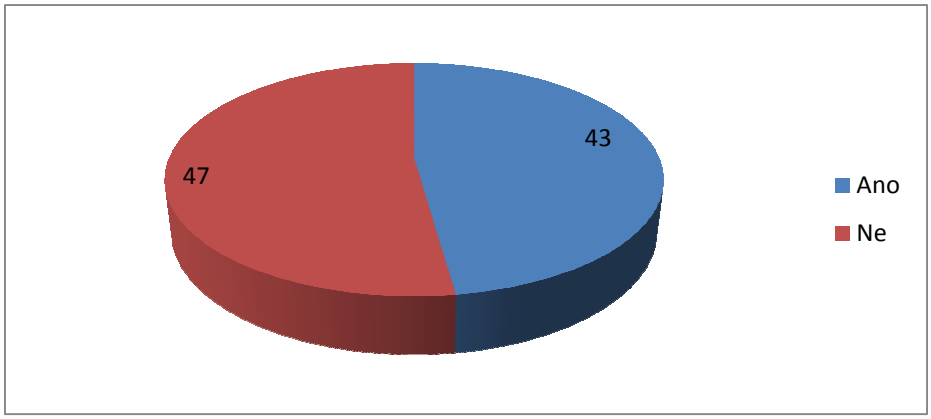


Vyhodnocení odpovědí na otázku „*Stahoval/a jste někdy soubory z neznámých/neověřených zdrojů?*“ je v tabulce 4 a znázorněno v grafu 4 (zodpovězeno 90krát).

Tabulka 4: Statistika stahování souborů z neznámých/neověřených zdrojů

Odpověď	**Odpovědi**	**Podíl**
Ano	43	47,77 %
Ne	47	52,22 %

Graf 4: Statistika stahování souborů z neznámých/neověřených zdrojů

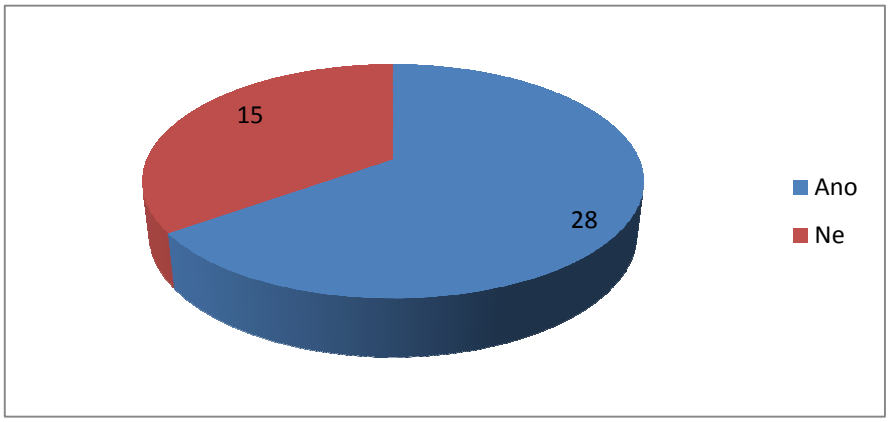


Vyhodnocení odpovědí na *otázku „Pokud došlo ke stahování souborů z neznámých/neověřených zdrojů, detekoval Váš antivirus nějakou hrozbu?*“ je v tabulce 5 a znázorněno v grafu 5 (zodpovězeno 43krát).

Tabulka 5: Detekce hrozby antivirovým programem po stažení souborů z neznámých/neověřených zdrojů

Odpověď	**Odpovědi**	**Podíl**
Ano	28	65,11 %
Ne	15	34,88 %

Graf 5: Detekce hrozby antivirovým programem po stažení souborů z neznámých/neověřených zdrojů

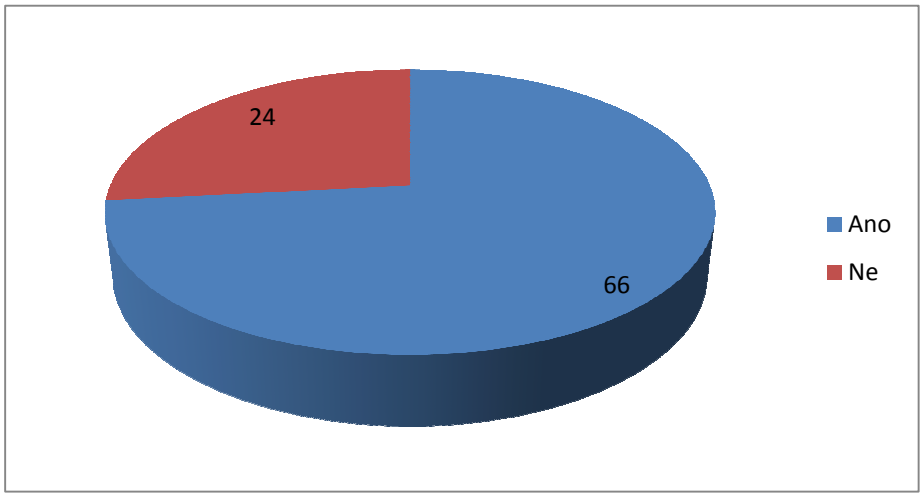


Vyhodnocení odpovědí na *otázku „Detekoval někdy Váš antivirový program jakoukoliv hrozbu ve Vašem počítači, která byla následně odstraněna, případně odeslána do antivirové karantény?*“ je v tabulce 6 a znázorněno v grafu 6 (zodpovězeno 90krát).

Tabulka 6: Detekce hrozby v počítači, která byla odstraněna případně odeslána do karantény

Odpověď	**Odpovědi**	**Podíl**
Ano	66	73,33 %
Ne	24	26,66 %

Graf 6: Detekce hrozby v počítači, která byla odstraněna případně odeslána do karantény

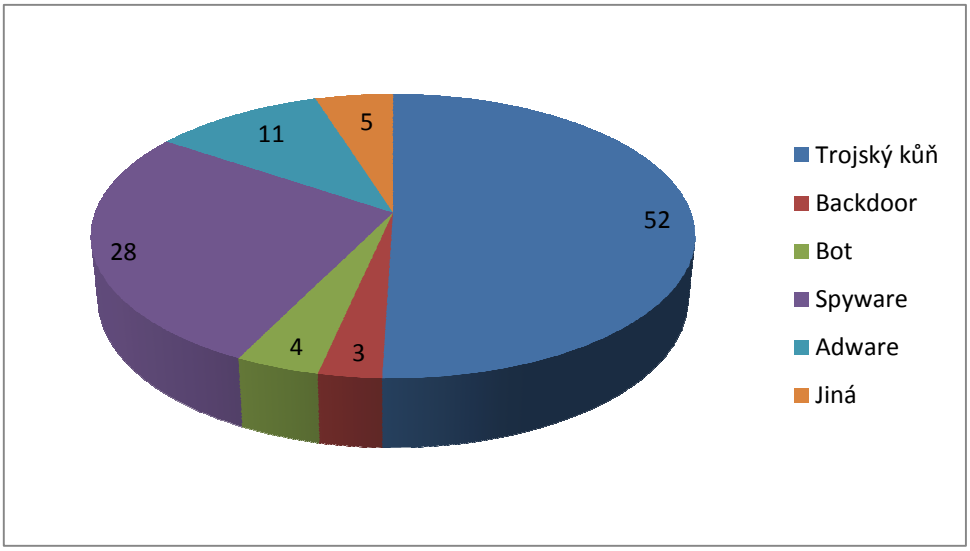


Vyhodnocení odpovědí na otázku „*V případě detekování hrozby ve Vašem počítači, o jaký druh hrozby se jednalo? Pokud si vzpomenete dle historie v registru. (lze označit více možností)*“ je v tabulce 7 a znázorněno v grafu 7 (zodpovězeno 66krát).

Tabulka 7: Druhy detekovaných hrozeb

Odpověď	**Odpovědi**	**Podíl**
Trojský kůň	52	78,78 %
Backdoor	3	4,54 %
Bot	4	6,06 %
Spyware	28	42,42 %
Adware	11	16,66 %
Jiná, uveďte	5	7,57 %

Graf 7: Druhy detekovaných hrozeb



Vyhodnocení odpovědí na otázku **„***Pokud byl Váš počítač někdy jakkoli napaden, jaké byly následky? (lze označit více možností)*“ je v tabulce 8 a znázorněno v grafu 8 (zodpovězeno 75krát).

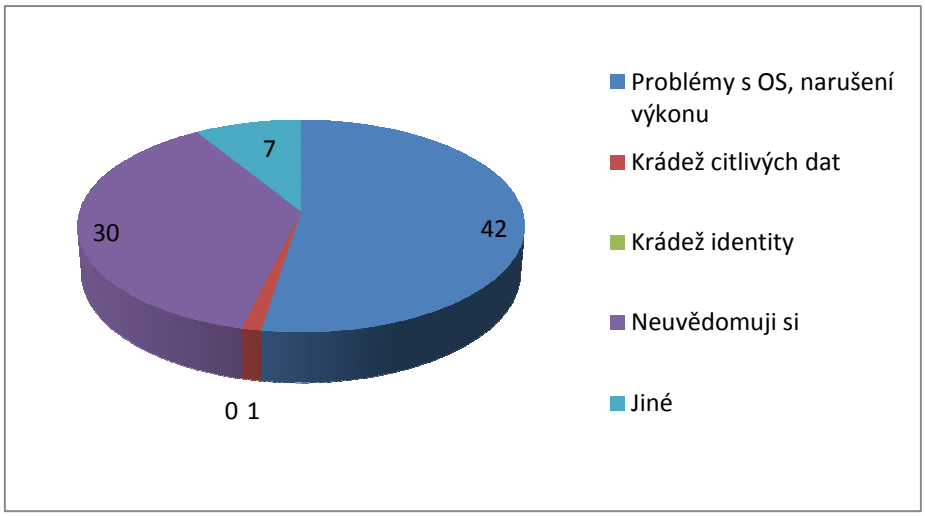
Tabulka 8: Následky po případném napadení počítače

Odpověď	Odpovědi	Podíl
Problémy s operačním systémem, narušení výkonu počítače (zpomalení, nemožnost aktualizací apod.)	42	56,00 %
Krádež citlivých dat	1	1,51 %
Krádež identity	0	0,00 %
Neuvědomuji si	30	40,00 %
Jiné	7	9,33 %

Jiné:

- problém s policií,
- manipulace s účtem na Facebooku,
- žádné, hrozba byla odstraněna antivirovým programem,
- kompletní nefunkčnost počítače.

Graf 8: Následky po případném napadení počítače

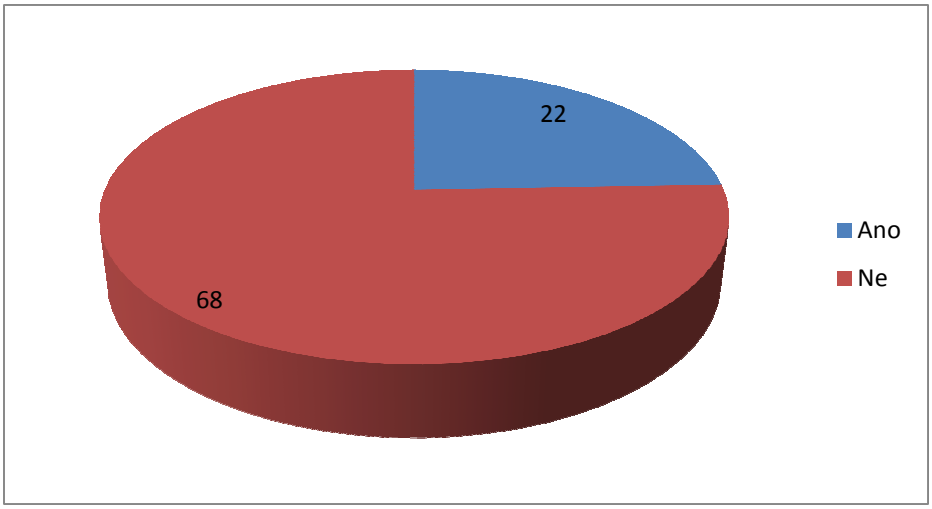


Vyhodnocení odpovědí na otázku „*Byly někdy Vaše údaje nebo údaje Vašich blízkých, které používáte prostřednictvím Internetu, nějakým způsobem zneužity?*“ je v tabulce 9 a znázorněno v grafu 9 (zodpovězeno 90krát).

Tabulka 9: Statistika zneužití údajů prostřednictvím Internetu

Odpověď	**Odpovědi**	**Podíl**
Ano	22	24,44 %
Ne	68	75,55 %

Graf 9: Statistika zneužití údajů prostřednictvím Internetu



Vyhodnocení odpovědí na otázku „*V případě, že byly údaje zneužity, jak se to stalo*? *(lze označit více možností)*“ je v tabulce 10 a znázorněno v grafu 10 (zodpovězeno 22 respondenty).

Tabulka 10: Způsoby, kterými byly údaje zneužity

Odpovědi	**Odpověď**	**Podíl**
Sociální sítě	15	68,18 %
Podvodné stránky	5	22,72 %
Podvodná transakce při nákupu/prodeji zboží	3	13,63 %
Nigerijský spam – žádost o pomoc při převodu dědictví ze vzdálené země, zaplacení „úhrady“ za převod	11	50,00 %
Jiná	10	45,45 %

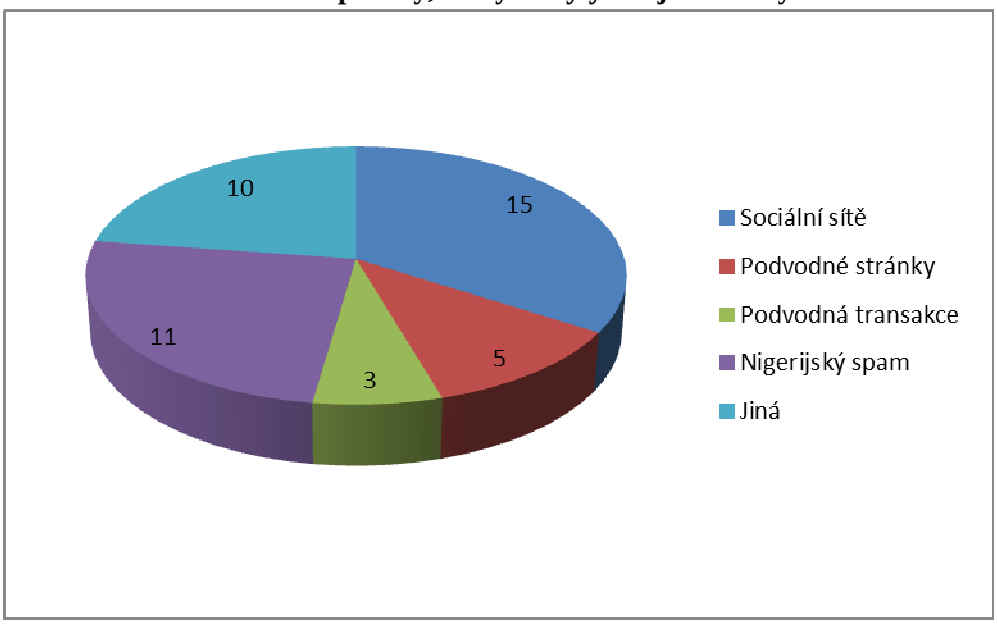
Jiné:

- Wi-Fi;
- nevyžádaná nabídka bankovních služeb od banky, která je dcerou mé hypoteční banky;
- podvodníci se dostali k mé e-mailové adrese pravděpodobně prostřednictvím procházení webových stránek, zasílali mi pak různé nabídky „výhodných“ finančních produktů;
- známý, kterému jsem půjčila notebook, „ukradl“ e-mailovou adresu i hesla, které jsem měla uložené v notebooku pro vstupy na webové stránky;
- řekl/a jsem to nevědomě sám/sama po sofistikovaných dotazech ze strany partnera/partnerky, známého (7 krát);
- měl jsem hesla pro vstupy uložené v mobilu, který mi byl ukraden, došlo k pokusu o vstup na internetové bankovnictví;
- byl mi odcizen notebook, který nebyl zaheslován a ve kterém jsem měl uložena hesla pro vstupy k e-mailovým účtům, z jednoho účtu došlo k odeslání řetězového spamu;
- fotka, kterou jsem publikoval na Facebooku, byla stažena a následně „prodána“ médiím;
- stažení mých fotografií a komentářů publikovaných na Facebooku, jejich předání mým nadřízeným v práci, měla jsem pak problémy s vysvětlováním informací vytržených z kontextu. Akce byla provedena formou „printscreenu“ jedním z mých „facebookových přátel“. Mám

podezření, kdo je pachatelem, ale bohužel jsem to nemohla prokázat a účet jsem raději deaktivovala;

- nahackerování se do mého Facebookového účtu, deaktivace účtu;
- neoprávněný vstup do Facebookového účtu, stažení fotek.

Graf 10: Způsoby, kterými byly údaje zneužity



Vyhodnocení odpovědí na otázku *„Byl někdo z* respondenty *Vašich známých jakýmkoliv způsobem šikanován prostřednictvím Internetu?(lze označit více možností)“* je v tabulce 11 a znázorněno v grafu 11 (zodpovězeno 90krát).

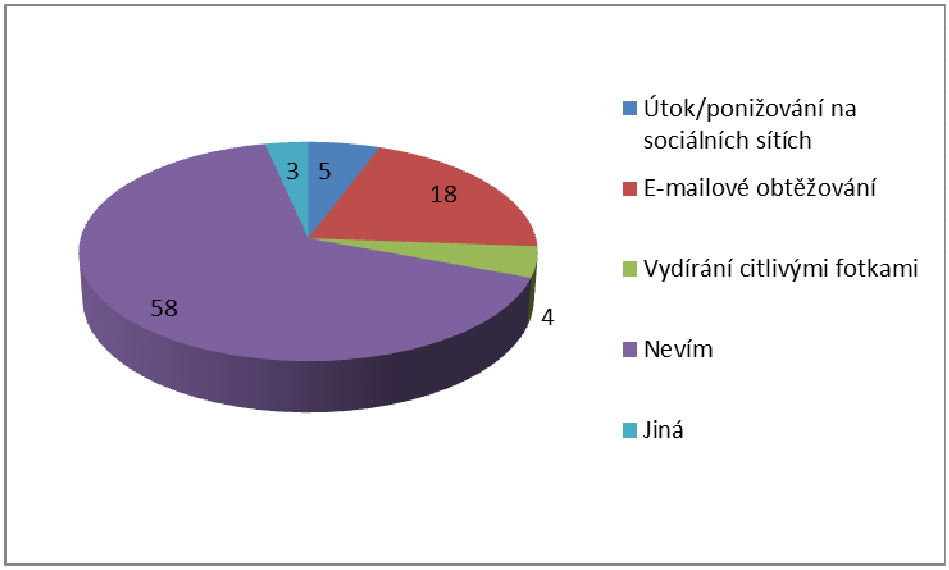
Tabulka 11: Případy šikany prostřednictvím Internetu

Odpověď	**Odpovědi**	**Podíl**
Útok/ponižování v rámci sociálních sítí	5	5,55 %
E-mailové obtěžování	18	20,00 %
Vydírání zveřejněním citlivých fotek	4	4,44 %
Nevím	58	64,44 %
Jiná	3	3,33 %

Jiné:

- Policie ČR.

Graf 11: Případy šikany prostřednictvím Internetu

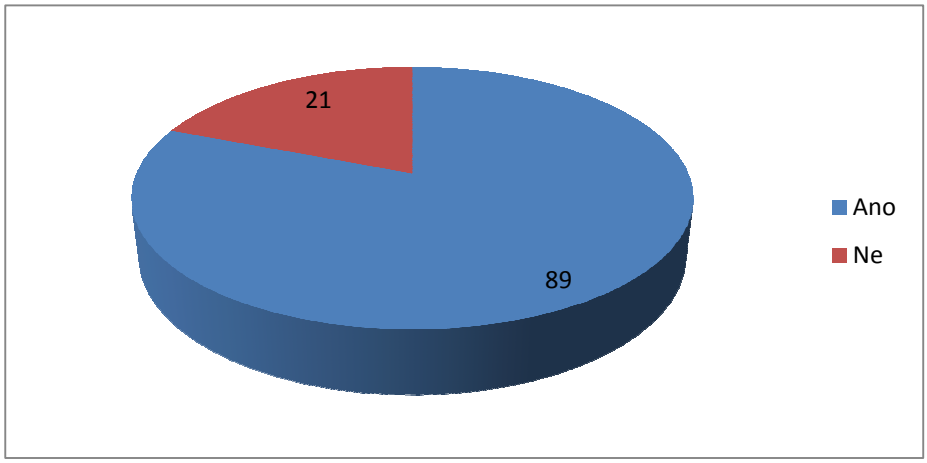


Vyhodnocení odpovědí na otázku *„Využíváte sociální sítě?“* je v tabulce 12 a znázorněno v grafu 12 (zodpovězeno 110krát).

Tabulka 12: Statistika využívání sociálních sítí

Odpověď	**Odpovědi**	**Podíl**
Ano	89	80,90 %
Ne	21	19,09 %

Graf 12: Statistika využívání sociálních sítí

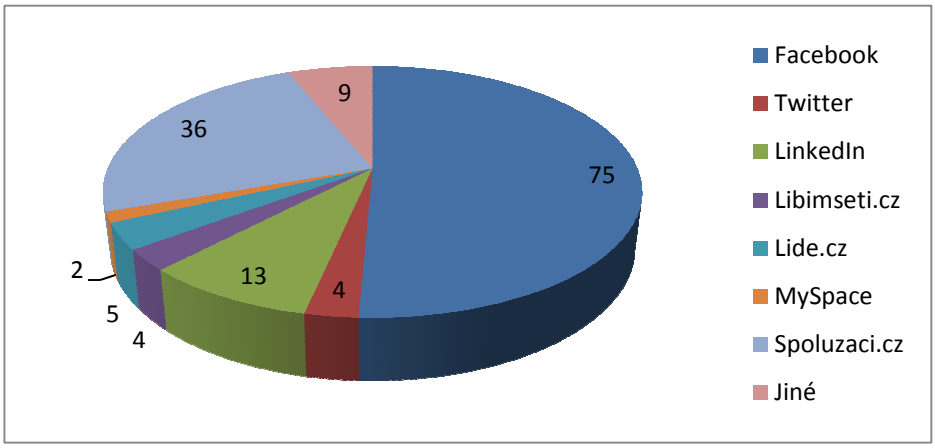


Vyhodnocení odpovědí na otázku *„Které sociální sítě využíváte? (lze označit více možností)*“, je v tabulce 13 a znázorněno v grafu 13 (zodpovězeno 89krát).

Tabulka 13: Typy využívaných sociálních sítí

Odpověď	**Odpovědi**	**Podíl**
Facebook	75	84,26 %
Twitter	4	4,49 %
LinkedIn	13	14,60 %
Libimseti.cz	4	4,49 %
Lide.cz	5	5,61 %
MySpace	2	2,24 %
Spoluzaci.cz	36	40,44 %
Jiné	9	10,11 %

Graf 13: Typy využívaných sociálních sítí

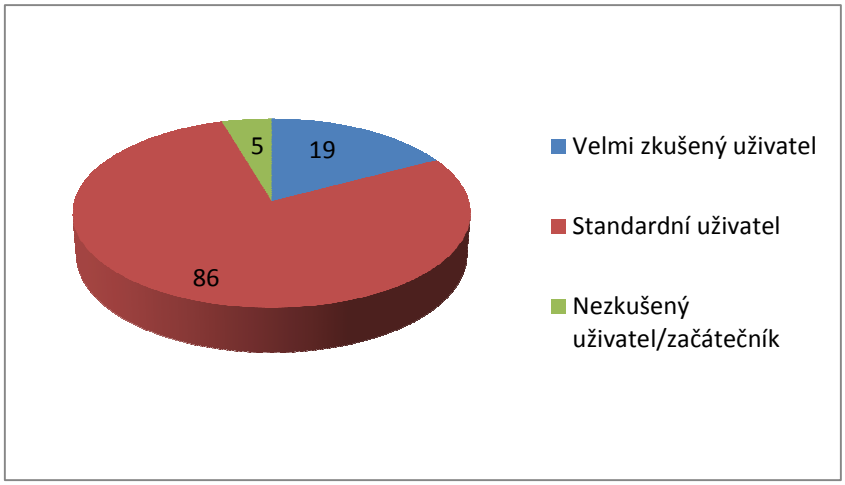


Vyhodnocení odpovědí na otázku *„Do které kategorie uživatelů byste se zařadil/a?“* je v tabulce 14 a znázorněno v grafu 14 (zodpovězeno 110krát).

Tabulka 14: Kategorie uživatelů Internetu dle jejich zkušeností

Odpověď	**Odpovědi**	**Podíl**
Velmi zkušený uživatel	19	17,27 %
Standardní uživatel	86	78,18 %
Nezkušený uživatel/začátečník	5	4,54 %

Graf 14: Kategorie uživatelů Internetu dle jejich zkušeností



BIBLIOGRAFICKÉ ÚDAJE

Jméno autora:	Danka Biľová
Obor:	Sociální a mediální komunikace
Forma studia:	Kombinované studium
Název práce:	Rizika Internetu a internetové komunikace a jejich dopad na běžného uživatele
Rok:	2013
Počet stran textu:	98
Celkový počet stran příloh:	27
Počet titulů českých použitých zdrojů:	13
Počet titulů zahraničních použitých zdrojů:	6
Počet internetových zdrojů:	73
Vedoucí práce:	doc. RNDr. Dana Procházková, DrSc.