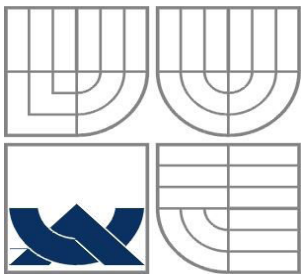


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY


FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY
FACULTY OF BUSINESS AND MANAGEMENT
DEPARTMENT OF INFORMATICS

# KRIMINALITA NA INTERNETU
INTERNET CRIMINALITY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR
SANDRA REICHMANNOVÁ

VEDOUCÍ PRÁCE
SUPERVISOR
JUDr. TOMÁŠ SOUKUP, BA

BRNO 2007

## Abstrakt bakalářské práce

Tato práce se pokouší zmapovat problém internetové kriminality ve světě a v České republice. Popisuje jednotlivé druhy kriminality, které lze provádět přes internet a pomocí počítačů. Cílem práce je seznámení s touto činností a s výsledky získanými na základě dotazníku.

## Abstract

The bachelor thesis strives for charting the problem of internet criminality in the world and in Czech Republic. It is relating criminality, what is done by internet and computer. The goal of this paper work is the identification with this activity and the conclusions based on the questionnaire.

## Klíčová slova

Internet, počítač, kriminalita, zákon, právo

## Key words

Internet, computer, criminality, law, justice

## Bibliografie

REICHMANNOVÁ, Sandra. *Kriminalita na internetu.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2008. 55 s. Vedoucí bakalářské práce JUDr. Tomáš Soukup.

## Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 30. dubna 2008

---

Podpis

# Obsah

# 1 Úvod

V dnešní době se s informačními technologiemi setkáváme na každém kroku. Pronikly snad do všech odvětví výroby, obchodu, komunikace nebo zábavy. Tento rychlý rozvoj s sebou přinesl ale i negativní stánky. Vznikl tak nový druh kriminality, který byl před pár lety ještě úplně neznámý. V posledních letech tak počítačová a internetová kriminalita zažívá velký rozmach. Děje se tak díky anonymitě, kterou pachatelům poskytuje internet. Ti proto vyhledávají pro své útoky taková místa, kde je velmi obtížné někoho vystopovat. Volí tak různé internetové kavárny, školy, úřady a mnoho dalších míst.

Člověk je stále závislejší na bezchybném fungování informačních technologií, a tudíž roste společenský požadavek na ochranu těchto technologií před zločinci. Tento požadavek je o to významnější, že počítačová kriminalita je stále více spojována s organizovaným zločinem.

V České republice není zákon, který se přímo věnoval počítačové nebo internetové kriminalitě. Tento pojem není ani v legislativě definovaný, ale existuje více různorodých pojetí, podle toho, z jakého hlediska se autoři na problém dívají. Počítačovou kriminalitu je třeba chápat jako specifickou trestnou činnost, kterou je možné spáchat pomocí výpočetní techniky a internetu. Počítačovou kriminalitou můžeme označit i trestné činy, kdy je výpočetní technika předmětem trestného činu.

Pod pojmem internetová kriminalita se skrývá několik oblastí, jsou to: urážky, oslavování a propagace násilí, politický extremismus, podvody, pornografie, elektronický obchod a praní peněz, vydírání, sabotáže, špionáže, nekalá soutěž, loterie a hazardní hry, porušování autorského práva, dokonce i ublížení na zdraví a usmrcení.

Cílem práce je poskytnout přehled o možné kriminalitě na internetu v České republice i ve světě. Zároveň bych chtěla ukázat stav na konkrétních případech a seznámit s výsledky dotazníku provedeného na Podnikatelské fakultě. Cílem práce je i navržení možných opatření, které by mohly vést ke zlepšení stávajícího stavu.

# 2 Internet

## 2.1 Co je to internet

Internet je největší světová počítačová síť, která propojuje všechny rozvinuté země dnešního světa. Její význam je v dnešní době obrovský a neustále roste a rozvíjí se. Internet tak v dnešní době umožňuje okamžitou komunikaci s kýmkoli a kdekoli na světě.

## 2.2 Internet z právního hlediska

V první řadě byla věnována pozornost internetu především z hlediska jeho technické a programátorské stránky. Až pozdější úvahy směřovaly směrem futurologickým a filozofickým. Právní stránka je z celkového objemu a globálního dosahu internetu okrajovou otázkou tohoto masového média. Z pohledu kriminální prevence je však tato otázka velmi důležitá.

Internet jako takový sám o sobě není subjektem práva. Právně neexistuje a nemůže nabývat práv a ani se zavazovat. Internet není ani věcí, tedy hmotným předmětem, jak je chápáno v základních právních normách. (§118 ObčZ.). „Internet není ani čistě nehmotným statkem, tj. právem nebo jinou majetkovou hodnotou – např. informací.“ (SMEJKAL, 2001 str. 17)

„Jedná se o složitý informační systém, který se skládá ze všech výše uvedených komponent, tj. z různých subjektů práva: lidí a organizovaných sdružení lidí (právnických osob) včetně státu, dále z majetku tj. věcí, práv a jiných majetkových hodnot.“ (SMEJKAL, 2001 str. 18)

To že Internet nemá žádného majitele, nám do určité míry znesnadňuje schopnost vnímat odpovědnost za to, co se na internetu odehrává. Každý ví, že v obchodě se krást nemá. Jinak je to ale v případě internetu. Tady jaksi chybí povědomí o tom, co se smí a co ne. Málokdo vidí za daty, které získá z internetu, nějakého vlastníka nebo autora. Všichni víme, že pokud přijdeme do obchodu s CD a DVD nosiči, tak za ně v případě koupě musíme zaplatit. To ovšem na internetu v dnešní době moc neplatí.

## 2.3 Historie internetu

**1969 – 1983**

První etapa je ohraničena zrodem sítě ARPANET, experimentálního projektu severoamerické agentury ministerstva obrany a pozdějším odštěpením vojenské sítě MILNET od původní sítě ARPANET. Projekt byl zaměřen na sdílení síťových zdrojů a při jeho zadávání byl formulován požadavek, aby při řešení byl vzat v úvahu požadavek funkční akceschopnosti sítě při výpadku některých jejích částí. Respektování tohoto požadavku, odrážejícího tehdejší „studenou válku“, se ukázalo jednou z hlavních příčin budoucích úspěchů zvoleného řešení. Umožňovalo totiž nejen odpojování nefunkčních částí sítě bez podstatného vlivu na chod zbytku sítě, ale i obrácený proces, rozšiřování sítě o nové komponenty bez vážnějších těžkostí a problémů. (VRABEC, 1995 str. 18)

Druhá etapa znamenala prudký rozvoj internetu. Tento rozvoj probíhal zejména v akademickém prostředí. Na začátku této etapy bylo Internetem propojeno asi tisíc počítačů, na konci etapy byl k Internetu připojen již asi milion počítačů. Nejvýznamnější událostí této etapy bylo vytvoření sítě NSFNET v roce 1986. Dřívější přístup k sítím ARPANET a MILNET byl omezen na vojenskou sféru. (VRABEC, 1995 str. 18)

Situace se ke konci druhé etapy začala měnit. Prvním signálem obratu v postoji ke komerční sféře byly některé legislativní akty USA, především HIGH PERFORMANCE COMPUTING ACT. Následovat proces privatizace a komercializace severoamerického Internetu. Jádrem tohoto procesu bylo soustředění vládních financí na výzkum a vývoj nové, velmi rychlé síťové páteřní infrastruktury a vstup velkého businessu do té provozní sféry severoamerického Internetu, která byla doposud financována vládou, tedy i do NSFNET. Uvedený proces zasahuje i do následující, třetí etapy.

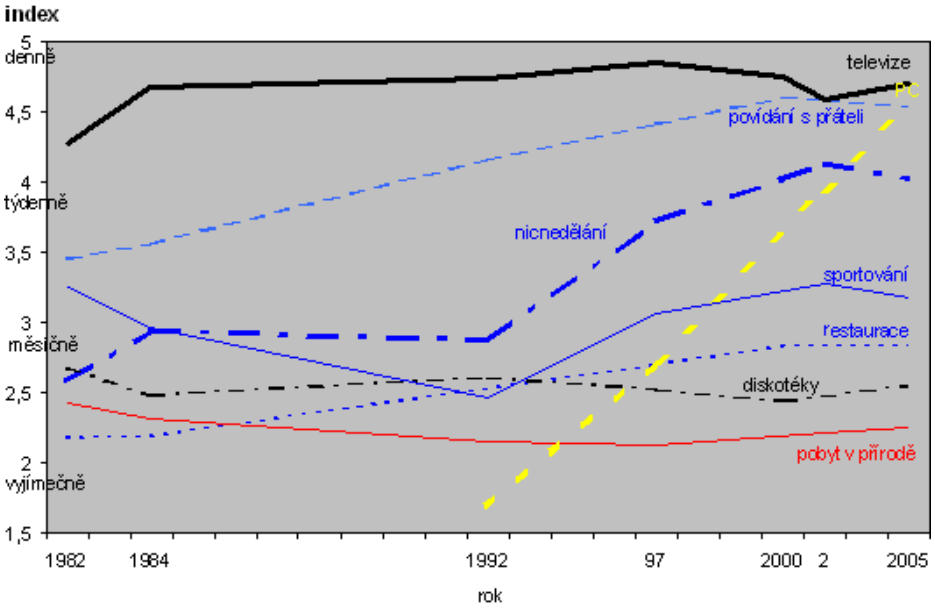
## Od 1993

Období 1993 – 1995 je charakterizováno velkým zvýšením komerčních aktivit v Internetu. Zvýšení počtu dvou milionů počítačů připojených do Internetu je převážně přírůstkem počítačů z komerční sféry, která nejen vidí v globální síti zdroj zajímaných a potřebných informací, ale i novou formu nadějného trhu s obrovskou dynamikou. Internet tedy začíná sloužit už univerzálně, nejen akademické a vládní sféře, ale i sféře komerční. (VRABEC, 1995 str. 19)

V posledních letech se Internet stal běžnou součástí našeho každodenního života stejně jako televize, rozhlas či mobilní telefony. Mnohdy se stává spíše ale zcela nejdůležitějším a nezbytným jak komunikačním prostředkem, tak zdrojem zábavy a vzdělání.

### Vývoj volnočasových aktivit mládeže

Tento graf sleduje vývoj aktivit mládeže od 15 do 18 let v období od roku 1982 do roku 2005. Vidíme přesně to, co se stalo ve vývoji počítačů a internetu od roku 1992 do roku 2005 - obrovský nárůst.




Obrázek 1 Aktivity ve volném čase

## 2.4 Struktura internetu

### 2.4.1 Základní pojmy

**URL - Uniform Resource Locator**

URL „jednotný lokátor zdrojů“ je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací (ve smyslu dokument nebo služba) na Internetu.

URL definuje doménovou adresu serveru, umístění zdroje na serveru a protokol, kterým je možné zdroj zpřístupnit.(11)

**Pakety**

Pokud chceme přenést data z jednoho počítače na druhý pomocí internetu, jsou tato data přenášena tak, že jsou rozdělena do menších datových jednotek – paketů. Každý z paketů obsahuje adresu zdroje, adresu cíle a číslo paketu. Jednotlivé pakety nemusí být adresátovi doručeny stejnou cestou. Server je může posílat více trasami.

**Směrovač - router**

Směrovač slouží při přenosu paketů. Je to vlastně počítač, který rozhoduje, který paket, kterou cestou pošle. Při posílání se přihlíží k průchodnosti spojů a v případech, kdy jsou spoje neprůchodné, vyhledává další možné varianty kudy pakety nejrychleji poslat.

**IP adresa**

Každý počítač, který je připojený k internetu má svoji IP adresu. IP adresa je 32bitové číslo, které se uvádí jako čtyři dekadická čísla oddělená tečkami. Tato adresa je pro každý počítač jedinečná.

### Doménové jméno

Protože IP adresa není pro zapamatování zrovna nejlepší, bylo zavedeno používání doménových jmen. V roce 1984 tak bych zaveden DNS – Domain Name System – který umožňuje vyjádření IP adresy ve slovní podobě, a naopak ze slovní podoby je schopen vyjádřit číselnou IP adresu.

### Domény nejvyšší úrovně - Top-Level Domains (TLD)

Podívejme se třeba na adresu http://www.fbm.vutbr.cz. Na konci adresy je uvedeno označení domény nejvyššího stupně. To je představováno dvou-písmenným označením státu. Tato doména patří do skupiny geografických TLD. Další skupina, která tvoří TLD, je skupiny generických domén. Tyto domény se nevztahují k místu, ale spíše k oboru či účelu použití.

### Přehled některých generických domén

| Název domény | Účel použití |
|---|---|
| .biz | obchod |
| .com | Komerční organizace |
| .edu | Vzdělávací organizace |
| .gov | Vládní organizace USA |
| .info | Informační servery |
| .jobs | Lidské zdroje |
| .mil | Vojenské organizace USA |
| .mobi | Mobilní operátoři |
| .net | Síťové organizace |

### Subdomény

Před doménou nejvyššího stupně bývá zpravidla jedna nebo více subdomén. V našem případě http://www.fbm.vutbr.cz jsou dvě subdomény, které nám říkají, že se jedná o počítač z VUT, konkrétně z Fakulty podnikatelské.

**Protokoly**

Aby se všechny tyto počítače mezi sebou navzájem domluvily, musí používat stejný jazyk - protokol. V internetu existují postupně 3 vrstvy protokolů. První se nazývá TCP (Transmission Control Protocol) - protokol pro řízení přenosu. Zajišťuje správnou cestu pro tok dat a zároveň je rozděluje na malé balíčky - pakety. Druhý protokol - IP (Internet Protocol) má na starosti, aby dostaly všechny balíčky dat dostaly na správné místo ve správném pořadí a tam se opět poskládaly. Tyto dva protokoly se většinou spojují do názvu TCP/IP. Poslední protokol se jmenuje aplikační protokol (Aplication Protocol) a ten je specifický pro jednotlivé služby internetu - například pro HTTP (HyperText Transfer Protocol) nebo FTP (FileTransfer Protocol) pro přenos souborů po internetu.

# 3 Počátky kriminality na internetu

## 3.1 První hacker

V době vzniku počítače vznikl i pojem hacker. Nebyl to ovšem termín ve smyslu, který mu přisuzujeme v dnešní době.

První programátoři, kteří pracovali s prvními programy na obrovských sálových počítačích, si potřebovali stejně jako v dnešní době, poradit s problémy, které přinášely nově vznikající programy. Tak vznikl pojem hacker, ovšem v dobrém slova smyslu. Tito programátoři se snažili odstranit chyby a vylepšit první primitivní programy.

Časem ale význam tohoto termínu změnil význam. Jako hackeři se začali označovat souhrnně všichni pachatelé, kteří se dopouštěli útoků proti počítači.

„V roce 1978 byla sestrojena první BBS, neboli Bulletin Board System. Právě tak došlo k propojení světa telefonie a počítačů. Sálové počítače sice byly spojovány do sítí již v letech šedesátých, ale právě vznikem první BBS získal každý majitel příslušně vybaveného počítače s telefonní linkou možnost stát se součástí kyberprostoru. Samozřejmě k závratnému rozšíření těchto technologií do běžných domácností nedošlo až do počátku 80. let, kdy společnost IBM poprvé představila své IBM PC.“ (MATĚJKA, 2002 str. 22)

## 3.2 Počátky porušování autorských práv

První případy porušování autorských práv jsou z průběhu šedesátých let. V těchto letech se rozšířily kotoučové magnetofony, které umožňovali kopírování nahrávek. Další rozvoj znamenalo rozšíření kazetového magnetofonu.

O masovém pirátství lze mluvit s příchodem PC. Ve velkém se tak začaly vyměňovat počítačové programy mezi jednotlivými uživateli a stejně tak se rozmohl i prodej takových nosičů.

## 3.3 Autorský zákon dnes

Autorský zákon (AZ) - z.č. 121/2000 Sb., o právu autorském a právech souvisejících s autorským právem.

**Autor** – fyzická osoba, která vytvořila autorské dílo

**Základní znaky autorského díla**

1. Literární, umělecké, vědecké dílo
2. Jedinečný výsledek tvůrčí činnosti autora
   (počítačové programy a fotografie postačuje „původnost“)
3. Vyjádřeno v jakékoliv objektivně vnímatelné podobě

**Osobnostní práva autora**

- rozhodnout o zveřejnění díla („zpřístupnění“)
- osobovat si autorství (vč. práva na označení)
- právo na nedotknutelnost (vč. tzv. autorského dohledu)

**Majetková práva autora**

- Právo dílo užít, zejména (tzn. lze užít i jinak než uvedenými způsoby):
  - rozmnožování díla
  - rozšiřování originálu nebo rozmnoženiny díla
  - pronájem originálu nebo rozmnoženiny díla
  - půjčování originálu nebo rozmnoženiny díla
  - vystavování originálu nebo rozmnoženiny díla
  - sdělování díla veřejnosti
- právo udělit licenci
- „další majetková práva“
  - právo na odměnu při opětném prodeji originálu díla
  - právo na odměnu v souvislosti s rozmnožováním pro osobní potřebu
  - právo na odměnu za pronájem (SOBOTKA, 2007)

## 3.4 Situace na území tehdejší ČSSR

Do konce 80. let se kriminalita spojená s počítači v ČSSR nevyskytovala. Počítače patřily k západnímu zboží, které nebylo možno dovážet. Takže už samotný dovoz počítače byl vlastně nelegální.

Situace se začala obracet na konci 80. let. V této době k nám byly dovezeny první osmibitové počítače např. Sinclair, Atari nebo Commodore. A i u nás se začaly vyrábět počítače značky Didaktik, IQ nebo PMD. A začaly i první primitivní hry např. Pacman nebo Manic Miner. Tyto hry byly nahrávány do malých pamětí z magnetofonových kazet. Nahrávání trvalo hrozně dlouho a neustále hrozilo přerušení a nutnost začínat znova. Je jasné, že takto šířený software nemohl být legální, ale česká legislativa z oblasti autorského práva s existencí počítačů nepočítala. K nelegálnímu rozšiřování napomáhal i stát, když podporoval kroužky počítačové techniky.

### 3.4.1 První případy počítačové kriminality v ČSSR

První z případů, které literatura[1] uvádí, spadá do 70. let. Existence tohoto případu není ověřená, ale mělo se jednat o poškození záznamových pásek magnetem. Neexistují ani oficiální informace o rozsudku. Případ měl být kvalifikován jako sabotáž.

Doložený je naopak případ z roku1987, kdy byl poškozen počítač sovětské výroby SMEP. Programátoři chtěli cíleným poškozením dosáhnout toho, aby dostali nový lepší počítač západní výroby. I v tomto případě se mělo jednat o sabotáž. Později byl případ změněn na poškozování socialistického majetku a nakonec bylo trestní stíhání z důvodu amnestie zastaveno.

[1] Smejkal, Vladimír. *Informační a počítačová kriminalita v České republice*. MV ČR 1997

Dalším případem, který se stal, byla zpronevěra za pomocí počítače. Pracovnice zásilkového obchodu Magnet se dopustila trestného činu, když v počítači měnila status objednávek učiněných svou matkou z „nezaplaceno“ na „zaplaceno“.

Další trestné činy se týkaly zneužívání počítačů zaměstnavatele. Jeden takový případ se udál i na Vysokém učení technickém. Zaměstnanec počítačového centra si pro své vlastní potřeby na počítačích zaměstnavatele zpracovával agendu bytových družstev.

Poslední zajímavá událost, která však nebyla trestným činem, se stala 13. 2. 1992. Československá republika byla připojena k internetu. Toto připojení bylo zatím možné jenom na akademických půdách. Ovšem od této doby se i u nás začalo tvořit nové prostředí pro další neznámé trestné činy.

# 4 Počítačová kriminalita

Všechny definice se v zásadě shodují v tom, že je nutné počítačovou kriminalitu rozlišit na dvě základní kategorie:

A) „Protiprávní jednání směřující proti počítači. Počítač je zde přímo terčem útoku. Jedná se především o průniky do systémů za účelem například krádeže dat, průmyslové špionáže, bankovního podvodu, zneužití osobních údajů z elektronické databáze apod.
B) Protiprávní jednání spáchaná s využitím počítačů. Počítač slouží pouze jako nástroj trestné činnosti, respektive jejího usnadnění. Na předním místě zde stojí porušování autorského práva.“ (MATĚJKA, 2002 str. 6)

Toto rozdělení je pouze jakýmsi jednoduchým rozdělením. Počítačovou kriminalitu respektive kriminalitu páchanou pomocí internetu je poté ještě nutno rozdělit z jiného hlediska. Může totiž jít:

A) „O protiprávní jednání tradiční, kde počítač pouze usnadňuje jejich spáchání, ať už je přímo jejich terčem (online loupež v bance) nebo toliko jejich nástrojem (šíření pornografie).

B) O protiprávní jednání zcela nová, která se objevila až s nástupem moderních informačních technologií, ať už směřující proti počítači (hacking), či používající počítač v roli nástroje (cracking).“ (MATĚJKA, 2002 str. 6)

# 5 Trestné činy ve vztahu k počítači, jeho příslušenstvím a jiným nosičům informací jako věcem movitým

V tomto případě se jedná o činy, které mají za cíl počítač jako movitou věc. Tyto činy se ale mohou vztahovat k jakékoli jiné věci. Může se tak jednat o:

## 5.1 Tradiční jednání

### 5.1.1 Krádež (§ 247 TrZ)

(1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a

a. způsobí tak škodu nikoliv nepatrnou,
b. čin spáchá vloupáním,
c. bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí,
d. čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo
e. byl za takový čin v posledních třech letech odsouzen nebo potrestán,

bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci.

(2) Odnětím svobody na šest měsíců až tři léta nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu nikoli malou.

(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a. spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b. způsobí-li takovým činem značnou škodu nebo jiný zvlášť závažný následek.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.(10)

### 5.1.2 Zpronevěra (§ 248 TrZ)

(1) Kdo si přisvojí cizí věc, která mu byla svěřena, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci.
(2) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu nikoli malou.
(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a. spáchá-li čin uvedený v odstavci 1 jako osoba, která má zvlášť uloženu povinnost hájit zájmy poškozeného, nebo
b. spáchá-li takový čin jako člen organizované skupiny, nebo
c. způsobí-li takovým činem značnou škodu nebo jiný zvlášť závažný následek.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.(5)

### 5.1.3 Podvod (§ 250 TrZ)

(1) Kdo ke škodě cizího majetku sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci.
(2) Odnětím svobody na šest měsíců až tři léta nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu nikoli malou.
(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a. spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b. způsobí-li takovým činem značnou škodu nebo jiný zvlášť závažný následek.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.(4)

### 5.1.4 Podílnictví (§ 251 a § 252 TrZ)

(1) Kdo ukryje, na sebe nebo jiného převede anebo užívá

a. věc, která byla získána trestným činem spáchaným jinou osobou, nebo
b. to, co za takovou věc bylo opatřeno, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

(2) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 značný prospěch.

(3) Odnětím svobody na dvě léta až osm let nebo propadnutím majetku bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 prospěch velkého rozsahu.(6)

### 5.1.5 Zatajení věci (§ 254 TrZ)

(1) Kdo si přisvojí cizí věc nikoli nepatrné hodnoty, která se dostala do jeho moci nálezem, omylem nebo jinak bez přivolení osoby oprávněné, bude potrestán odnětím svobody až na jeden rok nebo peněžitým trestem.

(2) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 značný prospěch.(1)

## 5.2 Nová jednání

### 5.2.1 Hacking – pronikání do systémů

Hacking (z angl. slova hack – znamená sekat) jako snaha dělat věci, ke kterým není dáno oprávnění, ale hackeři (skupina lidí, nebo jednotlivci) většinou získaná data nezneužívají. Typický hacker je talentovaný, tvořivý programátor (většinou vysokoškolsky vzdělaný), který hledá nedostatky v počítačových a jiných komunikačních systémech. Tito hackeři sice vstupují neoprávněně do počítačových informačních systémů jiných uživatelů, ale hledají problémy a jejich řešení s použitím nových technologií. V nejobecnějším slova smyslu se u nás nesprávně používá termín

hacking pro označení všech osob, snažících se o průnik do počítače. Hacking má velmi bohatou historii. Jde o nejvýraznější oblast počítačové kriminality. Nebezpečí, že se někteří z hackerů pokusí proniknout do našeho domácího počítače je velmi mizivé. Hackeři se většinou pokoušejí nabourat firemní počítače a velké servery a sítě.

**Rozdělení hackerů:**

- **Script Kiddies** – tvoří nejnižší stupeň hackerského žebříčku. Jsou označováni
- za tzv. lamery – začátečníky, ne skutečné hackery
- **white hats** – tzv. „hodní“ hackeři, kteří nezpůsobují žádné škody a upozorňují administrátory systémů na objevené bezpečnostní chyby, někdy jsou také označování jako „ethical hackers“ – jde tedy o hackery v původním pravém slova smyslu,
- **black hats** – hackeři s kriminálními motivy, účelem je vlastní obohacení – jde tedy o tzv. crackery
- **grey hats** – šedá zóna hackerů stojící na pomezí mezi předchozími typy, typické je pro ně zveřejňování bezpečnostních děr, tzv. exploitů v internetu za účelem růstu úrovně bezpečnosti systémů (výše uvedený samuraj)
- **elite** – hackeři proslavení nejlegendárnějšími kousky (PAUKERTOVÁ, 2006)

V souvislosti s hackingem přibývají případy tzv. násilného hackingu. Spočívají v přímém fyzickém útoku na osobu s administrátorskými právy k systému, která je násilím nebo výhružkami násilí donucena vyzradit přístupové heslo, případně sama udělat operaci ve prospěch útočníka. Podle historie hackingu větší nebezpečí než od anonymních hackerů, hrozí organizacím nebezpečí ze strany lidí, kteří mají oprávnění pohybovat se v systému.

„Co se týče právní úpravy hacking, samotný průnik do systému je trestný podle §257 TZ, poškození a zneužití záznamu na nosiči informací, ovšem jen tehdy, pokud hacker touto aktivitou způsobí jinému škodu či jinou újmu, nebo sobě či jinému neoprávněný prospěch.“ (MATĚJKA, 2002 str. 55)

### 5.2.2 Carding

Pojmem carding označujeme zneužívání platebních karet. Vznik tohoto oboru souvisí především se vznikem a rozvojem internetového bankovnictví. Platební karta se tak stala převažujícím platebním nástrojem, ale zabezpečení je v mnoha případech nedostačující.

V počátcích tohoto druhu kriminality se jednalo především o tzv. kreditní nákup (způsob jak získat zboží bez placení v hotovosti). Toho se dá docílit více způsoby – krádeží čísla platební karty nebo krádeží karty samotné. Na zjištění čísla platební karty se používají generátory, které v krátkém čase dokáží vygenerovat číslo kreditní karty. Pachatelé cardingu získávají osobní údaje majitelů účtů různými způsoby. Oblíbený je způsob, kdy zavolají majiteli účtu, kterému se představí jako pracovník banky, která mu kartu vydala a předstírá, že nastaly problémy v počítačovém systému a že ztrátu dat je možné opravit tak, že mu dotyčná osoba znovu nadiktuje svoje osobní údaje. Nikdy bychom tak neměli sdělovat svoje osobní údaje a čísla karet přes telefon. V dnešní technicky vyspělé společnosti nevíme, kdo další nás poslouchá nebo jestli je volající opravdu pracovník banky. Stejně to platí i pro posílání dat přes mail.

Na začátku vzniku elektronického obchodu bylo hodně případů tzv. vyluxování účtu (obchodník si při platbě přes internet z účtu zákazníka strhne víc, než je stanovená cena zboží). Nejvíc se podobné případy stávaly při platbách za různé pochybné služby – přístup na pornostránky apod. V zahraničí se objevovaly případy, kdy nad bankomat pachatel nainstaloval kameru a zjistil tak číslo kreditní karty a následně oběť okradl.

„Z hlediska českého trestního práva připadá pro tuto činnost kvalifikace především podle §249 TZ, neoprávněné držení platební karty, případně podle okolností konkrétního činu, §250 TZ, podvod, §257a, poškození či zneužití záznamu na nosiči informací, nebo případně §178, neoprávněné nakládání s osobními údaji.

# 6 Trestné činy, při kterých je počítač a internet prostředkem k jejich páchání

S rozvojem počítačů a rozšířením internetu dostaly i trestné činy novou podobu. Tato technika znamená velké usnadnění v mnoha situacích. Umožňuje tak pachatelům vytvářet stále dokonalejší možnosti jak zákony obejít.

## 6.1 Tradiční jednání

### 6.1.1 Podvody, letadla

V době, kdy počítače nebyly běžnou součástí našeho života a o internetu nemluvě, jsme dostávali hry typu letadlo klasickou poštou. Dále jsme dopis museli třeba 20krát opsat a poslat dál. Toto ale není minulostí. Tento úkon se s využitím počítače a internetu mnohokrát zjednodušil, zrychlil a hlavně rozmohl. V dnešní době asi není nikdo, kdo by takový e-mail nedostal.

Kromě letadel se na internetu vyskytují i podvodné e-shopy, které se snaží vylákat peníze za neexistující služby. Toto se rozmohlo především ve spojení s pornografickými stránkami. Jsou tak nabízeny sexuální služby například za poslání čísla dobíjecího kuponu některého z mobilních operátorů.

### 6.1.2 Padělání a penězokazectví

Právě v tomto oboru počítače významně pomohly usnadnit práci. V dřívějších dobách byl tento trestný čin velmi náročný a byl pouze pro dobré kreslíře a rytce. Dnes stačí zvládnout příslušný software, zakoupit kvalitní technologie pro tisk a kvalitní papír. Proto se stále musí zlepšovat ochranné prvky na penězích a musí být nestále vyvíjeny.

Do této kategorie patří i padělání a pozměňování veřejné listiny. Občanský soudní řád vymezuje v ust. § 134 pojem veřejné listiny tak, že veřejnými listinami jsou:

1. listiny vydané soudy České republiky nebo jinými státními orgány v mezích jejich pravomoci,
2. listiny, které zvláštní předpis prohlašuje za veřejné.

Může se jednat například o padělání vysokoškolských diplomů. Tento případ se stal v roce 2001 i v České republice.

### 6.1.3 Útoky na čest a pověst, elektronická msta, pomluvy

Tuto trestnou činnost může páchat kdokoli s přístupem k internetu. Může tak zveřejňovat jakékoliv informace, které vytipovanou osobu mohou poškozovat jak v osobním, tak i v profesním životě. Větší dopad tohoto trestného činu je především u známých osobností a vlivných řídících pracovníků velkých podniků.

Další formou této činnosti může být i to, že pachatel zaregistruje osobu např. na erotických stránkách, a oběti pak chodí nevyžádaná pošta nebo je obtěžována nežádoucími telefonáty.

### 6.1.4 Flejmy

Flejma je zpráva, která se šíří na internetu. Její autor se snaží provokovat nebo urazit čtenáře. Většinou se vyskytují v různých internetových debatách a diskusích. S tímto jednáním se můžeme setkat, například pokud napíšeme na internet svůj názor na nějaký zveřejněný článek. Když nám někdo odpoví, že to co jsme napsali, je úplná blbost a že to vypovídá o našem IQ a přidá další urážky, dostali jsme flejmu. A jestliže se připojíme a začneme oplácet flejmařovi stejným způsobem, začneme tak prostřednictvím internetu flejmovou válku.

Při flejmování můžeme podstupovat riziko, že budeme trestně stíháni - můžeme se dopustit křivého obvinění.

„Představte si, že vedete na Síti v renetové diskusní skupině *comp.os.mx-windows. advocacy* spor o to, je-li lepší uživatelské rozhraní Microsoft Windows nebo Macintosh. Najednou váš oponent zaútočí: „Nevíš, o čem mluvíš, a já se tomu nedivím, když jsi loni seděl za to, že jsi řídil auto pod vlivem alkoholu.“ Dobře, dejme tomu, že je to pravda; opravdu jste byl ve vězení za to, že jste řídil auto v podnapilém stavu. Tento výrok tedy není urážka na cti, protože taková urážka musí být lživá. Avšak obvinění z toho, že jste si opilý sedl za volant, nemá nic společného s vaší schopností porovnat uživatelská rozhraní a takový výrok může na Síti poškodit vaši pověst počítačového odborníka. V tom případě se váš oponent zřejmě dopustil deliktu proti zákonu o soukromí, který se odborně nazývá veřejné odhalení osobních informací. Pokud byla vaše pověst touto větou poškozena, měli byste podat žalobu k soudu.“ (BARRETT, 1999 str. 179)

### 6.1.5 Vydírání a elektronické výpalné

I v případě vydírání došlo k zmodernizování této činnosti a k částečnému přesunu do sféry informačních technologií. V dnešní době se tak objevují výhružky na zničení dat nebo jejich zneužití, průniku do systému nebo databáze pokud majitel nezaplatí e-výpalné. Mnoho firem než by riskovali ztrátu dat, raději požadovanou částku zaplatí. Tímto způsobem se do světa počítačů a Internetu začíná dostávat organizovaný zločin. Tyto případy zatím nejsou moc časté, ale lze předpokládat, že postupem času můžeme čekat jejich pomalý nárůst. (MATĚJKA, 2002 str. 65)

### 6.1.6 Šíření pornografie

Toto odvětví zažívá v poslední době obrovský rozmach. Tyto servery existovaly už v dobách, kdy elektronické obchodování bylo teprve na začátku, a vydělávaly obrovské peníze. Je to jedna z nejčastějších činností, která je prováděna pomocí Internetu. Zákazníkovi tak Internet poskytuje jakousi anonymitu při hledání těchto

materiálů. V dřívější době, kdy existovaly pouze tištěné časopisy, nemuselo být jejich pořízení vždy snadné. To ale omezovalo, aby se k těmto materiálům dostaly děti. Sice jsou stránky s touto tématikou označeny, že jejich obsah není pro mladší 18 let, ale pokud nezletilý odsouhlasí, že je mu 18 let, pak už mu nic nebrání v tom, aby na stránky vstoupil.

„Z hlediska české právní úpravy je otázky šíření pornografie řešena v §205 TZ, ohrožování mravnosti. Tak je podle této úpravy trestná výroba a distribuce pornografických materiálů, ve kterých jsou znázorněny násilné a lidskou důstojnost ponižující činnosti, styky s dětmi a zvířaty, případně jiné patologické sexuální praktiky, dále je trestné zpřístupňování jakýchkoli pornografických materiálů nezletilým. Jinak šíření pornografie samo o sobě v České republice trestné není.“ (MATĚJKA, 2002 str. 66)

### 6.1.7 Extremismus

Internet poskytuje vhodné prostředí pro aktivity různých extrémistických skupin (neonacisté, komunisté, anarchisté, náboženské sekty). Postižitelnost extremismu je velmi obtížná. Většinou jsou stránky tvořeny nebo registrovány v zahraničí, kde není prezentace takových názorů trestná. To ale nic nemění na tom, že obsah takových stránek je přístupný i tam, kde je taková činnost nepřípustná. Například neonacisté si tak mohou registrovat stránky v USA, kde jejich projevy nejsou trestné.

„V Česku je nejčastějším důvodem k obvinění trestný čin podpora a propagace hnutí směřujících k potlačení práv a svobod člověka. Za to hrozí až tři roky vězení. Pokud někdo extremistické hnutí propaguje v rámci organizované skupiny, nebo prostřednictvím sdělovacích prostředků či internetu, může dostat až osm let.

Popírání holocaustu je méně častým trestným činem. Kdo veřejně zpochybňuje či schvaluje nacistické nebo komunistické genocidium, může dostat až tříleté vězení.“(7)

## 6.2 Nová jednání

Na rozdíl od předchozích trestných činů vznikaly níže uvedené převážně až s nástupem moderních technologií. Pokud některý z těchto činů existoval již v nedávné minulosti, tak počítače a Internet dodali tomuto konání úplně jiný rozměr. To co se provádělo v nepatrném množství se dnes děje denně, aniž by každý věděl, zda je to trestné.

### 6.2.1 Spamming

„Co se týče právního posouzení spammingu, podle českého trestního práva samotný spamming není trestným činem. Sběrem adres pro spamming by ovšem mohl být spáchán trestný čin neoprávněného nakládání s osobními údaji podle §178 TZ, a to tehdy, poskytne-li je spammerovi třetí osoba bez souhlasu subjektu údajů. V případě jiného zneužití osobních údajů pro spamming hrozí spammerovi pokuta až 10 000 000Kč, která může být uložena Úřadem pro ochranu osobních údajů ve správním řízení.“ (MATĚJKA, 2002 str. 70)

Spamming označuje rozesílání nevyžádané pošty. Odesílatel rozesílá zprávy většinou komerčního charakteru, které mají adresáta přimět alespoň k návštěvě propagovaných stránek. Pro spammery je takové rozesílání velmi výhodné. Nic je to nestojí a pomocí Internetu mohou oslovit obrovské množství lidí. Vysledovat člověka rozesílajícího spamy je velmi obtížné. Spammer může změnit údaje v hlavičce dopisu nebo použít bezplatnou anonymní službu.

Absolutně účinná a obecně aplikovatelná obrana proti spamům v současnosti v podstatě neexistuje. Existuje však několik přístupů, které mohou pomoci problémy v dané oblasti alespoň zmírnit. Zahrnují jednak přístupy o omezení množství spamů, které dostává daná konkrétní osoba či skupina osob (filtrování pošty a blokování spamovských zdrojů, skrývání adres, žaloby proti spammerským firmám), jednak přístupy všeobecně prospěšné snažící se bojovat s fenoménem spamu obecně (osvětou,

tlakem na providery a správce systémů aby neposkytovali spammerům prostor pro jejich činnost, lobováním za přijetí účinnější antispamové legislativy, apod.). (KOLAJA, 2002)

### 6.2.2 Warez

Warez je termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem. Člověk zabývající se warezem je lidově řečený warezák, spisovně zvaný pirát. Tito piráti tvoří většinou warezové skupiny. Každý jedinec má svoji funkci. Jedni se věnují obcházení ochran proti kopírování programů a druzí se věnují vytváření www stránek a propagaci svých produktů. I warezové skupiny bývají rozdělené, jedny se věnují obcházení filmů, další hudby, programů atd.

„Právní posouzení warezu je jasné, jedná se o trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle §152 trestního zákona.“ (MATĚJKA, 2002 str. 72) Postihy za tento trestný čin jsou trest odnětí svobody až na dva roky, peněžitý trest nebo propadnutí věci. Pokud pachatel spáchá čin ve značném rozsahu, může dostat až pět let vězení.

### 6.2.3 Phreaking

Tímto termínem označujeme zneužívání telekomunikačních služeb. Je to činnost, kdy pachatel využívá telefonní linky, ale neplatí za tyto služby provozovateli.

Phreaking má delší historii. Vznikl v 70. letech v Americe a jeho účelem bylo ušetřit za telefonní hovory. Ve stručnosti jde o to, že si vezmeme pevnou linku do batohu, k ní přidáme trochu nářadí a z ulice se napojíme přes dráty na telefonní rozvodnu. Voláme tedy z čísla někoho, koho vůbec neznáme a on ty hovory potom i platí. Když nechceme nikomu ubližovat a chceme radši volat na účet telefonní společnosti, napíchneme se na telefonní budku. V dnešní době má phreaking další

význam – ušetřit na poplatcích za internet. Začít s touto činností není nijak složité. Návod jak všechno provést je na internetu. „Telefanda“ musí mít alespoň nějaké znalosti z elektrotechniky, jinak bude mít tuto činnosti trochu ztíženou.

„Co se postihu těchto aktivit týče, český trestní zákon na ně pamatuje v §182 TZ, poškozování a ohrožování provozu obecně prospěšného zařízení, dojde-li při páchání této činnosti i k poškození majetku třetích osob, tak i §257 TZ, poškození cizí věci, případně §257a, poškození či zneužití záznamu na nosiči informací. Dojde-li při této činnosti k porušení telekomunikačního tajemství, připadá pak v úvahu i §239 TZ, porušování tajemství dopravovaných zpráv.“ (MATĚJKA, 2002 str. 73)

### 6.2.4 Cracking

S pojmem cracking jsou spojeny tyto pojmy:

**Crack** - narušení zabezpečení ochrany a integrity programu nebo systému.

**Cracker** - podle jednoho pohledu jde o osoby schopné prolomit kód určitého SW a umožnit tak jeho nelegální kopírování, z jiného hlediska jde o osoby, které pronikají do počítačových systémů s úmyslem jejich poškození.

**Cracking** je činnost, kdy dojde k narušení informačního systému zvenčí (prolomení ochrany). Cracker zpravidla nepracuje sám, ale ve skupinách. Členové skupiny bývají hierarchicky rozděleni, každý má na starosti konkrétní činnost. Skupiny bývají tematicky specializované na herní oblasti, weby a aplikace. Crackeři se sami často považují za hackery, avšak jejich znalosti informačních systémů, internetových protokolů a programování nejsou na tak vysoké úrovni jako u hackerů. Crackeři používají k průniku do informačních systémů především zveřejněné slabiny, na které ještě administrátoři nezareagovali. Zásadní rozdíl, odlišující tyto osobnosti od hackerů, spočívá v pronikání do systémů s cílem data získat a následně zneužít ve vlastní prospěch. K těmto charakteristikám lze ještě přiřadit potěšení z destrukce systému.

# 7 Vyšetřování počítačové kriminality

Vyšetřování počítačové kriminality není nijak jednoduché. Na jedné stránce je nestále se rozrůstající internetová síť, která poskytuje dostatečnou anonymitu, a na druhé straně v současné době chybí v České Republice policii detektivové, kteří by se měli zabývat internetovou kriminalitou. Tito policisté by měli potírat dětskou pornografii, šíření nelegálního softwaru, hudby, filmů nebo třeba extremismu. V současné době je k internetu připojena asi polovina českého národa a tím také přibývá počítačové kriminality, ale chybí lidé, kteří by tuto problematiku řešili. Policejní prezidium přiznává, že na pozice těchto detektivů je velmi těžké sehnat lidi. Souvisí to i s tím, že na tyto místa jsou kladeny vysoké požadavky. „Zájemci totiž musí mít odslouženo u policie nejméně devět let a k tomu vysokoškolské vzdělání. To je problém zvláště nyní, kdy od policie kvůli novému služebnímu zákonu zkušení detektivové spíše odcházejí. Příliš neláká ani nástupní plat třicet tisíc korun hrubého - softwaroví specialisté dostávají po nástupu dvakrát tolik.

Výsledkem je, že například ve východních Čechách se bude informační kriminalitou zabývat jediný policista. V regionu přitom žije 1,2 milionu lidí.“ (Eichler)

## 7.1 Domovní prohlídka

„Domovní prohlídku lze vykonat, je-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících (obydlí) je věc nebo osoba důležitá pro trestní řízení. (zákon č. 141/1961 Sb.)“ (2)

Domovní prohlídku vykonává na příkaz soudce nebo předsedy senátu policejní orgán. Příkaz musí být vydán písemně a musí být odůvodněný.

„V sobotu 7. 10. 2006 byl během předávky 7 ks pirátských disků s filmovými tituly svému domnělému zákazníkovi - ve skutečnosti vyšetřovateli České protipirátské unie - zadržen pirátský prodejce a inzerent vystupující pod jménem Karel Polák. Vyšetřovatel si od něj objednal disky prostřednictvím jeho e-mailové adresy, přičemž si tematicky smluvili místo předání na sobotní ráno na parkovišti Blešich trhů

Kolbenova v Praze. Následně po zadržení pachatele byla vykonána prohlídka v autě, kterým se na sjednané místo dostavil. Zde byly nalezeny přepravky se 157 ks DVD-R s nejrůznějšími filmovými tituly. Po obdržení souhlasu státního zástupce se kriminalisté přesunuli do pachatelova bytu, kde bylo zajištěno dalších 571 ks DVD-R s filmy, osobní počítač a tiskárna. Policisté pachatele ztotožnili jako B. K., invalidního důchodce z Prahy 9, který byl již za obdobný trestný čin jednou odsouzen. Tehdy - v roce 1994 - pro změnu za prodej pirátských videokazet. Jeho zkušenosti tím ale bohužel nekončí, před měsícem byl tento čiperný pirát zadržen pro prodej pirátských DVD-R pracovníky Celního úřadu Kolín.“(3)

## 7.2 Student VŠB se pokusil nelegálně získat miliony

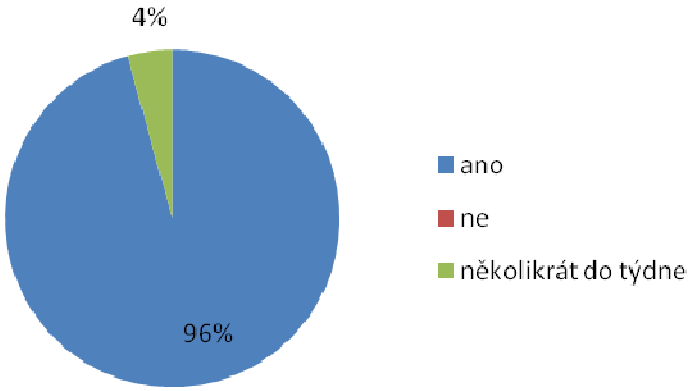
„Přes tři miliony korun se pokusil nelegálním způsobem získat třicetiletý student z Ostravy. Prostřednictvím školního počítače se snažil převést téměř z osmdesáti účtů peníze na své konto. Banka podvod včas odhalila. Podezřelý nyní prchá před policií, hrozí mu totiž až 15 let vězení.

Lumír Herič, student Vysoké školy báňské – Technické univerzity v Ostravě, nainstaloval do jednoho z univerzitních počítačů speciální program, jehož prostřednictvím získal v roce 2006 hesla k účtům. Studenti totiž počítače využívají i k ovládání svého konta přes internet. Poté se snažil z účtů převést peníze. Heričovi se to podařilo pouze u čtyř bankovních účtů. Česká spořitelna totiž zaznamenala podezřelé transakce a později podala trestní oznámení na neznámého pachatele. Policie při domovní prohlídce zajistila několik stovek datových nosičů a počítače. Studenta z Ostravy policie podezřívá mimo jiné z padělání peněz a pokusu o podvod.“ (9)

# 8 Dotazníkové šetření

Na základě bakalářské práce jsem vytvořila krátký dotazník, který jsem rozeslala mezi studenty podnikatelské fakulty Vysokého učení technického v Brně. Snažila jsem se v dotazníku zachytit široký záběr situací, se kterými se při používání internetu můžeme setkat. Konkrétně byl tento anonymní dotazník rozeslán mezi studenty prvních a druhých ročníků oborů Manažerská informatika a Daňové poradenství. Celkově byl dotazník poslán asi 1000 studentům vysoké školy, odpovědělo 392 dotazovaných. Odhaduji, že věk dotazovaných respondentů je převážně od 19 do 22 let.

**Otázka č. 1 Používáš denně internet?**

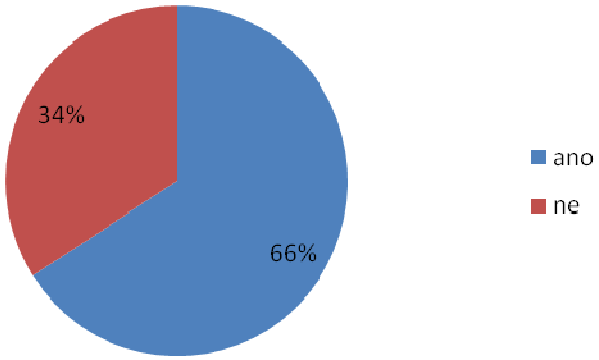



Graf č. 1 Četnost používání internetu

Na dotaz ohledně používání internetu uvedlo 352 studentů, že tento komunikační prostředek používají každý den. Pouze asi 16 studentů uvedlo, že internet používá několikrát to týdne. Nikdo z dotázaných neuvedl frekvenci používání internetu nižší než několikrát do týdne.

Z výsledků je vidět, že studenti si v dnešní době život bez internetu umí už jen asi těžko představit. Jeho používání vyžaduje i samotné studium na vysoké škole, které bere připojení k internetu jako samozřejmost. Převážná většina výukových materiálů je k dispozici přes internet, přihlašování ke zkouškám a všechny důležité informace jsou k nalezení na stránkách školy a fakulty. Velmi vysokou četnost používání internetu potvrzuje také to, že většina odpovědí na dotazník přišla během prvního týdne od odeslání.

**Otázka č. 2 Používáš legální verzi operačního systému?**

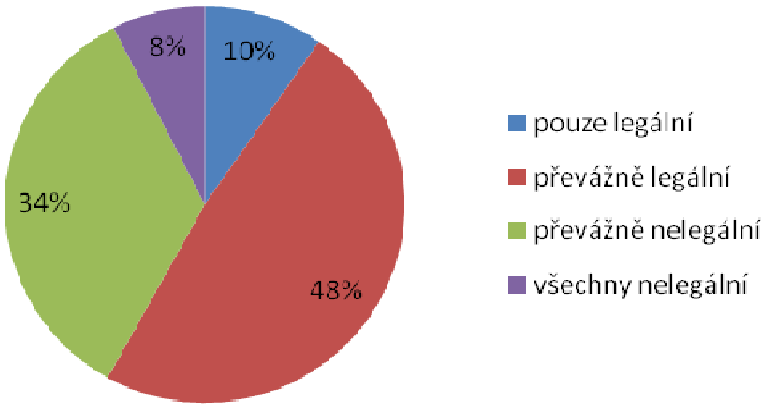



Graf č. 2 Operační systém

66% tj. 248 osob uvedlo, že používá legálně získanou kopii operačního systému. Přesto poměrně velké procento studentů (34% tj. 128 osob) používá nelegálně získané kopie operačních systémů. Většina uživatelů počítačů používá operační systémy od firmy Microsoft, přesto se začíná rozmáhat i používání operačních systémů, které jsou dostupné zdarma např. Linux, FreeDos, DR-DOS, FreeBSD, BeOS. Několik studentů také uvedlo, že v zaměstnání používá legální verzi operačního systému a pro soukromé účely používá pirátskou kopii.

V dnešní době notebooků napomáhá používání legálně získaného operačního systému i to, že většina těchto počítačů je dodávána přímo s nainstalovaným operačním prostředím. Myslím, že je proto lepší si něco připlatit a používat legální verzi operačního systému, než řešit problémy se získáním a používáním nelegálně získaných kopií.

**Otázka č. 3 Jaké verze programů převážně používáš?**

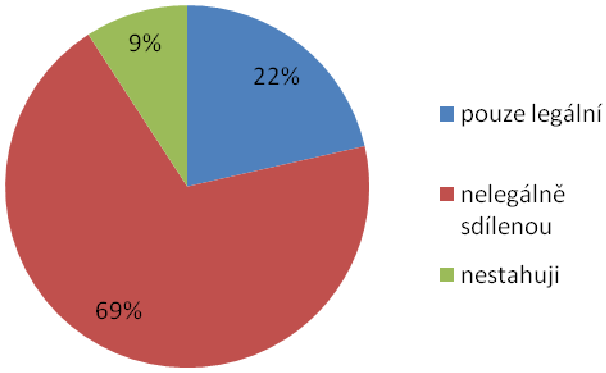



Graf č. 3 Používání software

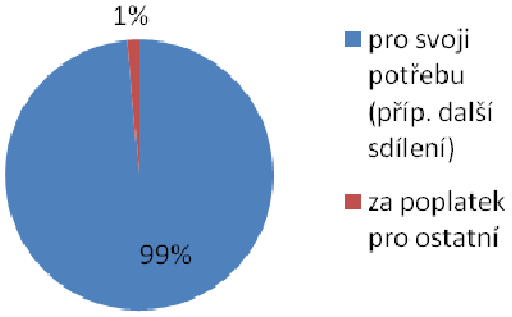
Přestože na internetu je k dispozici mnoho legálně vystavených programů, které si můžeme zdarma stáhnout, 8% studentů tj. 28 uvedlo, že používá pouze nelegálně získané programy. Stejně tak pouze 10% tj. 36 studentů uvedlo, že používá pouze legálně získané programy. Více jak 1/3 – 34% tj. 128 studentů uvedlo, že používá převážně nelegálně získané programy. Pokud si stáhneme z internetu hudbu nebo filmy pro vlastní účely, není toto nijak trestné (pokud soubory dále nesdílíme). Jestliže ale vlastníme kopii nějakého software (je jedno jak získaného) a používáme jej, aniž bychom měli k tomuto programu zakoupenou licenci, je toto užití trestné.

Nejvíce studentů (48%) uvedlo, že používá legálně získané programy. Mezi tento software patří volně stažitelný freeware nebo shareware, který má různá omezení např. časové nebo funkční omezení. Dále sem patří klasicky zakoupený produkt nebo stažený program a k němu zakoupená licence.

**Otázka č. 4 Stahuješ hudbu a filmy z internetu?**




Graf č. 4 Stahování dat

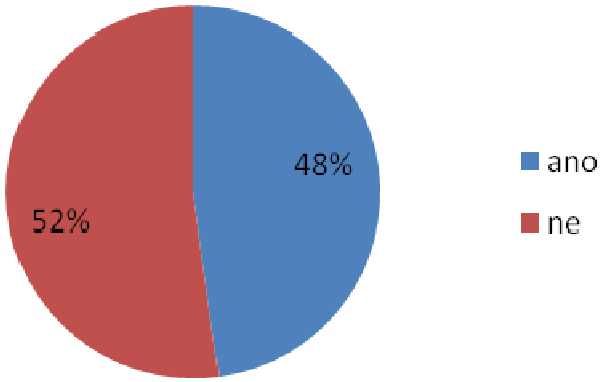



Graf č. 5 Využití stažených dat z nelegálního sdílení

Z 69% tzn. 272 dotazovaných, kteří stahují z internetu nelegálně sdílenou hudbu, jich většina (99%) stahuje pouze pro svoji potřebu nebo dále soubory sdílí s ostatními uživateli. Sdílet soubory nesmíme, ale co je ještě horší, že 1% z dotazovaných přiznalo, že stahovanou hudbu a filmy dále distribuuje za poplatek i ostatním zájemcům. Tento čin je podle našeho práva trestný.

Zároveň graf ukazuje, že se začíná rozrůstat i legální stahování hudby po internetu. 22% studentů tj. 84 lidí využívá možností stahovat hudbu legálně. Jednak je možné si stáhnout volně přístupnou autorem vystavenou skladbu nebo si skladbu stáhnout za určitý poplatek. Pouze 9% tzn. 36 studentů uvedlo, že z internetu nestahuje vůbec.

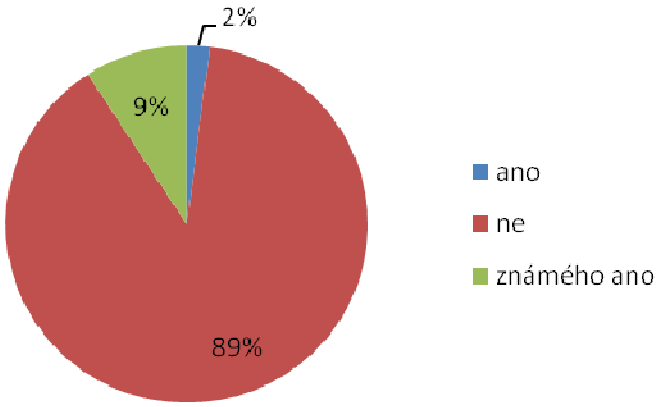
**Otázka č. 5 Sdílíš s ostatními hudbu nebo filmy pomocí internetu a stahovacích programů?**




Graf č. 6 Sdílení dat

Z výsledků je vidět, že polovina dotazovaných studentů sdílí s ostatními uživateli internetu soubory. Samotné stažení hudby a filmů a používání pro vlastní potřebu, trestné není. To ale neplatí v případě sdílení těchto stažených souborů. Sdílení dat trestné je. To že stahování hudby a filmů je pro vlastní účely legální, ale neznamená, že je legální stahování komerčního software. Stahování software je nelegální a stejně i jeho používání, natož sdílení. Nesmí se používat "cracky" ani "serials" nebo odstraňovat ze softwaru ochrany. V praxi je ale druhou věcí, kdo a jak to zkontroluje, kdo a jak dokáže, jaká škoda vznikla a kdo ji způsobil.

**Otázka č. 6 Vydíral tě někdo přes internet?**




Graf č. 7 Vydírání

Převážnou většinu 89% tj. 348 dotazovaných přes internet nikdo nevydíral. Osm studentů tj. 2% přiznalo, že se stalo obětí vydírání přes internet. 9% tj. 36 studentů uvedlo, že znají někoho, kdo byl přes internet vydírán.

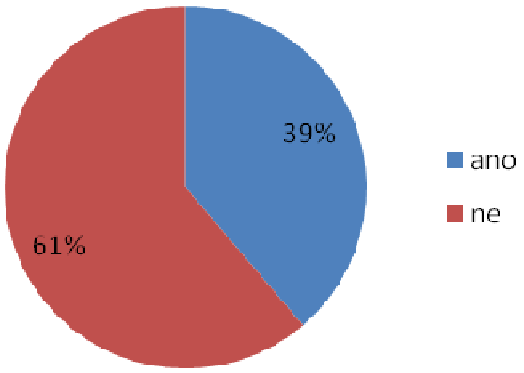
I když většina dotazovaných se s vydíráním nesetkala, je z grafu vidět, že i tyto trestné činy se začínají pomalu ale jistě přenášet do virtuálního prostředí.

Může se nám třeba stát, že přijdeme ke svému počítači a budeme chtít spustit soubor, který zde máme uložený. Ale soubor bude ke svému spuštění vyžadovat heslo. Možná si z nás mohl někdo pouze vystřelit, ale je také možné, že soubory zakódoval někdo, kdo bude chtít za jejich zpřístupnění zaplatit.

Tento nový způsob útoku je již pojmenovaný jako ransom-ware (vyděračský software).

Většina případů vydírání po internetu probíhá však na úrovni doručování elektronické pošty, kdy vydíraná osoba dostane e-mail a musí splnit požadavky odesílatele pod různými nátlaky.

**Otázka č. 7 Urážel tě někdo přes internet?**



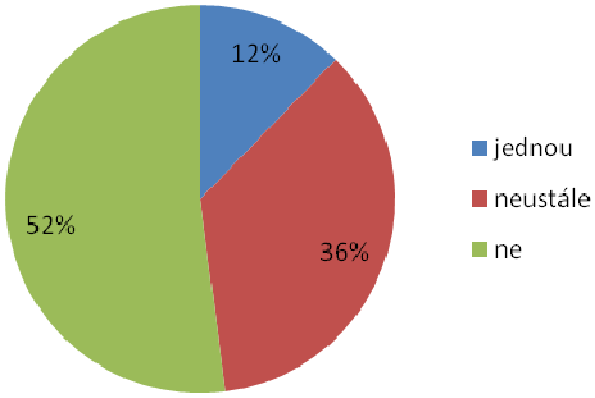

Graf č. 8 Urážení

Zatímco s vydíráním se setkalo pouze zanedbatelné množství dotazovaných, s urážkami přes internet je setkání častější. S urážením se setkalo 39% studentů tj. 152 osob.

S urážkami se můžeme setkat například při internetové diskusi, takže stát se obětí urážek není nijak obtížné. Stačí odpovědět na zveřejněný článek a hned můžeme obdržet urážku – flejmu.

Internet přináší i nové možnosti v oblasti šikany. Zatímco například ve škole jsou děti omezeny na dobu vyučování, k internetu mají přístup téměř kdykoli. Je tak snadné rozesílat škodlivé zprávy nebo šířit lživé pomluvy a v daleko větší míře a anonymitě.

**Otázka č. 8 Setkal ses s propagací násilí na internetu?**



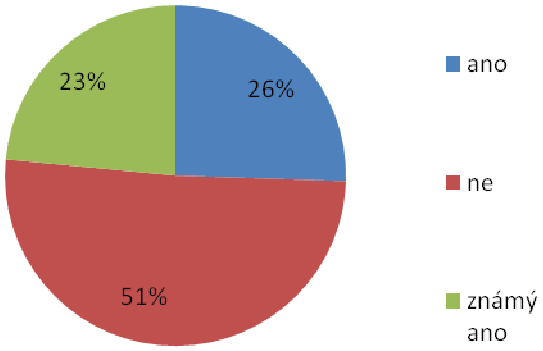

Graf č. 9 Propagace násilí

Polovina (52% tj. 204) dotázaných uvedlo, že se s propagací násilí na internetu nesetkalo vůbec. Naopak 36%, tzn. 140, dotázaných uvedlo, že se s propagací násilí setkává na internetu neustále. Zbylých 12% uvedlo, že se s touto propagací setkalo asi jedenkrát. Může se jednat o propagaci nacismu, propagační snímky skupiny Al-káida, znásilňování, domácí násilí atd.

Ve Finsku se stal případ, kdy se student rozhodl, že vyvraždí své okolí. Svůj zločin začal propagovat na Internetu a než bylo jeho nenávistné prohlášení odstraněno, zhlédlo ho sto padesát dva lidí, kterým se líbilo a kteří jej obodovali nejpozitivnějším hodnocením.

Dnes se můžeme setkat s propagací násilí i v počítačových hrách. Největší vliv pak mají tyto hry na děti, které si chtějí scény z hry samy vyzkoušet.

**Otázka č. 9 Setkal ses s podvodem na internetu?**

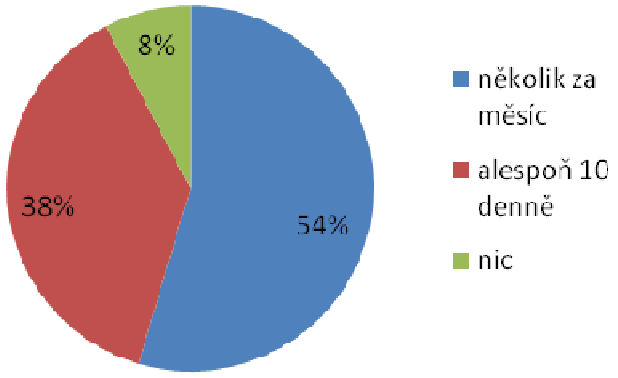



Graf č. 10 Podvody přes internet

S podvody pomocí internetu se nesetkala polovina dotazovaných tj. 200 studentů. To může naznačovat, že firmy jsou při obchodování přes internet většinou korektní nebo že ještě nejsme na nákupy přes internet tak závislí. Myslím, že většina našich spoluobčanů dává ještě přednost osobnímu prohlédnutí zboží a osobní koupi v kamenném obchodě.

Přesto se s podvodem spáchaným pomocí internetu setkalo 26% studentů, tj. 100 osob. Může se jednat například o nedoručení koupeného zboží z internetu, různé podvodné půjčky a poplatky za ně nebo domácí práce přes internet.

**Otázka č. 10 Chodí ti do e-mailové schránka spamy?**




Graf č. 11 Spamy

Pouze malé množství dotázaných (8%) uvedlo, že nedostávají žádné spamy. Více jak polovina (54% tj. 214) studentů uvedlo, že dostanou několik spamů do měsíce a 38% tj. 148 studentů uvedlo, že dostávají každý den alespoň 10 e-mailů nevyžádané pošty.

Dnes e-mailové schránky nabízejí možnost zablokovat určité adresy a nedostávat tak nevyžádané maily. Pokud si zřídíme e-mailovou na některém z komerčních serverů, tak tato schránka už obsahuje složku spam koš, kam se automaticky zatřiďují rozpoznané spamy.

# 9 Návrhy na zlepšení stávající situace

Boj proti počítačové kriminalitě, má stejně jako ostatní druhy kriminality, dvě složky – prevence a represe. Bez prevence by šlo asi těžko kriminalitu páchanou pomocí internetu snižovat. Mnohdy se trestných činů dopouští i nezletilé děti aniž by věděli, že se to nesmí. Takový malý pirát si stáhne z internetu hru a pak ji ve škole prodává vypálenou spolužákům. Rodiče většinou ani neví, co jejich potomek dělá. Pak se ale mohou divit, za co všechno jsou odpovědní.

## 9.1 Prevence

Prevence internetové a počítačové kriminality se dá rozdělit na prevenci psychologickou a technologickou. Jedna bez druhé by asi těžko fungovala.

### 9.1.1 Prevence psychologická

Již výše jsem zmiňovala případ, kdy potomek prodává ve škole spolužákům hry. Takový malý pirát může tušit, že se to nesmí, ale většinou o nějakém porušování autorství nemá vůbec tušení. A protože všeobecně povědomí o právech spojených s internetem a porušování autorských práv není nijak vysoká, rodiče svým dětem asi těžko něco zakážou.

Proto je úkolem psychologické prevence zvyšovat povědomí o tom, co se smí a co ne. Může se tak dít pomocí různých reklamních kampaní nebo upoutávek nebo pomocí různých internetových diskusí, kdy odborníci radí, co je trestné a co ne. Do psychologické prevence by mohlo patřit i zvýšení postihů za internetovou kriminalitu. Do povědomí občanů by se to zajisté dostalo pomocí sdělovacích prostředků.

Následující obrázky ukazují, jak se může pomocí reklamní kampaně zvyšovat povědomí o využívání nelegálního software.


Obrázek 2 Roman Neviděl


Obrázek 3 Tomáš Neslyšel

Mnohdy ani nevíme, za co všechno můžeme být potrestáni. Sestavila jsem proto krátký přehled vybraných trestných činů týkajících se využívání internetu a počítačů a jaké tresty je možné za ně uložit.

Tabulka 1 Trestné činy

| Čin | § TZ | Trest |
|---|---|---|
| **Poškození a zneužití záznamu na nosiči informací** | 257a | až 1 rok, zákaz činnosti, peněžitý trest, propadnutí věci; při značné škodě trest až 3 roky a při škodě velkého rozsahu až 5 let |
| **Podvod** | 250 | až 12 let |
| **Neoprávněné nakládání s osobními údaji** | 178 | až 5 let |
| **Provozování nepoctivých her a sázek** | 250c | až 5 let, případně peněžitý trest |
| **Pomluvy** | 206 | až 2 roky |
| **Vydírání** | 235 | až 3 roky, při velkém rozsahu nebo smrti až 12 let |
| **Ohrožování mravnosti** | 205 | až 1 rok, peněžitý trest nebo propadnutí věci |
| **Podněcování k nenávisti vůči skupině** | 198a | až 2 roky |
| **Podpora a propagace hnutí směřujících k potlačení práv a svobod člověka** | 260 | až 5 let, případně i 8 let |
| **Projevování sympatií k podobným hnutím z §260** | 261 | až 3 roky, při velkém rozsahu nebo smrti až 12 let |
| **Porušování autorského práva** | 152 | až 2 roky, peněžitý trest nebo propadnutí věci; při značném rozsahu trest až 5 let |
| **Porušování tajemství dopravovaných zpráv** | 239 | až 1 rok |

Snížit kriminalitu by se dalo i tak, že distributoři hudby a filmů sníží ceny za nosiče. Ceny by se musely dostat na takovou úroveň, kdy by se stahování a vypalování přestalo vyplácet. V dnešní době tomu v oblasti filmů napomáhá prodej DVD v novinách a časopisech. Takovéto DVD stojí do 50 Kč a je to rozhodně levnější než film 3 dny stahovat a pak vypalovat.

### 9.1.2 Prevence technologická

V případě technologické prevence se jedná především o technologické zabezpečení. Tak jak se stále zvyšuje počet uživatelů internetu a hlavně počítačů vůbec, tak je stále nutné vyvíjet nestále nové formy zabezpečení. Pořád jsou tak vyvíjeny nové ochrany proti kopírování nebo vniknutí do systému. Antivirové programy jsou mnohdy aktualizovány denně. Antivirové programy jsou aktualizovány denně, ale i ostatní formy ochran jsou vyvíjeny velmi rychlým způsobem. Někdy trvá totiž jen několik málo hodin, než útočník ochranu překoná. Je to takový nekonečný boj mezi útočníky a vývojáři těchto chránících prvků.

Je také nutné neustále vyvíjet a zdokonalovat ochranné prostředky v elektronickém bankovnictví. Neustále se objevují nové případy, kdy jsou zaznamenávány pokusy o nelegální převody peněz pomocí internetu.

Zabezpečení je nutné vyvíjet neustále a ve všech směrech. Například změna v lékařské zprávě provedená útočníkem přes internet může vést v extrémním případě až ke smrti pacienta. Takové scénáře jsou dobrými náměty pro různé filmy. Může se ale stát, že pro teroristické skupiny bude tato forma odstranění nepohodlných lidí, vítaným způsobem.

A tak záleží především na každém z nás, jak se budeme chovat a k čemu budeme internet využívat.

# 10 Závěr

V současné době je možno vidět obrovský nárůst informačních technologií a s tím spojené pronikání výpočetní techniky, vybavené softwarem, do celé společnosti. Tento vývoj pomohl již před několika lety vzniku nových druhů kriminality. Dnes se množství internetové a počítačové kriminality rozrůstá a obměňují se způsoby, jakými jsou tyto trestné činy prováděny. V posledních letech tak například vznikl kyberterorismus. Tento druh trestné činnosti využívají pro své cíle teroristické skupiny. A tak jak se neustále rozšiřuje počítačové a internetové povědomí společnosti, můžeme čekat, že vzniknou nové další formy trestné činnosti, která budou využívat informačních technologií.

Internetovou a počítačovou kriminalitu by šlo snížit tím, že softwarové společnosti by své produkty zlevnili a umožnili tak koupi legálních programů i chudším lidem. Přestože počítač je skoro pro každou domácnost v dnešní době již samozřejmostí, tak legální pořizování programů již zdaleka samozřejmostí není. Většina lidí u nás dává většinou přednost získání software a čehokoli nelegální cestou, aby náklady byly co nejnižší. Tato situace se týká především našich domácností a osobního užití. Poněkud lepší situace je na úrovni firem a podnikatelů, kterým hrozí obrovské sankce za používání nelegálně získaného software. Ve firemní sféře je větší možnost odhalení používání nelegálního software – například některým z bývalých zaměstnanců, který si s bývalým zaměstnavatelem takovým způsobem vyřizuje účty.

Používané metody a prostředky pachatelů jsou dnes na velmi vysoké technické a intelektuální úrovni. Ve většině případů je vyšetřování velmi složité. Pokud jsou útoky prováděny z veřejně přístupného internetu, je skoro nemožné pachatele vysledovat a zajistit dostatečné množství důkazů. V mnoha ohledech závisí stav a budoucí trend internetové kriminality i na každém z nás. Záleží, jaký postoj zaujmeme k získávání software a ostatních dat. Dnes je na internetu mnoho programů, které jsou freeware. Jejich hlavní výhody jsou v široké dostupnosti, že jsou zadarmo a jejich získání a používání je legální.

Důležitým faktorem prevence počítačové kriminality, je naučit se chránit si svůj počítač a svoje osobní data. Dnes pokud jsme on-line je nemyslitelné, abychom pracovali s internetem bez antivirového software. Stejně tak bychom se měli naučit neotvírat neznámé e-maily nebo poskytovat komukoli prostřednictvím internetu nebo i přes telefon svoje osobní údaje, čísla účtů nebo přístupová hesla.

I když výhled do budoucnosti internetové kriminality není nijak optimistický, je nutno neustále zvyšovat povědomí občanů o této problematice. Svůj vliv by mělo určitě i zvýšení právních postihů za tyto nelegální činnosti. Samozřejmě, že by úprava zákonů a dořešení trestů za počítačovou trestnou činnost, musela být provázena větší reklamní kampaní, aby se tyto změny dostaly do povědomí společnosti a staly se tak jakýmsi strašákem alespoň pro určitou část občanů.

# 11 Seznam použitých zdrojů

## 11.1 Klasické zdroje


**BARRETT, Daniel J. 1999.** *Bandité na informační dálnici.* Brno : Computer Press, 1999. str. 235. ISBN 80-7226-167-3.

**ČERMÁK, Jiří. 2003.** *Internet a autorské právo.* 2. aktualiz. a rozš. vydání. Praha : Linde, 2003. ISBN 80-7201-423-4 (brož.).

**CHALOUPKOVÁ, Helena.,SVOBODOVÁ, Hana. a HOLÝ, Petr. 2004.** *Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) a předpisy související : komentář.* 2. vydání. Praha : C. H. Beck, 2004. str. 515. ISBN 80-7179-840-1.

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

**POLČÁK, Radim. 2007.** *Právo na internetu : spam a odpovědnost ISP.* 1. vydání. Brno : Computer Press, 2007. str. 150. ISBN 978-80-251-1777-4 (brož.).

**SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. 1995.** Počítačové právo. Praha : C. H. Beck, 1995. str. 264. ISBN 80-7179-009-5.

**SMEJKAL, Vladimír. 2001.** *Internet a §§§.* 2. aktualiz. a rozš. vydání. Praha : Grada, 2001. str. 284. ISBN 80-247-0058-1.

**VRABEC, Vladimír, ČEPEK, Aleš. 1995.** *Internet :-) CZ.* Praha : Grada Publishing, 1995. str. 210. ISBN 80-7169-229-8.

## 11.2 Elektronické zdroje

EICHLER, Pavel. *Zpravy.idnes* [online]. 1998-2008 [cit. 2008-04-03]. Dostupný z WWW: <http://zpravy.idnes.cz/policii-schazeji-lide-pro-boj-s-internetovou-kriminalitou-pa2-/krimi.asp?c=A071227_140808_krimi_pei>

KOLAJA, Marcel, BARTOŠEK, Miroslav. *Jemný úvod do (anti)spamové problematiky*. *Zpravodaj ÚVT MU* [online]. 2002 [cit. 2008-02-11], s. 1-6. Dostupný z WWW: <http://www.ics.muni.cz/bulletin/articles/251.html>. ISSN 1212-0901.

KULHAVÝ, Petr. *Root.cz* [online]. 1998-2008 [cit. 2008-03-17]. Dostupný z WWW: <http://www.root.cz/clanky/kevin-mitnick-podvodnik-hacker/>. ISSN 1212-8309.

PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita*. *Ikaros* [online]. 2006, roč. 10, č. 8 [cit. 2008-02-25]. Dostupný z WWW: < http://www.ikaros.cz/node/3554 >. ISSN 1212-5075.

PŘIBYL, Tomáš. *SecurityWorld* [online]. 2006 [cit. 2008-04-14]. Dostupný z WWW: <http://www.securityworld.cz/sew.nsf/print/A0CFDD5E6BE3017AC12573D100441801>.

SOBOTKA, R. *Autorské právo a internet* [online]. 2007 [cit. 2008-04-14]. Dostupný z WWW: <http://www.kn.vutbr.cz/az-prednaska/071024-az-ppv-magnet-sobotka.pdf>.

*(1) Business center.cz* [online]. 1998- [cit. 2008-01-25]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/trestni_zakon/cast2h9.aspx#par254>. ISSN 1213-7235 .

(2) *Business center.cz* [online]. 1998-2008 [cit. 2008-04-12]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/trestni_rad/cast1h4.aspx>.

(3) *Filmy nejsou zadarmo* [online]. 2006- [cit. 2008-03-31]. Dostupný z WWW: <http://www.filmynejsouzadarmo.cz/cs/kauzy/p3/>.

*(4) Juristic.cz* [online]. 1999- [cit. 2008-01-25]. Dostupný z WWW: <http://trestni.juristic.cz/489552/clanek/trz>. ISSN 1802-789X.

(5) *Juristic.cz* [online]. 1999- [cit. 2008-01-25]. Dostupný z WWW: <http://trestni.juristic.cz/489548/clanek/trz>. ISSN 1802-789X.

(6) *Juristic.cz* [online]. 1999- [cit. 2008-01-25]. Dostupný z WWW: <http://trestni.juristic.cz/489556/clanek/trz>. ISSN 1802-789.

(7) *Policie je krátká na weby popírající holocaust*. *IDnes.cz* [online]. 2006 [cit. 2008-02-07]. Dostupný z WWW:<http://zpravy.idnes.cz/krimi.asp?r=krimi&c=A060222_114752_krimi_ton <>

(8) *Soom.cz* [online]. 2003-2008 [cit. 2008-03-17]. Dostupný z WWW: <http://www.soom.cz/index.php?name=recenze/show&aid=282>

(9) *Studentské městečko* [online]. 2007-2008 [cit. 2008-03-31]. Dostupný z WWW: <http://www.studentskemestecko.cz/view.php?cisloclanku=2008030002>. ISSN 1802-3185.

(10)*Trestné činy* [online]. 2006- [cit. 2008-01-25]. Dostupný z WWW: <http://www.trestni-rizeni.com/Trestneciny/247.html>.

*(11)Wikipedie* [online]. 2002 , 22.12.2007 [cit. 2008-01-16]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Uniform_Resource_Locator>.

## 11.3 Zdroje obrázků

obrázek č. 1
http://www.insoma.cz/paper/2006_06a/graf_1.gif
obrázek č. 2
http://i.idnes.cz/06/101/maxi/NYV163a9f_8_date_08_10_2006_time_11_31_17.jpg
obrázek č.3
http://i.idnes.cz/06/101/maxi/NYV163a9e_51_date_08_10_2006_time_11_31_04.jpg
obrázek č. 4
http://www.gtsav.gatech.edu/students/studentcenter/archive/news/kevin.mitnick.story.vert.jpg
obrázek č. 5
http://www.ovni007.com/sitebuildercontent/sitebuilderpictures/gary_mckinnon_2.jpg
obrázek č. 6
http://www.latinoseguridad.com/LatinoSeguridad/HCyP/Poulsen.jpg

## Seznam obrázků

# 12 Přílohy

## 12.1 Zločinci na internetu

### Kevin Mitnick

Obrázek 4 Kevin Mitnick

Kausa Kevina Mitnicka zahýbala světem počítačů v 90. letech minulého století. Šlo patrně o nejdiskutovanější a nejmedializovanější proces s počítačovým hackerem v historii vůbec.

Mitnick se již od dětství věnoval amatérskému radiovému vysílání. Později ho zaujal phone-phreaking, experimenty s telefony, voláním zadarmo a hrátky s ústřednami. Na střední škole se poprvé dostal k počítačům, kde ho téměř ihned zaujalo nabourávání se do systémů, zjišťování cizích hesel, neboť to všechno byl velmi dobrý zdroj zábavy. Z jeho životopisu se můžeme dočíst, že byl několikrát chycen a potrestán za hacking, což mu přinášelo stále větší popularitu.

Poslední kausa ho však proslavila nejvíce. V ní byl obviněn z napáchání škody 300 miliónů dolarů, byť mu nikdy nebylo prokázáno obohacení. Navíc "okradené" firmy na burze nevykázaly žádnou ztrátu, jak jim ukládá zákon.

Mitnickova image nejobávanějšího hackera je v podstatě mýtus vytvořený novináři. Sám Mitnick přiznává, že proces proti němu byl oprávněný, neboť on se nelegálně dostával do počítačových systémů a získával tajné informace, ale trest 5 let vězení plus zákaz používání počítačů a mobilních telefonů po dobu 3 roků od propuštění, nehledě na zacházení s podezřelým při vyšetřování (upírání základních svobod plynoucích z Ústavy), byl neadekvátní.

Jako každý hacker, Mitnick se prostě nabourával do cizích systémů, ale narozdíl od mnohých jiných se ani neobohacoval, ani neničil důležitá data. Hacking bral jako zábavu a jako výzvu, všechno dělal "pro vlastní potřebu". (KULHAVÝ)

## Gary McKinnon

Obrázek 5 Gary McKinnon

Gary McKinnon byl zatčen koncem roku 2002 za to, že pronikl do více než 90 počítačů americké armády ve Velké Británii. Jeho dílo je označováno jako: "největší vojenský hack historie" a tento nezaměstnaný Londýňan si tím vysloužil slávu.

Pronikl do 53 amerických vládních institucí. V počítačové síti US Space Command "nalezl důkazy o mimozemské misi". Ve zveřejněném interview se dostáváme k dalším informacím. Gary McKinnon se (podle svého vyjádření) zaměřoval na vyhledávání důkazů o mimozemšťanech - UFO existují, USA měly vyvinout antigravitační zařízení, 11. září je spojeno s dalšími podezřelými aktivitami atd…

Američané viní Brita nejen z nabourání se do přibližně stovky osobních počítačů, ale také z poškození celé sítě složené z více než 300 strojů základny US Naval Weapons Station Earle v New Jersey. McKinnon to údajně způsobil vymazáním určitých složek z napadených počítačů.

Tehdy 39letý Gary se podle svých slov velmi rád zajímal o UFO a hacking. Když se jedné noci potloukal v „modré sféře“, zdálo se, že konečně nalezl, co hledal. Zajímavé informace o UFO, které ještě nikdy neviděl…. Problém byl, že server ho k těmto datům nechtěl pustit, vyžadoval heslo. Gary byl zkušený hacker, prolomit jednoduchá hesla, která na serveru byla, pro něj nebyl žádný velký problém… Když už

prolomil ochranu, nemohl uvěřit svým očím. Mašina, kterou teď ovládal, byla vládní server. Gary vždy tvrdil, že byl motivován pouze svojí zvědavostí a nedostatečným zabezpečením. Rozhodně prý neměl v úmyslu způsobit jakoukoliv škodu.

Podle obžaloby pronikl McKinnon do amerického armádního počítače umístěného ve městě Fort Myer ve státě Virginia, získal práva správce systému a odeslal kódy, informace a rozkazy a pak vymazal asi 1300 uživatelských identifikací. Je také obviňován, že "vymazal klíčové systémové soubory", zkopíroval si soubor, obsahující uživatelské kódy a zašifroval hesla pro přístup k tomuto armádnímu počítači. Pronikl také do počítačů amerického námořnictva a letectva. K tomuto hackerskému útoku došlo bezprostředně po útocích z 11. září. Celý vojenský systém byl vyřazen z provozu po dobu jednoho týdne. Celkově měl McKinnon získat přístup k 53 počítačům, které přímo využívala americká armáda, 26 námořním systémům, 16 strojům organizace NASA a po jednom PC z amerického ministerstva obrany a oddělení US Air Force. Jeho proniknutí do americké vojenské počítačové sítě způsobilo, že byla vyřazena z provozu americká armádní síť v oblasti kolem Washingtonu. Celková škoda byla vyčíslena na 14,3 milionů korun.

Úřady Velké Británie ho chtěly propustit bez trestu, ale vložily se do toho Spojené státy, jejichž počítače byly napadeny. Požadovali vydání Garyho do USA, kde by mu jako maximální možný trest hrozilo 70 let ve federálním vězení…

Edmund Lawson, advokát, poukázal u soudu na fakt, že pokud by byl McKinnon vydán, čelil by možnému držení ve vazbě na časově neurčitou dobu bez možnosti složení kauce. Tím by byla porušena jeho základní lidská práva. Britský soud ho nakonec propustil na kauci 5000 liber, což je asi 200 000 Kč. A to nejen to, Gary se musí pravidelně hlásit na policejní stanici, aby necestoval do zahraničí a k tomu všemu mu bylo zakázáno připojovat se k internetu.

## Kevin Lee Poulsen

Obrázek 6 Kevin Lee Poulsen

„Kevin Lee Poulsen vystupující pod přezdívkou Dark Dante měl první konflikty se zákonem už v období puberty. Několikrát byl i odsouzen a začal sekat dobrotu. Stal se uznávaným specialistou na počítačovou bezpečnost. Ale dlouho mu to nevydrželo, v roce 1990 ve věku 25 let podlehl pokušení a opět se vrátil na šikmou plochu. Tehdy jistá rozhlasová stanice v Los Angeles vyhlásila lákavou soutěž o nový automobil Porsche 944S2 - měl jej získat soutěžící, který se jako 102. v pořadí dovolá na jisté telefonní číslo.

Poulsen nelenil a napadl místní telefonní ústřednu, kterou modifikoval tak, že v okamžiku spuštění soutěže bylo právě pro něj vyhrazeno ono vítězné 102. místo. Cenu sice převzal, ale vzhledem k určitým nesrovnalostem (jejich podstata nebyla nikdy zveřejněna) začala celou soutěž vyšetřovat FBI. Ta v dubnu 1991 Poulsena zadržela a obvinila jej ze sedmi trestných činů. Sazba byla čtyři roky vězení, 58 tisíc dolarů pokuty a tři roky zákazu práce s počítačem k tomu. Poulsen se údajně dostal/snažil dostat i do počítače FBI, když zjistil, že je jeho "vítězství" vyšetřováno. Chtěl zjistit, co se na něj chystá.

A ještě jeden kousek, který se povedl Kevinovi Poulsenovi - tentokrát v útlém věku. V roce 1983 jako osmnáctiletý mladík napadl síť Arpanet, předchůdce dnešního internetu. Našel totiž v její architektuře chybu, čímž dokázal (byť jen velmi dočasně) převzít do svých rukou kontrolu nad celou sítí. Toto nedokázal nikdo před ním a nikdo po něm. A už asi těžko dokáže.“(PŘIBYL, 2006)