Počítačová kriminalita a distanční delikty páchané prostřednictvím internetu

Computer Crime and Offenses Committed at a Distance Over the Internet

Bc. Petr Kolísek

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr KOLÍSEK**
Osobní číslo:	**A10425**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Počítačová kriminalita a distanční delikty páchané prostřednictvím internetu**

Zásady pro vypracování:

1. **Vypracujte rešerši aktuálních trendů počítačové kriminality.**
2. **Analyzujte problematiku počítačové kriminality.**
3. **Uveďte možné způsoby páchání distančních deliktů v oblasti počítačové kriminality.**
4. **Zpracujte statistiky počítačové kriminality a poměr distančních deliktů.**
5. **Na vzorku uživatelů zjistěte a vyhodnoťte způsoby ochrany dat před neoprávněným přístupem k počítačovým systémům a uloženým datům.**
6. **Navrhněte možné vylepšení zjištěné ochrany dat.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **CRAIG, Paul P a Ron HONICK. Softwarové pirátství bez záhad. 1. vyd. Překlad Tomáš Hlaváč. Praha: Grada, 2008, 212 s. ISBN 978-802-4717-654.**
2. **JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-802-4715-612.**
3. **ONDREJKA, Viliam. Podvody na internetu: o peníze můžete velmi rychle přijít nebo je podvodem velmi snadno získat. České Budějovice: Nová Forma, 2010, 55 s. ISBN 978-808-7313-824.**
4. **KALAMÁR, Štěpán a Josef POŽÁR. Vybrané aspekty informační bezpečnosti. Vyd. 1. Praha: Policejní akademie České republiky v Praze, 2010, 190 s. ISBN 978-807-2513-390.**
5. **JANSA, Lukáš a Petr OTEVŘEL. Softwarové právo: praktický průvodce právní problematikou v IT. Vyd. 1. Brno: Computer Press, 2011, 340 s. ISBN 978-802-5134-580.**
6. **ROGERS, Vanessa. Kyberšikana: pracovní materiály pro učitele a žáky i studenty. Vyd. 1. Překlad Ondřej Vágner. Praha: Portál, 2011, 97 s. ISBN 978-807-3679-842.**

Vedoucí diplomové práce: **Ing. Radek Šilhavý, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá problematikou aktuálních trendů počítačové kriminality se zaměřením na delikty páchané distančním způsobem. Rozborem jednotlivých trestných činů spolu se stručným vysvětlením jejich skutkových podstat a shrnutím způsobů, kterými jsou tyto trestné činy páchány. Cílem práce bylo upozornit na nejčastější způsoby páchání distančních deliktů v rámci počítačové kriminality, se zaměřením na rizikové chování uživatelů počítačové sítě Internet a uvedením možných úprav chování pro minimalizaci následků spáchaných činů.

Klíčová slova: Bezpečnost, Internet, počítačová kriminalita, trestné činy, distanční delikty

ABSTRACT

This thesis addresses the current trends in cyber crime, focusing on the offenses committed by distance means. Analysis of individual crimes, along with a brief explanation of the facts and a summary of the ways in which these crimes are committed. The aim is to highlight the most common ways of committing distance crimes within computer crimes, with a focus on risk behaviour of users of the Internet and an indication of potential behavioural adaptations to minimize the consequences of crimes committed.

Keywords: Security, Internet, computer crime, crimes, Offenses Committed at a distance

Tímto děkuji panu Ing. Radek Šilhavý, Ph.D. za velmi užitečnou metodickou pomoc, spolupráci a ochotu při zpracování mé diplomové práce. Děkuji svojí rodině a zejména manželce a dětem za toleranci a pomoc při zpracování práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně 14.5.2012 …….

podpis diplomanta

OBSAH

ÚVOD

Informace, počítače, soukromí, Internet a anonymita. Tato nesourodá skupina pojmů, které si vzájemně mohou i odporovat, se v jedné oblasti lidské společnosti prolíná způsobem, jež nemá v současné společnosti obdobu a jež v posledních desetiletích zažila obrovský rozmach. Jde o oblast informačních a komunikačních technologií.

Výsledkem tohoto vývoje je „informační“ společnost, ve které mají nejvyšší hodnotu informace a jejich okamžité a bezchybné využití. Pro možnost určitého využití informací, případně vytvoření informací pro konkrétní osoby, je však základním předpokladem jejich určitá exkluzivita a znalost pouze omezenému okruhu jedinců. Zároveň však musí být relativně veřejná z důvodu potřeby sdělit informace cílenému subjektu. Zde vzniká problém, kterým je ukládání a předávání informací. Toto se děje prostřednictvím počítačů a různých datových úložišť, zejména prostřednictvím počítačové sítě Internet. Rozsah této sítě zaručuje prakticky okamžité předání informace kdekoli na světě.

Stinnou stránkou této činnosti je však to, že čím exkluzivnější informace je, tím větší hodnotu má pro zájemce o ni a tím větší je motivace pro její získání. Zároveň díky rozsahu sítě Internet a relativní anonymitě jejich uživatelů roste počet osob, jejichž motivací k získání není samotný obsah informace, ale skutečnost, že je informace uchovávána v soukromí a nějakým způsobem zabezpečena.

Tímto se dostáváme k trestné činnosti, jež je označována pojmem „počítačová kriminalita“. Počítačová kriminalita je z pohledu trestněprávní ochrany nejmladším oborem, přesto se v posledních letech jedná o obor, který je nejdynamičtěji se rozvíjející.

Ve své diplomové práci se zabývám aktuálními trendy a způsoby páchání počítačové kriminality. Rozvedu, jaké jsou formy páchání těchto trestných činů. Zaměřím se na skutky a způsoby páchání počítačové kriminality distančním způsobem.

V praktické části zpracuji statistiky a provedu analýzu počítačové kriminality s poměrem distančních deliktů. Formou dotazníku u vzorku uživatelů zjistím a vyhodnotím, jaké jsou nejčastější způsoby ochrany dat před neoprávněným přístupem a navrhnu možné vylepšení této ochrany.

I. TEORETICKÁ ČÁST

1 INTERNET

Celosvětová počítačová síť, mezinárodní síť, síť sítí, web, informační dálnice. Počítačová síť Internet je označována různými názvy. Všechny však popisují jedinou věc a to miliony počítačů, které spolu komunikují díky vzájemně propojeným sítím a uživatelé si jejich prostřednictvím předávají různá data. Dá se říci, že Internet je běžná počítačová síť odlišující se pouze rozsahem. Díky této síti mohou prakticky ihned komunikovat uživatelé na různých místech na světě. K síti Internet se připojují nejen samotné počítače, ale i různé firemní a jiné menší sítě. Internet je síť typu WAN (původem v anglickém Wide Area Network), což je síť umožňující komunikaci na velké vzdálenosti a pracující na základě protokolu TCP/IP, který dále vysvětlím. Počítače na Internetu pracují buď jako klienti, nebo jako servery. Servery poskytují služby a klienti tyto služby využívají. Na základě žádosti klienta jsou zaslána požadovaná data. Množství a rozmanitost dat, která jsou na Internetu umístěné je nezměrné množství. Od osobních stránek, které uživatelé schválně zpřístupňují pro své zviditelnění pro úplně neznámé osoby, až po soubory obsahující tajné státní materiály. [1]

1.1 Historie Internetu ve světě

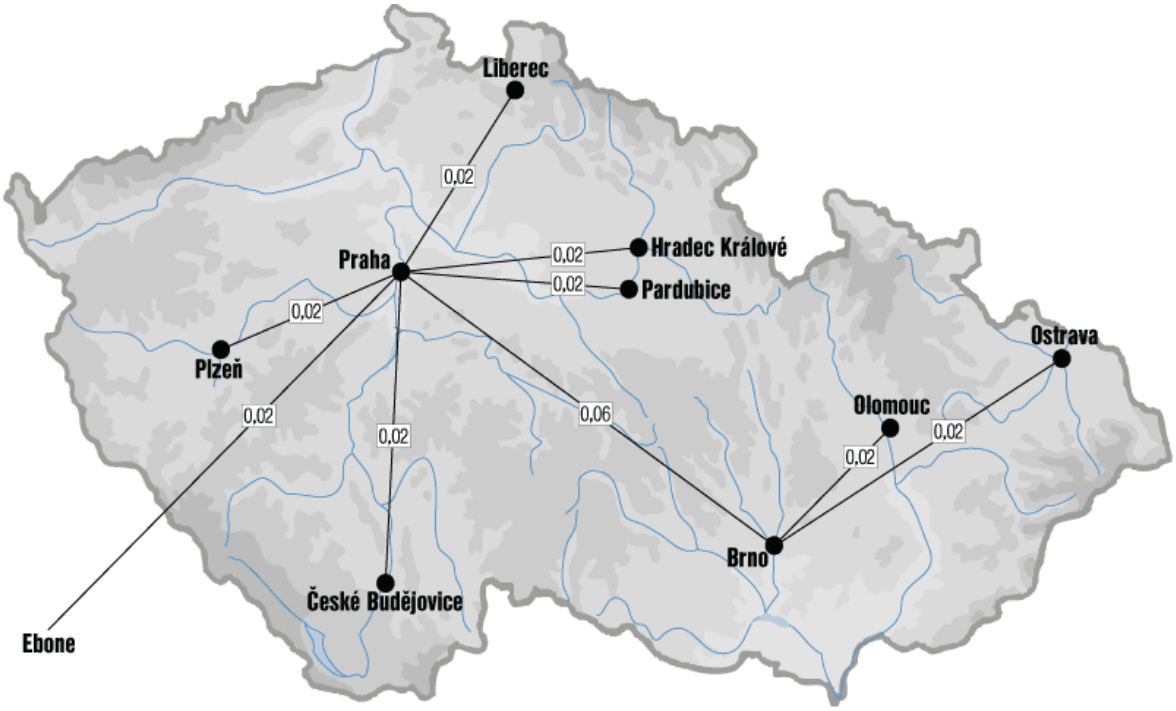
Základním kamenem Internetu zajisté byla počítačová síť ARPANET, která vznikla v roce 1968. Tato síť byla pojmenována podle agentury ARPA (Advanced Research Projects Agency), což byla agentura ministerstva obrany USA. Jedním ze základních požadavků na vývoj této sítě bylo, aby byla decentralizovaná a odolná vůči výpadkům. V průběhu let docházelo k vývoji a přerodu této sítě. Jako velice důležitá se ve vývoji Internetu ukázala léta osmdesátá. V roce 1983 došlo k oddělení vojenské části sítě ARPANET. Ve stejném roce byl zaveden systém doménových jmen DNS (Domain Name System) což znamenalo zadávání uživatelsky přívětivějších jmen místo číselného zadávání adresy IP (Internetový Protokol). Třetím důležitým bodem ze stejného roku byl začínající nástup TCP/IP (Transmission Control Protocol/Internet Protocol). Pomocí protokolu TCP/IP je možné propojit dva počítače na aplikační úrovni, což nám umožňuje zavádět síťové služby aplikační úrovně a například spouštět hypertextové stránky. Od roku 1989 dochází k rozvoji WWW (World Wide Web). Základ systému WWW stránek tvoří hypertextové dokumenty. Tyto dokumenty obsahují odkazy na další stránky, které zobrazují a umožňují další práci s těmito objekty. Přesto, že činnost sítě ARPANET byla oficiálně v roce 1990

ukončena, základní kameny již byly položeny. K poslednímu dni roku 2000 bylo k Internetu připojeno 360,985,492 lidí dne 31.12.2011 jich již bylo 2,267,233,742 z celkového počtu 6,930,055,154 obyvatel planety je to zajímavých 32.7 %. To znamená, že za 11 let se zvýšil počet připojených lidí o 528.1 %. [2]

1.2 Historie Internetu v České republice

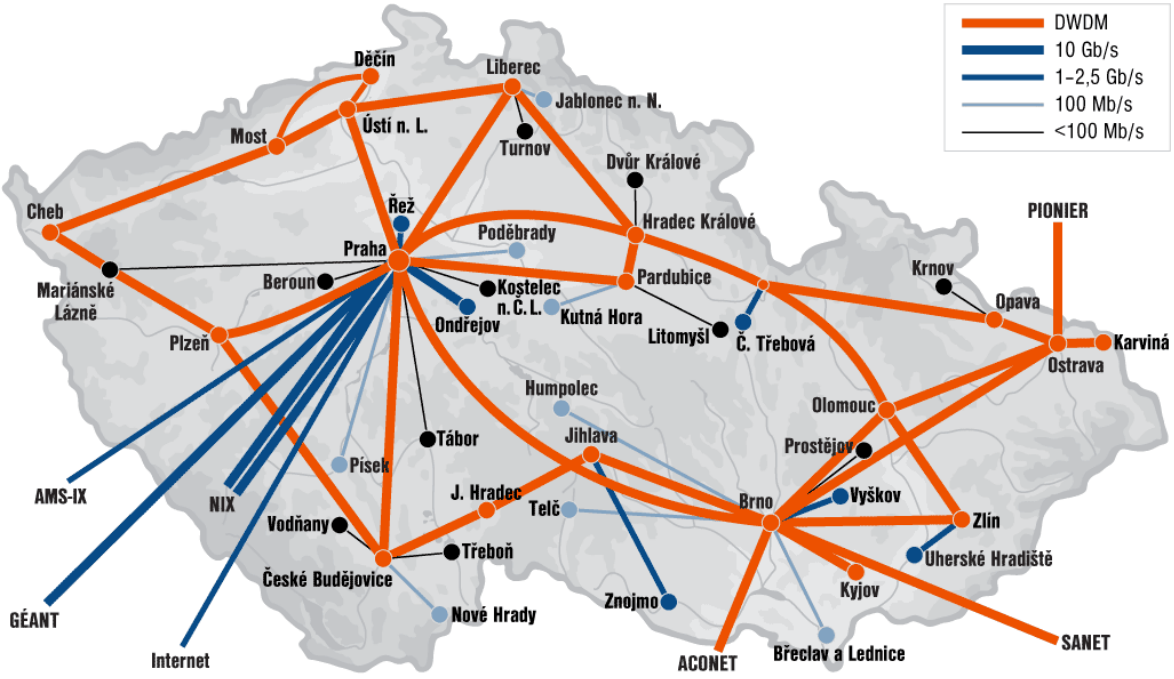
Připojení k Internetu bylo v České republice oficiálně uvedeno do provozu v roce 1992. [3]

V roce 1993 bylo páteřní spojení mezi Prahou a Brnem realizováno rychlostí 64 kb/s a připojení dalších 7 měst rychlostí 19,2 kb/s,



Obr. 1 Stav počítačové sítě Cesnet v roce 1993 [3]

V současné době je spojení více než 20 měst zajištěno rychlostí 10 Gb/s.



Obr. 2 Stav počítačové sítě Cesnet2 v roce 2010 [3]

Samostatnou překážkou počátečního rozšiřování Internetu v České republice bylo monopolní postavení jediného telekomunikačního operátora a nechuť v zavádění nových technologií. V roce 1998 je založeno sdružení NIC CZ, které nadále spravuje Českou národní doménu „.cz“. Tato doména vznikla z důvodu rozdělení Československa v roce 1993. Do roku 1995 se používala jako národní doména, doména cs, která tak následně zanikla. V roce 1996 byl spuštěn první katalogový vyhledávací server v ČR seznam.cz. Sdružení NIC.CZ je zároveň zakladatelem CSIRT.CZ. CSIRT (Computer Security Incident Response Team) je organizace, která řeší bezpečnostní incidenty vzniklé v počítačových sítích, koordinují jejich řešení a snaží se jim předcházet. [4] CSIRT.CZ je Národní CSIRT České republiky. CSIRT teamů je několik Národní CSIRT ČR byl deklarován podpisem Memoranda mezi Ministerstvem vnitra České republiky a sdružením CZ.NIC, ke kterému došlo dne 16. prosince 2010. S platností od 1. dubna 2012 nahradilo memorandum s MV ČR nové memorandum uzavřené s Národním bezpečnostním úřadem. Ten se stal gestorem problematiky kybernetické bezpečnosti v říjnu roku 2011.[5]

2 POČÍTAČOVÁ KRIMINALITA

Přesto že termín počítačová kriminalita není v české legislativě zakotven již ze skladby tohoto slovního spojení, je patrné, o co se jedná. Samotný termínem kriminalita vychází z latinského slova criminalitas, což v doslovném překladu znamená zločinnost. Kriminalita obecně a její jednotlivé druhy jsou sociálně - patologickým jevem a je pro ně příznačná jejich společenská škodlivost. [6] V rámci svojí diplomové práce se omezím na konání, jež naplňují znaky skutkové podstaty trestného činu, tedy činu, jež je uveden v trestním zákoníku.

Přidáme-li pojem počítačová, bavíme se o trestných činech, při kterých je nějakým způsobem využita výpočetní technika. Výjimkou z tohoto jsou případy, kdy je výpočetní technika chápána jako věc movitá a pachateli jde pouze o získání a následné zhodnocení materiálu, nikoli obsažených dat. V oblasti počítačové kriminality není tedy zájmem pachatele hardware, ale předmětem útoku jsou informace a veškerá data, která jsou na datových úložištích. Tato data ve velké části případů hodnotově převyšují hardwarové vybavení. Termínem počítačová kriminalita soubor nelegálních, nemorálních a neoprávněných jednání, které zahrnují změnu, případně jejich užití dat získaných prostřednictvím výpočetní techniky. [7] Počítačová kriminalita je však stále častěji chápána v širším kontextu, když k tomuto druhu kriminální činnosti jsou používány i další zařízení než klasické počítače. Pokud totiž srovnáme výkon počítačů a síťové služby z konce 20. století s mobilními zařízeními roku 2012 zjistíme, že mobilní zařízení se současným připojením jsou přes svoji minimální velikost výrazně výkonnější a rychlejší. Proto se stále častěji používá obecnější a zřejmě i přesnější termín „cybercrime“, tedy kybernetická kriminalita. [8] Definicí kybernetické kriminality existuje celá řada. Zjednodušeně se dá říci, že jí rozumíme kriminalitu páchanou v kyberprostoru, tedy ve virtuálním světě ovšem s dopadem ve světě reálném. V diplomové práci je tedy termínem počítačová kriminalita označována také kriminalita kybernetická.

Útoky vedené proti informačním technologiím mohou vyvolat obrovské škody a to nejen materiální. V případech, kdy by se jednalo o útok na prvky kritické infrastruktury, by mohl být ohrožen i život a zdraví obyvatel.

Přes to, že se počítačová kriminalita v některých oblastech podobá kriminalitě klasické, má určitá specifika. Například u trestného činu vydírání je možné spáchání jak osobním přístupem, tak prostřednictvím počítače. Rozdílem je pak absence násilí, užití zbraně,

případně jiné fyzické újmy. Počítačová kriminalita je velice rychle rozvíjejícím se odvětvím kriminálního prostředí. Stejně jak mají počítače zjednodušit a zpříjemnit práci lidem, zjednodušují a zpříjemňují práci pachatelům trestných činů. Počítačová kriminalita se pak vyznačuje možností spáchání trestného činu v tisícinách sekundy a ve většině případů je páchána znalým a technicky vybaveným pachatelem. Z uvedeného důvodu je třeba vyšetřování této kriminality pověřovat odborníky s dostatečným legislativním zajištěním. K tomuto se dá uvést, že dlouhodobým trendem je absence legislativy, když například Zákon o kybernetické bezpečnosti je ve fázi připomínkového řízení.

Obecně se počítačová kriminalita dá rozdělit na dva druhy kriminality a to na kriminalitu páchanou na počítači a kriminalitu páchanou prostřednictvím počítače. [9] V prvním případě jde o trestnou činnost pachatele, jež má zájem o data, která jsou uložena na počítači. K těmto datům se pak může dostat buď přímou krádeží datového nosiče, na kterém jsou uloženy údaje a pachatel je následně nějakým způsobem využije k prospěchu sebe, nebo další osoby, případně pro způsobení další škody poškozenému. Tato forma páchání však v sobě zahrnuje pro pachatele jednu zvlášť nepříznivou skutečnost a to je potřeba přítomnosti pachatele na místě trestného činu. V současné době, kdy je monitorování prostoru a různé formy zabezpečení objektu standardem pro stále více firem je pro pachatele páchání činu a následné zahlazení stop stále obtížnějším, ne-li nemožným úkolem. Zřejmě i právě z tohoto důvodu začíná být čím dál větší část trestných činů páchána druhým způsobem. Tímto způsobem je páchání prostřednictvím počítačů a počítačových sítí. Zde není přítomnost pachatele na místě činu nutná a žádoucí, čímž se dostáváme k druhé formě páchání, kde počítač je pouze prostředníkem a s jeho využitím dochází k páchání trestných činů. V některých případech je také tento způsob dělení nemožný, protože je počítače užito k získání dat z jiného počítače například prostřednictvím počítačových sítí.

2.1 Z Historie kybernetické kriminality

Mezi vývoj kybernetické kriminality a vývoj počítačových technologií můžeme s trochou benevolence a s určitým zpožděním dát rovnítko. Vždy když se objeví nová technologie, případně nový projekt je po určitém čase zjištěna snaha o jeho napadení a zneužití.

Různé zdroje uvádí různé etapy vývoje kybernetické kriminality.

Za rozumné se dá považovat rozdělení Viktora Porady, který hovoří o třech časových úsecích. [10]

- Období technologického procitnutí
- Období fascinace technologiemi
- Období masové konzumace technologií

Toto dělení je vhodné zejména z důvodu, že do roku 1999, tedy v prvních dvou případech, nejsou v rámci statistik Policie ČR samostatně evidovány trestné činy související s počítačovou kriminalitou. [11] V rámci literatury jsou tak do roku 2000 uváděny pouze jednotlivé skutky. Od roku 2000 jsou již například trestné činy porušování autorského práva uváděny jako konkrétní činy s počtem spáchaných případů.

2.1.1 Období technologického procitnutí (první polovina 90. let 20.století) [10]

V období předcházejícímu této době bylo spácháno a vyšetřováno minimum trestných činů. Díky nástupu PC začíná období páchání kybernetické kriminality. Protože byla kupní síla obyvatelstva nesrovnatelně menší, než v západní Evropě stává se kopírování a užívání nelegálního společensky přijatelným a relativně normálním. Nelegální užívání však v této době nebylo realizováno jako výdělečná činnost v masovém rozsahu. Spíše se jednalo o individuální uživatele. Absence legislativy a minimální zkušenosti orgánu činných v trestním řízení dávaly uživatelům téměř jistotu, že užívání software nebude postihováno.

2.1.2 Období fascinace technologiemi (druhá polovina 90. let 20. století) [10]

Toto období je charakterizováno prudkým rozvojem a nástupem počítačových technologií. Dochází k rozvoji intranetových sítí. Zájem pachatelů se přesouvá ke zneužívání citlivých údajů, které jsou nedostatečně chráněny proti zcizení. Dále dochází k centralizaci dat zpracovávaných státními institucemi. Internet je pro občany stále technologicky a cenově nedostupným. Nejrozšířenější operační systém Windows 95 nebyl dostatečně připraven na práci v síti a jeho slabiny jsou využívány pro páchání trestných činů. Citlivé údaje se stávají žádaným obchodním artiklem. Vzniká legislativa na ochranu osobních údajů. Jsou realizována instituce na ochranu osobních údajů.

2.1.3 Období masové konzumace technologií (začátek 21. století) [10]

V plném rozsahu se projevuje globalizace s rozvojem technologií včetně Internetu. Dochází k masovému rozmachu mobilních komunikací a digitálních zařízení. Díky nastaveným standardům jsou zařízení kompatibilní a data je možné přenášet mezi různými zařízeními. Rozvoj technologií však zvyšuje hrozby kybernetického terorismu a globálních teroristických útoků, které mohou vyřadit z činnosti i kritickou infrastrukturu země, čímž může docházet nově nejen k hmotným škodám, ale i škodám na životech a zdraví obyvatel. Nebezpečím je paradoxně i uživatelská přívětivost systémů, protože od uživatelů již nejsou vyžadovány potřebné znalosti a pachatelé toho mohou využít. Vytváří se nové obory průmyslové špionáže a kybernetické kriminality. Síť Internet se stává nepostradatelnou i v oblasti mezilidských vztahů, když dochází k masivnímu rozvoji sociálních sítí. Na druhou stranu však díky tomuto dochází k omezení soukromí.

2.2 Kybernetičtí zločinci

Pokud jde o historii kybernetické kriminality z hlediska světového, je třeba se vrátit k přelomu 60. a 70. let minulého století. V této době John T. Draper, známý již spíše jako Captain Crunch [8] zjistil, že píšťalka, která byla jako hračka přibalená ke každému balení cornflakes po přelepení některých dírek vydávala tón, kterým bylo možné manipulovat s telefonní ústřednou pro meziměstské hovory. Přesto, že jeho způsob byl vylepšován, byl Draper dozajista průkopníkem kybernetického zločinu.

Historicky prvního Internetového červa vytvořil Robert Tappan Morris, známý také pod zkratkou RTM. [12] V listopadu roku 1988 naprogramoval Morris-červa. Nejednalo se sice o první virus, ty byly známé již asi 30 let, ale vir RTM byl prvním, který se šířil prostřednictvím Internetu. Zajímavostí je, že RTM se původně snažil zjistit, jak je velký Internet. Naprogramoval program, ve kterém ale udělal chybu a program se začal po Internetu nekontrolovatelně šířit a počítače napadal tak dlouho, dokud úplně nevyčerpal jeho prostředky a nevyřadil jej z provozu. Uživatelům pak nezůstalo nic jiného, než odpojení od sítě a restart systému.

Že i jedním případem se dá vstoupit do historie, dokazuje Vladimír Leonidovich Levin, o kterém se v podstatě dá říci, že udělal jen jednu hackerskou operaci. [13] Tato byla ale na

svoji dobu svým rozsahem výjimečná. Levin spolu s dalšími spolupracovníky v roce 1994 získal kódy a hesla pro přístup do systému americké banky Citibank, kde postupně převedl více než 10 miliónů dolarů na několik účtů umístěných v různých státech po světě. Citibank se podařilo vyjma 400.000,- USD dostat všechny peníze zpět, avšak Levinův kousek stál banku hlavně ztrátu důvěry klientů v zabezpečení banky a následný odchod i některých hlavních zákazníků.

Jedním z největších hackerů byl rozhodně Kevin Mitnick [14]. Tento muž byl zřejmě prvním sociálním inženýrem, protože pro to, aby se dostal do počítače, využíval nejslabší článek v počítačové bezpečnosti, kterým je člověk. O Mitnickovi se traduje mnoho legend a údajně měl být schopen se nabourat do záznamů FBI a změnit záznamy o své osobě. Faktem však zůstává, že v roce 1995 byl zatčen, souzen a odsouzen za způsobení škody ve vyšší než 300.000.000 dolarů a to pře skutečnost, že mu nebylo prokázáno, že by získal nějaký prospěch. U Mitnicka bylo zajímavé, že na rozdíl od mnoha jiných ho uspokojovalo překonání bezpečnostního systému a nepotřeboval pro sebe získat nějaký prospěch.

Ze zpráv Policie ČR je zřejmé, že i v našich končinách se ojediněle také setkáváme s případy počítačové kriminality, která se svým rozsahem v něčem vymyká. Například v listopadu roku 2010 bylo zahájeno trestní stíhání proti dvacetiletému muži s bydlištěm okres Nymburk pro trestný čin Vydírání a Porušení tajemství dopravovaných zpráv. [15] Muž v rozmezí doby od září do října roku 2010 kontaktoval uživatele Internetové sociální sítě, ze kterých za pomocí vytvořených podvodných stránek vylákal hesla k emailovým schránkám, ke kterým tak získal přístup. Schránky dále prohledával za účelem získání intimních fotografií. Nalezené fotografie si uschoval a poté několik dívek prostřednictvím získaných fotografií vydíral. Požadoval po nich další intimní fotografie, video nebo intimní kontakt prostřednictvím kamer. Dívkám vyhrožoval zveřejněním fotografií. V některých případech získal požadované materiály. Počet poškozených uživatelů emailových schránek byl v řádu několika tisíců.

Stálé rozšiřování páchání kybernetické kriminality v České republice není nic neočekávaného, když stejně jak na celém světě dochází i zde k razantnímu růstu osob, připojených k Internetu. Ke dni 31.12.2011 bylo z celkového počtu 10,190,213 obyvatel České republiky bylo k Internetu připojeno 7,220,732 lidí, což je celkem 70.9 % [2], přičemž v roce 2009 to bylo pouze 9,7 %[16]. Tento trend je zajímavý nejen pro poskytovatele Internetového připojení a všechny podnikatele s Internetem spjaté, ale zejména pro pachatele trestných činů z ekonomického hlediska. Také možnost oslovení

takového počtu osob je prakticky nemožné a jakékoli osvěta tímto směrem je náročná. Existuje množství stránek, které se snaží uživatele Internetu varovat před riziky. Přes maximální snahu však nelze oslovit všechny uživatele a nikdy nebude možné upozornit na všechna možná rizika, protože pachatelé protiprávních činů budou mít vždy výhodu prvního kroku ve výběru zbraní a způsobů útoků.

2.3 Způsoby napadení počítače

Tato oblast se dá rozdělit na dvě kategorie. První jsou útoky silou. Zde se útočník snaží zjistit data, poškodit systém, nebo získat jinou výhodu útokem, jehož hlavní stránkou je využití množstevní převahy nad obětí. Typickým prvkem je určitá nezávislost prováděného útoku, když není vyžadována přílišní interakce s útočníkem. Útočník spustí program a může jej nechat pracovat samostatně. Patří sem Brute force attack, Denial of service, Dictionary attack, Hoax, Počítačové viry Worm (červ). Druhou kategorií jsou útoky logické. Útočník se snaží využít informace, které pro poškozeného nejsou známé, nebo je poškozený nepovažuje za důležité. Tyto útoky jsou více orientované na útočníka a je nutná určitá znalost systému a prováděného útoku. Při zjištění určité informace je potřeba zásah útočníka s rozhodnutím jak s informací naložit. Do těchto typů útoku patří Backdoor, Keylogger, Pharming, Phishing, Sniffer, Spoofing, Trojští koně, Sociální inženýrství.

2.3.1 Brute force attack (útok hrubou silou)

Jde o způsob útoku, při kterém program zjišťuje veškeré možné kombinace do doby, zjištění skutečného hesla. Ze způsobu útoku je jasné, že heslo bude dříve, nebo později prolomeno. Při dostatečně dlouhém hesle je však také jisté, že heslo může být zjištěno až za několik století. [17]

2.3.2 Denial of service (odmítnutí služby)

Jde o takový útok na Internetové stránky, který zabrání ostatním uživatelům v přístupu na tyto stránky. Tento typ útoku i mezi laickou veřejnost rozšířila skupina Anonymous, která na začátku roku 2012 tímto způsobem zaútočila na stránky několika institucí (mimo jiné FBI, RIAA, v České republice ODS). [18]

2.3.3 Dictionary attack (slovníkový útok)

Útočník pomocí programu testuje heslo na všechna slova, která jsou ve slovníku. Tento typ útoku je možné použít jedině tam, kde je jistota, že uživatel použil slovo, případně jejich kombinaci, která se může ve slovníku nacházet. Při dodržení zásady při používání hesla použít kombinaci velkých, malých písmen, čísel a speciálních znaků je tento druh útoku zcela nepoužitelný. [8]

2.3.4 Hoax (falešné zprávy)

Tyto zprávy by se daly s trochou fantazie podřadit pod termín červ. Nejsou sice automatické, ale využívají chyb a slabin uživatelů. Hoax je falešná zpráva, jež se tváří jako pravdivá. Často je zpráva kombinací skutečnosti se lží a může být doplněna o falešné vyjádření nějaké věrohodné osoby. V každém případě je ale zpráva strukturovaná tak, aby ji adresát poslal co největšímu okruhu dalších uživatelů. [19]

2.3.5 Počítačové viry

Jedná se o počítačové programy, které tajně pracují v počítači a dále se šíří. Převážná část počítačových virů je určena ke škodlivé činnosti (mazání dat, šifrování disku bez možnosti přečtení zašifrovaných dat, obtěžování uživatele, zpomalování systému). Viry se šíří na další zařízení, bez zásahu útočníka. [20]

2.3.6 Worm (červ)

Počítačový virus, jehož primárním cílem je šířit se. Využívá chyb systému, nebo uživatelů, napadá systém a následně se jeho prostřednictvím dál šíří. Při optimální situaci je schopen se klonovat tak dlouho, až síť zahltí. Prvním červem byl v předchozí kapitole uvedený Morris-červ. [21]

2.3.7 Backdoor (zadní vrátka)

Útočník získává přístup k počítači tím způsobem, že do počítače vloží program, případně využije chyby v programu, což mu umožní přístup k počítačovému systému. Program pracuje tajně, bez vědomí uživatele. [17]

2.3.8 Keylogger (záznam stisknutých kláves)

Speciální software, nebo zařízení, které zaznamenává a případně odesílá informace o stisku kláves. Jsou dva druhy. Hardwarový, zde se jedná o zařízení, které je fyzicky připojené

k počítači a softwarový, což je pouze program. U hardwarového je problém potřeby fyzické přítomnosti na místě při instalaci, u softwarového je zase nebezpečím možné zjištění bezpečnostním programem. Největší překážkou ve využití tohoto útoku je právě instalace a zajištění funkce keyloggeru. [22]

2.3.9 Pharming (farmaření)

Jde o útok, kde se předpokládá vyšší aktivita útočníka. Útočník musí buď získat přístup k serveru, na kterém dochází k překladu doménového jména na IP adresu. Tyto servery jsou však obecně považovány za jedny z nejlépe chráněných zařízení. Nebo může jednodušším způsobem získat přístup k počítači oběti, kde stačí upravit URL s přidělenými IP adresami. Při požadavku na přihlášení se na stránku dochází k přesměrování na stránku s podvrženým obsahem, zpravidla identického obsahu jako stránky originální. Pokud poškozený zadá přístupové jméno a heslo, dochází k uložení, nebo odeslání těchto informací útočníkovi. [22]

2.3.10 Phishing (rybaření)

Doslovný překlad tohoto slova vystihuje jeho účel. Pachatel se snaží „nahazovat“ návnady a čeká, zda se někdo chytne. Nejčastější forma tohoto útoku probíhá tak, že pachatel rozešle možným obětem emailovou zprávu, kde je například upozorní na to, že byl napaden server společnosti vydávající bankovní karty. Upozorní uživatele na nebezpečí zneužití bankovní karty a účtu a vyzve ho k zadání všech údajů z účtu a platební karty včetně čísla PIN a dále ke hesla do banky. Často je zpráva doplněna o informaci o tom, že ke změně hesla dojde až za nějakou dobu, aby poškozenému nebylo divné, že číslo ještě nebylo změněno. Pachatel pak může tyto údaje zneužít například při různých platbách a převodech. V dobách, kdy tyto útoky začínali se útočníci příliš nesnažili o profesionální výraz zprávy. Zprávy obsahovaly chyby, pokud byla jako šablona použita zahraniční verze útoku, byl překlad strojový a nepřesný. V současné době je velké množství těchto chybných zpráv zachyceno filtry v emailových schránkách a útočníci se snaží, aby překlady byly jazykově správné. [23]

2.3.11 Sniffer (čmuchač)

Program na odposlech Internetové komunikace. Program využívá skutečnosti, že většina komunikace na Internetu je nešifrovaná a tuto komunikaci zobrazuje útočníkovi. Ve své podstatě jde o odposlech, který umožní útočníkovi zjistit veškerá přenesená data.

Problémem je že i v rámci přenosů které nejsou šifrované dochází k přenosu přístupových jmen a hesel. V případě, že oběť používá stejná hesla pro různé stránky získává útočník přístup i ke stránkám jejichž data jsou při přenosu šifrované. [24]

2.3.12 Spoofing (mystifikace)

U tohoto útoku útočník pro potencionální oběť předstírá, že je někým jiným. Nejčastěji osobou, se kterou se poškozený zná, ale nejsou v přímém kontaktu, případně jako zástupce pro oběť důvěryhodné instituce. Spoofing může být páchán například prostřednictvím sms (použití sms brány), nebo e-mailu (podvržení hlavičky emailu). [25]

2.3.13 Trojští koně

Tak jako dřevěná verze zařízení se stejným názvem má i počítačová verze za úkol propašovat za hradbu uživatelovi obrany nechtěnou „návštěvu“. Ve většině případů použití trojského koně jde o program ke škodlivé činnosti. Rozdíl mezi trojským koněm a počítačovým virem je, že trojský kůň sám nedokáže vytvářet své kopie. [20]

2.3.14 Útoky za využití sociálního inženýrství

Nejedná se o typický útok, který by se dal přiřadit k již uvedeným, ale jde o metodu kybernetických útoků. Útok je zde již směřován na konkrétního poškozeného a pravděpodobnost úspěchu je tak pro pachatele vyšší. Pachatel se snaží získat co nejvíce informací o oběti. Správně položenými otázkami ve správný čas také získává informace, které poškozený nemusí považovat za důležité. Následným využitím těchto informací se může například vydávat za člověka ze stejné firmy s tím, že si zrovna někam založil nějaký dokument a nutně jej potřebuje. Osoba realizující útok s využitím sociálního inženýrství musí být zejména výmluvná a pohotově reagovat, protože nikdy přesně neví jaké požadavky budou druhou stranou žádány. [14]

3 TRESTNÉ ČINY

Trestným činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně (§ 13 odst. 1 tr.z). [26]

K trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti (§ 13 odst. 2 tr.z). [26]

Trestný čin musí mít všechny znaky uvedené v trestním zákoně, což znamená, že jeho obsah musí odpovídat skutku popsanému ve zvláštní části trestního zákona. Jde o formální znak trestného činu.

Jednání právním řádem dovolená nemohou být trestným činem a to ani v případě, že by po formální stránce naplňovaly znaky skutkové podstaty trestného činu. Nemůže být trestným činem záznam telekomunikačního provozu, k němuž dochází v rámci příkazu vydaného soudem. Znakem tr. činu je tedy také protiprávnost.

3.1 Působnost trestního zákoníku

Místní působnost - vymezuje území, na kterém působí účinky trestního zákona. Podle zákona České republiky se posuzuje trestnost činu, který byl spáchán na jejím území. [26] Není možné posuzovat trestný čin podle zákona účinného na území České republiky, pokud byl skutek spáchán na území státu s odlišnou suverenitou. Není však důležité, zda je pachatelem občan České republiky, nebo cizí státní příslušník.

Podle této zásady je možno postihnout i tzv. distanční delikty (§ 4 odst. 2), tedy jednání, kterého se pachatel zcela nebo zčásti dopustí na území České republiky i když k následku byť i jen z části došlo, nebo mělo dojít v cizině, případně pokud se pachatel dopustil jednání v cizině, ale zde porušil, nebo ohrozil zájem chráněný trestním zákonem nebo měl-li tu alespoň zčásti takový následek nastat. [26]

Z uvedeného je zřejmé, že distanční delikty jsou delikty, při kterých není místo spáchání skutku totožné s místem, kde došlo k následku. Toto hledisko však má jedno zásadní úskalí při vyšetřování trestných činů a tím je možnost přítomnosti mezinárodního prvku. V případě spáchání činu v České republice, pokud použije znalý pachatel jako mezičlánek server, který je v zahraničí zkomplikuje tak šetření tohoto činu. V rámci vyspělých států je spolupráce.

Zásady, uplatňující se u pachatele distančního deliktu, se vztahují i na osobu účastníka (§ 4 odst. 3 tr. zák.). [26] Tato zásada se použije i v případě, že čin, jehož se pachatel dopustil v cizině není trestný (§ 4 odst. 4 tr. zák.). [26]

Typickým příkladem může být distribuce nelegálně upravených počítačových programů. V některých státech nemusí být tento čin postihován. Osoba, která bude u počítače v České republice a pomůže například radou jakým způsobem odstranit ochranu proti kopírování se dopouští trestného činu, přes skutečnost, že pachatel není v cizím státě trestně odpovědný.

3.2 Skutková podstata trestného činu

Skutková podstata trestného činu je jedním z formálních znaků trestného činu. Jde o právní formu vyjadřující typové znaky trestného činu uvedené v trestním zákoně. Tutéž myšlenku můžeme vyjádřit formulací, že skutková podstata trestného činu je souhrnem objektivních a subjektivních znaků, které určují jednotlivé druhy trestných činů a odlišují je navzájem. [27] Skutkové podstaty trestného činu se dělí na základní, kvalifikované a privilegované.

Základní skutkové podstaty se zpravidla uvádí v prvých odstavcích konkrétních ustanovení trestných činů.

Kvalifikované skutkové podstaty popisují okolnosti, při jejichž splnění hrozí pachateli přísnější postih z důvodu zvýšení stupně nebezpečnosti činu pro společnost. Jsou uváděny v dalších odstavcích konkrétních paragrafů. Jedná se například o případy, kdy jedná pachatel jako člen organizované skupiny, nebo činem způsobí závažnější následek.

Privilegované skutkové podstaty uvádí okolnosti spáchání trestného činu, jež zdůvodňují uložení nižšího trestu, než v případě základní skutkové podstaty. Jedná se například o vraždu novorozeného dítěte matkou, kde nehrozí trest jako za trestný čin vraždy, ale protože se předpokládá, že matka skutek spáchá v rozrušení způsobeném porodem je hrozící trest mírnější. [26]

Obligatorními (povinnými) znaky skutkové podstaty trestného činu jsou objekt, objektivní stránka, subjekt a subjektivní stránka.

Objektem trestného činu jsou společenské vztahy, zájmy a hodnoty společnosti, které jsou chráněné trestním zákonem.

Objektivní stránka je stránka trestného činu, která se projevuje navenek a kterou vnímáme svými smysly. Objektivní stránka zahrnuje:

- Jednání – jde o projev vůle pachatele navenek. Může jít o konání, ale i opomenutí (zdržení se konání)
- Následek – je jím porušení nebo ohrožení hodnot, které jsou objektem trestného činu.
- Příčinnou souvislost – pachatel musí jednáním způsobit následek, aby byl za skutek odpovědný.

Subjektem trestného činu je pachatel, který proto, aby byl trestně odpovědný, musí být v době spáchání činu starší 15 let a být příčetný, tedy musí být schopen ovládat své jednání a rozpoznat jeho protiprávnost. S platností od 1.1.2012 došlo ke změně zákonů a pachatelem tak může být nejen fyzická, ale i právnická osoba. V případě, že se hovoří o skutečnosti, že pachatelem může být kdokoliv, je tím myšlena osoba trestně odpovědná dle tohoto odstavce.

Subjektivní stránkou je zavinění.

3.3 Vydírání (§ 175) [27]

Objektem trestní ochrany je svobodné rozhodování člověka v obecné rovině.

Objektivní stránka záleží v tom, že poškozený má něco konat, trpět, nebo opominout a děje se tak násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy.

Pachatelem může být kdokoli.

Po subjektivní stránce je třeba zavinění úmyslného.

Poškozený je tak v případě vydírání donucen k jednání, které by v případě rozhodování výhradně dle jeho vůle neudělal. Pro to, zda jde o vydírání, není podstatné, zda se poškozený choval dle požadavku pachatele, ale zda došlo k nucení. Zároveň není podstatné, zda je jednání v zájmu poškozeného. Pachatel například sdělí poškozenému, že mu zapálí dům, pokud neukončí svoje podnikání a neuhradí dluhy na tomtéž domě, který má díky podnikání v zástavě. Přes skutečnost, že poškozený může díky nevhodnému způsobu podnikání o dům opravdu přijít a podnikání tak ukončit jedná se o vydírání. Nejde však o vydírání, pokud pachatel poškozenému sdělí, že se bude chovat dle zákona. V případě, že pachatel sdělí poškozenému, že pokud neodstraní jeho hudební dílo ze svých stránek, podá na něj trestní oznámení nejedná s o vydírání. O vydírání by se jednalo v případě, že by mu vyhrožoval například finančním postihem, ke kterému není oprávněn.

Pohrůžkou těžké újmy může být nespočet případů. Může se jednat o majetkovou, ale i nemajetkovou škodu (rozvrat rodiny, propuštění z práce, veřejné opovržení). Intenzitu hrozící újmy bude třeba zkoumat vůči konkrétnímu poškozenému a případu.

3.4 Porušení tajemství dopravovaných zpráv (§ 182) [27]

Objektem trestného činu je tajemství dopravovaných zpráv. Toto tajemství je vymezeno v čl. 13 Ústavního zákona č. 2/1993 Sb., Listiny základních práv a svobod, kde je uvedeno, že nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

Objektivní stránka trestného činu dle §182 odst. 1 spočívá v úmyslném porušení tajemství

- uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením

- datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá

- neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data.

Porušením tajemství je myšleno zjištění informace přenášené vymezeným způsobem, která měla mimo odesílatele a adresáta zůstat dalším osobám utajena. Není nutné, aby byl obsah sdělen další osobě. Není zde rozlišováno, jaká je skutečná hodnota zjištěné informace. Například se může jednat i o propagační materiály jinak veřejně dostupné.

Objektivní stránka trestného činu dle §182 odst. 2 spočívá v tom, že pachatel

- prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu

- nebo takového tajemství využije

V tomto případě se předpokládá již určitá hodnota utajované informace a to ať již pro poškozeného, pachatele, nebo třetí osobu a je vyžadováno užití této informace.

Subjektem, pachatelem může být kdokoli.

Po subjektivní stránce je třeba zavinění úmyslného.

3.5 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183) [27]

Objektem trestného činu je stejně jako v případě ustanovení § 182 listovní tajemství a tajemství jiných písemností a záznamů avšak v tomto případě jde o informace uchovávané v soukromí. Chráněno je tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí před neoprávněným přístupem.

Objektivní stránka spočívá v tom, že pachatel neoprávněným zveřejněním, zpřístupněním třetí osobě nebo jiným způsobem použití, poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného.

Subjektem, pachatelem může být kdokoli.

Po subjektivní stránce jde o trestný čin úmyslný.

Ani v tomto případě není důležité, jaká je hodnota uchovávané informace, je již však vyžadováno, aby se o informaci dozvěděla další osoba. Rozdíl mezi zpřístupněním a zveřejněním spočívá v tom, že u zveřejnění se předpokládá vyšší aktivita pachatele směrem k poskytnutí informace většímu počtu osob.

3.6 Sexuální nátlak (§ 186) [27]

Objektem trestní ochrany je svobodné rozhodování člověka v sexuální oblasti.

Objektivní stránka první základní skutkové podstaty se skládá ze dvou jednání. Pachatel musí nutit poškozeného k pohlavnímu sebeukájení, k obnažování nebo jinému srovnatelnému chování a zároveň tak musí činit buď násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy, případně zneužívat jeho bezbrannosti.

Objektivní stránka druhé základní skutkové podstaty spočívá v tom, že pachatel k pohlavnímu styku, k pohlavnímu sebeukájení, k obnažování nebo jinému srovnatelnému chování, přiměje poškozeného tak, že zneužije jeho závislosti nebo svého postavení a z něho vyplývající důvěryhodnosti nebo vlivu.

Subjektem, pachatelem může být kdokoli.

Po subjektivní stránce je třeba zavinění úmyslného.

Pachatel a oběť nemusí být při páchání činu ve fyzickém kontaktu. Právě proto k uvedenému jednání dochází často v rámci on-line komunikace, kdy pachatel využije již získané informace k přesvědčení poškozeného k chování zaměřeném na sexuální vzrušení pachatele. Právě toto chování odlišuje trestný čin Sexuální nátlak od trestného činu Vydírání. Jde tedy pouze o zájem pachatele, zda je cílem pachatele sexuální zneužití oběti, nebo nucení k jinému jednání. Obnažováním, nebo jiným srovnatelným chováním je zde myšleno například svlékání a hlasové sexuální projevy. V případě uvedené druhé základní skutkové podstaty musí být poškozený na pachatele nějakým způsobem odkázán a pachatel musí mít psychologickou převahu a poškozený se tak nemůže zcela svobodně rozhodovat. Pachatelem může být například rodič, učitel, nebo opatrovník.

3.7 Šíření pornografie (§ 191) [27]

Objektem trestného činu šíření pornografie je zájem na ochraně mravnosti dospělých vzhledem k vyjmenované pornografii (odstavec 1) a mravní výchovy dětí před obtěžováním obecnou pornografií (odstavec 2).

Objektivní stránka spočívá v jednání pachatele, který:

- vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří pornografické dílo, ve kterém je zachyceno násilí či neúcta k člověku, případně pohlavní styk se zvířetem,

- nabízí, přenechává nebo zpřístupňuje pornografické dílo dítěti v případě odst. 2 písm. a),

- na místě, které je dětem přístupně, vystavuje nebo jinak zpřístupňuje pornografické dílo u odst. 2 písm. b).

Subjektem, pachatelem může být kdokoli.

Po subjektivní stránce jde o trestný čin úmyslný.

Termín pornografie není v trestním zákoně definován. Obecně se však za pornografii označují díla, jejichž cílem je vyvolání, nebo zvýšení sexuálního vzrušení. Za pornografii se ale nepovažují díla umělecká, výchovná, vědecká a obdobná, která slouží k jiným

účelům. Násilí a neúcta k člověku mohou mít různé formy, vždy se ale bude jednat o určitou formu ponížení objeti. Dítětem je myšlena osoba mladší 18 let.

3.8 Výroba a jiné nakládání s dětskou pornografií (§ 192) [27]

Objektem trestného činu je zájem společnosti na ochraně dětí a to jak jejich vývoje, tak ochraně před sexuálním zneužíváním.

Objektivní stránka spočívá v tom, že pachatel:

- přechovává dětskou pornografii (dle odst. 1),

- vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří dětskou pornografii (dle odst. 2 alinea 1),

- kořistí z dětského pornografického díla (dle odst. 2 alinea 2).

Subjektem, pachatelem může být kdokoli.

Jedná se o úmyslný trestný čin.

K postihu držení a vyrábění dětské pornografie zavazuje Českou republiku rámcové rozhodnutí Rady EU č. 2004/68/SVV ze dne 22. 12. 2003, o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, které v čl. 3 odst. 1 nařizuje členským státům přijmout opatření proti nakládání s dětskou pornografií, včetně jejího držení.

Přechováváním se rozumí jakékoli držení a to nejen v místě bydliště pachatele, ale i například v práci, uložené v bance, u kamaráda. Dítětem se rozumí osoba mladší 18 let. Dle aktuálního znění tohoto ustanovení je trestné nakládání nejen s pornografií, kde je zobrazeno dítě, ale také osoba, jež se jeví být dítětem. Z uvedeného tedy plyne, že se nemusí jednat o dítě žijící a nemusí se jednat ani o reálnou osobu. Stačí, když zobrazení bude dostatečně realistické. Formulace tohoto ustanovení není úplně přesná, protože rozhodnutí o tom, zda se osoba jeví býti dítětem, bude na subjektivním pocitu pachatele. V některých případech se tak bude jednat o určení obtížné a soudy zde mohou rozhodovat v pochybnostech ve prospěch pachatele. Zákon zde tak primárně nechrání děti, ale zájem společnosti na nastavených morálních hodnotách.

3.9 Podvod (§ 209) [27]

Objektem trestného činu podvodu je majetek cizí osoby.

Objektivní stránka trestného činu podvod spočívá v tom, že pachatel jiného uvede v omyl, jeho omylu využije nebo mu zamlčí podstatné skutečnosti, v důsledku čehož tato osoba provede operaci s majetkem, přičemž vznikne škoda nikoli nepatrná na cizím majetku a zároveň dojde k obohacení pachatele nebo jiné osoby.

Subjektem, pachatelem může být kdokoliv.

Po subjektivní stránce jde o trestný čin úmyslný.

Omylem je rozpor mezi představou a skutečností. Není potřeba, aby se pachatel alespoň přičinil k navození omylu. Stačí, aby jej využil. Je však vyžadováno, aby pachatel byl informován o skutečném stavu věci již v době, kdy se poškozený rozhoduje o dalším jednání (například uzavření smlouvy). Není také nutné, aby mylná představa byla jediným argumentem. Postačí, že v případě znalosti skutečného stavu věci by toto rozhodnutí nebylo poškozeným učiněno. Škodou nepatrnou se rozumí škoda dosahující částky nejméně 5 000 Kč § 138 odstavec 1 TZ. Obohacenou osobou může být i osoba neustanovená.

3.10 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230) [28]

Objektem tohoto trestného činu je zájem na ochraně dat uložených na nosiči informací, nebo v počítačovém systému a ochrana počítačových systémů, případně jejich částí před neoprávněným přístupem.

Objektivní stránka je vymezena ve dvou samostatných základních skutkových podstatách a spočívá v tom, že pachatel:

- překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, ustanovení § 230 odst. 1,
- nebo dle ustanovení § 230 odst. 2 získá přístup k počítačovému systému nebo k nosiči informací a zároveň splní nejméně jednu z dalších podmínek, tedy že

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

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

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

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat.

Subjektem, pachatelem může být kdokoli.

Po subjektivní stránce jde o trestný čin úmyslný.

Překonáním bezpečnostního opatření je myšleno překonání jakékoli ochrany před neoprávněným přístupem. Není podstatné, jak kvalitní ochrana proti přístupu je. Počítačovým systémem je nejméně jedno zařízení, které automatickým způsobem provádí zpracování dat. Nejedná se tedy o spáchání trestného činu dle tohoto ustanovení, pokud pachatel získá přístup k emailové schránce poškozeného. V rámci první skutkové podstaty také není vyžadováno, aby pachatel data využil, ale postačí překonání hesla. Nosičem informací je myšleno jakékoli elektronické zařízení, jež umožňuje záznam dat.

3.11 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231) [28]

Objektem trestného činu je zájem na ochraně před určitou přípravou spáchání trestných činů porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1,2, konkrétně opatřením a přechováváním zařízení, nástrojů a prostředků umožňující neoprávněný přístup do sítě elektronických komunikací, k počítačovému systému nebo k jeho části.

Objektivní stránka spočívá v tom, že pachatel vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává:

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

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

Pachatelem může být kdokoli.

Z hlediska subjektivní stránky je třeba úmyslného zavinění.

Uvedené jednání je svým způsobem pouze speciální příprava pro spáchání vyjmenovaných trestných činů, která by jinak trestná nebyla. Přístupové zařízení je jakýkoli hardware, případně počítačový program, pomocí něhož lze získat neoprávněný přístup, přičemž postačí opatřování či přechovávám pouze součásti takového zařízení. Postupem je určitý návod, nebo metodika jak přístup získat. Počítačovým heslem, nebo kódem je myšlen určitý pevně stanovený sled znaků pro přístup k počítačovému systému, nebo jeho části. Termínem jiný prostředek jsou ošetřeny přístupové metody v zákoně taxativně nevymezené a to i v budoucnu realizované. Sítí elektronických komunikací se rozumí přenosové systémy umožňující přenos signálů. Nemusí jít o veřejnou komunikační síť, jako je Internet.

3.12 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270) [28]

Objektem tohoto trestného činu je zájem na ochraně práva autorského a práv souvisejících.

Objektivní stránka záleží v jednání pachatele, který neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.

Pachatelem může být kdokoli.

Subjektivní stránka vyžaduje úmysl.

Ustanovení tohoto trestného činu je specifické, protože jde o trestněprávní normou s blanketní dispozicí. Znamená to, že odkazuje na právní pojmy upravené normami jiného právního odvětví. V tomto případě se jedná o zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), kde je v § 2 odst. 1 definováno autorské dílo jako dílo literární a jiné dílo umělecké a dílo

vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam.

Za neoprávněný zásah do práva autorského není považováno takzvané volné užití díla, jež je uvedeno v § 30 zákona č. 121/2000 Sb., kde v § 30 odstavci 1 je uvedeno, že „za užití díla podle tohoto zákona se nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak“ [29] a dle odstavce 2 tak „do práva autorského nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla“. [29] Toto užití má však vzhledem k počítačům dvě, podstatné omezení. Jedním je počítačový program a elektronická databáze, který je uveden v odstavci 3 § 30, na který se volné užití nevztahuje a druhým je obcházení obchází účinné technických prostředků ochrany práv. Obecně se dá říci, že pro svoji potřebu je možné díla chráněná autorským zákonem držet a kopírovat, pokud se nejedná o počítačový program, nebo databázi, pokud nejsou data zabezpečena proti rozmnožování a nejedná se o záznam audiovizuálního díla při reprodukci.

Škodou nepatrnou se rozumí škoda dosahující částky nejméně 5 000 Kč § 138 odstavec 1 TZ.

3.13 Nebezpečné pronásledování (§ 354) [28]

Objektem tohoto trestného činu je zájem na ochraně klidného mezilidského soužití, chráněného před rušením, spočívajícím v obtěžování a znepříjemňování života oběti nad rámec únosných mezí.

Objektivní stránka spočívá v jednání pachatele, který jiného dlouhodobě pronásleduje tím, že:

a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,

b) vyhledává jeho osobní blízkost nebo jej sleduje,

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.

Zároveň platí, že toto jednání je způsobilé vzbudit v poškozeném důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých.

Subjektem, pachatelem může být kdokoli.

Po subjektivní stránce jde o trestný čin úmyslný.

Tímto ustanovením je postihováno zlovolné pronásledování obecně nazývané stalking. Za stalking je považováno opakované a dlouhodobé obtěžování jiné osoby, která toto pociťuje jako příkoří. Forma stalkingu není specifikována, tudíž může jít o přímý či nepřímý fyzický kontakt. Vyžadována však je dlouhodobost tohoto jednání a zároveň musí vzbuzovat důvodnou obavu o život nebo zdraví své, nebo blízkých osob. Je zřejmé, že intenzita pronásledování bude nepřímo úměrná její dlouhodobostí. Při vyšší intenzitě a četnosti pronásledování bude vyžadována kratší doba tohoto jednání. Opakováním se rozumí více než 10 pokusů o kontakt a trvajícím obdobím pak minimálně doba 4 týdnů. Zároveň bude brán zřetel na tradice a případnou odlišnost kultur (např. rituální rozchod)

II. PRAKTICKÁ ČÁST

4 ANALÝZA TRENDU VÝVOJE DISTANČNÍCH POČÍTAČOVÝCH TRESTNÝCH ČINŮ V ČR

Vývoj kriminality ve všech oblastech je sledovaný různými institucemi. Zřejmě nejkomplexnějšími výstupy disponuje Policie České republiky, pod jejichž působnost mimo jiné spadají evidence statistických údajů o průběhu a výsledku trestního řízení. Tyto údaje jsou mimo jiné, podkladovými materiály pro hodnocení bezpečnostní situace v konkrétních místech. Počítačová kriminalita, respektive delikty, které jsou páchané distanční formou, však evidovány nejsou. Evidovány jsou spáchané trestné činy s uvedením konkrétních paragrafů, nikoli však způsob spáchání činu. Dalším hlediskem, jehož absence je také velmi podstatná, je neuvádění počtu poškozených osob. V rámci jednoho pachatele, pokud se jedná o pokračující trestný čin, kdy pachatel páchá po určitý časově ohraničený úsek stejný trestný čin, se dle statistik jedná o jeden trestný čin. Není rozlišováno, zda pachatele například při trestném činu podvodu zaslal poškozenému místo telefonu balíček s cihlou, nebo zda pachatel vytvořil podvodné stránky s elektronickým obchodem, kam se za dobu dvou měsíců přihlásilo několik stovek lidí, kteří si objednali a zaplatili zboží, které jim nebylo doručeno. Je tedy zřejmé, že distanční delikty jsou z tohoto hlediska závažnější. Dotazem na oddělení analytiky, které se zabývá statistickými údaji, bylo zjištěno, že údaje o počtu poškozených osob není možné získat žádným způsobem, protože informační systémy Policie nejsou k zaznamenávání těchto údajů uzpůsobeny. Jediným způsobem jak zjistit počet spáchaných trestných činů bylo porovnání oznámených trestných činů, které byly v rámci prověřování postoupeny z důvodu odlišného místa následku a místa, kde se pachatel skutku dopustil. Zdrojem informací pro statistické srovnání v kapitole 4 práce, tak byly statistické přehledy kriminality za jednotlivé roky[30] a dále samostatně zjištěná a vyčleněná data o distančních deliktech.

Dále uváděné tabulky jsou uvedeny od roku 2010, kdy došlo k rekodifikaci zákona č. 140/1961 Sb. trestního zákona a vešel v platnost zákon č. 40/2009 Sb. trestní zákoník. Rok 2010 je k datu 31.12.2010. V roce 2011 je uvedeno přesné datum 31.3.2011 a to z důvodu, že v dubnu roku 2011 bylo ve sbírce zákonů vyhlášeno rozhodnutí Ústavního soudu České republiky, kterým dochází ke ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů a vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. [31] Protože se jedná

o změnu, která se přímo dotýká vyšetřování distančních trestných činů, bylo na místě zjistit jak se toto rozhodnutí projevilo v objasněnosti těchto trestných činů. Konečné datum ruku 2011 bylo k 31.12.2011 a datum 2012 je k 31.3.2012, ke kterému byly zpracovány statistiky v rámci Policie ČR.

4.1 VYDÍRÁNÍ (§ 175) A SEXUÁLNÍ NÁTLAK (§ 186)

Tab. 1 VYDÍRÁNÍ (§ 175)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	1 359	976	72	**43**	**3**	**26**	**60**
Do 31.3.2011	*422*	*227*	*54*	***14***	***3***	***9***	***64***
2011	1 522	1 173	77	**51**	**3**	**34**	**67**
2012	457	277	61	**33**	**7**	**24**	**73**

Tab. 2 SEXUÁLNÍ NÁTLAK (§ 186)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	22	16	73	**12**	**55**	**7**	**58**
Do 31.3.2011	*9*	*2*	*22*	***5***	***56***	***4***	***80***
2011	27	23	85	**15**	**56**	**11**	**73**
2012	11	9	82	**7**	**64**	**6**	**86**

Příklad: Pachatel najde na Internetu fotografie, kde je jeho známá zachycena po požití omamných látek. Následně žádá po ženě finanční obnos za to, že nebude informovat rodinu, známé, školu. Zde jde o vydírání. Pokud však bude žádat například pohlavní sebeukájení, jde již o sexuální nátlak.

Příklad distančního deliktu: Pachatel vydávající se za dívku se prostřednictvím sociální sítě seznámí s chlapcem. Přesvědčí ho o tom, že jsou kamarádi. Chlapec se mu svěří s nějakým tajemstvím. Pachatel chlapce začne následně vydírat a nutit jej například k páchání trestné

činnosti zde se jedná o vydírání. V případě, že muž chlapce nutí například ke svlékání se před kamerou, jde o sexuální nátlak.

Rozdíl je v zájmu pachatele. V případě vydírání se jedná o výhodu, nebo prospěch, kdežto v případě sexuálního nátlaku se pachatel snaží od poškozeného získat materiál pro sexuální vzrušení.

U trestného činu vydírání se z hlediska páchání distančních deliktů vůči zjištěným činům jedná o setrvalý stav, do nějž rozhodnutí Ústavního soudu České republiky nijak podstatně nezasáhlo. Objasněnost se každým rokem mírně zvyšuje.

Trestný čin sexuální nátlak je ve většině případů páchán distanční formou. V prvních třech měsících roku 2011 byla objasněnost na úrovni 80 %. Po rozhodnutí Ústavního soudu České republiky zaznamenala objasněnost na konci roku 2011 7 % pokles. Objasněnost se každým rokem mírně zvyšuje.

4.2 PORUŠENÍ TAJEMSTVÍ DOPRAVOVANÝCH ZPRÁV (§ 182) A PORUŠENÍ TAJEMSTVÍ LISTIN A JINÝCH DOKUMENTŮ UCHOVÁVANÝCH V SOUKROMÍ (§ 183)

Tab. 3 PORUŠENÍ TAJEMSTVÍ DOPRAVOVANÝCH ZPRÁV (§ 182)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	19	5	26	**10**	**53**	**6**	**60**
Do 31.3.2011	*10*	*1*	*10*	*6*	*60*	*4*	*67*
2011	22	12	55	**13**	**59**	**10**	**77**
2012	9	5	56	**6**	**67**	**4**	**67**

Tab. 4 PORUŠENÍ TAJEMSTVÍ LISTIN A JINÝCH DOKUMENTŮ UCHOVÁVANÝCH V SOUKROMÍ (§ 183)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	15	11	73	**10**	**67**	**6**	**60**
Do 31.3.2011	*5*	*3*	*60*	*4*	*80*	*3*	*75*
2011	13	10	77	**11**	**85**	**7**	**64**
2012	10	6	60	**9**	**90**	**5**	**56**

Příklad: Pachatel najde ve schránce dopis, určený jeho spolubydlícímu. Dopis otevře a jeho obsah si přečte. Zde se jedná o trestný čin Porušení tajemství dopravovaných zpráv. Pokud dopis najde otevřený v bytě, přečte si ho a řekne přítelkyni, co v dopise četl, bude se jednat o trestný čin Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí.

Příklad distančního deliktu: Pachatel získá přístupová hesla do emailové schránky spolužáka a zde si přečte novou doručenou zprávu od jeho přítelkyně, ještě před tím, než se do schránky přihlásí právoplatný uživatel. Zde se jedná o trestný čin Porušení tajemství dopravovaných zpráv. Pokud však pachatel získá dálkový přístup k počítači svého učitele v kanceláři, kde nalezne již uložený email se záznamem z webové kamery a tento záznam umístí na Internet, bude se jednat o trestný čin Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí.

Rozdíl mezi těmito trestnými činy je v tom, že dle ust. § 182 jsou chráněny doručované zprávy, tedy pouze zprávy, které oprávněný držitel dosud neobdržel, kdežto ust. § 183 chrání materiály, které máme uchovány v soukromí a to nejen v domě, ale například i v místech veřejných, pokud v nich je místo, jež máme ve své moci. Může se jednat i například o šatní skříň ve škole, která je samostatně uzamčena.

U trestného činu Porušení tajemství dopravovaných zpráv dochází k nárůstu páchání distančních deliktů vůči zjištěným činům. Rozhodnutí Ústavního soudu České republiky však nijak podstatně do objasněnosti nezasáhlo. Objasněnost nemá setrvalý stav.

Trestný čin Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí je v naprosté většině případů páchán distanční formou. V prvních třech měsících roku 2011

byla objasněnost 75 %. Po rozhodnutí Ústavního soudu České republiky zaznamenala objasněnost na konci roku 2011 11 % pokles. Objasněnost je kolem 60 %.

4.3 ŠÍŘENÍ PORNOGRAFIE (§ 191) A VÝROBA A JINÉ NAKLÁDÁNÍ S DĚTSKOU PORNOGRAFIÍ (§ 192)

Tab. 5 ŠÍŘENÍ PORNOGRAFIE (§ 191)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	88	72	82	**63**	**72**	**50**	**79**
Do 31.3.2011	*44*	*34*	*77*	***31***	***70***	***24***	***77***
2011	77	68	88	**52**	**68**	**36**	**69**
2012	17	8	47	**12**	**71**	**8**	**67**

Tab. 6 VÝROBA A JINÉ NAKLÁDÁNÍ S DĚTSKOU PORNOGRAFIÍ (§ 192)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	159	114	72	**96**	**60**	**61**	**64**
Do 31.3.2011	*77*	*55*	*71*	***53***	***69***	***38***	***72***
2011	255	168	66	**174**	**68**	**91**	**52**
2012	61	27	44	**42**	**69**	**18**	**43**

Příklad: Pachatel vidí, jak muž znásilňuje ženu a toto si nahraje na telefon. Jedná se o šíření pornografie v 1 odstavci. V případě, že toto video ukáže spolužákovi, který ještě nemá 18 let, jde o šíření pornografie v 2 odstavci. Pokud některá z osob zachycená na videu nebude mít 18 let a toto video si druhý spolužák uloží a uchová doma, jedná se v jeho případě o trestný čin Výroba a jiné nakládání s dětskou pornografií v 1 odstavci a ten kdo video natočil, se zároveň dopustil trestného činu Výroba a jiné nakládání s dětskou pornografií ve 2 odstavci.

Příklad distančního deliktu: Pachatel vyrobí fotografie, kde je znázorněn sex člověka se zvířetem a tyto odešle svému známému. Jedná se o šíření pornografie v 1 odstavci. V případě, že je známým osoba, která ještě nemá 18 let, jde také o šíření pornografie v 2 odstavci. Pokud bude na fotografiích aktérem dítě a adresát si povídku v emailu uloží, dopouští se trestného činu výroba a jiné nakládání s dětskou pornografií dle 1 odstavci a ten kdo fotografie vyrobil se zároveň dopustil trestného činu Výroba a jiné nakládání s dětskou pornografií ve 2 odstavci.

Rozdíl mezi těmito trestnými činy je v tom, že při šíření pornografie jde o vyjmenovaná pornografická díla, nebo jakákoliv pornografická díla (i písemná, tedy může jít o nereálné fantazie), zpřístupněná dítěti, ale u trestného činu Výroba a jiné nakládání s dětskou pornografií jsou zde jako aktéři zapojeni děti. Zde je na místě upozornit na skutečnost, že pohlavní styk je přípustný pro osoby starší 15 let, ale pokud se u toho tato osoba vyfotí, či pořídí jiný záznam, dopouští se trestného činu Výroba a jiné nakládání s dětskou pornografií a to i v případě, že mimo autora není na záznamu zachyceno další dítě.

Trestný čin šíření pornografie je z velké části páchán distanční formou. Dochází ke stagnaci procent zjištěných skutků, oproti tomu došlo k 8 % poklesu objasněnosti v roce 2011. Objasněnost nemá setrvalý stav.

Trestný čin Výroba a jiné nakládání s dětskou pornografií je v naprosté většině případů páchán distanční formou. V prvních třech měsících roku 2011 byl objasněno téměř každé 3 ze 4 spáchaných trestných činů distanční formou. Po rozhodnutí Ústavního soudu České republiky zaznamenala objasněnost na konci roku 2011 o 1/5 skutků. Objasněnost od uvedené doby klesá.

4.4 PODVOD (§ 209)

Tab. 7 PODVOD (§ 209)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	9 369	4 904	52	**1 502**	**16**	**661**	**44**
Do 31.3.2011	*2 745*	*944*	*34*	***533***	***19***	***262***	***49***
2011	9 063	4 876	54	**1 759**	**19**	**840**	**48**
2012	3 051	1 185	39	**621**	**20**	**270**	**43**

Příklad: Pachatel si koupí motorové vozidlo, ale již při podpisu smlouvy ví, že nemá prostředky na jeho zaplacení a přesto smlouvu podepíše, s vozidlem odjede a následně jej prodá.

Příklad distančního deliktu: Pachatel si vytvoří webové stránky, kde si vytvoří elektronický obchod s elektronikou a vydává se za již existující firmu, při objednávce požaduje platbu před odesláním zboží. Po provedení platby s kupujícím již nekomunikuje a zboží nedodá.

Trestný čin Podvod je co do rozsahu páchání distanční formou zastoupen v menší míře. Jak však bylo uvedeno dříve, konkrétně u tohoto trestného činu je nejzávažnější skutečností, že se za každým jedním skutkem mohou skrývat stovky poškozených s milionovými škodami. Po rozhodnutí Ústavního soudu České republiky zaznamenala objasněnost jen minimální pokles, což je možné vysvětlit skutečností, že k ustanovování pachatelů dochází ve značné míře i jiným způsobem (zjištění čísla účtu pachatele, adresy odesílatele aj.).

4.5 NEOPRÁVNĚNÝ PŘÍSTUP K POČÍTAČOVÉMU SYSTÉMU A NOSIČI INFORMACÍ (§ 230) A OPATŘENÍ A PŘECHOVÁVÁNÍ PŘÍSTUPOVÉHO ZAŘÍZENÍ A HESLA K POČÍTAČOVÉMU SYSTÉMU A JINÝCH TAKOVÝCH DAT (§ 231)

Tab. 8 NEOPRÁVNĚNÝ PŘÍSTUP K POČÍTAČOVÉMU SYSTÉMU A NOSIČI INFORMACÍ (§ 230) A OPATŘENÍ A PŘECHOVÁVÁNÍ PŘÍSTUPOVÉHO ZAŘÍZENÍ A HESLA K POČÍTAČOVÉMU SYSTÉMU A JINÝCH TAKOVÝCH DAT (§ 231)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	101	30	30	**42**	**42**	**24**	**57**
Do 31.3.2011	*50*	*12*	*24*	***22***	***44***	***14***	***64***
2011	134	54	40	**58**	**43**	**27**	**47**
2012	42	19	45	**21**	**50**	**12**	**57**

Příklad: Zaměstnanec v továrně v době nepřítomnosti vedoucího spustí jeho počítač s upraveným CD diskem a zjistí přístupové heslo do systému Windows s kterým se přihlásí do systému (§230/1 TZ). Pokud zde pozmění informace o docházce s tím, že si například

dopíše dny, kdy nebyl v práci jako odpracované, dopouští se trestného činu dle § 230 odst. 2 TZ. Pokud je na uvedeném CD disku počítačový program, který má rozluštit přístupové heslo do systému, dopustil se zaměstnanec trestného činu dle ust. § 231 TZ již opatřením si tohoto hesla.

Příklad distančního deliktu: Žák ve škole, si zjistí jaký počítačový systém je používán na zkoušky. Na Internetu si opatří návod, jak zjistit heslo do tohoto systému (§231 TZ). Z domu se k tomuto systému připojí a přihlásí se do něj (§ 230/1 TZ). V případě, že si v systému změní známku na lepší, dopustí se trestného činu dle ust. § 231 TZ.

Trestné činy Neoprávněný přístup k počítačovému systému a nosiči informací a Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat nejsou ve statistikách v rámci Policie ČR rozděleny na samostatné skutky a není tedy možné ani distanční delikty rozdělit a srovnávat je s napadenými trestnými činy. Distanční skutky se na páchání těchto trestných činů podílí v necelé polovině, až k polovině případů. V roce 2011 došlo k poklesu objasněnosti distančních deliktů proti roku 2010 o 10 % a oproti prvním třem měsícům roku 2011 dokonce o 17 %. V roce 2012 se objasněnost vrací na úroveň roku 2010.

4.6 PORUŠENÍ AUTORSKÉHO PRÁVA, PRÁV SOUVISEJÍCÍCH S PRÁVEM AUTORSKÝM A PRÁV K DATABÁZI (§ 270)

Tab. 9 PORUŠENÍ AUTORSKÉHO PRÁVA, PRÁV SOUVISEJÍCÍCH S PRÁVEM AUTORSKÝM A PRÁV K DATABÁZI (§ 270)

	spáchané celkem			**distanční delikty**			
		objasněno				**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**	**% vůči všem skutkům**	**počet**	**%**
2010	650	464	71	**420**	**65**	**344**	**82**
Do 31.3.2011	*118*	*47*	*40*	***46***	***39***	***32***	***70***
2011	412	240	58	**162**	**39**	**42**	**26**
2012	153	36	24	**64**	**42**	**19**	**30**

Příklad: Společnost zabývající se návrhem a výrobou součástek do motorů zakoupí jednu licenci na program pro návrh těchto součástek. Následně program nainstaluje na další počítačové stanice, aniž by zakoupila další licenční klíče.

Příklad distančního deliktu: Muž si v kině nahraje na kameru právě uváděný film, tento si uloží do počítače a následně jej uloží na veřejně dostupné úložiště a odkaz na stažení filmu rozšíří prostřednictvím Internetových stránek.

Trestný čin Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi je ve většině případů páchán nedistanční formou. Výjimka z tohoto závěru je v roce 2010. Zde však byla v rámci Krajského ředitelství Policie ČR Olomouckého kraje každá jedna poškozená společnost vykázána jako jednotlivý skutek. Tím došlo k tomu, že Krajské ředitelství Policie ČR Olomouckého kraje vykázalo téměř polovinu (309) zjištěných a více než 60 % (298) objasněných skutků. Tento způsob vykazování je sice správný, ale v rámci ostatních útvarů Policie ČR neaplikovaný. Po vydání rozhodnutí Ústavního soudu České republiky došlo k razantnímu poklesu objasněnosti distančních trestných činů. Z 82 % objasněnosti v roce 2010, byl v roce 2011 pokles na 26 %, který v roce 2012 mírně vzrostl na 30 %. Je zřejmé, že rozhodnutí Ústavního soudu České republiky v tomto případě výrazně zasáhlo do možnosti Policie ČR vyšetřovat tuto trestnou činnost.

4.7 NEBEZPEČNÉ PRONÁSLEDOVÁNÍ (§ 354)

Tab. 10 NEBEZPEČNÉ PRONÁSLEDOVÁNÍ (§ 354)

	spáchané celkem			**distanční delikty**			
		objasněno			**% vůči všem skutkům**	**objasněno**	
Rok	Zjištěno	počet	%	**Zjištěno**		**počet**	**%**
2010	537	390	73	**41**	**8**	**24**	**59**
Do 31.3.2011	*199*	*84*	*42*	***18***	*9*	***11***	***61***
2011	535	410	77	**49**	**9**	**26**	**53**
2012	164	66	40	**16**	**10**	**9**	**56**

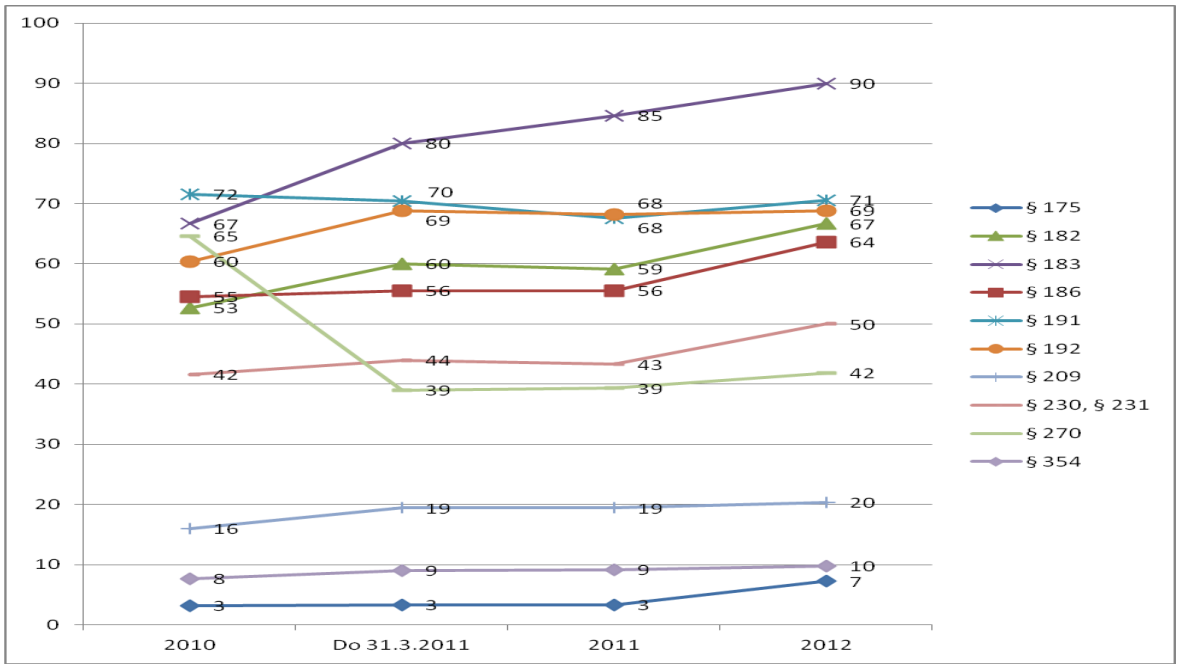
Příklad: Muž, který byl trestán pro násilnou trestnou činnost, po rozchodu čekal na bývalou přítelkyni před prací a domem. Poškodí jí auto, aby se nemohla dostat do práce a musela ho požádat o pomoc. Každý den jí několikrát volá a píše zprávy. Volá jí i do práce. Ve zprávách jí nadává a uráží ji. Volá i společným přátelům a rodině, kde bývalou přítelkyni pomlouvá a rodině říká, že pokud se k němu bývalá přítelkyně nevrátí, tak že ji nechá zbít, nebo si počká až bude večer sama.

Příklad distančního deliktu: Dívka se přes Internet seznámí s mužem, který se vydává za chlapce v jejím věku. Začnou se spolu bavit, ale muž se prozradí, že je starší. Dívka se s ním přestane bavit a zablokuje si ho na sociální síti. Muž si zjistí kamarády dívky a podaří se mu zjistit její adresu a telefonický kontakt. Začne jí psát dopisy, emaily, sms zprávy a chce, aby byli dále přátelé. Dívka odmítá a muž jí pošle fotografie její rodiny, její a jejího malého sourozence a vyhrožuje, že pokud nebudou kamarádi, tak rodině ublíží.

Trestný čin Nebezpečné pronásledování je páchán distanční formou pouze desetinou případů. Tato skutečnost je zapříčiněna tím, že většina pachatelů preferuje osobní kontakt. 68 % pachatelů se potuluje v blízkosti oběti. Str 64 ISBN **978-80-247-2207-8** Rozhodnutí Ústavního soudu České republiky nemělo na vyšetřování tohoto trestného činu zásadní význam, což se dá vysvětlit právě snahou o osobní kontakt s poškozenou osobou vedoucí k ustanovení pachatele.

4.8 Poměr spáchaných distančních deliktů vůči činům spáchaným osobně pachatelem

Trestné činy, které jsou páchány distančně, prochází určitým vývojem. Tento vývoj presentuje graf, který je uveden a vychází z dat, které byly získány u konkrétních trestných činů.

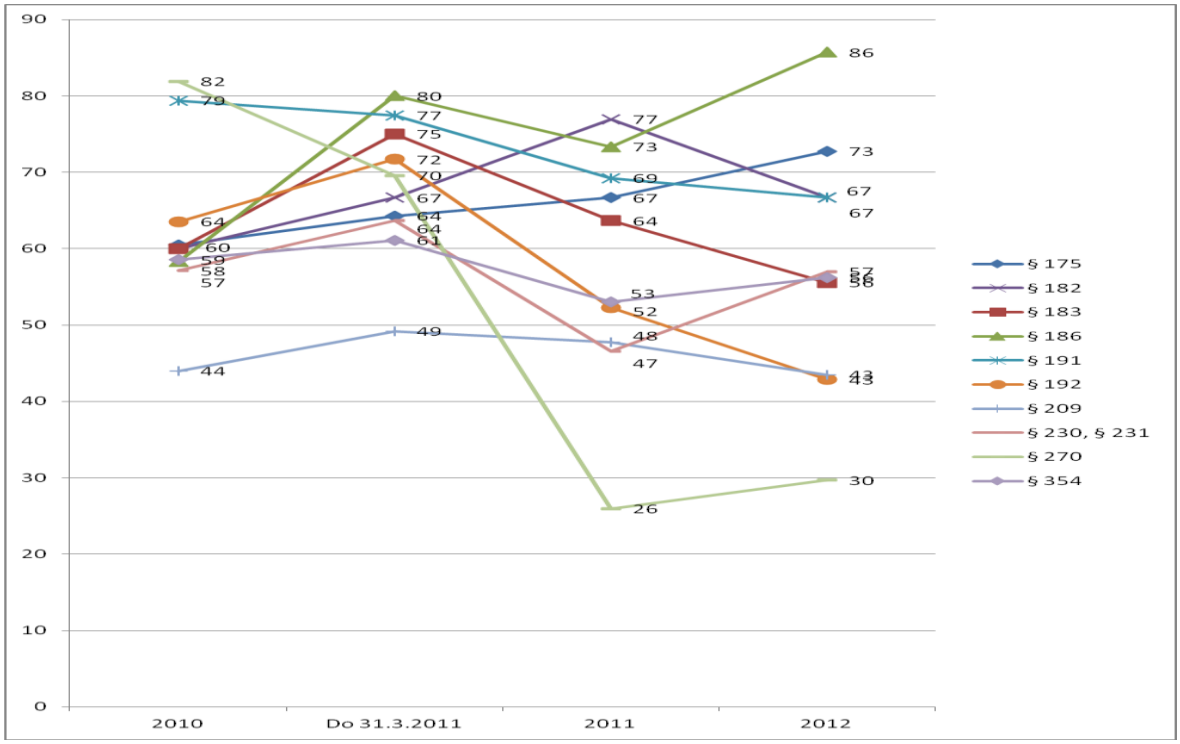


Obr. 3. Graf vývoje distančních trestných činů

Z uvedeného grafu vyplívá, že až na výjimky má páchání distančních trestných činů stagnující, případně mírně rostoucí tendenci vůči skutkům spáchaným běžným způsobem. Uvedené výjimky jsou dvě. Tou první je trestný čin Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí § 183. U tohoto trestného činu je značný procentuální rozdíl způsoben tím, že ročně jsou spáchány řádově jednotky činů a každý jeden spáchaný skutek se tak ve statistikách promítá deseti procenty. Druhou výjimkou je trestný čin Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi § 270. K tomuto razantnímu poklesu mezi lety 2010 a 2011 však došlo tím způsobem, že Krajským ředitelstvím Policie ČR Olomouckého kraje byla jinak vykázána statistická data, jak je uvedeno v kapitole 4.6.

4.9 Vývoj objasněnosti distančních deliktů

Do vývoje objasněnosti distančních deliktů zasahují různé faktory. Patří sem vývoj komunikačních technologií, personální a materiální situace u Policie ČR, znalosti uživatelů a další. Jako nejpodstatnější okolnost zasahující do vývoje objasněnosti ve sledovaném období se však ukazuje zásah Ústavního soudu České republiky.

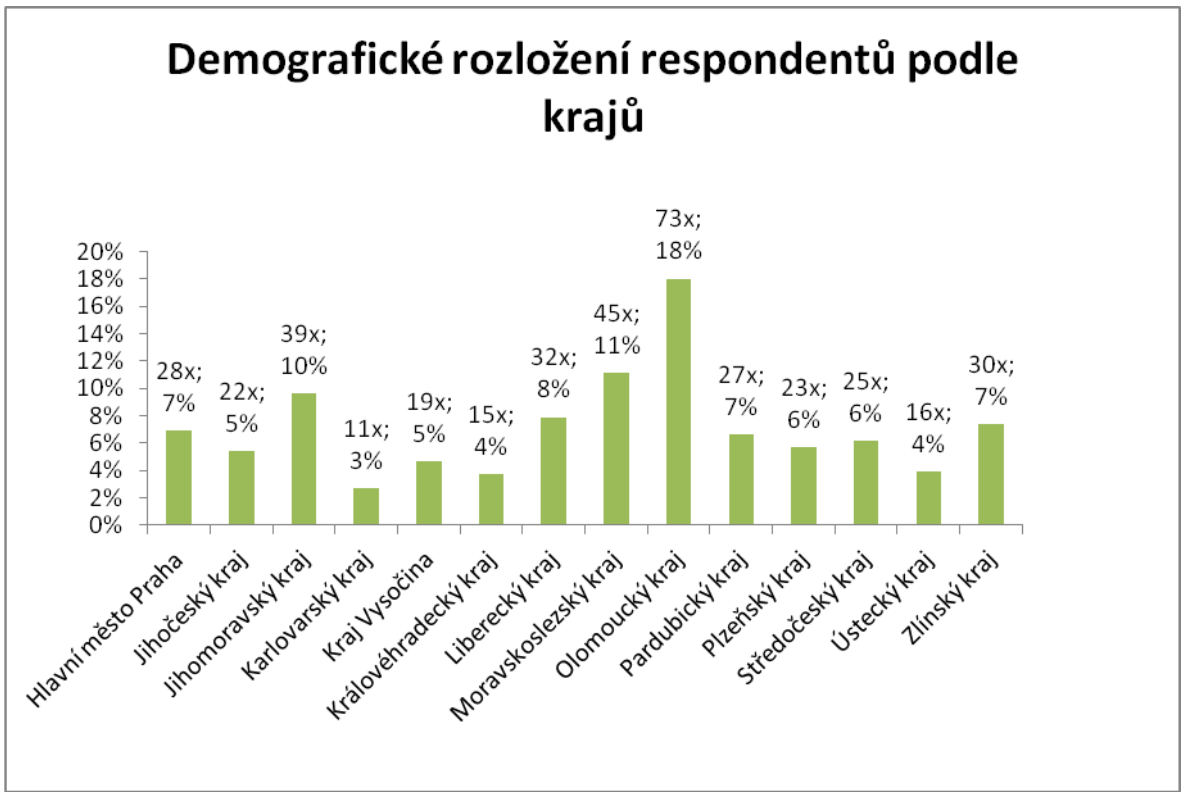


Obr. 4 Graf vývoje objasněnosti distančních deliktů

Vyjma trestných činů Vydírání § 175 TZ a Porušení tajemství dopravovaných zpráv § 182 TZ, u kterých se rozhodnutí Ústavního soudu České republiky neprojevilo, došlo u všech sledovaných distančních deliktů k poklesu objasněnosti. Nejmarkantnější rozdíl byl u trestného činu Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi § 270 TZ, kde během roku došlo k 44 % poklesu. Druhý největší pokles je u trestného činu Výroba a jiné nakládání s dětskou pornografií dle § 192 TZ, kde došlo během roku k poklesu o 20 %.

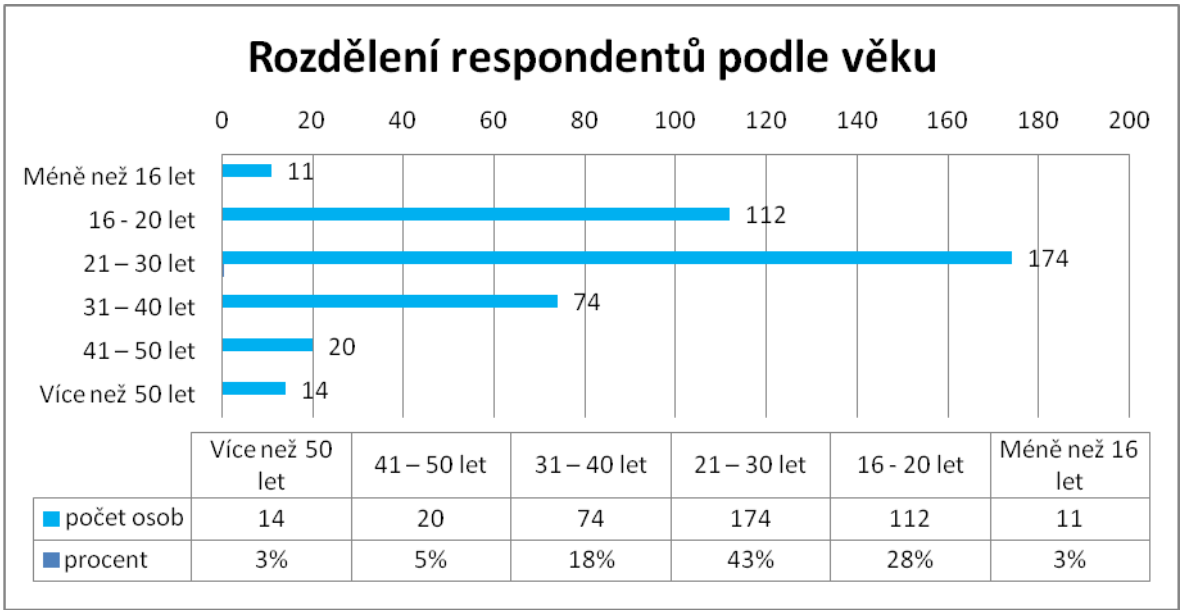
5 ZPŮSOBY OCHRANY DAT A RIZIKOVOST CHOVÁNÍ UŽIVATELŮ

Informace o tom, jakým způsobem mají uživatelé chráněna data a jak rizikově se chovají, byly zjišťovány výzkumem. Jako výchozí výzkumná procedura byla zvolena metoda dotazníku. Dotazník byl umístěn na bezplatné službě na Internetu a byl distribuován elektronicky. Sběr dat probíhal v období od 1.3.2012 do 15.4.2012. Vyhodnocení dat bylo realizováno v období od 16.4.2012 do 7.5.2012. Dotazník obsahoval otázky rozdělené celkem do tří okruhů, přičemž se jednalo o zabezpečení počítače, chování v počítačové síti a prevence proti sociálnímu inženýrství. Výzkumný vzorek sestával z 72% (293) mužů a 28% (112) žen. Z demografického hlediska byl nejméně zastoupen Karlovarský kraj z 2 % a nejvíce Olomoucký kraj 18 %.



Obr. 5 Demografické rozložení respondentů

Dle věku bylo nejvíce osob mezi 21-30 lety 43 % a nejméně osob ve věku méně než 16 let a více než 50 let. Obojí zastoupeni 3 %.



	Více než 50 let	41 – 50 let	31 – 40 let	21 – 30 let	16 - 20 let	Méně než 16 let
počet osob	14	20	74	174	112	11
procent	3%	5%	18%	43%	28%	3%

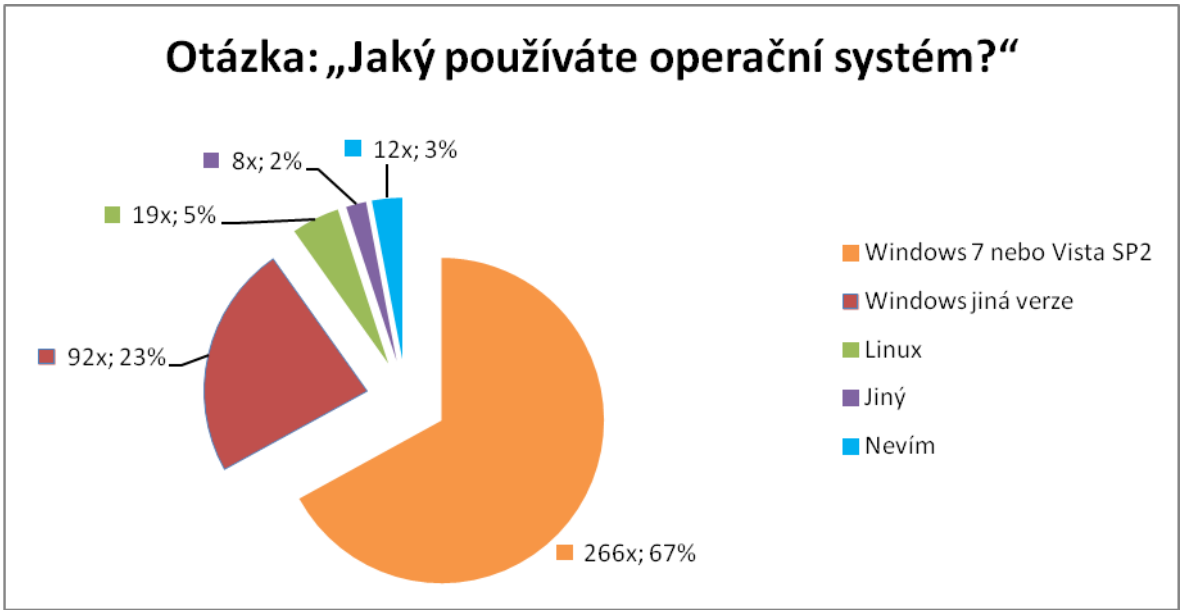
Obr. 6 Rozdělení respondentů podle věku

5.1 Zabezpečení počítače

Programové zabezpečení počítače a způsob jeho připojení k síti je základním ochranným prvkem, který je uživateli realizován. Cílem otázek v tomto bloku bylo zjistit, jaké procento uživatelů umožňuje útočníkům z vlastního přičinění využití známých chyb a postupů.

5.1.1 Používaný operační systém

Operační systém je základním programem každého počítače. Čím je program rozšířenější, tím je zajímavější pro počítačového útočníka, protože se stejným úsilím může napadnout více počítačů. Starší verze programů také přestávají být výrobcem aktualizovány a podporovány.

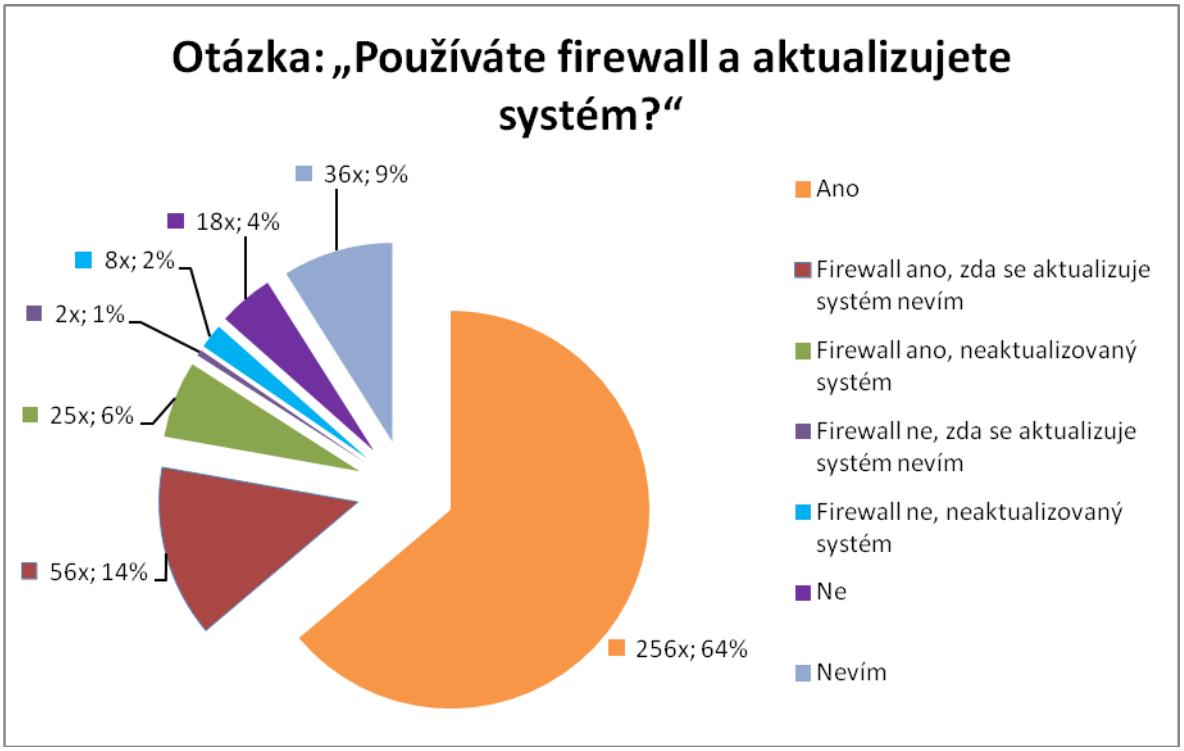


Obr. 7 Používaný operační systém

Na otázku odpovědělo 397 respondentů. Naprostá většina používá operační systém Windows 7, nebo Vista se Service Pack 2. Tyto operační systémy jsou stále aktualizovány a dají se považovat za bezpečné. Operační systémy Linux a ostatní jsou uživateli zastoupeni pouze 7 %. 23 % uživatelů však používá operační systém Windows jiné verze, což znamená Windows Vista SP1, případně starší. Tento systém však již není aktualizován a není tedy chráněn proti aktuálním bezpečnostním hrozbám. Jedná se tak o systém, jež je náchylný k napadení například počítačovými viry.

5.1.2 Aktualizace systému a firewallu

Použití firewallu a aktualizace systému jsou základním bezpečnostním prvkem, který je pro útočníka překážkou. V případě zjištění chyby v systému je tato chyba, ze strany útočníků rychle využívána a výrobci software se snaží o její odstranění formou aktualizací.

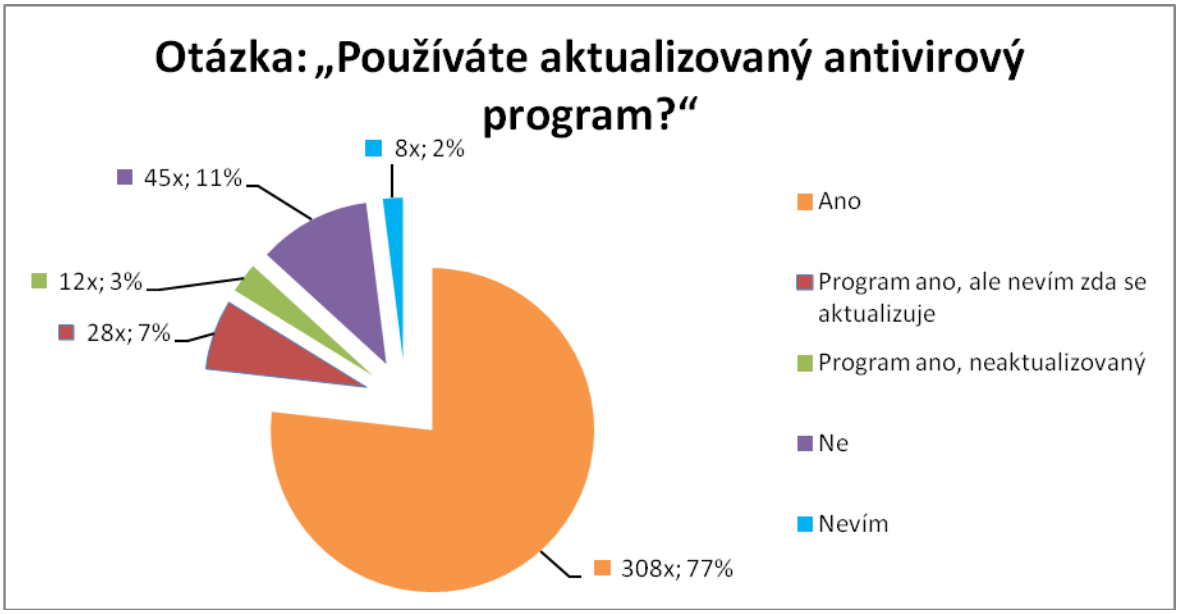


Obr. 8 Aktualizace systému a firewallu

Na otázku odpovědělo 401 respondentů. Naprostá většina 64 % používá firewall a aktualizuje systém. Dalších 27 % dotázaných však uvedlo, že nepoužívá jeden z prvků, případně nepoužívá ani jeden. Jedná o bezpečnostní hrozbu, kterou využívají zejména počítačové viry a trojské koně.

5.1.3 Antivirový program

Antivirové programy obsahují databázi známých virů a jsou schopny je odhalit. Nad uvedené jsou schopny na základě analýzy programů zjistit i programy, které v databázi uvedeny nejsou.

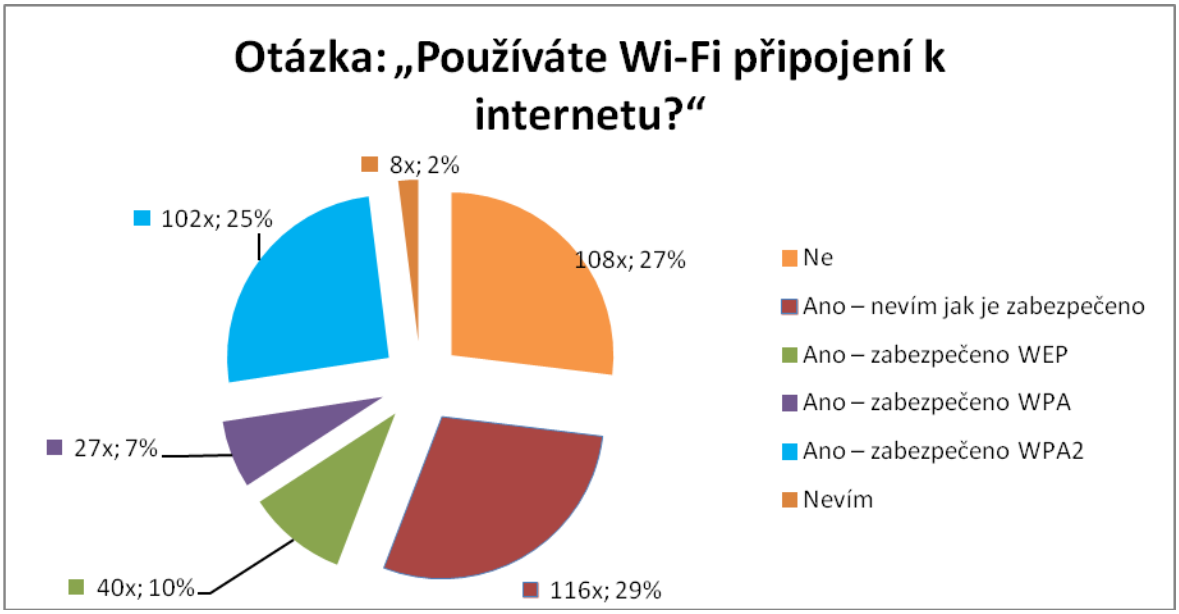


Obr. 9 Antivirový program

Na otázku odpovědělo 401 respondentů. Naprostá většina 77 % používá aktualizovaný antivirový program. Všichni ostatní, tedy 23 % odpovídajících však nemá počítač proti virům zabezpečen. Použití antivirového programu je důležité, pokud ale není aktualizovaná virová databáze, není program schopen reagovat na aktuální viry a systém se stává napadnutelným.

5.1.4 Používání WiFi připojení k Internetu

WiFi připojení umožňuje připojit do počítačové sítě různá zařízení, které spolu mohou komunikovat a v domácnostech se hojně využívá.



Obr. 10 Používání WiFi připojení k internetu

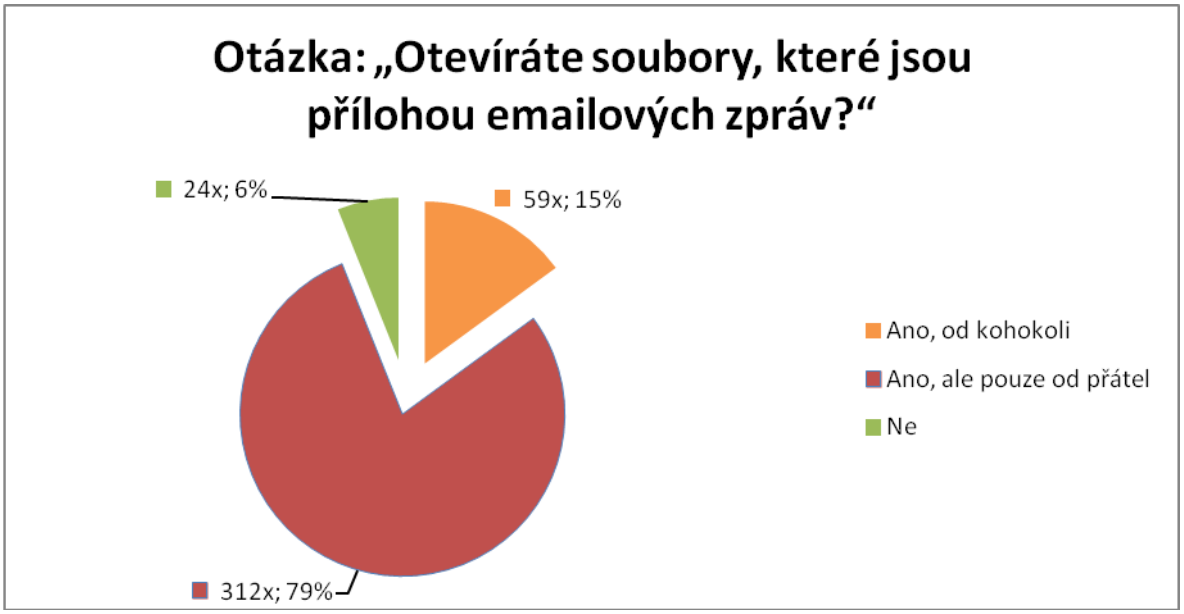
Na otázku odpovědělo 401 respondentů. Většina respondentů, celkem 52 %, buď toto připojení nevyužívá, nebo používá zabezpečení WPA2, které je považováno za bezpečné. Dalších 7 % respondentů používá zakódování WPA, které již sice není považováno za bezpečné, využití jeho chyb je však se současnými prostředky nereálné. Ostatní respondenti však vůbec neví, zda WiFi připojení používají, neví jaké kódování používají, případně používají kódování WEP, které je při použití specializovaného počítačového programu jednoduše překonatelné.

5.2 Chování v počítačové síti

Chování uživatelů na počítačích připojených k počítačové síti je z hlediska bezpečnosti rizikovější, protože uživatelé musí brát v potaz možná rizika spojená s elektronickou poštou, užívaní programů z těchto sítí a absenci přímého kontaktu s protistranou. Cílem otázek v tomto bloku bylo zjistit, kolik procent uživatelů umožňuje útočníkům vlastní neznalostí, případně neopatrností získat přístup ke svému počítači, nebo i financím bez vynaložení velkého úsilí.

5.2.1 Otevírání doručených souborů

Soubory, jež tvoří přílohy emailových zpráv mohou obsahovat viry, případně trojské koně, které dovolí útočníkovi přístup do systému, případně poškodí soubory v počítači uložené. [32]

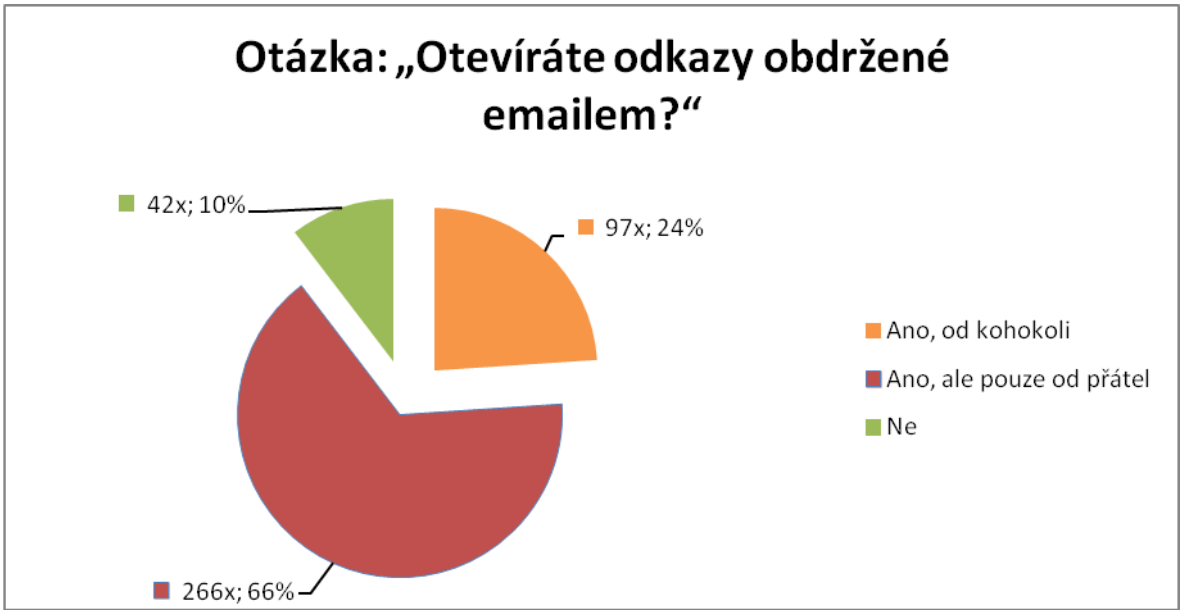


Obr. 11 Otevírání doručených souborů

Na otázku odpovědělo 395 respondentů. Pouze 6 % respondentů uvedlo, že soubory v emailových zprávách neotevírá. Ostatní, tedy 94 % soubory otevírá. Není podstatné, kým je soubor doručen. Může se stát, že osoba, kterou považujeme za přítele se rozhodne nás poškodit. Druhou variantou je, že se k jeho schránce dostane někdo další. Nejjednodušší variantou však je možnost, že se útočník vydává za osobu kterou není. Podvržení odesílatele emailové zprávy není věc složitá a pro útočníka ani není potřeba mít rozsáhlé znalosti.

5.2.2 Otevírání doručených odkazů

Odkazy, které jsou doručeny emailem je možné upravit tak, aby se uživateli jevili jako v pořádku, přesto, že to tak není.



Obr. 12 Otevírání doručených odkazů

Na otázku odpovědělo 405 respondentů. Pouze 10 % respondentů uvedlo, že odkazy v emailových zprávách neotevírá. Ostatní, tedy 90 % odkazy otevírá. Stejně jak bylo uvedeno a vysvětleno v kapitole 5.2.1 není podstatné, kým je soubor doručen. K této otázce byla položena navazující otázka, která zněla: “Víte bez kliknutí na odkaz, co je na stránkách „www.googIe.com“?“

Možné odpovědi byly:

1. Vyhledávací stránka. Tuto odpověď označilo 377 respondentů, tedy 93,00%odpovídajících.
2. Nevím, případně může být cokoliv“ Tuto odpověď označilo 28 respondentů, tedy 7,00% „odpovídajících.

Uvedený odkaz www.googIe.com, je složeninou malých a velkých písmen. Místo malého písmene L je použito velké písmeno I. Pokud je tento odkaz doručován emailem, případně pokud je na něj odkazováno na stránkách, je rozdíl mezi těmito písmeny nerozeznatelný. Uživatel se tak připojí na podvržené stránky. Pokud se tyto stránky zdají být těmi na které je uživatel zvyklý může po požadavku zadat přihlašovací údaje, které jsou následně doručeny útočníkovi.

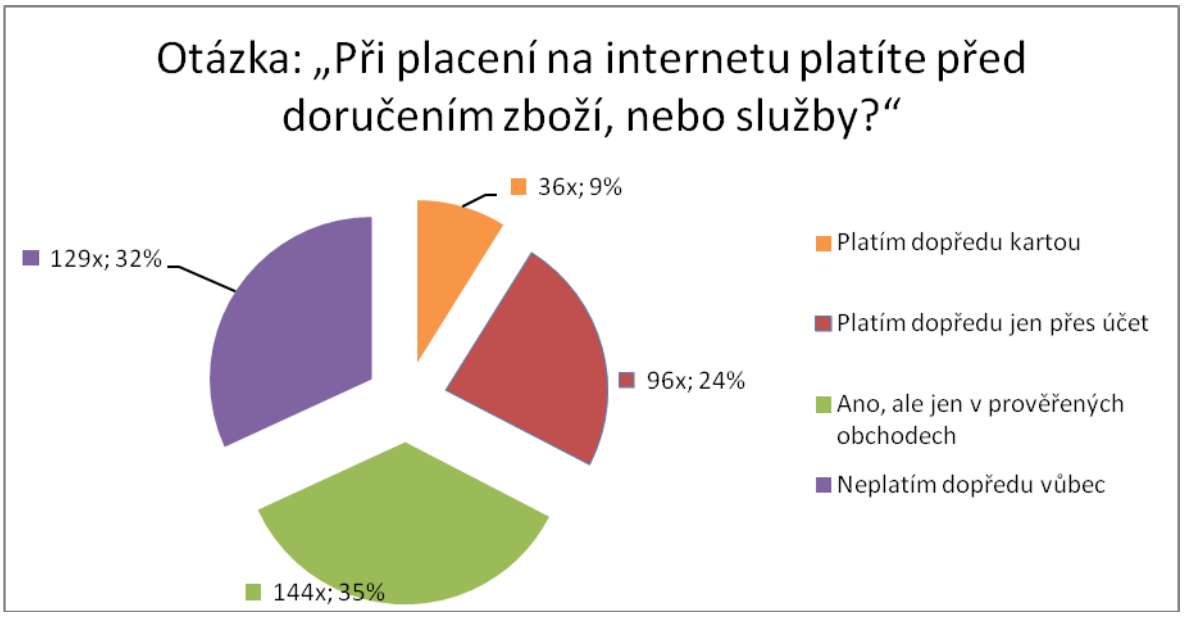
5.2.3 Používání programů z neznámých zdrojů

Používání programů stažených ze stránek na Internetu je potencionální hrozbou, když není možné ověřit, co obsahuje instalační soubor a s těmito soubor ještě před zpřístupněním uživatelům pracuje větší množství osob. [33]

Položená otázka zněla: "Používáte programy získané z neznámých zdrojů na Internetu (warez, výměnné sítě)?" Možné odpovědi byly pouze ano, nebo ne. Větší část, 56 % (222x) respondentů odpovědělo, že ne. 44 % (175) však tyto programy používá. V rámci instalace těchto programů je však možné, že při instalaci dojde k instalaci i škodlivého kódu. Pokud je osoba, která program na Internet vystavila natolik schopná, aby překonala ochranu, případně vytvořila program pro generování licenčních čísel, dá se předpokládat, že je schopná také vytvořit škodlivý program, který může být součástí instalační procedury. Zároveň jde ze strany osoby, která program instaluje, o spáchání trestného činu. [36]

5.2.4 Využívání platební karty

Platební karta a její využití v případě transakcí v rámci elektronických obchodů je pohodlný způsob jak ušetřit čas a většinou i peníze při nákupu zboží a služeb. Ne vždy jde ale o bezpečný způsob. [34]



Obr. 13 Využívání platební karty

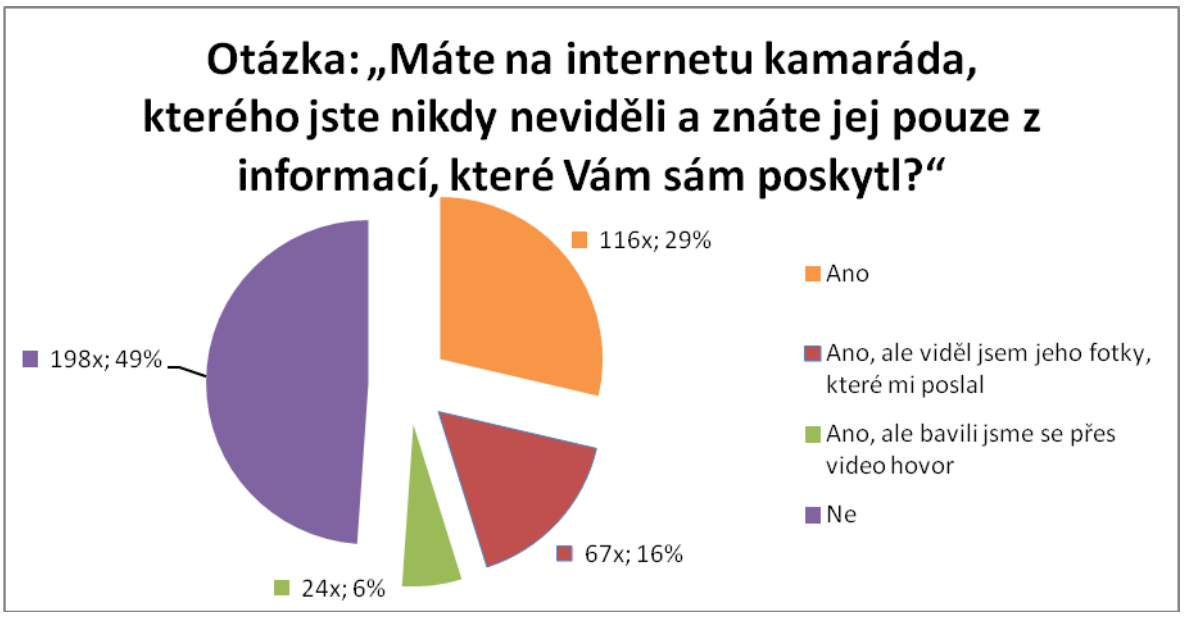
Na otázku odpovědělo 405 respondentů. 67 % respondentů uvedlo, že dopředu vůbec neplatí, nebo že platí, ale jen v prověřených obchodech. Celkem 33 % respondentů však uvedelo, že dopředu platí. Ve svém důsledku není důležité, zda platí kartou, nebo jinak. Účet na který byla platba doručena je sice Policií ČR dohledatelní v případě, že se jedná o spáchání trestného činu, doba vrácení zaplacené částky však může být značná a v případně platební neschopnosti pachatele k ní nemusí dojít vůbec. Vzhledem k množství zjištěných trestných činů a jejich stoupající tendenci, jak je popsáno v kapitole 4.4 je obezřetnost při elektronických platbách na místě.

5.3 Prevence proti sociálnímu inženýrství

K použití sociálního inženýrství tak, jak je popsáno v kapitole 2.3 je zapotřebí získání maxima informací o oběti. Tyto informace je možné zjistit buď přímo od cíle, nebo od jeho kamarádů a známých. Proto, aby bylo možné informace zjišťovat je ale nutné vědět, od jakých osob má útočník informace zjišťovat. Cílem tohoto bloku otázek bylo zjistit, jaké procento uživatelů usnadňuje útoky ze strany sociálních inženýrů poskytováním informací o svojí osobě.

5.3.1 Virtuální kamarádství

Kamarádství prostřednictvím počítačových sítí je neodstranitelnou součástí využívání sítě Internet. Tohoto však mohou využívat osoby páchající nejrůznější trestnou činnost. Zejména pokud se mohou skrývat za anonymitu Internetu.



Obr. 14 Virtuální kamarádství

Na otázku odpovědělo 405 respondentů. 49 % respondentů uvedlo, že nemá kamaráda, kterého by nikdy neviděli. 6 % uvedlo, že spolu komunikovali přes video hovor. Tento způsob není ideální, ale podvržení video hovoru by u pachatele již vyžadovalo vyšší snahu a prostředky. V rovině běžných uživatelů sítě Internet není předpokladatelné vyvinutí tak značného úsilí pachatele. Jedná se tak o jeden ze způsobů alespoň minimálního ověření uživatele na druhé straně komunikačního kanálu. Naproti tomu celkem 45 % respondentů prakticky neví s kým komunikují, protože vycházejí pouze z informací poskytnutých protistranou. Podvržení fotografie i například s umístěním nějaké známé osoby na fotografii je v dnešní době poměrně jednoduchou záležitostí.

5.3.2 Sdělování osobních údajů

Osobní údaje jsou zejména v oblasti sítě Internet velice zneužitelé. Čím více informací útočník získá, tím jednodušší je pro něj vydávat se za konkrétní osobu i před jeho kamarády. [35]

Obr. 15 Sdělování osobních údajů

Na otázku odpovědělo 405 respondentů. 41 % z nich, nikdy neuvedli ani své jméno s příjmením osobě, kterou by neznali. 59 % respondent však cizí osobě sdělilo jeden,

případně více osobních údajů. Uživatelé si v tomto případě zřejmě neuvědomují, že sdělení telefonního čísla může vést k obtěžujícím sms zprávám, nebo hovorům. Místo bydliště pak může sloužit například zloději k využití doby kdy nikdo není doma. Případně místo zaměstnání, nebo adresu školy může využít osoba s trpící nějakou duševní poruchou. Samostatnou kapitolou jsou pak uživatelé, kteří neznámé osobě sdělí heslo pro přístup k emailovému účtu. Není možné zajistit, aby útočník u tohoto účtu nezměnil heslo a nevydával se za vlastníka tohoto účtu.

5.3.3 Sdělování soukromých informací a diskreditujících materiálů

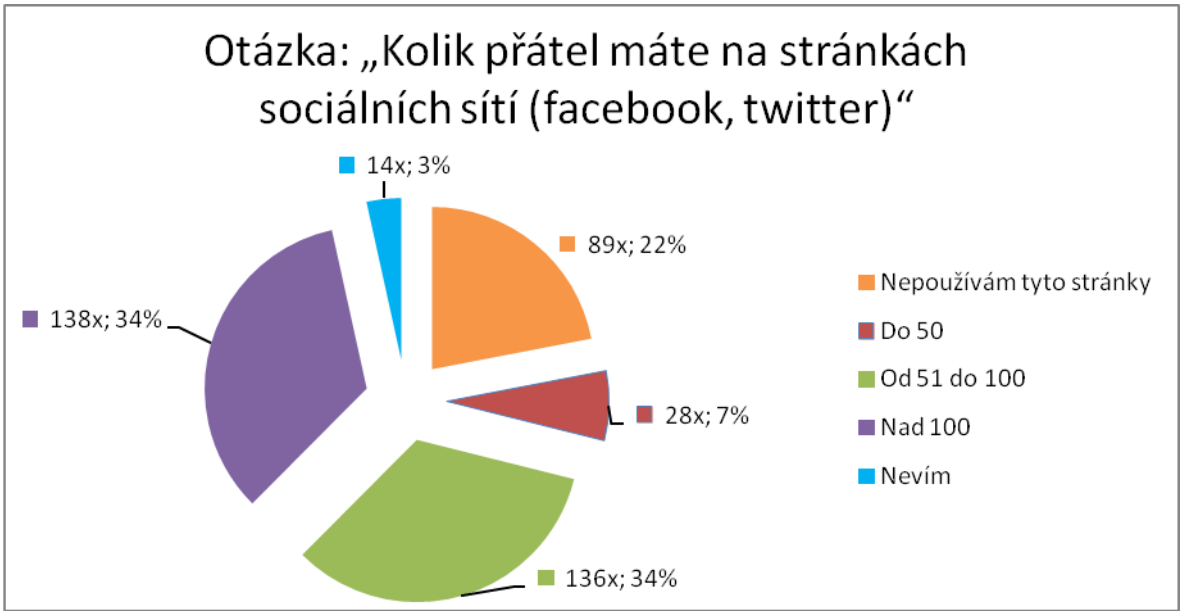
Soukromé a intimní informace jsou z pohledu útočníka přesně tím co hledá. Tyto informace je možné využít nejen proti osobě která je poskytla, ale je možné využít je i na přesvědčení dalších osob k tomu aby mylně uvěřili, že útočník je opravdu osobou za kterou se vydává. K tomuto tématu byly položeny dvě otázky:

1. „Sdělil jste někdy soukromou informaci kterou jste nechtěl aby se dozvěděl někdo další osobě, kterou znáte jen z Internetu?“
2. „Zaslal jste někdy jiné osobě vaše erotické, nebo zesměšňující fotografie, nebo video?“

Možné odpovědi byly: Ano; Ano, ale jen člověku, který mě osobně nezná; Ne. Na obě otázky odpovědělo 399 respondentů. Záporně odpovědělo 74 % (295) respondentů u první a 82 % (332) u druhé otázky. Z uvedeného tedy plyne, že 26 % respondentů v případě soukromých informací a 18 % respondentů v případě zesměšňujících, nebo intimních materiálů tyto posykytlo další osobě. Není přitom podstatné zda se osobně znají či nikoliv. Pokud odesílatel nezná adresáta, není nikdy možné zaručit, že tento vztah je pravdivý i opačně. Zároveň se jedná o informace u nichž je nebezpečí zneužití výrazně vyšší.

5.3.4 Množství přátel na sociálních sítích

Sociální sítě jsou místem, kde komunikuje značné množství lidí. Zároveň se ale jedná o místo, které je z pozice útočníka značným zdrojem informací.



Obr. 16 Množství přátel na sociálních sítích

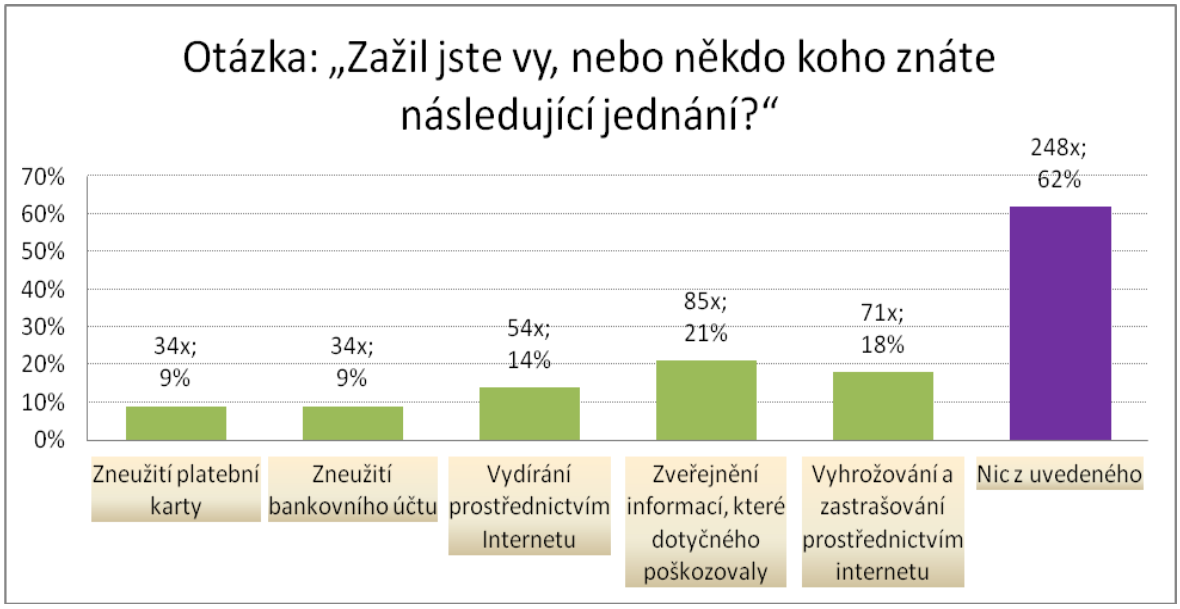
Na otázku odpovědělo 405 respondentů. 22 % z nich, stránky sociálních sítí nepoužívají. 7 % má do 50 přátel. Do tohoto počtu se ještě může jednat o osoby, které uživatel přímo, nebo prostřednictvím dalších osob zná. 34 % uživatelů má více než 50 a méně než 100 přátel. V tomto případě má již útočník práci značně ulehčenou, protože z uvedeného množství osob lze získávat informace po menších částech, aniž by vzbuzoval větší podezření. Dalších 34 % respondentů pak uvedlo, že má více než 100 přátel, což je značné množství a útočník tak může informace i ověřovat od dalších osob. Zároveň pro útočníka je usnadněna i možnost stát se přítelem oběti bez zjišťování velkého množství informací.

5.4 Protiprávní jednání

Protiprávní jednání v rámci kybernetické kriminality zahrnuje značné množství rozmanitých činů, jak bylo popsáno v teoretické části práce. Protože byl dotazník realizovaný anonymní formou lze předpokládat, že respondenti neměli potřebu uvádět nepravdu. Cílem tohoto bloku otázek bylo zjistit, jaké je reálný stav páchání distančních deliktů, jaké mají respondenti zkušenosti s kybernetickou kriminalitou a jak ji vnímají, ať už jako oběti, nebo pachatelé a zároveň jak vnímání protiprávnosti konkrétních skutků.

5.4.1 Trestné činy z pohledu obětí

Spáchané trestné činy nejsou vždy předmětem šetření Policie ČR. Důvodů je několik. Může jít o neznalost trestního zákoníku ze strany poškozeného, strach před reakcí ostatních osob, případně strach z pachatele. Otázka slouží pro dotvoření představy o situaci v oblasti páchání trestných činů.

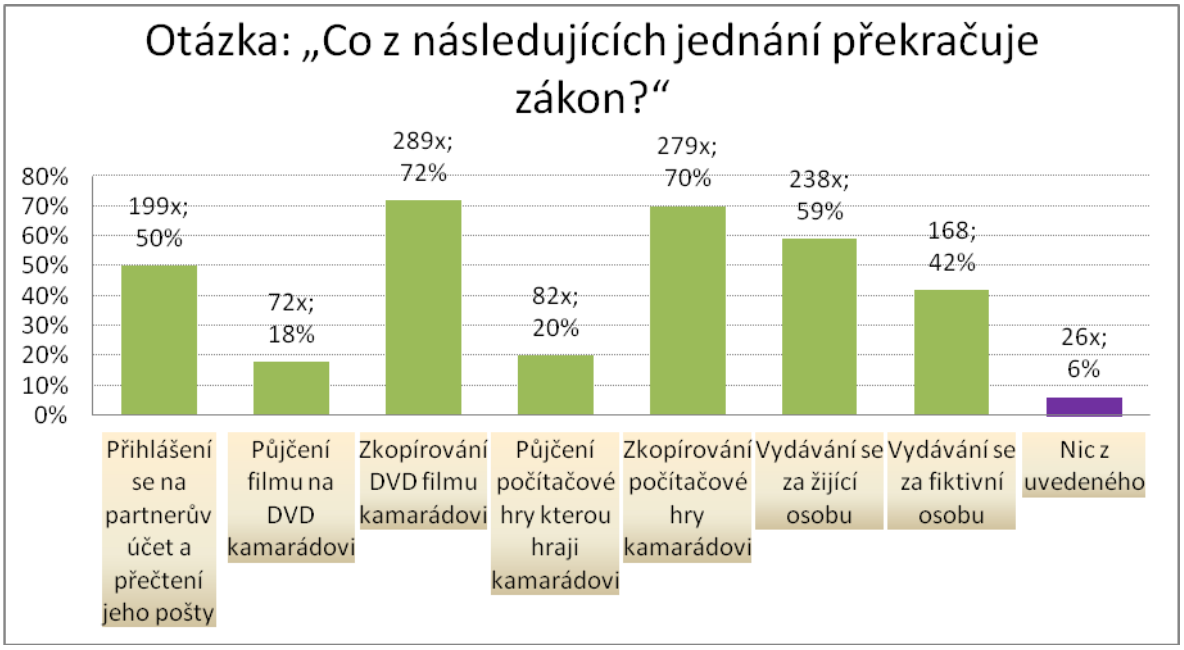


Obr. 17 Trestné činy z pohledu oběti

Uživatelé mohli vybrat více než jedno zaškrtávací políčko, takže procento může vzrůst na více než 100 %. Na otázku odpovědělo 399 respondentů. Z grafu je patrné, že 38 % respondentů se setkalo s jedním, nebo s více uvedenými činy. První tři činy, které jsou v grafu uvedeny jsou trestnými činy. U druhých dvou se pak bude jednat o trestný čin v případě splnění určitých okolností, například způsob získání informace, případně forma a způsob zastrašování.

5.4.2 Znalosti protiprávního jednání

Neznalost zákonů není důvodem pro netrestání pachatele. Proto byla poslední otázka v dotazníku zaměřena na znalost a informovanost uživatelů o protiprávních činech. [37]



Obr. 18 Znalosti protiprávního jednání

Uživatelé mohli vybrat více než jedno zaškrtávací políčko, takže procento může vzrůst na více než 100 %. Na otázku odpovědělo 405 respondentů. Poměrně zajímavým zjištěním je, že 6 % respondentů nepovažuje žádné uvedené jednání za překračující zákon. Vyjma možnosti půjčení filmu na DVD může být každé jednání trestné. V ostatních případech se vždy může jednat o protiprávní jednání, někdy však za předpokladu splnění další podmínky, jakou je například při vydávání se za fiktivní osobu uzavření smlouvy. Dalším zajímavým zjištěním u této otázky byla skutečnost, že pouze 20 % respondentů považovalo půjčení počítačové hry s licenčním klíčem další osobě za překračující zákon. Pokud je hra nainstalovaná a uživatel ji spolu s licenčním číslem půjčí další osobě, jedná se o další šíření a tedy protizákonné jednání.

6 NÁVRHY NA ZLEPŠENÍ ZAJIŠTĚNÍ DAT S PREVENTIVNÍMI OPATŘENÍMI

Návrhy na zlepšení zajištěných dat s preventivními opatřeními se dají rozdělit do tří skupin. První skupinou jsou návrhy na úpravy předpisů v rámci státu a státních orgánů. Podkladem pro návrhy jsou závěry z kapitoly 4 této práce. Druhá skupina vychází z kapitoly 5, kde je uvedeno rizikové chování osob. Preventivními opatřeními

Návrhy a prevence. U prevence se zaměřením na podvod uvést v rámci ověření bezpečnostních opatření zjištěný podvodný eshop s tím, že OČTŘ (OHK Středočeského kraje) byl zaslán poznatek a ve věci bylo zahájeno prověřování dle tr.ř.

6.1 Návrhy na úpravy předpisů v rámci státu a státních orgánů

Z hlediska páchání kybernetické kriminality dochází k nárůstu spáchaných distančních trestných činů. Nelze očekávat, že by se tento trend mohl v nejbližší době změnit. Zároveň je patrné, že zásahem Ústavního soudu České republiky došlo k poklesu objasněnosti u většiny sledovaných trestných činů. Z uvedeného tedy vychází závěr, že pro efektivní boj proti počítačové kriminalitě je zapotřebí realizace nejméně 2 bodů.

6.1.1 Změna zák. č. 127/2005 Sb. o elektronických komunikacích

Návrh: Změna zákona č. 127/2005 Sb. o elektronických komunikacích a doplnění o příslušnou vyhlášku o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. Těmito předpisy stanovit jakým způsobem budou uchovávány a předávány provozní a lokalizační údaje. V rámci odůvodnění Nálezu Ústavního soudu České republiky jsou uvedeny vytýkané skutečnosti, jež je třeba zohlednit v případě doplnění zákona.

Předpokládaný důsledek: Zvýšení objasněnosti páchaných distančních deliktů.

6.1.2 Doplnění zákona č. 40/2009 Sb. Trestního zákoníku

Návrh: Doplnění zákona č. 40/2009 Sb. o trestný čin zahrnující poskytnutí přístupu k elektronickému bankovnictví cizí osobě. Trestný čin by měl zahrnovat jednání, kdy zakladatel účtu poskytne dispozici s účtem další osobě bez vědomí banky. Jedná se o formy dálkového přístupu k účtům.

Předpokládaný důsledek: Zvýšení objasněnosti a zejména zvýšení podílu odsouzených pachatelů trestného činu podvod páchaném distanční formou.

6.1.3 Přijetí Zákona o kybernetické bezpečnosti

Návrh: Ukončení a vyhodnocení připomínkového řízení a přijetí zákona o kybernetické bezpečnosti.

Předpokládaný důsledek: Stanovení a možná vynutitelnost zajištění bezpečnostních standardů, které bude nutné dodržovat. Zároveň dojde ke snížení rizik a k rychlejšímu předávání informací o aktuálních hrozbách.

6.1.4 Vytvoření specializovaných pracovišť v rámci Policie ČR pro vyšetřování kybernetické kriminality

Návrh: V rámci každého územního odboru Policie ČR zřídit vyčlenit specializovaná pracoviště pro vyšetřování informační kriminality.

Předpokládaný důsledek: Protože kybernetická kriminalita zasahuje do oblasti obecné i hospodářské kriminality, nejsou pro vyšetřování těchto skutků stanoveni specialisté a tyto skutky řeší různí vyšetřovatelé, kteří nejsou vyškoleni pro danou problematiku. Došlo by k zefektivnění práce a zrychlení vyšetřování.

6.1.5 Zapracování informací o bezpečnostních hrozbách a kybernetické kriminalitě do školních osnov

Návrh: Do školních předmětů zabývajících se výukou informatiky a počítačů zapracovat pasáže o bezpečnostních hrozbách a nebezpečích kybernetické kriminality s možnostmi preventivních opatření ze strany uživatelů.

Předpokládaný důsledek: Zvýšení informovanosti žáků škol o hrozících nebezpečích a minimalizaci jejich výskytu, případně důsledků. S tím související snížení počtu spáchaných trestných činů, nebo snížení následků spáchaných činů.

6.2 Návrhy na snížení rizikovosti chování uživatelů

V kapitole 5 práce jsou uvedeny způsoby chování uživatelů počítačů a rizika z jijich chování vyplývající. Shrnutím zjištěných skutečností je možné dojít k závěru, jaké minimální bezpečnostní požadavky by měli uživatelé dodržovat:

- Používání nejnovějších verzí programů s pravidelnými aktualizacemi

- Používání aktualizovaných antivirových programů
- Nepoužívat programy získané z neznámých zdrojů
- V případě bezdrátových připojení používat nejvyšší možné způsoby šifrování přenášeného signálu
- Za kamarády považovat pouze osoby, které uživatel zná i jinak než přes Internet
- Na Internetu uvádět minimum údajů o svojí osobě
- Nikdy nesdělovat žádné údaje ani informace soukromého, nebo intimního charakteru jiné osobě
- Při doručení souborů, nebo odkazů emailovou zprávou tyto neotvírat a nepoužívat
- Při placení na Internetu platit dopředu jen u prověřených obchodníků, případně po doručení objednaného zboží, či služby

6.3 Preventivní opatření

Jak je uvedeno v předchozích částech práce, uživatelé sami mohou svým chováním podstatně snížit nebezpečí spáchání trestného činu, případně alespoň zmírnit jeho následky. Vhodným příkladem pro ukázku možného předcházení vzniku škod z páchané trestné činnosti je trestný čin podvod páchaný prostřednictvím elektronického obchodu. Tento trestný čin je pro pachatele lákavým z důvodu, že může získat značné finanční prostředky bez vynaložení přílišného úsilí. Z uvedeného však zároveň plyne, že pachatelé se mohou dopouštět podobných chyb, nebo alespoň jednat podobným způsobem. Klasický elektronický obchod je velmi jednoduchý a pohodlný způsob k objednávání a nakupování jakéhokoliv zboží prostřednictvím Internetu z domova. Objednávka se provádí elektronicky, formou vyplnění formuláře a může být realizována po zaregistrování se mezi klienty obchodu. Další komunikace mezi klientem a prodejcem probíhá zpravidla emailem. Platba za zboží probíhá různými způsoby, předem platbou na účet eshopu, vkladem na účet, platební kartou, nebo při převzetí zboží na dobírku.

Podvodný obchod pachatel založí s úmyslem vylákat z poškozených platbu a nic jim nedodat. Spojujícím faktorem podvodných obchodů je v drtivé většině případů požadavek platby předem a absence ověřitelných kontaktních údajů.

Z pohledu uživatele je možné ověřit určité informace, které mohou vést k závěru, že se skutečně jedná podvodný obchod.

Jedna z prvních indicií vedoucích k podezření, že se jedná o podvodný obchod je cena zboží nižší, než u srovnatelných obchodů.

Prvotní informací jsou kontakty, sídlo a pobočky, případně majitele obchodu. Pokud není možné osobní ověření konkrétní adresy, lze na Internetu vyhledat uvedenou adresu a zjistit, zda se na zadané adrese může nacházet sídlo obchodu. Vhodné jsou mapy, které zobrazují i fotografie konkrétních budov. Lze tak zjistit i sídla dalších společností telefonicky se na existenci obchodu dotázat. Pokud adresa neexistuje, nebo vyhledaný objekt evidentně nemůže být sídlem obchodu (pole, polorozpadlý dům…), jde o další signál, že se jedná o podvod.

Dalším signálem může být neexistence telefonního spojení nebo pouze kontakt na mobilní telefon. Seriózní a zavedené obchody se svými klienty komunikují i telefonicky, mají většinou v kontaktech uvedeny pevné linky a mohou mít i kamenné pobočky či místa k osobnímu vyzvednutí zboží.

V případě, že je u způsobu doručení zboží uvedena přepravní firma, lze se i zde dotázat, zda firma existuje, je ale možné, že odpověď nebude možné získat s ohledem na obchodní tajemství a ochranu klientů.

V rejstříku firem http://www.info.mfcr.cz/ares je možné prověřit místo podnikání a jaké jsou vydané povolení k podnikání a srovnat je s nabízeným zbožím, nebo službou.

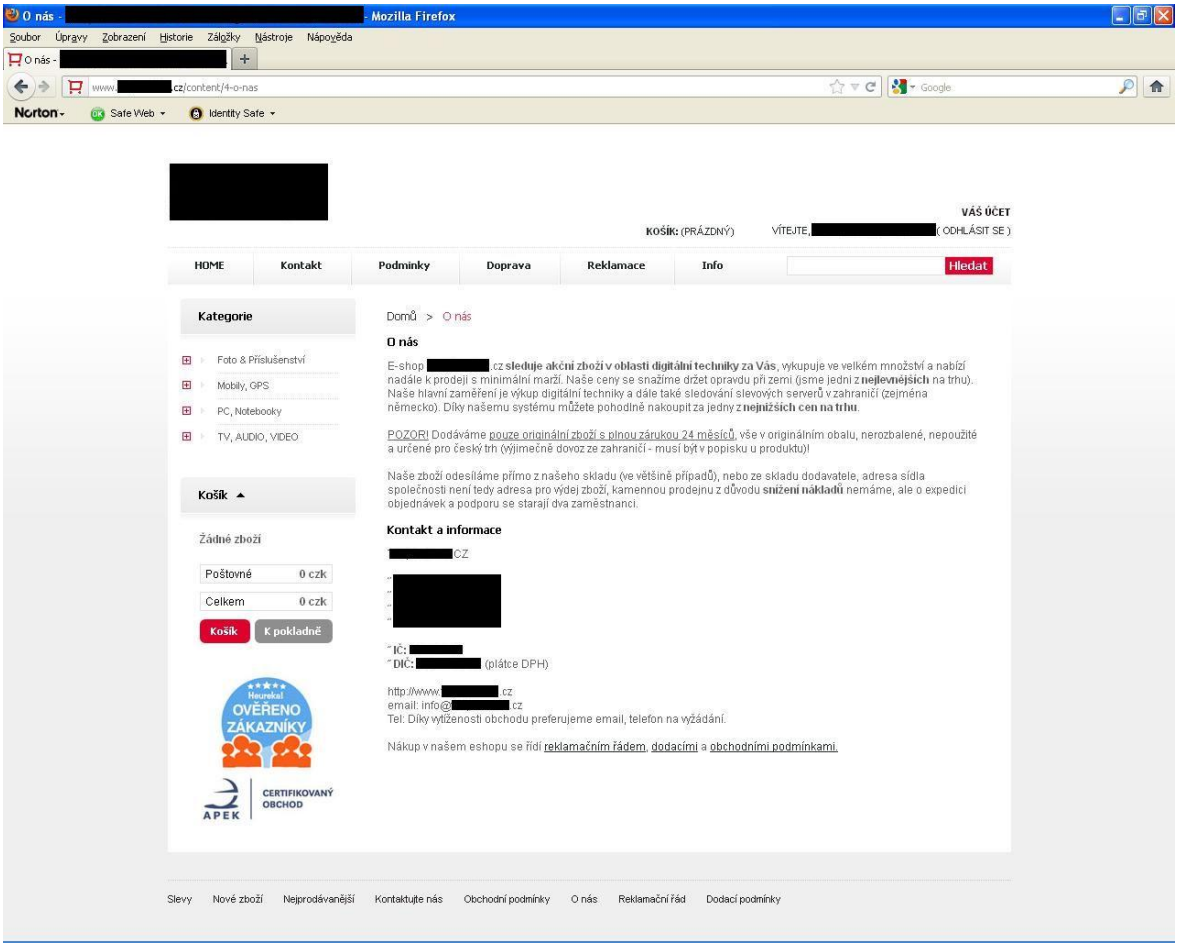
Důležitým prvkem jsou také různé diskuse na Internetu, kde se poškození domlouvají na postupu proti podvodníkům.

Dalším signálem o nižší důvěryhodnosti obchodu je doba od registrace domény. Na adrese http://www.nic.cz/ lze ověřit národní domény (přípona .cz). Zde je možné zjistit držitele domény a jejího registrátora.

Uvedeným způsobem je možné alespoň snížit nebezpečí zaslání peněz podvodníkovi.

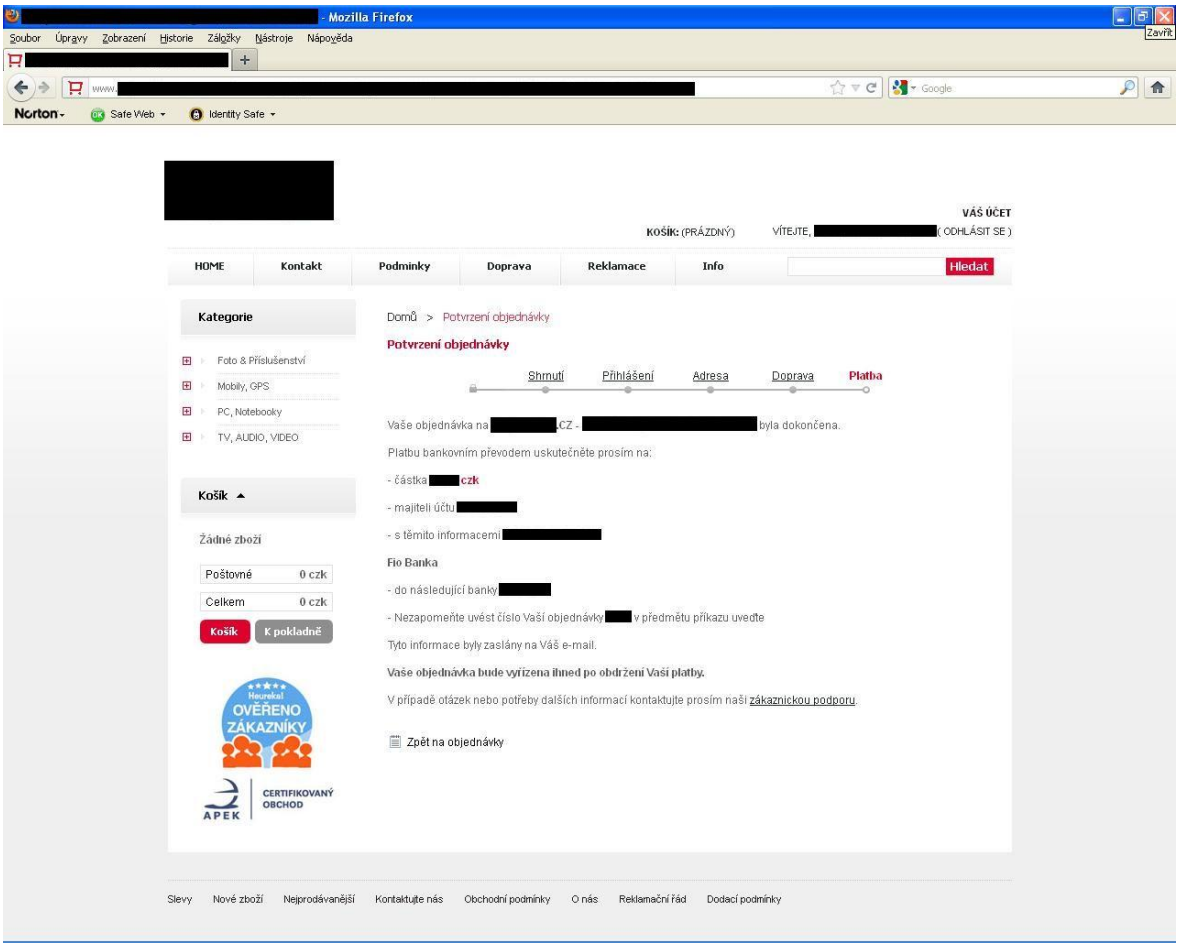
Při přípravě příkladu bylo na síti Internet zadáno vyhledání mobilního telefonu konkrétní značky a typu. Obchod, ve kterém byl zjištěn telefon za nejnižší cenu měl jako provozovatele uvedenou společnost zabývající se výrobou hutního materiálu. Z kontaktních údajů měl vyjma informací o firmě uvedený pouze email na stejné doméně

jako obchod a telefon měl být sdělen po přihlášení. Po registraci a přihlášení byla zobrazena pouze další zpráva, že telefon je na vyžádání.



Obr. 19 Stránka s kontaktními informacemi

V obchodních podmínkách obchodu byla jako způsoby platby uvedena i možnost platby na dobírku, při objednávce však tato možnost již nabídnuta nebyla.



Obr. 20 Informace o požadované paltbě

Kontrolou domény bylo zjištěno, že tato byla registrována 42 dní před dnem, kdy byl nákup prováděn. Jako registrující osoba byl uveden muž s adresou, s neexistující kombinací města a ulice.

Vzhledem k uvedenému byl na oddělení Policie ČR, kde je dle adresy sídlo společnosti, zaslán poznatek k prověření. Dle zprávy na základě požadovaného vyrozumění jsou ve věci prováděny úkony trestního řízení.

ZÁVĚR

Kybernetická kriminalita, její vyšetřování a boj proti ní, je v současné době stále opomíjeným tématem. Kybernetické kriminalitě není věnována dostatečná pozornost ani uživateli počítačů a sítí, státními institucemi, ale ani zákonodárci. Počty spáchaných činů a škody takto vzniklé mají stále vzestupnou tendenci. Pachatelé, jejich znalosti, metody a prostředky jsou často na výrazně vyšší úrovni, než znalosti, metody a prostředky orgánů činných v trestním řízení.

Cílem mojí diplomové práce bylo upozornit na nejčastější způsoby páchání distančních deliktů v rámci počítačové kriminality s rozborem těchto deliktů, ukázání způsobů jakými uživatelé Internetu usnadňují práci pachatelům a nastínění možných způsobů jak alespoň částečně minimalizovat následky těchto trestných činů.

Teoretická část práce byla věnována seznámení se základními pojmy vážícími se k oblasti Internetu a kybernetické kriminality a dále k rozboru skutkových podstat jednotlivých trestných činů, které jsou nejčastěji páchány distančním způsobem.

Praktická část je rozdělena na tři části. V první jsou analyzovány statistiky a výstupy z evidencí Policie ČR vztahující se k distančním deliktům páchaným v prostředí Internetu. Cílem této části bylo podat ucelený přehled o vývoji této problematiky za dobu platnosti zákona č. 40/2009 trestního zákoníku. Z vývoje páchání trestných činů a jejich objasněnosti je zřejmé, že při šetření některých trestných činů není postup orgánů činných v trestním řízení dostatečně efektivní. V druhé části jsou vyhodnocena data získaná prostřednictvím dotazníku, ve kterém odpovídalo celkem 405 respondentů různého pohlaví, věku a bydliště, na otázky vztahující se k distančním deliktům v rámci počítačové kriminality a k rizikovosti chování uživatelů počítačů na síti Internet. Ze závěrů této části se dá hodnotit chování uživatelů za velice rizikové a je zřejmé, že si někteří uživatelé stále neuvědomují, jaké důsledky může jejich chování mít. Ve třetí části jsou uvedeny návrhy na úpravy předpisů, snížení rizikovosti chování uživatelů a uvedení preventivních opatření, konkrétně proti pachatelům trestného činu podvod. V rámci této části při ověřování navržených preventivních opatřeních byl zjištěn elektronický obchod, jehož provozovatel je na základě zjištěných skutečností v současné době prověřován Policií ČR pro podezření ze spáchání trestného činu.

Zhodnocením všech shromážděných dat je možné ustanovit největší nebezpečí umožňující páchání kybernetické kriminality, jímž je samotný uživatel, který často nedodržuje ty nejzákladnější bezpečnostní opatření.

Závěrem bych chtěl uvést, že ze získaných dat a také z důvodu závěrečné pasáže praktické práce, které vedlo ke zjištění podezřelého elektronického obchodu jsem přesvědčen, že dodržováním bezpečnostních opatření je možné ze strany uživatelů pachatelům trestných činů práci pokud ne znemožnit, tak alespoň značně ztížit a cíle práce tak považuji za splněné.

ZÁVĚR V ANGLIČTINĚ

Cyber crime and its investigation and fight against it is currently still neglected topic. Computer users, networks, government agencies, but even legislators don't pay sufficient attention to Cyber Crime. Number of crimes committed and the resulting damages are still an upward trend. The offenders, their knowledge, methods and resources are often on significantly higher level than the knowledge, methods and means of law enforcement proceedings.

The aim of my thesis was to highlight the most common ways of committing distance crimes within the cybercrime with the analysis of these offenses, showing ways in which Internet users can facilitate the work of perpetrators and outline possible ways how to at least minimize the effects of some of these crimes.

The theoretical part was devoted to familiarization with the basic concepts of binding to the Internet and cyber crime and to analyze the facts of the individual crimes that are most often committed by distance means

The practical part is divided into three parts. Firstly the statistics are analyzed and the outcomes of police records relating to offenses committed in the distance over the Internet. The aim of this section was to provide an overview of the development of this issue for the duration of the Act No. 40/2009 of the Penal Code. The development of offending and their detection is clear that the procedures of law enforcement are not effective enough in investigation of certain crimes. Secondary the data collected through a questionnaire is evaluated, this equates to a total of 405 respondents of different gender, age and residence, issues relating to offenses within the distance computer crime and risk behavior of computer users on the Internet. The conclusions of this section could evaluate user behavior as very risky and it is clear that some users are still unaware of the consequences of their behavior can have. The last section provides suggestions for regulatory changes, to reduce the risk of user behavior and implementing preventive measures especially against perpetrators of fraudulent crime. When verifying proposed preventive measures within this section, an online shop was found, which operator based on established facts is currently reviewed by the Police on suspicion of committing a crime.

Evaluation of all collected data established that the greatest risk of committing cyber crime, is a user itself, who often does not follow the most basic security measures.

Finally, I would like to state that the data obtained and the practical work led to the detection of the suspicious e-commerce, it is my belief, that keeping the security measures, it is possible for users perpetrators of to commit offences however considerably more difficult and the goals of the work consider to be satisfied.

SEZNAM POUŽITÉ LITERATURY

[1]Wikileaks [online]. [cit. 2012-04-25]. Dostupné z: http://www.wikileaks.org/

[2]World Internet Usage Statistics News and World Population Stats. [online]. 2012 [cit. 2012-04-14]. Dostupné z: http://www.Internetworldstats.com/stats.htm

[3]CESNET: Historie národní sítě pro vědu, výzkum a vzdělávání [online]. [cit. 2012-04-04] Dostupné z: http://www.cesnet.cz/doc/historie.html

[4]CSIRT – FAQ [online]. [cit. 2012-04-07] Dostupné z: http://csirt.cz/page/885/faq/#cojecert

[5]CSIRT - O nás [online]. [cit. 2012-04-07]. Dostupné z: http://csirt.cz/page/882/o-nas/

[6]BOUŘA, Václav. Vybraná témata z kriminologie. Vyd. 1. Ostrava: Ostravská univerzita v Ostravě, Pedagogická fakulta, 2007, 105 s. ISBN 978-80-7368-309-2.

[7]SVATOŠ, Roman. Kriminologie ve světle nového trestního zákoníku. Vyd. 1. České Budějovice: Vysoká škola evropských a regionálních studií, 2010, 174 s. ISBN 9788086708218.

[8]JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[9] MATĚJKA, Michal. Počítačová kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Vyd. 1. Praha: Computer Press, 2002, 106 s. ISBN 80-722-6419-2.

[10]PORADA, Viktor a Roman RAK. Kriminalita související s informačními a komunikačními technologiemi a identifikace osob na základě projevu lokomoce člověka: (vybrané problémové okruhy výzkumu). Vyd. 1. Karlovy Vary: Vysoká škola Karlovy Vary, 2007, 261 s. ISBN 978-80-254-0797-4.

[11] Statistiky - kriminalita|archiv stranek mvcr.cz, cerven 2008 [online]. 2008 [cit. 2012-04-12]. Dostupné z: http://aplikace.mvcr.cz/archiv2008/statistiky/krim_stat/2000/index.html

[12] SOOM.cz - Robert Trappan Morris [online]. 2007 [cit. 2012-04-2]. Dostupné z: http://www.soom.cz/index.php?name=recenze/show&aid=297

[13] Galerie nejlepších hackerů historie - 12. díl | PC World.cz [online]. 2008 [cit. 2012-04-25]. Dostupné z: http://pcworld.cz/ostatni/galerie-nejlepsich-hackeru-historie-12-dil-3475

[14] MITNICK, Kevin a Roman RAK. Umění klamu: (vybrané problémové okruhy výzkumu). Vyd. 1. Gliwice: Helion, 2003, 348 s. ISBN 8373612106.

[15] Počítačová kriminalita - Policie České republiky [online]. [cit. 2012-03-19]. Dostupné z: http://www.policie.cz/clanek/pocitacova-kriminalita.aspx

[16] Czech Republic Internet Usage and Telecommunications Report [online]. 2010 [cit. 2012-04-22]. Dostupné z: http://www.Internetworldstats.com/eu/cz.htm

[17] CRAIG, Paul P a Ron HONICK. Softwarové pirátství bez záhad. 1. vyd. Překlad Tomáš Hlaváč. Praha: Grada, 2008, 212 s. ISBN 978-80-247-1765-4.

[18] Nejen DDoS: Anonymous se povedlo ovládnout web ODS | Cnews.cz [online]. 2008 [cit. 2012-04-23]. Dostupné z: http://www.cnews.cz/nejen-ddos-anonymous-se-povedlo-ovladnout-web-ods

[19] HOAX | Hoax | Co je to hoax [online]. [cit. 2012-04-22]. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax

[20] SZOR, Peter. Počítačové viry: analýza útoku a obrana. Vyd. 1. Brno: Zoner Press, 2006, 608 s. ISBN 80-868-1504-8.

[21] FOSTER, James C. Hacking - Buffer Overflow: [zneužití, detekce a prevence]. 1. vyd. Praha: Grada, 2007, 348 s. ISBN 978-80-247-1480-6.

[22] NEWMAN, Robert C. Computer security: protecting digital resources. Sudbury: Jones and Bartlett Publishers, c2010, 453 s. ISBN 978-0-7637-5994-0.

[23] JAMES, Lance. Phishing bez záhad. 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

[24] ERICKSON, Jon. Hacking: umění exploitace. 2., upr. a dopl. vyd. Překlad Jan Pokorný. Brno: Zoner Press, 2009, 544 s. ISBN 978-80-7413-022-9.

[25] E-BEZPEČÍ - SMS Spoofing: Skutečně jen vtip? [online]. 2008 [cit. 2012-04-25]. Dostupné z: http://cms.e-bezpeci.cz/content/view/48/63/lang,czech/

[27] VANTUCH, Pavel. Trestní zákoník s komentářem: komentář k zákonu č. 40/2009 Sb., ve znění pozdějších předpisů : informace z judikatury : k 1.8.2011. 1. vyd. Překlad Jan Pokorný. Olomouc: ANAG, 2011, 1367 s. ISBN 978-80-7263-677-8.

[28] JELÍNEK, Jiří. Trestní právo hmotné: obecná část, zvláštní část. 2. vyd. Překlad Jan Pokorný. Praha: Leges, 2010, 904 s. Student (Leges). ISBN 978-80-87212-49-3.

[29] GŘIVNA, Tomáš. Trestní právo hmotné: obecná část, zvláštní část. 2., aktualiz. vyd. Překlad Jan Pokorný. Praha: Wolters Kluwer Česká republika, 2010, 311 s. Student (Leges). ISBN 978-807-3575-090.

[30] TELEC, Ivo a Pavel TU . 1. vyd. Překlad Jan Pokorný. V Praze: C.H. Beck, 2007, 971 s. Student (Leges). ISBN 80-717-9608-5.

[31] Kriminalita - Policie České republiky [online]. 2012 [cit. 2012-04-25]. Dostupné z: http://www.policie.cz/statistiky-kriminalita.aspx

[32] Ústavní soud - Ústavní soud zrušil část zákona o elektronických komunikacích [online]. [cit. 2012-04-16]. Dostupné z: http://www.concourt.cz/clanek/5068

[33] JIROVSKÝ, Václav a Pavel TUMA. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Překlad Jan Pokorný. Praha: Grada, 2007, 284 s. Student (Leges). ISBN 978-802-4715-612. [34]978-802-4717-654

[35] ONDREJKA, Viliam. Podvody na internetu: o peníze můžete velmi rychle přijít nebo je podvodem velmi snadno získat. České Budějovice: Nová Forma, 2010, 55 s. ISBN 978-808-7313-824.

[36] ROGERS, Vanessa. Kyberšikana: pracovní materiály pro učitele a žáky i studenty. Vyd. 1. Překlad Ondřej Vágner. Praha: Portál, 2011, 97 s. ISBN 978-807-3679-842.

[37] JANSA, Lukáš a Petr OTEVŘEL. Softwarové právo: praktický průvodce právní problematikou v IT. Vyd. 1. Překlad Ondřej Vágner. Brno: Computer Press, 2011, 340 s. ISBN 978-80-251-3458-0.

[38] KALAMÁR, Štěpán a Josef POŽÁR. Vybrané aspekty informační bezpečnosti: praktický průvodce právní problematikou v IT. Vyd. 1. Překlad Ondřej Vágner. Praha: Policejní akademie České republiky v Praze, 2010, 190 s. ISBN 978-80-7251-339-0.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APRANET	Advanced Research Projects Agency Network..
Č.	Číslo
Čl.	Článek
ČVUT	České vysoké učení technické.
EARN	Evropské akademické a výzkumné sítě.
FAQ	Často kladené dotazy.
FBI	Federální úřad pro vyšetřování
IP	Internetový protokol.
ODS	Občanská demokratická strana
Sb..	Sbírka
SMS	Služba krátkých textových zpráv.
TZ	Trestní zákon.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK