ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Bakalářská práce

Analýza a vývoj počítačové kriminality v USA

Analysis and development of computer crime in the U.S.

Lenka Tenková

Plzeň 2012

ZADÁNÍ PRÁCE

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma

„Analýza a vývoj počítačové kriminality v USA“

vypracovala samostatně pod odborným dohledem vedoucího bakalářské práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni, dne …….

Lenka Tenková

OBSAH

ÚVOD

Současný svět je plný inovací, nových technologií a jde neustále kupředu. Není divu, že v posledních letech dosáhla technologického pokroku většina oblastí, co se výrobní, podnikatelské i průmyslové sféry týče. Jednou z oblastí, která radikálně postoupila vpřed, je oblast informačních technologií a komunikace.

Současně s vývojem všech oblastí naší i světové ekonomiky vzniká pojem tak zvané *nové ekonomiky*, která není v současné době přesně definována, ale týká se z velké části rozvoje ekonomiky a také radikálního rozšíření informačních technologií a komunikace. Se vznikem pojmu *nová ekonomika* [16] je spjata růstová fáze hospodářského cyklu ekonomiky Spojených států, Velké Británie a Irska v druhé polovině 90. let 20. století. V tuto dobu začaly vznikat otázky, jestli se nezačne ekonomika řídit novými pravidly nebo zdali nenastal čas vzniku nových ekonomických paradigmat. Důvodem vzniku tohoto pojmu je tedy skutečnost, že se ekonomika na počátku třetího tisíciletí svým charakterem zásadně liší od ekonomiky století dvacátého. *Novou ekonomiku* reprezentují [2] hlavně informační technologie, internet a telekomunikace. Radikálně se mění dříve zavedené způsoby komunikace v podnicích, dodávek mezi dodavateli a také způsob komunikace se zákazníky. Ve velké míře vznikají internetové obchody s nabídkou zboží a služeb pouze online. Nelze opomenout také komerční transakce, které je možné v dnešní době provádět bez použití fyzických peněz, a vznik komunikačních kanálů na internetu, mezi které patří například elektronická pošta, diskusní skupiny a groupwarové aplikace.

Vzhledem k tomu, že tímto nastoupil takzvaný *digitální věk*, není ani divu, že se začala rozvíjet počítačová kriminalita neboli kriminalita informačních technologií, která by se dala nazvat fenoménem naší doby. Dynamika vývoje moderních informačních technologií je natolik závratná, že je téměř nemožné vést krok s pachateli počítačové kriminality, natož je předbíhat.

Kvůli obrovskému rozvoji informačních technologií vznikají instituce, které řeší kriminální počiny a v dnešní době se počítačovou kriminalitou zabývají také mezinárodní instituce, jako je například Rada Evropy anebo OSN.

Nepřeberným zdrojem informací o této problematice je samozřejmě sám Internet, kdy je nutné rozlišovat, zdali jsou informace pravdivé, či nikoli. Není radno

důvěřovat každému internetovému zdroji a je žádoucí si veškeré informace o tématu ověřovat, což je samozřejmě velmi časově náročné. Z tohoto důvodu je na trhu k dispozici jen několik málo tištěných publikací, které byly ke zpracování teoretické části této bakalářské práce z velké části používány.

Dostupnost statistických informací o počítačové kriminalitě a různých kriminálních počinech je pro veřejnost takřka nulová. Například Česká republika nevede žádné statistiky byť o přestupcích nebo přímo spáchaných trestných činech počítačové kriminality. V ČR tuto problematiku žádná instituce detailně nesleduje, vyjma policie, která řeší její trestní otázky. Informační neboli počítačová kriminalita je v ČR sledována souhrnně pod hospodářskou kriminalitou, kdy jsou sledována jen podvodná jednání a hackerství**.** Například hlavním cílem celní správy České republiky [13] v oblasti internetové kriminality je odhalovat nelegální aktivity prostřednictvím monitoringu internetu se zaměřením především na ochranu práv duševního vlastnictví. Specializovaný útvar zaměřený na internetovou kriminalitu také vyhledává nelegální aktivity týkající se distribuce zboží, které podléhá dovoznímu clu, je zatíženo spotřebními daněmi, či které podléhá zákazům a omezením. Veškeré informace týkající se počítačové kriminality, které byly získány nejen touto institucí, zůstávají také uvnitř nich, žádná data nejsou veřejnosti dostupná a i nejobecnější otázky týkající se počítačové kriminality nebyly pro účely této práce vybranými institucemi v ČR zodpovězeny.

Skutečnost o tom, že u nás není počítačová kriminalita takřka řešena a informace o ní nejsou veřejnosti dostupné, byla také důvodem k tomu, současně se zájmem o tuto problematiku vůbec, že se tato práce zaměřuje na počítačovou kriminalitu v USA. Tato země eviduje statistická data o kyberkriminalitě a existuje zde mnoho institucí, které se této problematice intenzivně věnují.

Byly nalezeny oficiální stránky organizace vlády USA, která se věnuje stížnostem uživatelů internetu a zároveň spolupracuje s FBI, a která stížnosti přímo řeší. Jedná se o *Internet Crime Complaint Center (IC^3)* – centrum pro stížnosti týkající se internetového zločinu a přestupků, které poskytlo statistická data o spáchaných trestných činech v USA a další podrobné informace týkající se tématu.

Tato práce je rozdělena na tři dílčí části. První část je zaměřena na vznik a vývoj počítačové kriminality vůbec, popisuje druhy počítačové kriminality a vysvětluje základní pojmy. Druhá část práce je analytická a rozebírá vývoj kriminality v USA v posledních deseti letech. Poslední, třetí část, je věnována prevenci softwarového pirátství a obsahuje jednoduchá pravidla a rady, jak předejít počítačové kriminalitě.

1. Vznik a vývoj počítačové kriminality

Stejně tak, jako má historii lidstvo samo, má svou historii také kriminalita, která sahá hluboko do našich dějin. Kdy vznikl první zločin na světě vůbec? O tom lze možná jen polemizovat. Ale mluvíme-li o zločinu spáchaném v kyberprostoru anebo na počítačích, tak už můžeme mluvit konkrétněji. V následujícím textu jsou uvedené informace o historii počítačové kriminality a hlavních milnících v jejím vývoji.

1.1 Jak to všechno začalo – „Pravěk“

Dle autora Michala Matějky jsou události, týkající se počítačové kriminality, datované do roku 1981 označovány za „Pravěk“ [5] – tedy úplné počátky počítačové kriminality. Její vznik můžeme datovat do doby vynálezu telefonu, který se stal prvním prostředkem elektronické komunikace vůbec.

První počítače, které vznikly o více jak půl století déle, mezi sebou mohly komunikovat prostřednictvím telefonní linky, čímž se začal rozvíjet neidentifikovatelný prostor mezi počítači, tak zvaný *kyberprostor*. Tento pojem můžeme nazvat takovým prostorem, kde dochází ke vzájemnému spojení počítačů, probíhá zde komunikace, obchod, zábava a také zásadní téma této práce, kterým je kybernetický zločin.

Přesně datovat vznik počítačové kriminality ale bohužel nelze. Můžeme se zmínit o prvním zločinu tohoto typu vůbec, který byl uskutečněn v roce 1971 Johnem Draperem. Dotyčný objevil, že píšťalka, která byla přidávána do tehdy vyráběných cereálií se jménem *Cap „n“ Crunch*, vydávala zvuk o určité frekvenci, která narušila telefonní linku takovým způsobem, že bylo možno telefonovat bezplatně. Podvody tohoto typu se v USA stupňovaly a zneužívání telefonických linek získalo název *phreaking*.

Za zmínku stojí i rok 1973, kdy zaměstnanec spořitelny v New Yorku použil počítač ke zpronevěře přes dva miliony dolarů. Tato „pravěká“ doba může být považována i za počátky porušování autorských práv, protože v těchto letech (do roku 1981) vznikly kotoučové magnetofony, postupně i magnetické pásky, které bylo možno používat i prostřednictvím počítačů. [3]

Tehdy začalo dnes již tak známé kopírování například hudby a posléze i softwaru. V 70. letech bylo kopírování hudby ke svým vlastním potřebám legální, ale předvídatelně se na trhu začaly objevovat kopie za úplatu, což začalo představovat problém.

1.2 A je zde osobní počítač - „Středověk“

Počiny datované od konce roku 1981 až do roku 1994 jsou označovány za „Středověk“ [5]. Kyberkriminalita jako taková se začala masově rozvíjet až s dostupností prvních počítačů pro běžné domácnosti, což umožnila společnost IBM s představením svého prvního stolního počítače včetně telefonní linky s názvem IBM PC v roce 1981. Zajímavým se stal také rok 1984, kdy USA udělily soudní pravomoci „tajné službě“, aby mohla vyšetřovat počítačové podvody.

O rok později vzniká online magazín o „hackingu“ s názvem Phrack. Nutno poznamenat, že slovo „hacker“ nebo „hacking“ v minulosti nebylo spojováno tolik s kriminální činností, jako je tomu dnes. Hackeři své doby byly pozitivním faktorem pro rozvoj informačních technologií a softwaru, prováděli zásahy do programů z toho důvodu, že je chtěli nějakým způsobem vylepšit nebo byla potřeba zvýšit jejich využitelnost, úmyslem nebylo počítač či programy v jakémkoli slova smyslu zneužívat či znehodnocovat. Časem ale tento termín pozbyl svého významu a to zejména vlivem médií, která šířila informace o hackerství jen v negativním slova smyslu. Souhrnně se tak začali označovat všichni pachatelé útoků proti počítači a to i ti, kteří působili na počítač v pozitivním slova smyslu. V hackerské komunitě lze rozlišovat několik typů hackerů [4]:

- **Crackeři –** programátoři, kteří zneužívají hackerské metody pro finanční zisk, můžeme sem zařadit i uživatele internetu, který zneužívá internet pro vandalismus, finanční aktivity a další činnosti
- **White hats -** hackeři uznávající hackerskou etiku a jsou většinou zaměstnanci firem zabývající se bezpečností systémů – provádějí zásahy nebo napadení systémů, ale jen s vědomím a na žádost majitele, aby odhalili chyby či slabiny daného systému

- **Black hats –** hackeři provádějící činnosti stejně tak jako White hats, ale s tím rozdílem, že pracují pro nelegální organizaci. Tyto organizace se označují jako skupiny „H4H“ – Hackers For Hire a jejich členové nabízí své služby jiným kriminálníkům anebo extremistickým skupinám
- **Grey hats –** jedná se o taková hackery, kteří se svojí činností nacházejí na pomezí mezi Black a White hats. Dalo by se říci, že nemají ještě ujasněný svůj budoucí úkol
- **Guru –** výtečný programátor, který má dlouholeté zkušenosti a vyzná se v problematice
- **Wizard –** tak zvaný čaroděj, řeší problémy excelentním způsobem, který není pochopitelný ostatním programátorům

Roku 1986 byl v USA kongresem přijat federální zákon o počítačovém podvodu a zneužití počítače, ale do roku 1990 bylo odsouzeno jen minimum pachatelů, podrobněji viz níže. Jak již bylo zmíněno, povědomí o kyberkriminalitě získala široká veřejnost především sledováním médií, ale v roce 1983 k tomu také přispělo uvedení filmu War Games. Jednalo se o thriller z hackerského prostředí s víceméně klasickým scénářem: *„Mladý hacker pronikne do vojenského systému a díky snížené schopnosti rozpoznat realitu od hry málem rozpoutá třetí světovou válku.“* Vzhledem k tomu, že od té doby filmů s podobným námětem byla natočena celá řada, asi jen těžko může na tomto filmu dnes někomu připadat něco revolučního.

V roce 1983 byla ovšem situace zcela odlišná. Tento film společně s vydávaným časopisem Phrack inspiroval mnoho lidí k tomu, aby se o problematiku začali zajímat a tímto způsobem získávali informace a návody k tomu, jak například obejít rozličné systémy, jak se zdokonalit v oblasti phreakingu, jak získat čísla cizích kreditních karet a jak uskutečnit další nekalé aktivity ku svému prospěchu.

Dalším zajímavým datem v období středověku je 13. červen 1989, kdy došlo k tzv. floridskému skandálu. Volající do úřadu kurátora Palm Beach Country v Delray Beach na Floridě zjistil, že nemluví s nikým z personálu tohoto úřadu, ale se sexuální pracovnicí jménem „Tina“ ve státě New York. Kdykoli se pokoušel někdo kontaktovat tento úřad kurátora, byl záhadným způsobem přesměrován na linku vzdálenou stovky mil. Situace velice znepokojila tehdejšího telefonního operátora a bylo nutno zavést

důkladná šetření a stejně tak ani počítačová policie nezůstala sedět se založenýma rukama. Dalo by se říci, že tato událost doslova zvedla ze židle veškeré úřady, co se bezpečnosti týče, a muselo se již nějakým způsobem zakročit.

Policie si uvědomila vážnost hrozby, příště by to nemusel být jen nevinný žert amatérského hackera, ale koordinovaný zločin, který by mohl podstatně ovlivnit chod dalších událostí – mohlo by se jednat například o přeprogramování systému tísňového volání. Tento zlom, kdy se policie odhodlala situaci radikálně řešit, můžeme datovat do roku 1990, tehdy vyvrcholila operace Sundevil. Ze všech operací, které policie toho roku uskutečnila, byla Sundevil zdaleka nejznámější. Cílem byla celostátní razie na digitální underground – krádeže kreditních karet, zneužívání telefonních kódů - a zároveň byly podnikány razie proti hackerům. Dalším, ale ne přímo vytyčeným cílem byla skutečnost o tom, že trestná činnost týkající se kyberprostoru, nebude nadále tolerována.

Policie byla tehdy úspěšná, protože zadržela dokonce pachatele již zmíněného počinu se sexuální pracovnicí „Tinou“. Další osoby, které byly při operaci Sundevil zadrženy, byly především odborníky přes počítače a telekomunikaci, ale patřily mezi ně i sotva odrostlé děti, které byly zapálené pro moderní informační technologie. Tito zločinci páchali škody, které lze označit z minimální - neohrožovaly nikoho na životech a sami škůdci z toho neměli skoro žádný prospěch. Dalo by se říci, že to dělali jen pro zábavu a kvůli své zvědavosti.

1.2.1 Další významné události této doby [6]:

- 1986 – vytvořen první virus, který napadl počítače IBM
- 1988 – první Národní banka v Chicagu je obětí odcizení 70 milionů dolarů prostřednictvím počítače
- 1988 - dva studenti vytvořili tzv. „červa“ (virus), který měl napadnout vládní ARPANET (předchůdce internetu), ale vymyká se kontrole a rozšiřuje se do více jak 6000 propojených vládních a univerzitních počítačů

- 1989 – první podvodný virus, který je šířen jako spustitelný program, po jeho otevření uživateli počítače bylo virem oznámeno, že pokud nezaplatí 500 dolarů, budou jeho data z disku nenávratně smazána
- 1993 – podvod hackera Kevina Poulsena, zablokoval přístup ostatním volajícím do telefonní soutěže a sám tak vyhrál veškeré ceny (vyhrál 2 porsche, dovolené a 20 000 dolarů)

Co kdyby se ale několik odborníků a expertů spolčilo a začali by se snažit spáchat nějaký organizovaný zločin? Co kdyby stát a různé společnosti, které by byly napadeny, přicházely o miliony korun a lidé by přicházeli o život? Do této doby „Středověku“ tyto otázky ještě nepatří, jelikož se žádné podobné organizace neutvářely. O tomto fenoménu je nutno se zmínit až v další éře počítačové kriminality, která je nazývána jako „Novověk“ - vymezen rokem 1994 až dodnes.

1.3 Počítačová kriminalita a naše doba - „Novověk“

V této době přestávají hackeři páchat počítačové zločiny jen pro radost a mediální slávu, v čemž je obrovský zlom oproti předchozím érám. Počítačoví experti chtějí těmito činy získat peníze nelegálně a dochází k tak zvané profesionalizaci v oblasti hackerství. Samozřejmě nemůžeme opomenout „hodné“ hackery, kteří opravdu svojí činností přispívají společnosti, bohužel v současné době převládají ti, kteří svými praktikami poškozují ostatní.

Novověk je takové období, kdy se masově rozšiřují počítače s operačním systémem Microsoft Windows a osmibitové počítače jsou rychle vytlačeny technologií PC. Dochází také k rozšíření sítí typu Internet a především k rozvoji v oblasti grafického prostředí WWW (World Wide Web).

Internet již není k dispozici jen akademickému prostředí a vládě, ale rozšiřuje se do oblasti podnikatelské sféry. Internet bychom mohli označit za nový obchodní nástroj, skrz který začínají v obrovském množství téci peníze – podnikatelské subjekty vytvářejí pomocí grafického prostředí online prezentace a začínají vyvíjet svoje internetové obchody (e-shopy). Vzhledem k masovému rozšíření počítačů je samozřejmostí, že vzrůstá i počítačová kriminalita.

Prvním milníkem v době Novověku byl případ Citybank, kdy došlo k odcizení deseti miliónů dolarů a jednalo se již o organizovanou skupinu hackerů, kterou vedl ruský matematik Vladimír Levin. Tento případ ukázal, kudy se bude počítačová kriminalita nadále ubírat a analytici očekávali druhý a to mnohem nebezpečnější směr. Jejich předpoklady směřovaly k tomu, že by se informační technologie mohly stát účinným nástrojem mezinárodního terorismu. [5]

Prozatím k žádnému takovému předpokládanému masivnímu útoku nedošlo, což ale neznamená, že k tomu někdy v budoucnosti nemůže dojít. Od doby Citybank byl tento námět jen inspirací pro mnoho knih a také filmů. Zmíníme-li teroristické útoky v USA ke dni 11. Září 2001, nemůžeme jim, dle dostupných informací, nikterak připsat využití informačních technologií kromě jejich komunikační funkce.

Spojitosti mezi různými událostmi období novověku neexistují, proto označujeme rozličné počítačové zločiny jen za události této doby.

1.3.1 Nebezpečí plyne i od zaměstnanců

Jednalo se o průmyslovou špionáž od interního zaměstnance firmy, kdy pomocí internetu odeslal konkurenční společnosti okopírovanou topografii čipu Intel. Společnost ale jeho nabídky nevyužila, kontaktovala policii a zaměstnanec byl odsouzen k 33 měsícům odnětí svobody.

1.3.2 Omezení internetové komunikace

Zákonem byla stanovena nejednoznačná definice obscénního a neslušného obsahu internetové komunikace, kdy měla být zavedena i trestní odpovědnost za šíření obsahu komunikace po internetu. Přijetí zákona rozhořčilo mnoho členů internetové komunity a 10 000 subjektů včetně firmy Microsoft podali návrh proti jeho platnosti. Roku 1996 federální soud rozhodl o zrušení určitých sporných pasáží.

1.3.3 Ochrana autorských práv

Roku 1998 byl přijat kongresem Spojených států amerických další kontroverzní zákon o autorských právech, upřesňoval podmínky ochrany autorských práv. Z tohoto zákona plynulo například, že každý z manželů musí mít svojí vlastní licenci na autorské dílo. Dále zákon omezuje uživatele, aby si vytvořili kopii díla pro vlastní potřeby a navíc dle určitých rozhodnutí tohoto zákona je možno stíhat kohokoli, kdo publikuje na Internetu obsah, k němuž mohou mít přístup uživatelé (občané USA).

1.3.4 Virové hrozby

Masově se viry šířené po internetu rozšířili v období roku 1999 – 2001 jak do domácností, tak i do firem. Počet poškozených osob dosahuje řádu milionů a působí škody firmám a zapříčiňuje výpadky celých sítí. Viry se šíří především pomocí elektronické pošty, která je hlavním distribučním kanálem. První virus, který byl rozšířen do celého světa pomocí elektronické pošty, kdy se sám rozesílal prvním padesáti uživatelům z adresáře zasaženého počítače, se nazýval Melissa (březen 1999). Melissa nebyl destruktivní vir, ale přesto byl jeho tvůrce identifikován a zatčen. Další vir, který se na světě objevil, se jmenoval I Love You (květen 2000), jehož obsahem byl milostný vzkaz, který ale opět žádné soubory na napadeném počítači neničil ani žádným způsobem neměnil. Těmito dvěma uvedenými viry vše ale nekončí. Vznikají další nesčetná množství virů tohoto typu, ale i další, které páchají již škodu na napadeném počítači – mění nebo mažou soubory.

1.3.5 Další fenomény internetového světa

Do roku 2000 můžeme datovat novou kriminální aktivitu DOS (Denial of Service). Jedná se o odepření přístupu v tom slova smyslu, že útočníkova akce zahltí svými opakovanými požadavky cílový počítač a dokáže ho tímto úplně vyřadit z provozu. Tento typ útoku byl uskutečněn proti světově známým portálům a obchodům, jako jsou Amazon, Ebay, Yahoo a E-Trade, kterým způsobil velké ztráty.

V tomto roce také vytvořil student malý program, který dokázal dekódovat DVD takovým způsobem, aby bylo spustitelné pod operačním systémem Linux. Proti studentovi bylo vedeno trestní řízení, ze kterého následně sešlo.

Rok 2000 byl snůškou problému, co se světa internetu týče. Dalším studentem byl vytvořen program Napster, který umožňoval sdílet hudbu. Do této chvíle byl Internet organizován na principu klient-server, což znamená, že se uživatel připojoval na servery poskytovatelů obsahu a odtud stahoval požadovaná data, program Napster ale umožnil to, aby si uživatel mohl vyměňovat data s dalším uživatelem (tzv. síť P2P). Sdílení souborů pomocí programu Napster se masově rozšířilo a byla na něj podána žaloba. Bylo mu nařízeno, aby blokoval skladby, které jsou chráněny autorskými právy. Program byl nakonec koupen společností Bertelsmann, která ho měla spustit v podobě placené služby. Od té doby bylo vyvinuto spoustu nových programů na stejném principu, které nejsou kontrolními orgány vůbec sledované, protože by musely stíhat statisíce jejich uživatelů.

Hrozba týkající se počítačové kriminality by dle mnohých vlád mohla být regulována radikálním způsobem. Regulace kriminality by měla spočívat v tom, aby každý poskytovatel připojení umožnil státním orgánům monitorování dat a to nejen na základě soudního příkazu, ale kdykoli. K tomuto opatření by mělo patřit i omezení uživatelů v tom slova smyslu, že by neměli mít možnost si svoje data na počítači šifrovat.

Útoku na USA roku 2001 byla částečně připisována vina informačním technologiím a to kvůli tomu, že kdyby byla komunikace po internetu sledována, mohlo dojít k zamezení tohoto útoku. Představa, že by každý e-mail a komunikace na fórech byla sledována, je takřka nepředstavitelná pro řádné občany, kterým by tímto způsobem bylo narušováno soukromí a byli omezováni stejně tak jako již uváděným opatřením, kdy by mohly různé orgány kontrolovat obsah jejich počítačů.

Jako poslední fenomén této doby stojí za zmínku porušování autorských práv formou warezu. Warez jsou taková autorská díla, se kterými je nakládáno nelegálně například na různých fórech po internetu. Stejně tak můžeme nazvat šíření nelegálního software (dále jen SW), filmů a hudby například pomocí FTP serverů a sítě P2P. Způsob šíření warezu je vcelku jednoduchý. Verze komerčního SW, která má být dostupná na trhu v nějaký daný čas je získána warezovou skupinou ještě před jejím vydáním (odcizení z továrny, využití kontaktů), ze SW je odstraněna ochrana proti

kopírování a takto upravený program je rozšířen na volně přístupné servery. Stejně tak se zachází s filmy, které jsou obvykle dostupné na internetu ještě před oficiálním vydáním.

1.3.6 Další významné události této doby [6]:

- **1995** – federální internetové stránky jsou napadeny a poškozeny hackery
- **1996** – Američan (vedoucí účetního oddělení) se pokouší proniknout do souborů oddělení počítačové obrany a z jeho 250 000 pokusů je 65% úspěšných
- **1997** – America On-line (největší poskytovatel Internetu v USA), zablokoval přístup uživatelům z Ruska kvůli vysoké úrovni internetových podvodů
- **1997** – německý Chaos Computer Club prohlašuje, že proniknul do software Microsoftu a převáděl si peníze mezi účty, aniž by o tom poškozený uživatel ani provozovatel účtu věděl.
- **1997** – FBI v USA vydala prohlášení o tom, že 85% internetových stránek různých společností bylo v tomto roce napadeno, aniž by o tom správci stránek věděli
- **2000** – hackeři pronikli do firemní sítě Microsoft a zpřístupnili zdrojový kód nejnovější verze operačního systému Windows a také sady Office
- **2003** – virus vyřadil kritické bezpečnostní systémy v jaderné elektrárně v Ohiu
- **2004** – Brian Salcedo se snažil získat informace o kreditních kartách zákazníků a byl zatčen
- **2005** – telefon Paris Hilton byl zneužit počítačovým pirátem, který zveřejnil její fotografie na internetu.
- **2005** – e-mailový systém FBI byl napaden a zneužit hackerem
- **2006** – hackeři pronikají do počítačů vnitřní bezpečnosti, instalují zde malware a převádějí obsah do čínského jazyka
- **2006** – jaderná elektrárna v Alabamě je vyřazena z provozu kvůli přetížení sítě

- **2007** – DoS útoky jsou uskutečněny proti vládním internetovým stránkám v Estonsku, včetně policie, ministerstva financí a parlamentu
- **2008** – osobní fotky z MySpace a Facebook jsou dostupné komukoli prostřednictvím manipulace s URL (přesné umístění zdrojů na internetu)
- **2008** – těsně před Pensylvánskými demokratickými volbami jsou stránky Baracka Obamy přesměrovány hackery na stránky Hillary Clintonové.

Incidentů tohoto typu bylo nesčetně mnoho a neustále jich postupem času přibývá. Zde byly zdůrazněny jen některé z nich, aby bylo evidentní, že počítačová kriminalita je pro naši společnost skutečnou hrozbou a nelze ji v žádném případě opomíjet. Bližší informace o počítačové kriminalitě a jejím vývoji je možno najít v publikaci Michala Matějky [5].

2. Detailní pohled na počítačovou kriminalitu

Každý z nás si pod pojmem počítačová kriminalita nepředstaví určitě jen jednu konkrétní věc nebo jeden konkrétní zločin. Tento druh kriminality může být páchán různými formami a může obsahovat rozličné trestné a nemorální činy – jednoduše by se dalo říci, že se jedná o širokou mezioborovou disciplínu. Může jít o nelegální sdílení dat, šíření pornografie a další činnosti, o kterých jsme se již zmínili v úvodu této práce. Nadále se budeme věnovat dalším nelegálním aktivitám v kyberprostoru.

2.1 Definice počítačové kriminality

Počítačová kriminalitu lze jen těžko jednoznačně definovat a existuje spousta pohledů na vyjádření její podstaty. Každý pohled na tuto problematiku se určitým způsobem liší, ale její definování je stále nejisté a v průběhu času se mění. Je to zapříčiněno tím, že se informační technologie začínají prolínat do mnoha oblastí lidského počínání.

Uvedeme si zde dvě definice počítačové kriminality, které nejlépe vystihují její podstatu. Za první z nich můžeme považovat tu, která je akceptovaná v rámci Evropské unie a zní: „*Počítačová kriminalita je nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich změnu*.“ [23] Tato definice je shledávána za jednoduchou, ale ne dostatečně vystihující vzhledem k tomu, že zde není určeno, jakým prostředkem je kriminalita páchána. Proto je zde zmíněna ještě jedna definice, která je sice rozsáhlá, ale dostatečně vystihující. „*Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně vetší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti. Často se pojem počítačová kriminalita používá i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity, aby ji usnadnily. Určujícím operacionálním elementem je přitom vždy způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu*.“ [23]

Tato definice by mohla být rozšířena ještě o skutečnost, že za trestnou činnost (počítačovou kriminalitu) je považováno hlavně nekalé počínání, které je páchané v kyberprostoru. V dnešní době totiž počítačová kriminalita využívá z poměrně velké části k uskutečnění trestných činů právě Internet a jiné sítě.

2.2 Druhy počítačové trestné činnosti

Stejně tak jako není snadné definovat pojem týkající se kyberkriminality, není jednoduché jednoznačně určit druhy počítačové trestné činnosti. Někteří autoři člení druhy počítačové kriminality dle dvou hledisek. Může se jednat o takovou trestnou činnost, kdy terčem napadení je sám počítač (program, data, informační systém atd.), anebo jde o takové protiprávní jednání, jehož nástrojem k uskutečnění je přímo počítač (program, data, informační systém atd.).

Dále lze rozdělit druhy počítačové kriminality podle typu činu na protiprávní jednání *tradiční*, kdy je počítač buď nástrojem trestné činnosti, nebo je jejím terčem, a protiprávní jednání *nová*, která se objevují s nástupem moderních informačních technologií. [5] Dalo by se říci, že oba dva druhy kriminality jsou úzce propojeny vzhledem k tomu, že bez počítače do jiného počítače jednoduše proniknout nelze.

Za důležitý dokument, který vznikl v rámci činnosti Rady Evropy, je považována „Úmluva o počítačové kriminalitě“, kde je specifikováno dělení počítačové trestné činnosti z úplně jiného hlediska. Úlohou mezinárodních dokumentů Evropského společenství je totiž sjednotit úpravu trestního práva a tak tomu je i u počítačové kriminality. Tato Úmluva obsahuje seznam tzv. „minimálních“ a „volitelných“ trestných činů, do kterých jsou zahrnovány [7]:

Minimální seznam trestných činů:

- počítačové podvody
- počítačové falzifikace
- poškozování počítačových dat a programů
- počítačová sabotáž
- neoprávněný přístup

- neoprávněný průnik
- neoprávněné kopírování autorsky chráněného programu
- neoprávněné kopírování fotografie

Volitelný seznam trestných činů:

- změna v datech nebo počítačových programech
- počítačová špionáž
- neoprávněné užívání počítače
- neoprávněné užívání autorsky chráněného programu

Tímto seznamovým vymezením Evropského společenství je dáno, které trestné činnosti budou stíhány v zemích EU. Seznam minimálních trestných činů zahrnuje jednání, která by měla být zapracována do právních řádů jednotlivých zemí a volitelný seznam vyjadřuje, která je možno označit za trestné činy, ale není to nezbytné.

2.2.1 Bezpečnostní hrozby

Nejen pachatelé počítačové kriminality jsou hrozbou pro informační systémy a počítače. Oni sami by takovou hrozbou nebyli, kdyby neexistovaly byť sebemenší chyby v těchto systémech, které jsou výzvou právě pro hackery. Informační systémy totiž nejsou určeny jen pro správu informací, ale i pro řízení a správu jiných systémů. Hrozbou může být tedy cokoliv, co nějakým způsobem může vést k nežádoucím změnám například informací nebo chování systému. Některé základní bezpečnostní hrozby jsou uvedeny na obrázku č. 1.

Obrázek č. 1: Bezpečnostní hrozby

Únik informace	Situace, kdy jsou důvěrná data prozrazena neautorizovanému subjektu
Narušení integrity	Je porušena konzistence dat – ztráta, zničení, modifikace dat neautorizovaným subjektem
Potlačení služby	Úmyslné odepření přístupu oprávněnému subjektu k jeho informacím (viz již zmíněné zahlcení systému opakovanými požadavky - DOS)
Nelegitimní použití	Neoprávněný přístup a používání zdroje neadekvátním nebo nelegálním způsobem
Fyzický průnik	Útočník pronikne k ovládacím prvkům systému a získá nad ním kontrolu
Trojský kůň	Na první pohled nevinný software, který, po jeho spuštění, ohrožuje bezpečnost uživatele a jeho dat

Zdroj: Zpracováno podle [5]

Proti bezpečnostním hrozbám vůči informačním systémům je vícero možností ochrany, které budou zmíněny v závěru této práce.

2.3 Různé formy počítačové trestné činnosti

Tato část práce je zaměřena přímo na formy počítačové trestné činnosti, které jsou nejčastěji páchány v USA, ale vzhledem k tomu, že se jedná o kyberkriminalitu, můžeme konstatovat, že se jedná o trestné činy páchané globálně. Souhrnně se jedná o nové typy protiprávního jednání, jejichž klasifikace může být obtížnější.

3.3.1 Hacking

Hacking by se dal definovat jako neoprávněné vniknutí do systému nebo počítače nestandardní cestou. Aby se hacker do systému dostal, je nutné, aby obešel nebo prolomil bezpečností ochranu z vnějšku a to zpravidla ze vzdáleného počítače. Pachatel se nepřipojuje k počítači přímo, ale většinou přes více internetových serverů z různých částí světa, aby skryl svojí lokaci. Ti, kteří by chtěli získat informaci o pachateli, jsou většinou bezradní, protože dokážou získat pouze internetovou adresu předchozího počítače (serveru), přes který se daný hacker připojil.

Incidenty tohoto typu se liší zejména podle toho, co hackery motivuje (zábava, msta, zvědavost, hmotný zisk) a většinou se nejedná o situace, kdy jsou napáchány nevratné škody, ale jen o takové činy, které odrážejí zvědavost počítačových expertů. Není to samozřejmě ale pravidlem.

3.3.2 Cracking

Jedná se o prolamování nebo obcházení ochranných prvků elektronických nebo programových produktů s cílem jejich neoprávněného použití [4]. Oproti hackingu je zde jeden zásadní rozdíl a to ten, že pachatelé svými činy chtějí bezpodmínečně získat určitý obnos peněz anebo tak jednají s cílem poškodit druhou stranu nenávratným způsobem. Příkladem crackingu může být generátor hesel k programům, které je nutno si zakoupit s licenčním klíčem. Pomocí generátoru získá uživatel nelegálně licenční klíč, na základě kterého může program bezplatně, ale nezákonně užívat. Může se také jednat o takové programy, které crackeři vytvořili, aby překonali ochranu softwaru proti kopírování. Cracking tedy úzce souvisí i s již zmíněným pojmem *warez*.

3.3.3 Sniffing

Jednoduše řečeno se jedná o odposlouchávání komunikace na síti, které je neoprávněné. Může se zdát, že se jedná o nevinnou činnost, ale není tomu tak. Odposlouchávám lze zachycovat přístupová hesla do jiných systémů a také sledovat komunikaci, čímž je porušováno osobní tajemství a jeho prozrazením, například třetí straně, může být pachatel odsouzen až na dva roky vězení.

3.3.4 Zneužití internetových stránek

Tak jako si sprejeři označují svoje území pomocí graffiti, tak i hackeři označují svoje dobitá území (www stránky). Když prolomí nějaké internetové stránky, většinou na nich vyvěsí různorodé pomluvy či je nějakým způsobem poškodí, uvedou telefonní číslo s nějakou obscénní fotografií, vloží odkaz na další pobuřující stránky – je mnoho způsobů, jak se dají www stránky zneužít, záleží jen na vynalézavosti hackera. Příklad

zneužití internetových stránek, neboli hacknutí www stránek nalezneme v příloze č. 4 na konci této práce.

3.3.5 Šíření materiálů se závadným obsahem

Tolik informací, kolik jich můžeme nalézt na internetu, nedokážeme najít jinde na světě. Na úkor internetu musíme ale konstatovat, že zde nalezneme nejen informace, které můžeme považovat za pravdivé, ale také mnoho fikcí, které jsou občas od reality k nerozeznání. Mezi materiály se závadným obsahem patří především šíření pornografie a materiály podporující extremismus. Nejedná se o novou formu kriminality, nýbrž jen o nově nalezený způsob šíření závadného obsahu.

Následující dva podbody považujeme také za šíření materiálů po internetu, ale již se nejedná o šíření až zase tak závadného obsahu, jako tomu bylo v předchozím případě.

I. Spamming

Každý z nás se již jistě se *spammingem* setkal. Jedná se o šíření informací, které nejsou pro daný subjekt (příjemce informace) žádoucí. Doslova se jedná o nevyžádanou elektronickou poštu anebo také nevyžádanou *instant message* s reklamním nebo propagačním obsahem. E-mailové adresy a i například čísla ICQ jsou spammery získávány různými způsoby – nejčastějšími zdroji bývají www konference, ICQ, různé registrační stránky a další. Obranou před spammingem můžou být různé filtry poštovních klientů, které jsou založeny na základě Bayesových filtrů – vyhodnocují pravděpodobnost spamu pomocí analýzy struktury přijaté zprávy. Na základě vyhodnocení poštovní klient přesouvá SPAM do složky nevyžádaná pošta, aby uživatele neobtěžovala. Vhodnou obranou před spammingem je také znepřístupnění svých kontaktů na veřejných místech na internetu.

II. Hoax

Hoax v překladu znamená mystifikaci nebo žert a vystupuje v negativním slova smyslu na internetu ve formě nevyžádané pošty či zprávy. Tato zpráva nebo informace uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající jeho další rozeslání mezi přátele, případně na co největší množství dalších adres, proto se někdy označuje také jako řetězový e-mail, který jistě všichni důvěrně známe. Důvěřiví uživatelé tyto zprávy, v domnění, že někomu pomohou, zasílají svým přátelům a tím bohužel nevědomky šíří poplašné zprávy nebo dokonce viry. Příklad hoaxu je k nalezení v příloze č. 5. Využívá naivity a neinformovanosti uživatelů a nejčastěji vystupuje ve formě [10]:

- **Falešný poplach** – zpráva manipuluje s informacemi a snaží se uživatele přimět hlavně k dalšímu šíření (*Pozor ICQ je vir, pošlete to všem.*) nebo dokonce k nějakému destruktivnímu zásahu (*Smažte jbdmgr.exe z instalace Windows, je to virus.*)

- **Zábava** – dříve se řetězové dopisy šířily jen klasickou poštou, dnes se přesunuly na Internet. Tyto využívají uživatelovy touhy být vtipný nebo jeho pověrčivosti a vyhrožují (*Nepřepošleš-li, budeš mít smůlu.*). Naopak poslušnému uživateli slibují všechno možné

- **Prosby** – hoax většinou působí na city a prosí příjemce o darování krve, hledání ztracené osoby, případně přímo vylákává peníze. Některé z těchto zpráv původně opravdu rozeslali lidé ve svízelné životní situaci, ale hoaxy často přežívají mnohem déle, než měl autor v úmyslu. (Např. známý hoax s žádostí o krev pro Alexandra Gála šířený v prosinci 2004 více než čtyři roky po jeho smrti.)

3.3.6 Malware

Jedná se o škodlivý software, který při spuštění v počítači zahájí takovou činnost, která vede k poškození napadeného systému. Software je většinou naprogramován takovým způsobem, že se spustí automaticky po provedení předem dané činnosti – například se otevře určitá zpráva v elektronické poště. Může se jednat o *spyware*, kdy aplikace monitoruje napadeného uživatele a zasílá informace subjektu, který program vytvořil. Další formou malwaru je *infoware*. Jedná se o aplikace pro informatickou podporu klasických bojových akcí, respektive jako soubor aktivit, které slouží k ochraně, vytěžení, poškození, potlačení nebo zničení informací nebo informačních zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství nad konkrétním protivníkem.

Poslední formou malwaru je *adware* jehož účelem je předání reklamního sdělení i přestože si jeho příjemce vůbec žádné takové informace nevyžádal. [23]

I. Viry

Viry jsou pojmem pro nás všechny důvěrně známým a netřeba se o něm zmiňovat rozsáhle. Jedná se o podmnožinu malware a za vir je označován takový parazitující soubor, který se připojí k určitým programům nebo systémovým oblastem, které pozmění. Může se nekontrolovatelně rozšiřovat, nebo po svém spuštění zahájit destrukční proceduru (poškození, změnu či zničení dat, degradaci funkce operačního systému, stahování dalšího malware atd.). [23]

II. Trojské koně

Pod tímto pojmem si přímo můžeme představit historicky známého Trojského koně, který Řekům posloužil jako válečná lest a překvapení, díky kterému vyhráli trojskou válku. Stejně tak funguje trojský kůň v oblasti informačních technologií. Uživatel nemá ponětí o tom, že je v jeho počítači program, monitorující specifické činnosti, o které jeví tvůrce trojského koně zájem. Sleduje například navštívené internetové stránky a také znaky, které stiskl uživatel na klávesnici – tak může získat přístupové informace k webovým stránkám, bankovním účtům nebo kontům elektronické pošty.

Programy, které si dobrovolně instalujeme například za účelem zobrazování počasí, můžou jednoduše sbírat data o naší činnosti. Proč programy obsahují tento druh adware? Touha po zisku. Program je dán uživateli zdarma, na oplátku je ale s programem zobrazována uživateli reklamní plocha. Nejedná se o nebezpečné programy, ale ve větší míře mohou obtěžovat. Druhým typem trojských koní je již zmíněný spyware, který již není tak nevinný a sbírá hesla uživatelů.

III. Přesměrovače

Jedná se o takový malware, který uživatele přesměrovává na jiné stránky, než on sám chtěl navštívit. Jedná se o takové www stránky, kde dojde automaticky k instalaci dalšího viru anebo dojde ke značnému zvýšení poplatku za připojení k Internetu, pokud používá uživatel telefonní linku se zvýšeným tarifem. [23]

3.3.7 Kybernetické výpalné

Jedná se o formu zneužití informačních technologií, kdy pachatel vydírá svou vyhlídnutou oběť, která je například provozovatelem internetových stránek. Pod výhružkou zneužití nebo znepřístupnění stránek svoji oběť vydírá o určitý peněžitý obnos. Žádný systém není nikdy dokonale zabezpečen a jejich provozovatelé si bezpečností většinou nejsou sami jisti, a proto raději zaplatí tzv. *e-výpalné,* aby si zajistili ochranu svých dat.

3.3.8 Defacement

Pod tímto pojmem je skryt průnik do webových serverů protivníka a nahrazení jeho internetových stránek obsahem, který vytvořil útočník. *Defacement* není skryt, naopak - usiluje o medializaci. Jeho psychologická síla spočívá jednak ve vyvolání pocitu ohrožení a nedůvěry ve vlastní informační systémy napadené strany, jednak v prezentaci ideologie či postojů útočníka [23]. *Defacement* je úzce souvislý již se zmíněným tématem o zneužití internetových stránek.

3.3.9 Phishing

Jedná se o podvodnou techniku, která je používána na Internetu k získávání hesel, čísel kreditních karet a dalších důvěrných informací. Principem phishingu je rozesílání oficiálních žádostí e-mailem, které se tak tváří ale jen na oko – běžný důvěřivý uživatel vůbec nepozná, že se jedná o podvodnou zprávu. Vyzývají adresáta například k zadání jeho údajů na odkazovanou stránku, která může napodobovat přihlašovací stránku internetového bankovnictví. Jakmile uživatel svoje údaje zadá, tvůrce phishingové stránky získá přihlašovací jméno a heslo a jednoduše pak pronikne k jeho bankovnímu účtu.

Odhalit takového podvodné zprávy nelze jednoduše, ale existují dvě zásadní chyby, které tvůrci phishingu často dělají. V přijatém textu zprávy bývají viditelné gramatické chyby a stránka, na kterou nás e-mail odkazuje, vypadá podezřele – graficky se byť minimálně liší a také její načítání trvá delší (nebo naopak kratší) dobu, než jsme u oficiálních stránek zvyklí. Proto je nutné dbát na ochranu svých údajů a důkladně si ověřovat veškeré zprávy, jestli jsou opravdu věrohodné. Příklad phishingového dopisu je k nalezení v příloze č. 6 na konci tohoto dokumentu.

3.3.10 Cyberstalking

Jedná se o takzvaný „internetový lov“, jehož podstatou je zneužívání online komunikace k nabízení nepožadovaných služeb a věcí, virtuální pronásledování, obtěžování a zastrašování vybraných uživatelů přes internet. Oběti tohoto chování jsou pak pronásledovány a obtěžovány v chatovacích místnostech spamem, zanecháváním vzkazů v návštěvních knihách, zasíláním virů apod. V kriminologickém smyslu je pronásledování definováno jako úmyslné, zlovolné obtěžování jiné osoby, které snižuje kvalitu jejího života a ohrožuje její bezpečnost [8]. Při komunikaci je nutná obezřetnost a uvědomění si toho, že ne každý je tím, za koho vystupuje.

3.3.11 Cybersquatting

Tento výraz může být považován za velmi záhadný, ale není tomu tak. Slovní spojení vystihuje přesně jeho význam. Jedná se o blokování internetových domén formou registrace názvu nějaké velké společnosti, instituce, produktu nebo známé služby. Uživatel (společnost, instituce), která by si chtěla založit www stránky pod jménem svojí firmy, bude muset zaplatit poplatek tomu, kdo si doménu již zaregistroval – squatterovi. V tomto případě se spíše jedná o nekalou soutěž nežli počítačovou kriminalitu.

3. Analýza počítačové kriminality

Tato část práce se zaměřuje na celkovou analýzu počítačové kriminality v USA z dostupných dat od roku 2001 do roku 2010, které byly získány ze stránek již zmíněného IC^3 centra. Je nutné konstatovat, že dostupné informace o kriminalitě nejsou úplné. Je to jen zlomek informací, které bylo možno vysledovat na základě stížností, které podali uživatelé Internetu právě tomuto centru přímo online. Nejedná se tedy o všechny zločiny, které byly v průběhu let spáchány, ale jen o ty, které byly Centrem zaznamenány. IC^3 zaznamenává a řeší jen stížnosti v rámci USA. Přesto je nutné poukázat na skutečnost, že i přestože nejsou dostupná veškerá data o počítačové kriminalitě, v následující analýze je zobrazen vcelku reálný obraz vzrůstající kriminality našeho světa.

3.1 Nejčastěji páchané trestné činy (2001-2010)

V průběhu deseti let se spáchané trestné činy hodně měnily a každým rokem vzrůstal jak jejich počet, tak jejich druhy. Následující trestné činy na základě dostupných informací můžeme označit za „top stížnosti“ v USA, co se počítačové kriminality týče.

- **Aukční podvody (Auction Fraud)** – Podvody vztahující se na aukční portály na internetu, kdy zakoupené a zaplacené zboží není prodejcem odesláno zákazníkovi.

- **Nedodání zboží (Non-delivery of Merchandise)** – Skutečnost, kdy zákazník zaplatí za objednané zboží předem, ale zásilku se zbožím neobdrží. Do této skupiny stížností nezahrnujeme aukční podvody.

- **Podvody s kreditními kartami (Credit Card Fraud)** – Jak již název vypovídá, jedná se o zneužití kreditních karet, kdy se pachatel pokouší zaplatit odcizenou kartou za zboží a služby.

- **Krádež identity (ID Theft)** – Incident, který vzniká na základě krádeže osobních údajů. Jedná se o takové situace, při kterých nedochází zároveň k odcizení jiných věcí – např. peněz. Existují různé druhy krádeže identity, například:
    - *Vládní podvody* – takové podvody, které souvisí s daněmi, sociálním pojištěním a krádeži řidičských průkazů
    - *Bankovní podvody* – sem zahrnujeme změna údajů na šecích, PIN kódy
    - *Zaměstnanecké podvody* – jedná se o zaměstnance bez platného čísla sociálního zabezpečení, který si ho jednoduše půjčí od někoho jiného, aby získal práci
    - a další [20]

- **„Nigerijské dopisy“ (Niggerian Letter Fraud) –** V těchto dopisech obvykle ministr, konzul nebo třeba vdova po diktátorovi některé z afrických zemí nabízeli firmám i jednotlivcům možnost zisku ve formě provize za zprostředkování převodu větší finanční částky ze země. K získání několika desítek tisíc dolarů měl adresát zaslat své osobní údaje a údaje o bankovním účtu, popřípadě poskytnout i finanční zálohu. [18]

- **Zneužití důvěry (Confidence Fraud)** – Zneužití důvěry ve slova smyslu, že uživatelé spoléhají na diskrétnost ostatních. Jedná se o překroucení pravdy ze strany podvodníků anebo zatajení důležitých skutečností kdy výsledkem je finanční ztráta pro „věřitele“. [12]

- **Obchodní podvody (Business Fraud)** – Jedná se o takový podvod, kdy společnost vědomě zkresluje pravdu nebo skrývá jisté materiální fakta. Jako příklad můžeme uvést konkurzní podvody anebo porušování autorských práv. [12]

- **Šekové podvody (Check Fraud)** – Jedná se o trestný čin, kdy se neoprávněně používají anebo nelegálně získávají šeky. Může jít o také o půjčování peněz, které neexistují v rámci zůstatku na daném peněžním účtu. Příkladem může být přijetí soukromého nebo bankovního šeku od neznámého zahraničního partnera, jako formu úhrady za zboží a služby například v rámci internetového obchodu. Po přijetí nás může potkat zjištění, že šek je falešný – tedy nezískáme žádné peníze a navíc musíme uhradit poplatek za předložení šeku. [18]

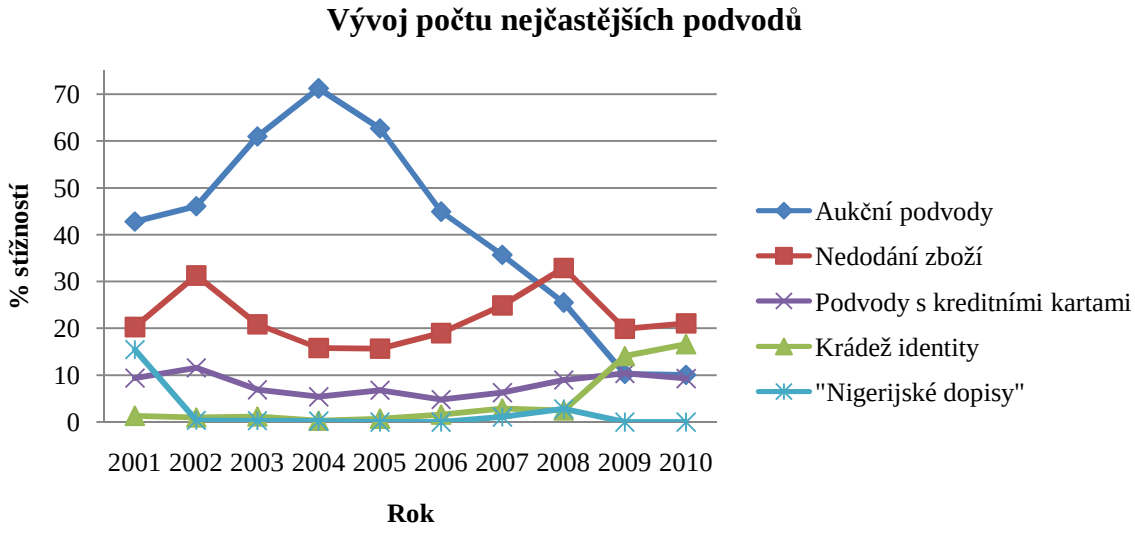
- **Počítačové podvody/poškození (Computer Fraud/Damage)** – Používá se pro klasifikaci stížností, zahrnující trestnou činnost, kdy dochází k počítačové destrukci, poškození anebo vandalismu vůči vlastnictví. Patří sem:

    - adware, spyware, hacking
    - zneužití počítače
    - počítačové virusy

V následující analýze jsou k nalezení některé další, a to méně časté stížnosti, které budou vysvětleny dodatečně s jejich výskytem v daných letech, pokud se nejedná o již vysvětlené pojmy ze sekce 3.3.

Od roku 2001 do roku 2010 se počty a druhy počítačové kriminality měnily, ale mezi nejčastější přečiny dle stěžovatelů IC^3 patří především aukční podvody, nedodání zboží, podvody s kreditními kartami, krádež identity a také Nigerijské dopisy. Vývoj těchto podvodů zaznamenává obrázek č. 2 na následujícím listu.

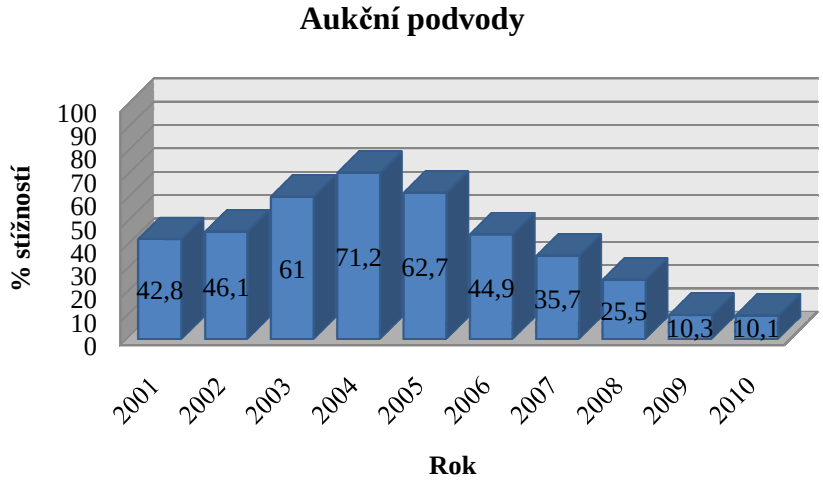
Obrázek č. 2: Vývoj počtu nejčastějších podvodů



Zdroj: Zpracováno podle [12]

Aukční podvody jsou stále ještě jednou z největších hrozeb, na kterou můžeme na Internetu narazit, přestože je z grafu zřejmé, že v průběhu posledních šesti let tyto podvody poklesly. Největší rozmach aukčních podvodů v USA byl v roce 2004, dokud se nezačala uplatňovat bezpečnostní opatření na aukčních serverech a lidé si nezačali uvědomovat rizika nakupování v online aukcích. Můžeme říci, že stejně tomu tak bylo i v České republice, kdy se uchytil jeden z dnes největších aukčních serverů www.aukro.cz. Detailnější vývoj aukčních podvodů můžeme vidět na obrázku č. 3.

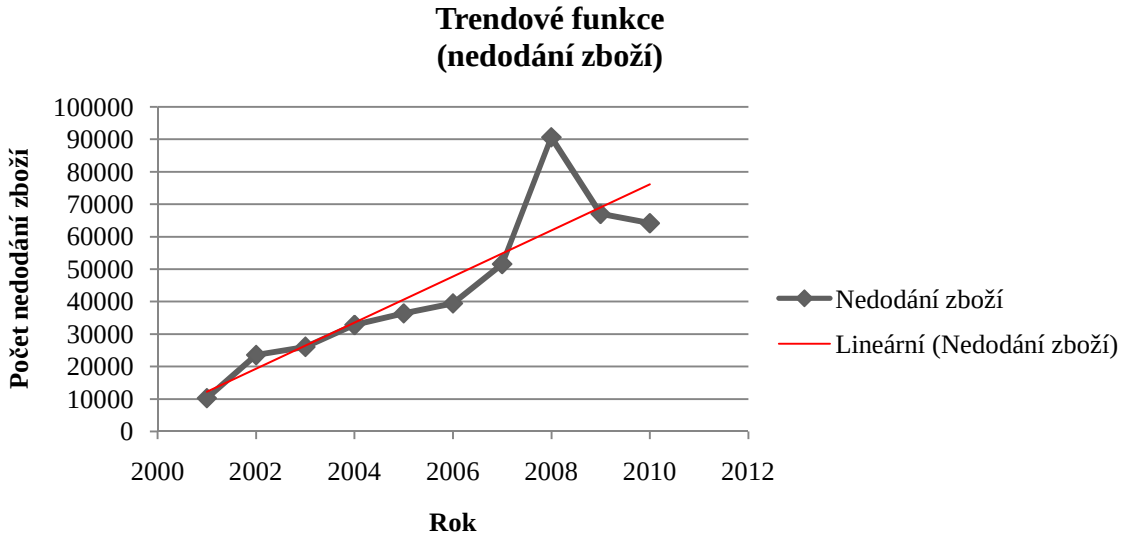
Obrázek č. 3: Vývoj aukčních podvodů



Zdroj: Zpracováno podle [12]

Nedodání zboží, při objednání z internetových obchodů, je také jedním ze stálých problémů, vyskytujících se při obchodování online. Je radno dbát na recenze a názory zákazníků, kteří již na některých z námi vybraných online obchodů zboží zakoupili. Na níže uvedeném grafu můžeme sledovat růst počtu stížností týkající se této problematiky v průběhu sledovaného období. Řetězové indexy a další data týkající se růstu přijatých stížností, nalezneme v příloze č. 1.

Obrázek č. 4: Vývoj počtu podvodů (nedodání zboží)



Zdroj: Zpracováno podle [12]

Co se podvodů s kreditními kartami týče, nejedná se o nerozšířenější typ trestné činnosti, ale za to přichází poškození k největším peněžitým ztrátám než při jakémkoli jiném online podvodu. Z obrázku č. 2 je zřejmé, že procento stížností na tento typ podvodu se drží neustále na 10 procentech a dalo by se předvídat, že nadále zůstane na této hladině anebo mírně poroste. Důkazem toho, že podvody s kreditními kartami jsou v USA stále aktuální, může být článek z října minulého roku, kdy bylo přes sto lidí obviněno z podvodů s platebními kartami. Policie USA sledovala gang několik měsíců a odhalila, že se jednalo především o pracovníky v bankách, restauracích – ti ukradli zahraničním turistům a tisícům Američanům kreditní karty a bankovní kódy. Tato síť je považována za jednu z nejdůležitějších, která byla v USA kdy odhalena. Gang totiž fungoval nejen v USA, ale platební karty kradl také v Evropě, v Asii, v Africe a na Blízkém východě [19].

Krádež identity v minulosti nebyla tak rozšířená, jako je tomu v posledních letech. V USA nastal obrovský růst koncem roku 2008, kdy statistiky zaznamenaly 10 milionů obětí tohoto trestného činu – nárůst oproti předchozímu roku činil 22%. Dle informací jedna oběť v průměru přišla ke ztrátě ve výši $ 851 – $ 1 378 a celkově ztráta činila 31 bilionů dolarů. Vzhledem k tomu, že tento rok byl opravdovým rozmachem krádeže identity, byla učiněna různá vládní opatření. Nehledě na jejich provedení, v roce 2009 nárůst kriminality nepoklesl. Krádež identity tento rok postihla 11,1 milionů lidí a celková ztráta vyčíslená v dolarech byla 54 bilionů. Jak můžeme pozorovat z obrázku č. 2, vývoj krádeže identity v USA neustále roste.

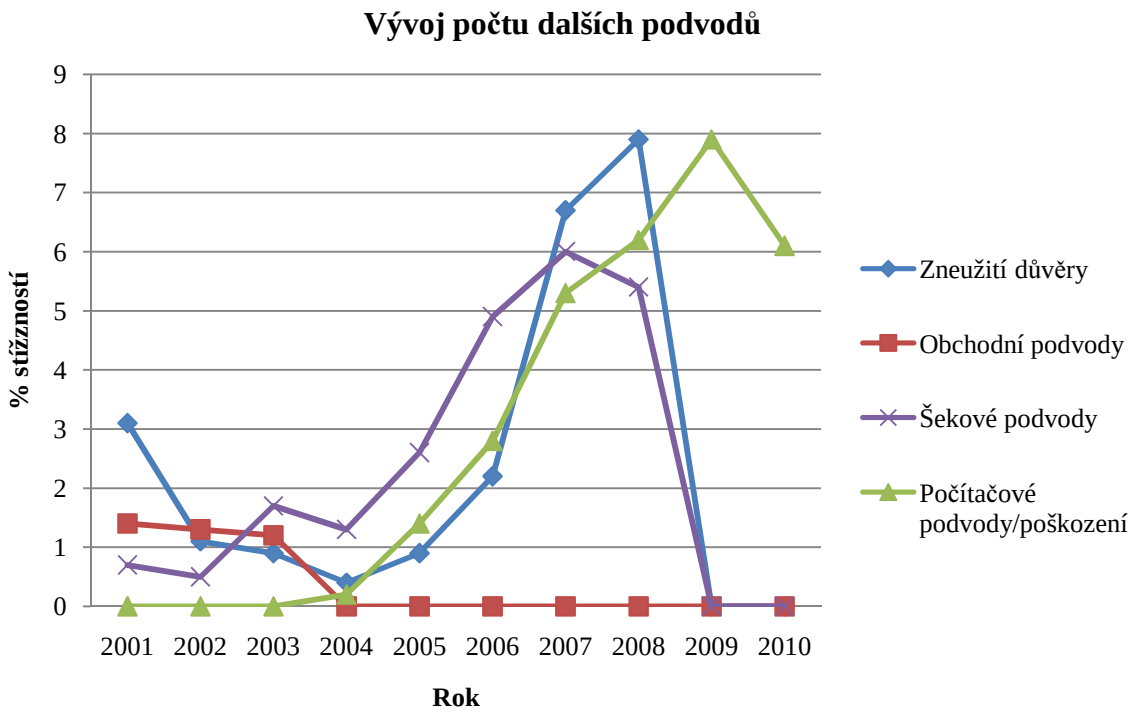
Poslední položkou z nejčastěji páchaných trestných činů jsou Nigerijské dopisy, které se ve velkém množství vyskytovaly především v roce 2001. Přestaly být aktuální skoro ihned po jejich vzniku, ale ze seznamu přečinů je zdaleka ještě vyškrtnout nemůžeme. S rozmachem sociální sítě Facebook se začaly „dopisy“ znovu šířit, ale ne zdaleka v takovém množství, jak tomu bylo v minulosti [15].

Následující obrázek č. 5 zobrazuje vývoj méně častých podvodů, na které si uživatelé internetu stěžují. Za nejvýznamnější položkou ze znázorněného grafu můžeme označit zneužití důvěry a také počítačové podvody/poškození.

Jak můžeme sledovat, zneužití důvěry se vyšplhalo ke svému vrcholu právě v roce 2008, kdy počet stížností dosáhl 7,9% z celku a každý z uživatelů, který nahlásil tento typ podvodu, přišel k újmě v průměrné výši $2,000. Zneužití důvěry uživatelů čítá 14,4% peněžité ztráty ze všech nahlášených trestných činů daného roku.

Počítačové podvody, na rozdíl od podvodů se zneužitím důvěry uživatelů, se objevily na seznamu stížností později a to až v roce 2004. Rokem 2009 si tyto dva podvody vystřídaly pozice, co se vedoucích příček týče – zneužití důvěry klesá k nule a počítačové podvody vedou se 7,9 %. Rok 2010 bohužel nepřišel s radikálním poklesem dané problematiky, ale přece jen se snížil o 1,8%.

Obrázek č. 5: Vývoj počtu dalších podvodů



Zdroj: Zpracováno podle [12]

Obchodní podvody nehrály v průběhu sledovaného období velkou roli, jak můžeme pozorovat z obrázku č. 5, ale šekové podvody se ukázaly být nebezpečným přečinem v průběhu let 2004-2008.

Zajímavým faktem je, že v roce 2010, kdy ustaly stížnosti od individuálních uživatelů, se ve velké míře objevily stížnosti od organizací, které byly poškozeny. Průzkum u 5 200 organizací ukázal, že 71% z nich mělo v tomto roce zkušenost s pokusem anebo opravdovým podvodem, co se šekových podvodů týče. [11]

3.2 „Nové“ podvody dnešní doby

Současný uvedený výčet trestných činů v této práci není zdaleka úplný. Za zmínku stojí uvést ještě další čtyři počiny, které se vyskytují nejčastěji v posledních dvou letech sledovaného období (2009-2010). Všechny čtyři trestné činy udeřily Internet ve velké míře v tu samou dobu a v minulosti se vyskytovaly jen zřídka. Respektive IC^3 centrum nezaznamenalo do roku 2009 žádné stížnosti v takovém rozsahu, aby přesahovaly 1% z celkových nahlášených stížností.

Jedním z možných důvodů, proč v minulosti nebyly tyto podvody zaznamenány, může být teorie, že oběti neshledávaly například SPAM a FBI podvody za závažné, a tak je nenahlašovaly. Níže uvedené podvody můžeme nazývat jako „nové“, kvůli jejich rozmachu v posledních dvou letech, přestože jsou dosti známé i z let minulých. Řadíme mezi ně:

- **Poplatky předem (Advance Fee Fraud)** – Jedná se o komunikaci např. po e-mailu, kdy jsou oběti přesvědčovány o skutečnosti, že když uhradí na daný účet určitou částku, obdrží zajímavý předmět nebo další „naslibované“ věci.

- **Přeplatkové podvody (Overpayment Fraud)** – Jako prodejci zboží na Internetu můžeme nabízet různé předměty a objeví se zájemce, který nám chce zaplatit o něco více, než my za zboží požadujeme. Po dohodě nám zájemce doloží doklad o zaplacení a z nějakého důvodu (omyl, rozdíl v poštovném atd.) zažádá o navrácení poměrné částky ze zaplacené sumy. Jakmile mu od nás dorazí poměrná část (přeplatek), a my zašleme zboží, které si on zakoupil, přijdeme o obojí. Platební příkaz má totiž druhá strana ještě možnost stornovat.

- **FBI podvody (FBI scams)** – Označovány jsou tímto názvem z prostého důvodu. Podvodníci, kteří chtějí od uživatelů získat například nějaké identifikační údaje nebo peníze, nevystupují samozřejmě pod svým vlastním jménem. Jednoduše se podepíšou jménem FBI anebo dalších institucí, kterým uživatelé důvěřují.

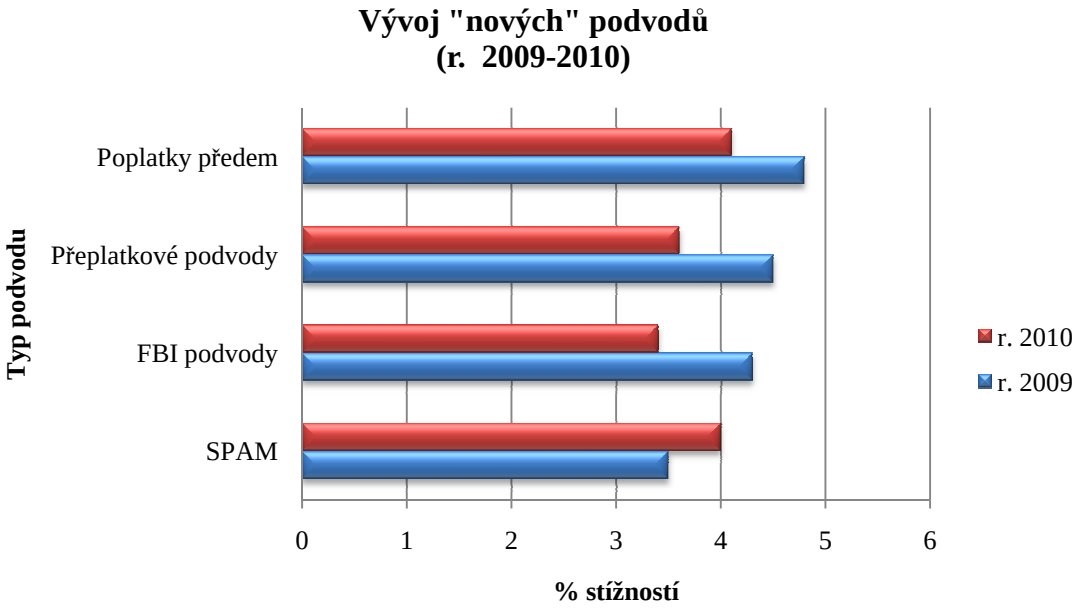
- **SPAM** – Nevyžádaný e-mail, který je obvykle masově rozšiřován (více k tématu v sekci 3.3.5 – I.)

Jak můžeme pozorovat na obrázku č. 6, v roce 2009 se ve velké míře objevily všechny čtyři typy podvodů, přestože v předchozích letech nebyly vůbec zaznamenány. Například poplatky předem dosáhly v roce 2009 z celkového počtu podvodů hodnoty 4,8%, přeplatkové podvody 4,5% a FBI podvody čítaly 4,3 %. Na rozdíl od „SPAMů“ tyto podvody v následujícím roce začaly klesat a všechny se průměrně se snížily o 0,83%.

Nevyžádané e-maily (SPAM) v roce 2009 byly na nižší úrovni než ostatní podvody (3,5%), ale v následujícím roce zato vyšplhaly na výši 4% z celkových stížností. Dle mého názoru lze očekávat ještě větší růst nevyžádané pošty a reklam do budoucna.

Lidé jsou zvědaví a žádostiví po informacích a i když se nezaregistrují na stránkách různých agentur (organizací, firem), když vyhledávají informace, vždy je zde možnost, že e-mailová adresa přijde do rukou nesprávné osobě. Výsledkem jsou zaplněné schránky nevyžádanou poštou.

Obrázek č. 6: Vývoj “nových” podvodů



Zdroj: Zpracováno podle [12]

Za zmínku stojí také trestný čin, za který je považováno šíření dětské pornografie po internetu. IC^3 centrum zaznamenalo nejvíce stížností v průběhu let 2005 a 2006, kdy počet stížností z celku přesáhl 1%. Jakkoli se toto číslo zdá nízké, vyjadřuje fakt, že společnost podniká správné kroky k tomu, aby se dětská pornografie po Internetu nešířila a vůbec aby vznikala.

3.3 Pachatelé počítačové kriminality

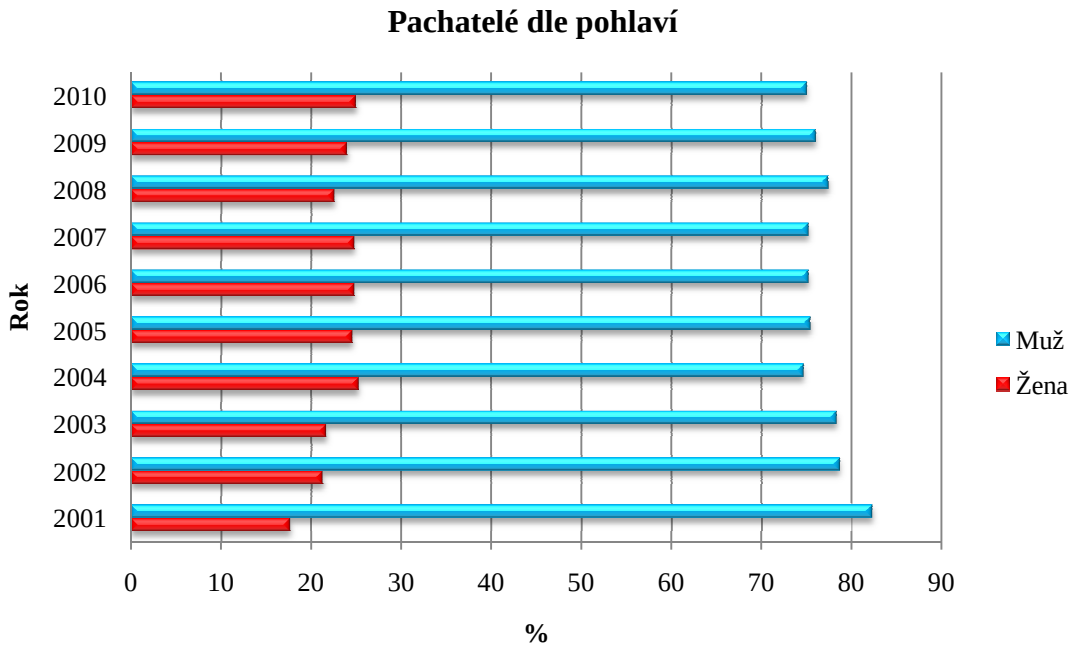
Většina pachatelů počítačové kriminality v USA, i mimo spojené státy, jsou jednotlivci. Samozřejmě se najdou i tací, kteří vystupují pod nějakou organizací (může se jednat dokonce i o firmy). Data o organizovaných zločinech v záznamech IC^3 bohužel nenalezneme. Dle dostupných a vysledovaných informací od IC^3 ale můžeme pachatele rozlišovat dle pohlaví a státu, odkud trestné činy, týkající se počítačové kriminality, jsou páchány.

3.3.1 Pohlaví pachatelů

Mluvíme-li o pohlaví pachatelů, jistě pro nás nebude žádným překvapením fakt, že ve větší míře jsou spáchané trestné činy připisovány na bedra silnějšího pohlaví, tedy mužům. Může tomu být tak kvůli skutečnosti, že vztah k počítačům a informačním technologiím mají především muži. Ženy se této oblasti moc nevěnují, ale přesto se samozřejmě najdou nějaké výjimky.

Jak je z obrázku č. 7 zřetelné, žádné radikální změny v průběhu sledovaného období nenastaly. Změny v tom slova smyslu, že vedoucí pozice při spáchaných trestných činech obsazují muži. Průměrně se procentuelní počet pachatelů z celku pohybuje u mužů na hodnotě 76,82 % a u žen je hodnota ve výši 23,18 %

Obrázek č. 7: Rozdělení pachatelů dle pohlaví



Zdroj: Zpracováno podle [12]

3.3.2 Pachatelé dle státu

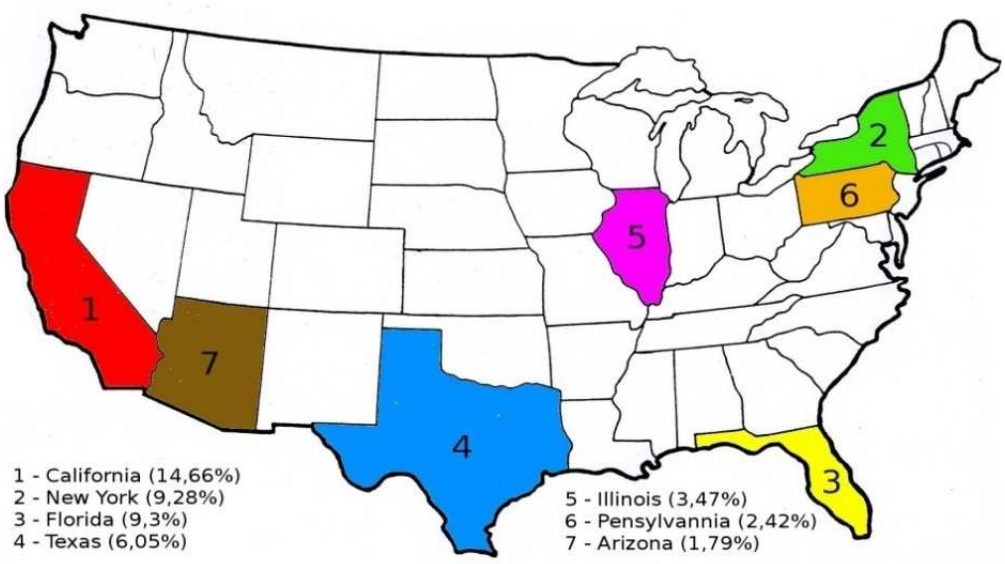
Jak již bylo zmíněno, pachatele je možné rozlišovat i dle státu, ze kterého je trestný čin páchán. Můžeme konstatovat, že se převážné jedná o oblasti s větší hustotou obyvatel, proč tomu tak je, o tom můžeme jen polemizovat. Možné vysvětlení by se dalo najít v teorii, že v méně zabydlených oblastech se lidé věnují především společenským aktivitám a dalším činnostem, které nemají nic společného s kriminalitou v jakémkoli slova smyslu. Kriminalita jako taková je ale ve velké míře sledována hlavně ve velkých a také hodně obydlených oblastech, kde se lidé mohou skrývat za davy jiných a nemají k sobě žádné vztahy.

Růst počítačové kriminality v určitých oblastech můžeme možná připsat také úrovni vzdělanosti a psychickému vývoji dnešní mládeže. Čím dál tím více se mezi pachateli objevují mladí jedinci, kteří předčí některé počítačové experty. Může tomu tak být kvůli faktu, že se celé dny nevěnují ničemu jinému než zkoumání dané problematiky a vynechávají svůj sociální život – vyjma sociálních internetových sítí jako je Facebook, Twitter a podobně. V dané míře je možné, že i rozvoj této sociální sítě dal vzniku větší počítačové kriminalitě. Jedná se ale pouze o polemizování.

Vědeckých článků nebo výzkumů na toto téma není v současné době ještě mnoho – jedná se již ale o další velmi diskutabilní téma, které by vystačilo na další obdobnou práci, jako je takhle.

Následující obrázek č. 8 zobrazuje procentuelní výčet počtu pachatelů na daném území v jednotlivých státech.

Obrázek č. 8: Oblasti s největším počtem pachatelů



Zdroj: Zpracováno podle [12]

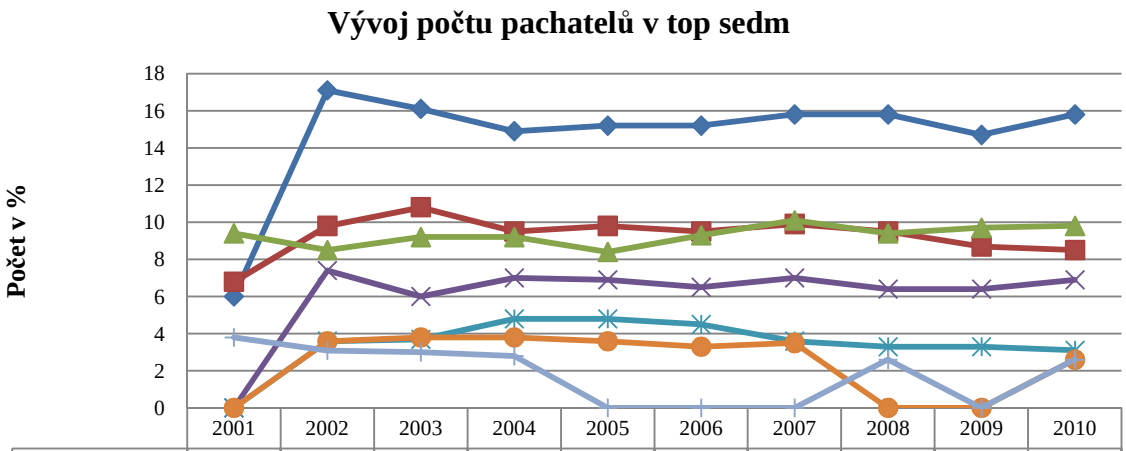
Informace byly získány shrnutím a zprůměrováním dat za sledované období deseti let. Vzhledem k tomu, že je USA rozděleno na 51 států, ve výročních zprávách IC^3 jsou uváděna data jen pro top deset z nich. V této práci je uváděno jen prvních *top sedm*, které jsou nejfrekventovaněji sledovány kvůli počtu spáchaných trestných činů, co se počítačové kriminality týče. Čísla na mapě od jedné do sedmi znázorňují žebříček dle počtu pachatelů. Číslo 1 znamená nejvíce pachatelů v oblasti a číslo 7 tedy opak.

Stát California si od roku 2002 drží až do současné doby první příčku v žebříčku. Z celkového počtu objasněných podvodů v USA se v Californii vyskytuje průměrně 14,66 % všech pachatelů. Tato hodnota se neustále drží svého trendu a v průběhu deseti let dosáhla svého minima v roce 2001, kdy čítala 6 %. Jen tehdy se Californie posunula poprvé a naposledy na třetí pozici.

Roku 2001 byla na první pozici Florida s hodnotou 9,4 %, ale následný trend se v průběhu období častokrát měnil (viz obrázek č. 9). Důvodem, proč je největší

množství pachatelů internetových podvodů právě v Californii, může být již zmíněná skutečnost, že tato lokalita, stejně tak jako New York, Florida, Texas a Illinois, patří k těm nejlidnatějším oblastem v zemi.

Obrázek č. 9: Vývoj počtu pachatelů



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
California	6	17,1	16,1	14,9	15,2	15,2	15,8	15,8	14,7	15,8
New York	6,8	9,8	10,8	9,5	9,8	9,5	9,9	9,5	8,7	8,5
Florida	9,4	8,5	9,2	9,2	8,4	9,3	10,1	9,4	9,7	9,8
Texas	0	7,4	6	7	6,9	6,5	7	6,4	6,4	6,9
Illinois	0	3,6	3,7	4,8	4,8	4,5	3,6	3,3	3,3	3,1
Pensylvania	0	3,6	3,8	3,8	3,6	3,3	3,5	0	0	2,6
Arizona	3,8	3,1	3	2,8	0	0	0	2,6	0	2,6

Zdroj: Zpracováno podle [12]

Druhou pozici v *top sedm* zaujímá tedy New York se svými 9,28 % pachatelů, následuje Florida (9,3%) a Texas (6,05%). Tyto státy si průměrně udržují svoje pozice v celkovém žebříčku.

Státy Texas a Illinois byly v roce 2001 předčeny v žebříčku *top sedm* státem Arizona a California, proto data pro rok 2001 nejsou známa. Průměrně ale počet pachatelů byl vyčíslen na 6,05% (Texas) a 3,47% (Illinois). Stejně tomu je tak u dalších států, které svými počty pachatelů již nejsou tak významné – Pensylvannia (2,42%), Arizona (1,79%).

3.4 Stěžovatelé na počítačovou kriminalitu

Mezi oběťmi počítačové kriminality není mnoho jedinců, kteří by si na svoji újmu v jakémkoli slova smyslu stěžovali. Většina obětí nevyhledává pomoc a neobrací se na různé instituce, které by pátrali po pachateli daného trestného činu. Jedná-li se ale o situace, kdy je škoda například výraznější částky anebo způsobí větší újmu, oběť vyplní elektronický formulář na internetových stránkách IC^3. Profil stěžovatelů obsahuje informace, jako jsou:

- Věk,
- pohlaví,
- utrpěná peněžitá ztráta,
- stát pobytu.

Do profilu stěžovatelů můžeme zahrnout také formu komunikace s pachatelem. Typy této komunikace mohou být samozřejmě různé. Mluvíme-li ale o počítačové kriminalitě, je zřejmé, že na prvním místě bude jednoznačně komunikace přes e-mail a následně komunikace přes webové formuláře. Minimální formou komunikace, figurující při jednání s pachatelem počítačové kriminality, je telefon, fyzická pošta, tištěné materiály, osobní kontakt a v neposlední řadě také chatovací místnosti a fax. Tyto formy komunikace jsou v poměru s e-mailem a webovými formuláři zanedbatelné.

3.4.1 Věk stěžovatelů

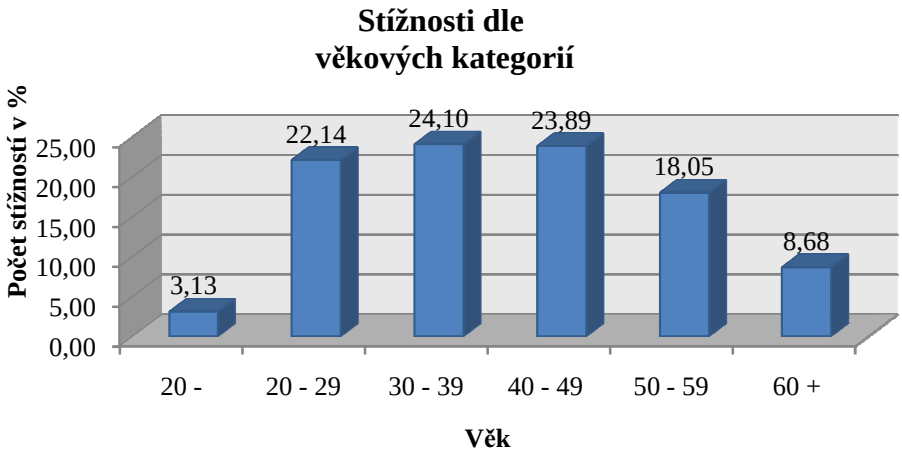
Věkový rozsah stěžovatelů se pohybuje mezi 20-ti a 60-ti lety s tím, že minimum stížností je zaznamenáváno mimo tento rámec. Populace lidí nad 60 let jistě v dnešní době Internet nevyužívá ve velké míře, a proto není evidováno velké množství stížností týkající se počítačové kriminality.

Mladí lidé pod 20 let také nemusí tak často manipulovat s Internetem, jako je tomu u lidí ve vymezeném věkovém rámci (20 – 60 let). Nemají tak mnoho možností se stát obětí počítačové kriminality. Může tomu být také kvůli důslednosti rodičů, kteří omezují jejich práva na používaném počítači. Většinou je tomu ale naopak – mladiství

se stanou obětí zločinu (porušují pravidla bezpečnosti), nedají o tom nikomu vědět a je zde velká pravděpodobnost, že trestnou činnost pak nahlásí místo nich rodiče, kteří samozřejmě celou situaci také řeší.

Níže uvedený obrázek č. 10 znázorňuje, v jaké míře si dané věkové skupiny průměrně za dobu deseti let stěžovaly na nějaký podvod anebo újmu spáchanou přes Internet. Největší skupinu stěžovatelů zastupuje věková kategorie 30-39 let, která průměrně dosahuje hodnoty 24,10 % ze všech stěžovatelů v průběhu sledovaného období. Následuje věková kategorie 40-49 let s 23,89 % a také kategorie 20-29 let s 22,14 % stížností. Tyto 3 skupiny jsou přibližně na stejné úrovni a můžeme je považovat za sobě rovné. Vývoj stížností dle jednotlivých let nevykazoval žádné významné změny, co se věkových kategorií týče, a svůj trend si zachovává nadále. Pouze u věkové hranice 60+ byl zaznamenán růst stěžovatelů a to ve výši 8 procentních bodů (rozdíl roku 2010 a 2001).

Obrázek č. 10: Stížnosti dle věkových kategorií



Zdroj: Zpracováno podle [12]

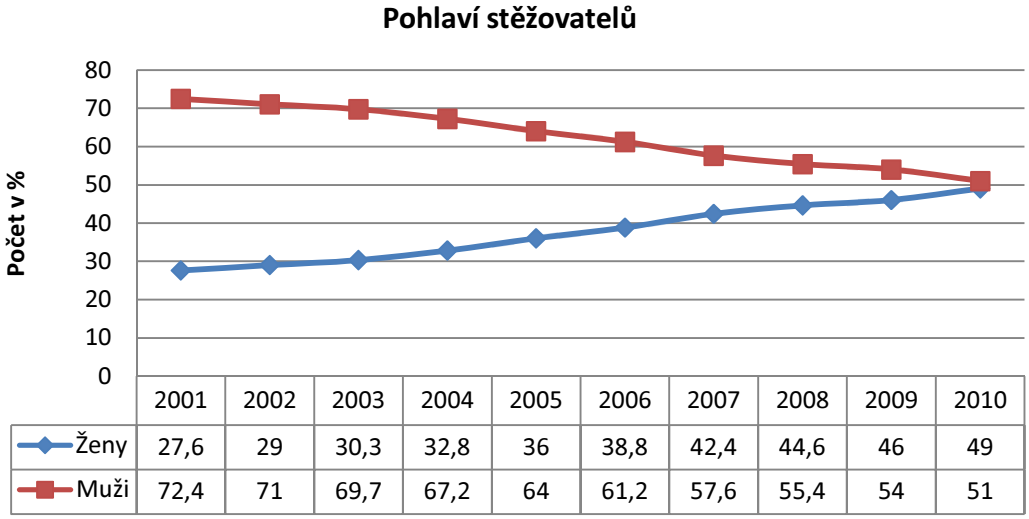
3.4.2 Pohlaví stěžovatelů

Mluvíme-li o pohlaví stěžovatelů, je tomu stejně tak, jako u pachatelů trestné činnosti - ve větší míře si na zpozorovanou trestnou činnost stěžují muži, alespoň tomu tak bylo v minulých letech.

Vývoj počtu stížností dle pohlaví stěžovatelů nám ukazuje, že trend se radikálně změnil v průběhu sledovaného období. Z obrázku č. 11 můžeme pozorovat, že počet stěžovatelů mezi muži a ženami v roce 2010 je takřka stejný, ale v roce 2001 byly zaznamenány stížnosti od mužů ve výši 72,4 % a od žen pouze ve výši 27,6 %.

Tato situace by mohla vyjadřovat, že ženy se o danou oblast začaly zajímat a není jím již tak lhostejná, jako tomu bylo v minulých letech. Na druhou stranu můžeme polemizovat o tom, že ženy začaly více využívat informační technologie a Internet než tomu bylo v minulosti a kvůli tomu jsou zaznamenávány stížnosti v radikálně větším množství od slabšího pohlaví.

Obrázek č. 11: Vývoj počtu stížností dle pohlaví stěžovatelů



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Ženy	27,6	29	30,3	32,8	36	38,8	42,4	44,6	46	49
Muži	72,4	71	69,7	67,2	64	61,2	57,6	55,4	54	51

Zdroj: Zpracováno podle [12]

3.4.3 Peněžitá ztráta stěžovatelů

Další charakteristikou stěžovatelů je peněžitá ztráta, kvůli které se většina lidí obrací na IC[3]. Postupem času se obnos peněžité újmy radikálně zvyšuje. Například v roce 2001 byla peněžitá ztráta rámcově vymezena od $100 do $10 000 ale již v roce 2002 bylo nutné rozmezí zvýšit na částku od $100 do $100 000, což je, dle mého názoru, nepředstavitelně obrovský skok, který sebou samozřejmě nese následky. Peněžitá ztráta tedy představuje v současné době, mimo jiné, největší riziko, které sebou počítačová kriminalita nese.

Dle výpočtů průměrný koeficient růstu ztráty uživatelů je 1,398 - ročně tedy peněžitá ztráta uživatelů vzrůstá o 39,8%. Největší růst byl zaznamenán řetězovým indexem o hodnotě 303,40 v roce 2002 a naopak nejmenší růst byl zaznamenán v roce 2010. V příloze č. 3 nalezneme graficky znázorněnou trendovou funkci pro vývoj peněžité ztráty.

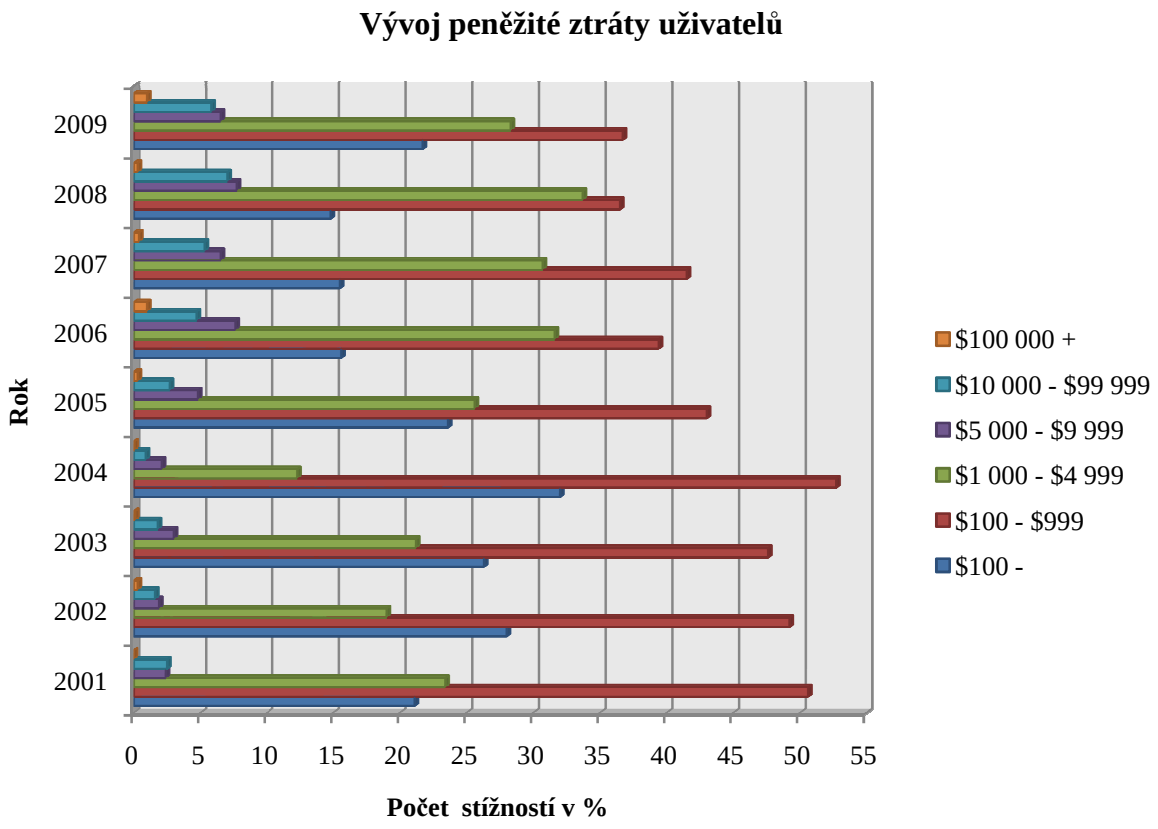
Obrázek č. 12: Tabulka výpočtů (peněžitá ztráta uživatelů)

Rok	Peněžitá ztráta v $	Absolutní přírůstky	Koeficienty růstu	Řetězové indexy Tempo růstu (v %)
2001	17 800 000	-	-	-
2002	54 000 000	36 200 000	3,034	303,40
2003	125 600 000	71 600 000	2,326	232,60
2004	68 140 000	-57 460 000	0,543	54,30
2005	183 120 000	114 980 000	2,687	268,70
2006	198 440 000	15 320 000	1,084	108,40
2007	239 090 000	40 650 000	1,205	120,50
2008	264 600 000	25 510 000	1,107	110,70
2009	559 700 000	295 100 000	2,115	211,50
2010	363 400 000	-196 300 000	0,649	64,90

Zdroj: Zpracováno podle [12]

Při pohledu na obrázek č. 12 je zřejmé, že uživatelé nahlašují nejčastěji ztrátu o hodnotě mezi $100 - $999. Peněžitá ztráta uživatelů v rozmezí $10 000 - $99 999 je nahlašována od roku 2001 čím dál tím častěji a v roce 2009 dosahuje hodnoty 5,8 % - roku 2001 byla na úrovni 2,5%. Stížnosti spadající do ostatních skupin také rok od roku narůstají, kromě skupiny ztráty o hodnotě $1 000 - $4 999, která neustále kolísá. Do sledovaného období bohužel nebylo možné zahrnout data z roku 2010, protože nejsou dostupná v dokumentech IC[3].

Obrázek č. 13: Vývoj peněžité ztráty uživatelů



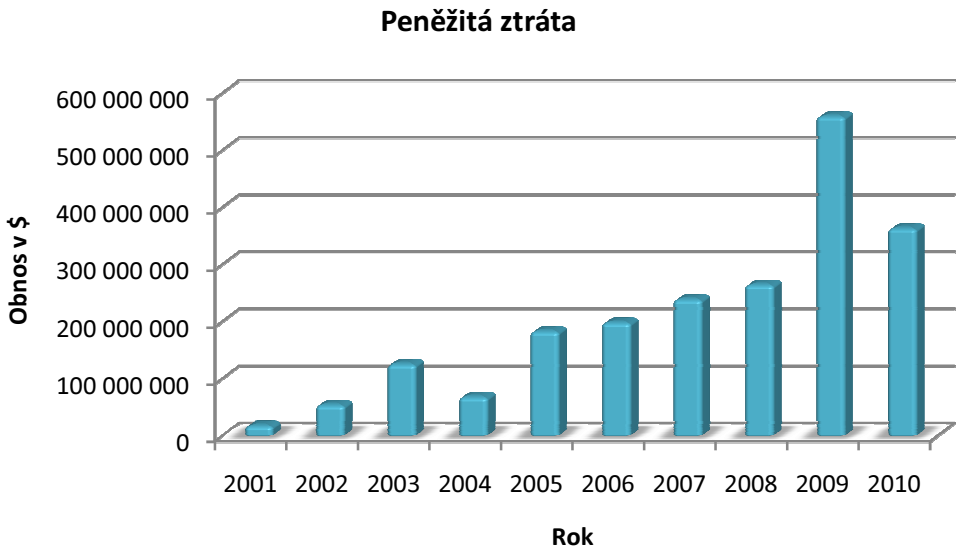
Zdroj: Zpracováno podle [12]

Prezentovaná data znázorňují, že uživatelé na Internetu denně přicházejí o stovky dolarů a částka se nesnižuje, ba naopak neúprosně roste.

Shrnutím veškerých dat o celkové peněžité ztrátě v jednotlivých státech v USA po dobu deseti let byla získána suma o hodnotě $ 2 073 890 000. Celkový obraz o tom, o kolik svých peněz uživatelé přišli kvůli internetovým podvodům, nám poskytuje obrázek č. 13.

V roce 2009 nahlášená peněžitá ztráta uživateli činila $ 559 700 000 a v historii sledování tak dosáhla svého vrcholu. Vinu můžeme připisovat především obrovskému rozmachu krádeže identity, která v minulosti nebyla známa v takovém rozsahu. Od roku 2008 totiž vzrostl počet stížností toho typu o 11,6%. Aukční podvody neovlivnily vývoj peněžité ztráty ve velké míře, protože v roce 2009 se jejich výskyt snížil oproti předchozímu roku o 15,2% (viz obrázek č. 2).

Obrázek č. 14: Celková peněžitá ztráta za sledované období



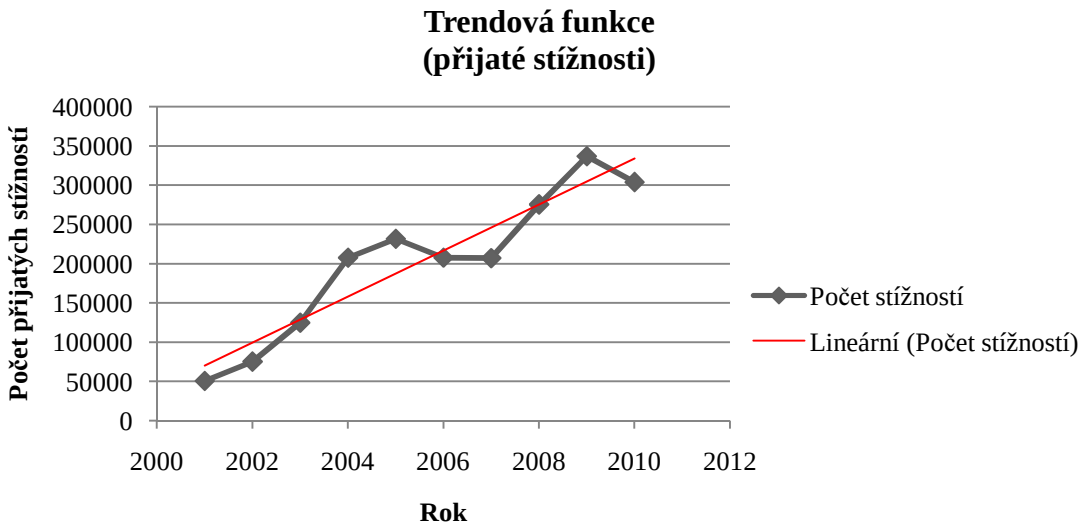
Zdroj: Zpracováno podle [12]

3.5 Přijaté stížnosti IC^3

Stížnosti jsou zaznamenávány IC^3 z velké míry jen prostřednictvím webových formulářů a také pomocí e-mailu, zřídkakdy telefonicky anebo jiným způsobem komunikace. Přijaté stížnosti na podvody rostou stejně tak, jako spáchané trestné činy po Internetu.

V následujícím obrázku č. 14 nám trendová lineární funkce znázorňuje vývoj počtu stížností za posledních 10 let, které IC^3 zaznamenalo. Průměrný koeficient růstu přijatých stížností je 1,22%, tedy stížnosti ročně vzrůstají o 22%.

Obrázek č. 15: Trendová funkce (počty stížností)



Zdroj: Zpracováno podle [12]

Komentář s výrazným varováním, že počítačovou kriminalitu nelze zanedbávat, myslím, není potřeba nijak zdůrazňovat. Samo grafické znázornění o tom svědčí a je varováním, i přestože v roce 2010 byl zaznamenán menší počet stížností od uživatelů Internetu. Řetězové indexy a další data týkající se růstu přijatých stížností znázorňuje obrázek č. 15. Nejvyšší růst stížností za celé sledované období byl zaznamenán roku 2004, jak ukazuje řetězový index o hodnotě 166,61.

Obrázek č. 16: Tabulka výpočtů (počet přijatých stížností)

Rok	Počet přijatých stížností	Absolutní přírůstky	Koeficienty růstu	Řetězové indexy Tempo růstu (v %)
2001	50 412	-	-	-
2002	75 064	24 652	1,489	148,90
2003	124 515	49 451	1,659	165,88
2004	207 449	82 934	1,666	166,61
2005	231 493	24 044	1,116	111,59
2006	207 492	-24 001	0,896	89,63
2007	206 884	-608	0,997	99,71
2008	275 284	68 400	1,331	133,06
2009	336 655	61 371	1,223	122,29
2010	303 809	-32 846	0,902	90,24

Zdroj: Zpracováno podle [12]

3.6 Zajímavá fakta o počítačové kriminalitě ve světě

Strohá data nám nastiňují, jak je počítačová kriminalita v dnešní době rozsáhlá, ale abychom si dostatečně uvědomili tuto problematiku, je třeba uvést zajímavá fakta, která leckomu otevřou oči. Na základě rozsáhlého průzkumu společnosti Norton, která poskytuje antivirový systém pro širokou veřejnost, je zde uváděno několik zajímavých faktů, co se počítačové kriminality týče. Průzkum byl prováděn ve 24 zemích a shrnuje data z celého průběhu roku 2011.

Prvním ze zajímavých faktů je skutečnost, že celková peněžitá ztráta uživatelů za poslední rok jen ve 24 zemích světa je přes 388 bilionů dolarů. Tato částka se blíží ztrátě na globálním černém trhu s marihuanou, kokainem a heroinem ($288 bil.) a vyrovná se hodnotě celému globálnímu obchodu s drogami ($411bil.). O co více, kyberkriminalitou přichází uživatelé Internetu o 100 krát více, než jsou roční výdaje organizace UNICEF ($3,65 bil.).

Peněžitá ztráta velice dobře vystihuje tento problém, ale uvedeme si ještě další fakt, kterým je počet obětí. Ten dosahuje hodnoty 431 milionů za poslední rok s odhadem, že denně je napadeno okolo 1 milionu lidí a každou sekundu trpí zločinem po Internetu 14 dospělých. Z výzkumu také plyne, že lidé neustále nepovažují kyberkriminalitu za tak významný problém, protože pouze tři z deseti dotazovaných si myslí, že v příštích dvanácti měsících by mohli být obětí počítačové trestné činnosti. Zbylá část respondentů považuje za reálnější, že budou napadeni v reálném světě – například vloupáním nebo okradením.

Průzkum také srovnává počet obětí s faktem, že denně je obětí kyberkriminality po celém světě dvakrát tolik, než je narozených dětí. Jen ve 24 zemích světa zločin tohoto typu ovlivnil tolik lidí, že hodnotu můžeme vyjádřit jako 9% populace celého světa.

Nejvíce zasažené oblasti kriminalitou jsou Mexiko, Brazílie, Čína a Jižní Afrika. Přes 54 % uživatelů zaznamenalo v těchto oblastech světa virus a nebo malware útoky. Jedna z obětí popsala svojí zkušenost s útokem následovně:

„Falešný download se mi z ničeho nic objevil na pracovní ploše a hned jsem věděl, že se někdo dostal do mého notebooku. Po několika vteřinách jsem měl 4 virusy a jeden Trojský kůň. Nějak získali všechny moje údaje k účtům a také i formace k e-mailovým

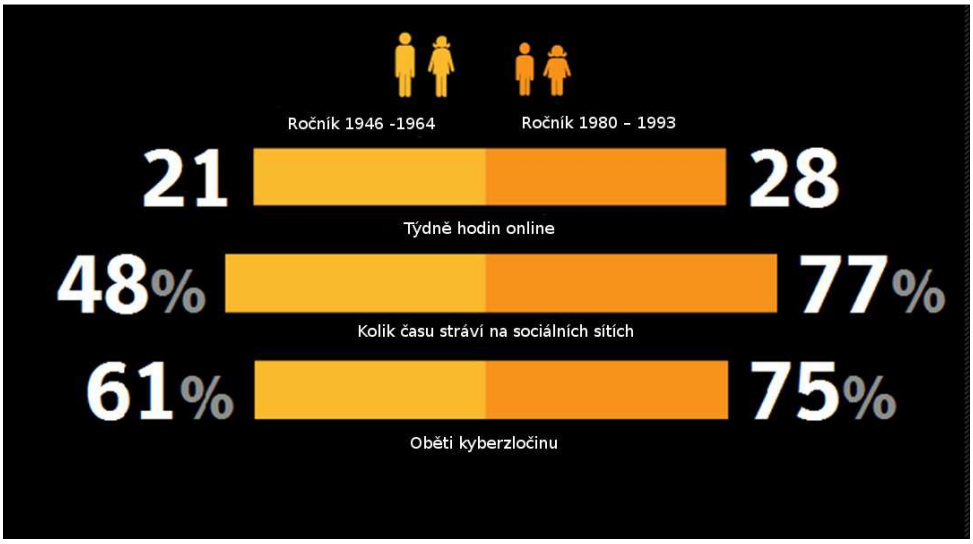
adresám a také všechna hesla. Všechno bylo vybíleno. Chyběly mi peníze na mém hlavním účtu. Nějak se dostali na jednu z mých karet. Změnili veškeré údaje a také hesla k e-mailovým adresám, také heslo k sociálním sítím – Nemohl jsem se dostat vůbec nikam.“ [17]

Někteří z nás si myslí, že tohle se stát přece jen tak nemůže, ale opak je pravdou. Na vzrůstající kriminalitu má vliv také to, jak často jsou uživatelé k Internetu připojeni. Čím více uživatelů je online, tím více roste motivace zločinců, aby vyzkoušeli svoje schopnosti a dovednosti na nových obětech.

Dle výzkumu společnosti Norton máme dostupné informace i o tom, kolik hodin týdně tráví určité věkové skupiny online, kolik z toho času věnují sociálním sítím a kolik z nich je obětí kybekriminality – viz obrázek č. 17.

Je zřejmé, že mladší generace je online na Internetu hlavně kvůli sociálním sítím a je i více napadnutelná útoky počítačové kriminality.

Obrázek č. 17: Uživatelé online



Zdroj: Zpracováno podle [17]

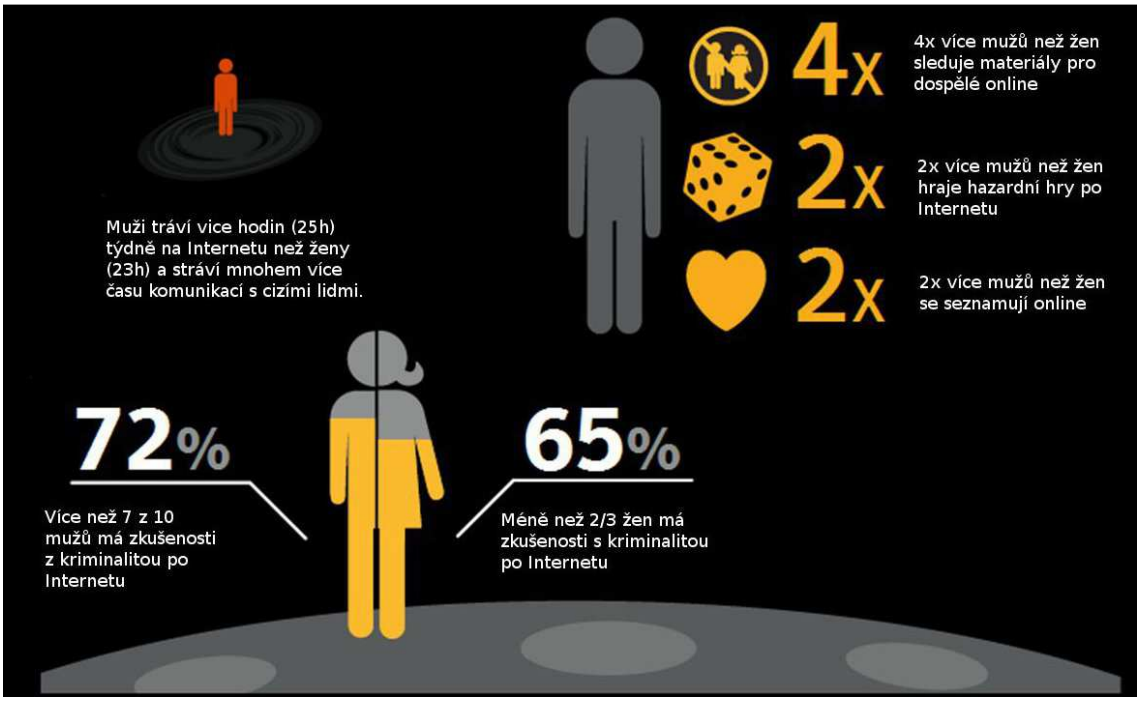
Sociální sítě jsou nedílnou součástí brouzdání po Internetu pro uživatele ve 32 % případů. Tato skupina jedinců má pocit, že by mohli ztratit kontakt se svými přáteli, pokud by měli žít bez sociálních sítí. Dalších 41 % respondentů prohlásilo, že Internet potřebují ke svému každodennímu životu, což přivádí k zamyšlení. Z medicínského hlediska je totiž možné přežít 10 dní bez vody a 4 týdny bez jídla, v dnešní době ale lidé

nedokážou žít bez Internetu. Zajímavou informaci poskytl výzkum také ohledně vztahu učitelů a jejich studentů na sociálních sítích, kdy 34% učitelů je „přáteli“ se svými studenty na sociálních sítích. Na druhou stranu sami učitelé a profesoři uznávají, že je to vystavuje velkému riziku, pokud jde o respektování hranice mezi učitelem a studentem.

Průzkum také ukazuje, jak obrovský rozmach nastal v používání Internetu v mobilních zařízeních. Dle uživatelů ze 24 zemí světa používá k přístupu na Internet 44 % vlastníků mobilních telefonů – z toho 10 % z nich již má zkušenost s kyberzločinem „přes mobil“.

Dalším zajímavým faktem dle výzkumu je, že muži jsou napadnutelnější kybernetickým zločinem o mnohem více než ženy. Důvodem pro to je navštěvování různých online materiálů s obsahem pro dospělé, hraní hazardních her online, seznamování se po Internetu a také komunikace s cizími lidmi online. Samozřejmě, že tyto činnosti ženy provádějí také, ale v menší míře, jak ukazuje obrázek č. 18.

Obrázek č. 18: Muži oběťmi kyberkriminality



Zdroj: Zpracováno podle [17]

4. Jak předejít počítačové kriminalitě

Obezřetnost při používání Internetu je nutná, jak o tom svědčí fakta uvedená v analytické části této práce. Chyba, proč se počítačová kriminalita tak rozšiřuje, není jen na straně pachatelů, ale ve velké míře je nutno přiřknout vinu samotným uživatelům, kteří nerespektují pravidla počítačové bezpečnosti. Bezpečnosti pro používání počítačů a také služeb, poskytovaných online.

Uživatelé si musí uvědomit, že jsou součástí určitého celku, který je snadno napadnutelný, pokud byť jediný článek z něj selže. Představit si můžeme třeba rybářskou síť, která když se protrhne, přeruší-li se jedna vazba mezi lanky, tak ztratíme celý úlovek. V našem případě přijdeme o velice důležitá data z našeho počítače a poskytneme je tak širokému světu, aniž bychom to měli v úmyslu. Nicméně narušením bezpečnosti v síti nepřijdeme k úhoně jen my sami, ale skrz naši „díru“ v bezpečnosti dovolíme útočníkům napadnout i další počítače v síti. Bezpečnost tedy není věcí pouze správce sítě, který nám poskytuje služby, o bezpečnost se uživatelé počítačů musí zajímat i sami.

V následujícím textu nalezneme jednoduchá, ale velice důležitá pravidla bezpečnosti, která se týkají každého z nás a každým z nás by měla být alespoň z poloviční míry respektována. Tato sekce je velké míře inspirována poznatky Tomáše Doseděla, které sepsal do publikace o počítačové bezpečnosti [1].

4.1 Bezpečnostní hesla

Tak jako chráníme svoje věci v reálném světě, zamykáme je pod zámek do trezoru nebo doma do skříně, od které mají klíč jen povolané osoby, stejně tak bychom měli chránit svoje data i v počítačovém světě. První ze zásadních pravidel, která bychom měli dodržovat, se týká bezpečnostních hesel.

Prvním z hesel, na které narazíme v našem počítači, by rozhodně mělo to, na které se nás operační systém zeptá, při zapnutí zařízení. Toto heslo můžeme přirovnat k našim klíčům od bytu – je stejně tak důležité. Lze samozřejmě „zaheslovat“ i adresáře a soubory různým softwarem, pokud uživatel například sdílí PC a chce mít svoje osobní věci přístupné jen svým očím anebo se jedná o velice důležité soubory.

Je všeobecně známo, že je nutné si zvolit složitější heslo a je potřeba ho po určitém časovém intervalu měnit. Nejlépe pravidelně v intervalu jednoho měsíce až půl roku. Heslo by mělo obsahovat minimálně 8 znaků a mělo by být tvořeno kombinací malých, velkých písmen a speciálních znaků. Není vůbec vhodné pro heslo zvolit jméno, slovo, datum narození a podobně. Také je nutné se vyvarovat stejných hesel na různých účtech a zaznamenávání si hesel na papírky anebo si je ukládat přímo do prohlížeče, pro usnadnění našeho brouzdání po Internetu.

Pokud má uživatel problémy se zapamatováním si hesel, je vhodné si hesla ukládat na externí médium (flash-disk, DVD, mobilní telefon), které je nutné chránit před odcizením. Jaké heslo je tedy nejbezpečnější? Můžeme jednoduše říci, že nejbezpečnější jsou nesmyslné kombinace znaků, ale zase jsou těžko zapamatovatelné. Dále je nutné mít na vědomí, že heslo nesmíme samozřejmě nikomu sdělovat a také hesla od nikoho přijímat. [21]

4.2 Aktualizace systémů a aplikací

Náš počítač, přestože je to velice chytré zařízení, neumí ochránit sám sebe, a proto je nutné systém a veškeré aplikace, pravidelně aktualizovat. Malware často napadá ty aplikace, ve kterých se v průběhu času od jejich vydání odhalily bezpečnostní „díry“. Tyto díry jsou aktualizacemi softwaru záplatovány a předchází se tak útokům zvenčí. Příkladem mohou být i aktualizace operačního systému, které jistě důvěrně známe – neváhejte s jejich instalací.

Uživatelé musí dbát také na to, jaký software si do počítače instalují. Je žádoucí instalovat jen takové aplikace a programy, které jsou legální a které potřebujeme. Je nutné se vyvarovat aplikacím, které poskytují neověřené servery, a které mohou obsahovat škodlivý kód – a o co více, porušuje se tím zákon, když se tento software používá v rozporu s licenčním ujednáním. [22]

4.3 E-maily, přílohy, online soubory

Čas od času se nám na e-mailu objeví nějaká zpráva, kterou jsme neočekávali – např. reklamní letáky a další zprávy, které mohou obsahovat škodlivý obsah. Neotvírat

a neukládat soubory z podezřelých e-mailů – to je nejlepší ochrana před viry skryté v přílohách.

Problematika „hoax“ (viz kap. 3.3.5 - II) s tímto tématem také hodně souvisí, až na to, že není až tak škodlivá a neztrácíme při ní svoje cenná data – nanejvýše tak dobré jméno. Tím, že zaplníme schránku hoaxem dalším deseti přátelům, nikoho nezachráníme, nezbohatneme a ani se nám nesplní naše tajná přání. Nestojí za to šířit svojí e-mailovou adresu a také adresu svých přátel jen kvůli poplašené zprávě.

Obezřetnost při otevírání souborů platí také pro informace získávané přímo online z Internetu. Není radno nic přímo otvírat anebo ukládat, pokud si nejsme jisti, co je obsahem daného souboru. Při prohlížení běžných internetových stránek se většinou ale tato hrozba nevyskytuje.

4.4 Antivirová ochrana, osobní firewall

Nezbytný program, který by definitivně neměl chybět v žádném počítači – „antivirus“. Prevence je základ a to platí i v tomto případě, chceme-li se vyvarovat problémům, které způsobují viry. Antivirový program slouží ke kompletnímu otestování počítače, prohledá soubor po souboru, zdali se v některém z nich nevyskytuje škodlivý obsah, kontroluje příchozí poštu a spolupracuje s poštovními klienty, jako je například Microsoft Outlook, Thunderbird a další. Antivirus také poskytuje rezidentní štít, který hlídá čistotu souborů otevíraných jak z disku, tak i z Internetu.

Tím, že budete mít jen nainstalovaný antivirový program, nezabráníte postupem času tomu, abyste se vyvarovali virům navždy. Vynalézavost tvůrců virů je nekonečná, a proto, jak již bylo zmíněno, je nutné antivirový program neustále aktualizovat.

Kromě virů můžeme v našem počítači, byť nechtěně, nalézt i trojské koně (kap. 3.3.6 - II). Některé z nich dokáže přímo odstranit antivirový program, ale lepší variantou je použít program určený přímo na odhalení a smazání adware a spyware.

Osobní firewall je další z programů, který bychom měli mít na svém počítači. Jedná se o software, který zabraňuje útokům na počítač uživatele zvenčí. Můžeme říci, že se jedná o zeď, která odráží útoky nebezpečného internetového světa. Dokáže odhalit pokusy o útoky prováděné z Internetu, ale také zastavuje programy, které se snaží komunikovat z uživatelova počítače.

Firewall upozorňuje na podezřelé situace a dotazuje se uživatele, zdali opravdu chce danou akci provést. Zakázáním nepovoleného spojení nic nezkazíte, ale některé komunikační programy (např. Skype, Microsoft Outlook) nemusí správně fungovat, můžete tak třeba zabránit poštovnímu klientovi stáhnout novou poštu. Samozřejmě komunikaci můžeme znova povolit a zprovoznit tak požadované úkony daných programů.

4.5 Prověřování médií před použitím

Ačkoli se může tato činnost zdát velice otravná a zabere nám pár minut času, jedná se dobře investovaný čas. Je jednodušší ztratit pár minut, než se posléze trápit se zavirovaným počítačem po dlouhé hodiny. Před otevřením jakéhokoli souboru z CD, DVD, flash disku anebo dalších médií, je vhodné otestovat, jestli se na nich nenachází nějaký závadný obsah, přestože v dnešní době jsou zaznamenané virové útoky ve velké míře jen prostřednictvím e-mailu. [22]

4.6 Chraňte své soukromí

Někteří uživatelé Internetu se za svůj počítač přímo schovávají a nikdy si skutečně nemůžeme být jisti, s kým vlastně komunikujeme. Oproti setkání tváří v tvář jsou zde mnohé nástrahy. Komunikace s člověkem, kterého jsme v životě nepotkali, se může pro někoho jevit jako zábava, ale nikdy tomu tak není. Veškeré informace, které o sobě uvedeme na Internetu, mohou být zneužity. Sociální sítě, jako je Facebook, nevyjímaje.

4.7 Aukční podvody

V analytické části práce jsme získali obrázek o tom, jak jsou aukční podvody v USA rozšířené. K vyvarování se těmto podvodům vedou jednoduché kroky, ale samozřejmě se můžou vyskytnout případy, kdy bohužel ani obezřetnost při nakupování v aukcích nepomůže.

Prvním krokem k bezpečnému dokončení aukce je se snažit pochopit, jak internetové aukce vůbec fungují, jaké jsou povinnosti kupujícího a jaké prodávajícího. Než se zapojíte do aukce jako účastník obchodu, prozkoumejte,

jaká opatření používá daná webová stránka (aukční server), když se vyskytnou potíže týkající se provedených transakcí a dodání zboží. Některé servery v dnešní době dokonce garantují navrácení určitého podílu částky za zboží kupujícímu, pokud prodávající daný předmět nedodá.

Zjistěte si co nejvíce informací o prodávajícím hlavně tehdy, když jediný kontaktní údaj na něj je e-mailová adresa. Jestli se jedná o společnost, navštivte jejich domovské stránky, pokud jsou dostupné, anebo rovnou online obchodní rejstřík. Důvodem pro to je ověření si skutečnosti, zdali je společnost reálná.

Dbejte také na zpětnou vazbu od kupujících z předchozích obchodů s daným prodejcem. Prozkoumejte metody platby, o které Vás prodávající bude žádat a jestli po Vás vyžaduje platbu předem či nikoli. V neposlední řadě je nutné se vyvarovat rozdílnostem mezi různými aukčními servery v jiných zemích. Všude nejsou podmínky aukcí stejné. V neposlední řadě se musíme vyvarovat poskytnutí prodejci více osobních informací, než je pro dokončení obchodu potřeba. [12]

4.8 Podvody s kreditními kartami

Kreditní karty jsou v dnešní době velice snadno zneužitelné. Již nejde jen o jejich fyzické odcizení, kdy má pachatel možnost vybrat peníze z bankomatu a platit v různých obchodech. Nyní jsou platby s kartami online další možností, jak si počítačoví zločinci mohou vylepšit svůj rozpočet.

Kupujeme-li zboží či služby po Internetu, většinou za ně i po Internetu platíme – žádná hotovost, žádné mince – jen pár čísel nám stačí k tomu, abychom převedli určitou sumu na účet například v úplně jiné zemi. Jak pohodlné, že? Ale také nebezpečné. Uživatelé si musí uvědomit, jak jsou údaje na platební kartě citlivé, a proto je důležité, aby číslo kreditní karty nebylo poskytnuto online, dokud není jistota, že webová stránka je zabezpečená a také věrohodná.

Při placení za zboží online, můžeme sledovat, že se občas objeví malá ikona v oblasti názvu www stránky, která signalizuje vyšší zabezpečení pro přenášená data. Tato ikona ale negarantuje zabezpečenou stánku, ale můžete si být jisti, že poskytuje záruku na určitou bezpečnost. Před vložením dat na danou internetovou stránku je možné použít software, který nám sdělí, zdali naše data budou chráněna.

Mezi další rady, ohledně bezpečnosti při placení s kreditními kartami online, patří:

- Ujistit se, že platíme věrohodné společnosti, stejně tak, jako tomu je u ujištění se o obchodnících z aukčních serverů.
- Je vhodné také zkusit poslat e-mail dané společnosti, abychom zjistili, že se nejedná o fiktivní adresu.
- Je nutné být obezřetní, když reagujeme na speciální nabídky obdržené ze zvláštních e-mailových adres a také od obchodníků ze zahraničí.
- Nikdy nenecháváme veškeré informace potřebné k přístupu ke kartě u karty. [12]

5. Závěr

Jak bylo již několikrát zdůrazněno v této práci, počítačová kriminalita je závratně rostoucí hrozbou naší společnosti. Byl nastíněn vývoj počítačové kriminality od jejího samého počátku a také byly uvedeny zásadní události, které ovlivnily její celkový rozvoj. Uvedená čísla, fakta a zajímavé informace, nejen v analytické části práce, jsou důkazem toho, že náš svět je protkán nejen výhodami, ale také hrozbami informačních technologií – konkrétně Internet je tou nejnebezpečnější z nich. Pravda, na technologie je nutno nahlížet s obdivem a oceňovat jejich funkce, ale na druhou stranu bychom měli být velice obezřetní při jejich užití, a to kvůli faktu, že se počítačová kriminalita neúprosně rozrůstá. Je možno říci, že sama tato práce je jedním z důkazů této skutečnosti - vystihuje vývoj počítačové kriminality, která neúprosným tempem roste.

Kriminální jednání, kterých je pácháno po Internetu nesčetně, neustále rostou a jejich výčet není reálné dokončit. Podvody, které znepříjemňují naši potřebu využívat informační technologie, se neustále rozšiřují především kvůli neznalosti bezpečnosti zacházení s počítači širokou veřejností. Zdá se, že uživatelé počítačů nedbají na varování médií, a neustále si nalhávají, že jsou v bezpečí. Sám Internet a informační technologie neznají pojem „hranice“, a proto téma počítačová kriminalita není aktuální jen v USA, ale i v ostatních zemích, mezi které patří samozřejmě i Česká Republika.

Je nutné, aby veřejnost byla více podněcována skutečnostmi, které se dějí v oblasti počítačové kriminality. Jedním z návrhů by mohlo být zformování jistého plánu, který by občanům, zákazníkům a také různým společnostem využívající informačních technologií, preventivně dával rady a poskytoval různé informace týkající se informační bezpečnosti. Pokud se totiž sami jednotlivci nezačnou zajímat o svou bezpečnost, společnost nemůže být plně ochráněna.

Cílem práce bylo mimo jiné také dokázat, že společnost nelze být vůči počítačové kriminalitě lhostejná. Analytická část nám ukázala, že počítačová kriminalita v USA je velice rozšířená a v průběhu sledovaných deseti let byl její rozmach alarmující. Největším problémem se ukázaly být přečiny týkající se aukčních podvodů, krádeže identity, nedodání zboží a v neposlední řadě také podvody s kreditními kartami. Rok od roku stížnosti na počítačovou kriminalitu radikálně rostou, a pokud společnost nezíská větší povědomí o informační bezpečnosti, můžeme očekávat, že počítačové kriminalita poroste nadále.

Zajímavým zjištěním práce byl závratný růst stěžovatelů ženského pohlaví na vzrůstající kriminalitu po Internetu. Ve sledovaném období byl zaznamenán nárůst stížností o 21,4 procentních bodů (rozdíl roku 2010 a 2001). Svědčí to o skutečnosti, že využívání informačních technologií není již tolik neznámé pro slabší pohlaví, jako tomu bylo v minulých letech a i to přispívá k růstu kriminality v kyberprostoru.

Již víme, že Internet je kyberprostorem, za který se může schovávat spousta lidí, lhát za účelem osobního zisku, šířit spoustu mylných informací, závadných materiálů. Na druhou stranu se cítí lidé na Internetu svobodní, a tak šíří svoje myšlenky a osobní data. Tyto informace jsou nejdůležitějšími věcmi, které by se lidé měli naučit chránit. S rozvojem sociálních sítí je to ale čím dál tím složitější a dokonce i společnosti, které se starají o bezpečnost na Internetu, nezvládají chránit svoje uživatele. Den ode dne se objevují nové viry a počítačoví piráti jsou čím dál tím více vynalézavější.

Cílem práce bylo také zhodnocení rozvoje počítačové kriminality v USA, kdy se ukázalo, že kriminalita je rozšířená především v oblastech s největší populací. V tomto případě se jedná o státy California, New York, Florida a Texas, kde byl zaznamenán v průběhu deseti let největší počet stížností na podvody spáchané po Internetu.

Jak se tedy tomuto fenoménu dnešní doby vyvarovat? Jak se nestát obětí počítačové kriminality? Odpověď nemůže být jednoznačně dána, ale jedním z nejdůležitějších faktů je to, že bychom se v kyberprostoru měli chovat tak, jak tomu je i v reálném světě. Dbát svojí bezpečnosti online tak, jako tomu je, když jdeme pouze do obchodu nakoupit a dáváme si pozor na svoji peněženku. Tato práce obsahuje několik rad, jak se lze vyvarovat problémům, týkající se počítačové kriminality a uvádí překvapující fakta, která by měla ne jednoho z nás nadzvednout ze židle. Rady a návody, jak se chovat v kyberprostoru, bohužel stárnou a přestávají být aktuální. Proto je nutné sledovat dění na Internetu, stejně tak jako denní regionální zprávy.

Práce by mohla být obohacena o srovnání vývoje počítačové kriminality s nějakými dalšími zeměmi, aby nám poskytla vskutku reálný obraz o tom, jak se rozvíjí kyberkriminalita ve světě. Dokument totiž obsahuje, kromě faktů o kyberkriminalitě v USA, pouze stručné a zajímavé informace, která se týkají světového kyberzločinu, a která byla získaná na základě průzkumu společnosti Norton. Získání detailních informací o této specifické trestné činnosti v jiných zemích než v USA není v současné době bohužel reálné.

Závěrem bychom mohli konstatovat, že jakýmkoli směrem se bude počítačová kriminalita ubírat, je možné ji redukovat pouze společně a hlavně za přispění vládních činností a kooperací s ostatními zeměmi. Protože, jak již bylo uvedeno, Internet a kyberzločin nezná žádné hranice.

6. Seznam obrázků

7. Seznam příloh

8. Seznam literatury

Tištěné publikace

[1] DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti*. Brno: CP Books a. s., 2005. ISBN 80-251-0574-1.

[2] GANGUR, Mikuláš. *Přednášky EPO – Nová ekonomika*. Plzeň: ZČU, 2007

[3] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium Praha, 2008. ISBN 978-80-903786-7-4.

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

[5] MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

Elektronické zdroje

[6] A Brief History of Cybercrime. *Wavefront Consulting Group* [online]. 2006-2012 [cit. 2011-03-11]. Dostupné z: http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html

[7] Convention on Cybercrime. *Council of Europe* [online]. Budapest, 23.11.2001 [cit. 2011-03-16]. Dostupné z: http://conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm

[8] Cyberstalking - praktické ukázky. *E-bezpečí* [online]. 2010 [cit. 2012-04-2]. Dostupné z: http://cms.e-bezpeci.cz/content/view/44/38/lang,czech/

[9] Etický hack ODS.cz je dobrou ukázkou toho jak protestovat v digitálním světě: Obrázek hacknuté stránky ODS. *Pooh.cz* [online]. 2.2.2012 [cit. 2012-04-9]. Dostupné z: http://www.pooh.cz/pooh/a.asp?a=2017587

[10] Hoax Encyclopedia. *Antivirus.about.com* [online]. 2011 [cit. 2011-04-2]. Dostupné z: http://antivirus.about.com/od/emailhoaxes/l/blenhoax.htm

[11] Information about Check Fraud. *Stopcheckfraud.com* [online]. 2009 [cit. 2012-03-9]. Dostupné z: http://www.stopcheckfraud.com/statistics.html

[12] Internet Crime Complaint Center: *Annual reports* [online]. 2001 - 2010 [cit. 2012-04-10]. Dostupné z: http://www.ic3.gov/media/annualreports.aspx

[13] Internetová kriminalita. *Celní správa* [online]. 2009 [cit. 2011-03-11]. Dostupné z: http://www.celnisprava.cz/cz/o-nas/kontakty/Stranky/internetova-kriminalita.aspx

[14] Mimořádně vydařený phishing mířící stále na Českou spořitelnu: Obrázek - phishingový e-mail. *Pooh.cz*[online]. 26.1.2008 [cit. 2012-04-9]. Dostupné z: http://www.pooh.cz/pooh/a.asp?a=2014601

[15] Na Facebooku se šíří Nigerijské dopisy. *Lupa.cz* [online]. 25. 2. 2011 [cit. 2012-02-19]. Dostupné z: http://www.lupa.cz/tiskove-zpravy/na-facebooku-se-siri-nigerijske-dopisy-na-uzivatele-utoci-i-malware-1/

[16] *Národohospodářský obzor 2-2007*: *Několik pohledů na novou ekonomiku* [online]. 2007 [cit. 2011-03-13]. Dostupné z: http://is.muni.cz/do/1456/soubory/aktivity/obzor/6182612/7372154/03HrncarkovaHOTOVO.pdf

[17] Norton Cybercrime Report. NORTON. *Us.norton.com* [online]. 1995 - 2012 [cit. 2012-03-20]. Dostupné z: http://us.norton.com/cybercrimereport/promo

[18] Pozor na padělané šeky!. *Měšec.cz* [online]. 27.3.2007 [cit. 2012-02-7]. Dostupné z: http://www.mesec.cz/clanky/pozor-na-padelane-seky/

[19] Přes sto lidí obvinili v USA z podvodů s platebními kartami. *Byznis.lidovky.cz* [online]. 9.11.2011 [cit. 2012-02-10]. Dostupné z: http://byznys.lidovky.cz/pres-sto-lidi-obvinili-v-usa-z-podvodu-s-platebnimi-kartami-pol-/moje-penize.asp?c=A111009_121247_ln_zahranici_spa

[20] Save more, live more: Official Identity Theft Statistics. *Spend.on.life.com* [online]. 9.11.2011 [cit. 2012-02-10]. Dostupné z: http://www.spendonlife.com/guide/2009-identity-theft-statistics

[21] Uživatel a počítačová bezpečnost. KROPÁČOVÁ, Andrea. *Zpravodaj ÚVT MU* [online]. 2010 [cit. 2012-03-26]. Dostupné z: http://www.ics.muni.cz/bulletin/clanky_tisk/353.pdf

[22] Základní bezpečnostní pravidla pro uživatele PC. *Cleverandsmart.cz* [online]. 2008 - 2012 [cit. 2012-03-27]. Dostupné z: http://www.cleverandsmart.cz/zakladni-bezpecnostni-pravidla-pro-uzivatele-pc/

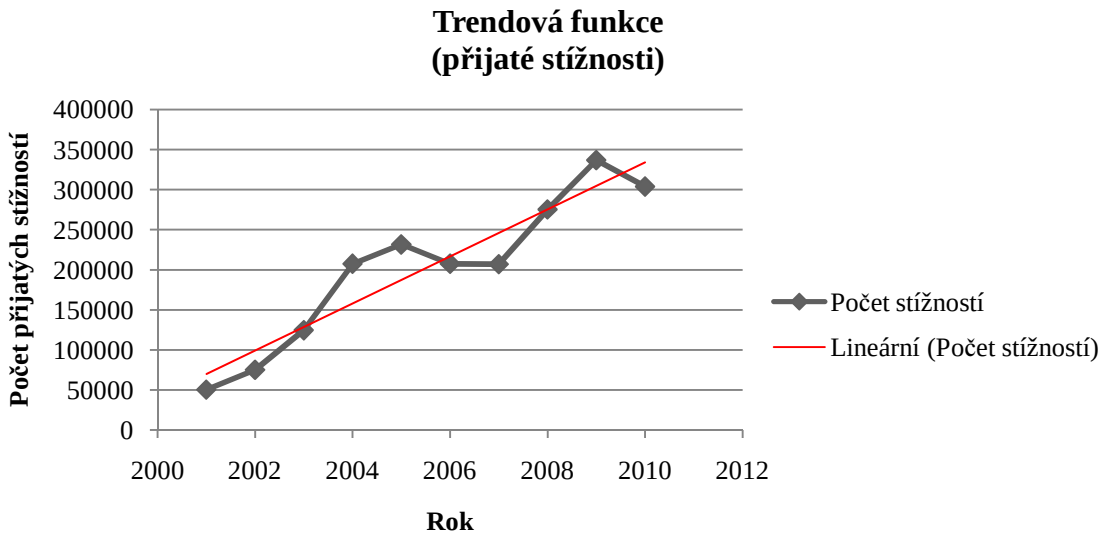
[23] Základní definice, vztahující se k tématu kybernetické bezpečnosti. *MVČR* [online]. 2006-2012 [cit. 2011-03-16]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

Příloha č. 1: Tabulka výpočtů (počty podvodů nedodání zboží)

Rok	Počet podvodů (nedodání zboží)	Absolutní přírůstky	Koeficienty růstu	Řetězové indexy Tempo růstu (v %)
2001	10234	-	-	-
2002	23495	13261	2,296	229,6
2003	26024	2529	1,108	110,8
2004	32777	6753	1,26	126
2005	36344	3567	1,109	110,9
2006	39423	3079	1,085	108,5
2007	51514	12091	1,307	130,7
2008	90568	39054	1,758	175,8
2009	66994	-23574	0,74	74
2010	64104	-2891	0,957	95,7

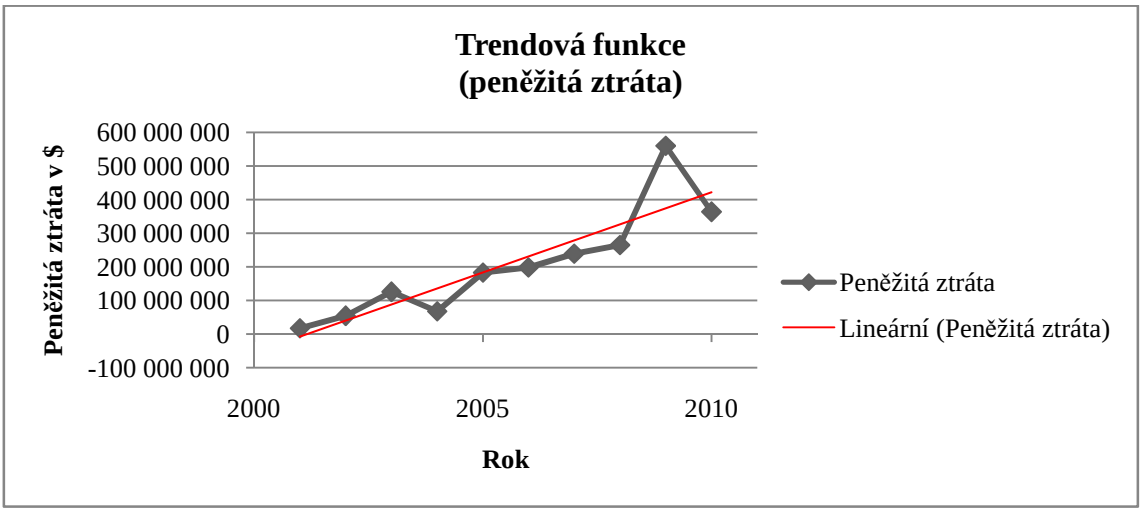
Zdroj: Vlastní zpracování dle [12]

Příloha č. 2: Trendová funkce (počty stížností)



Zdroj: Vlastní zpracování dle [12]

Příloha č. 3: Trendová funkce (peněžitá ztráta uživatelů)



Zdroj: Vlastní zpracování dle [12]

Příloha č. 4: Příklad hacknuté WWW stránky

Zdroj: [9]

Příloha č. 5: Příklad HOAXu

Vážení,

Nechcete někdo zadarmo štěňata retrívra (fotky přiloženy).

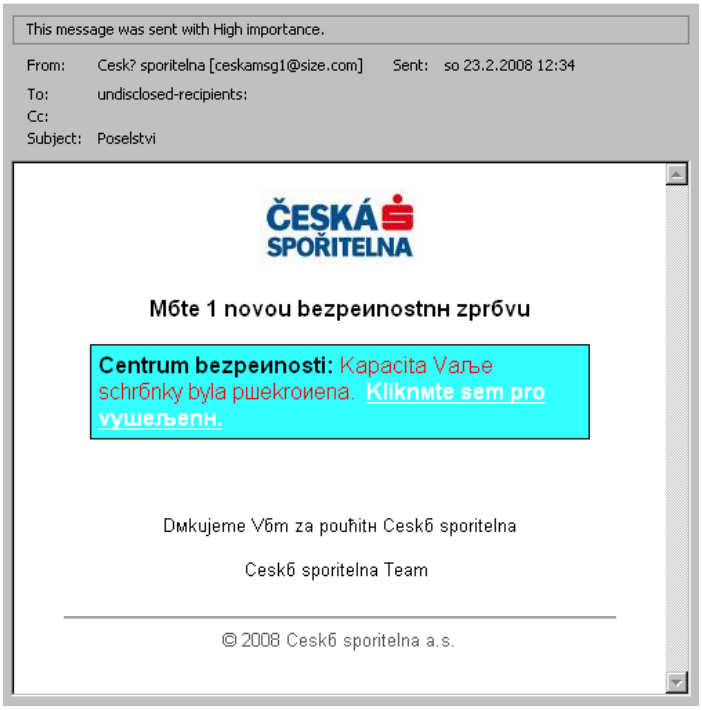
Hrozí jim, že budou utraceny.

Omlouvám se, že Vás tímhle obtěžuju, ale jsou nádherný a je mi jich líto.

v případě zájmu: xxxxxx@mail.xxxxxx.cz

Zdroj: Vlastní

Příloha č. 6: Příklad phishingového e-mailu



Zdroj: [14]

Abstrakt

TENKOVÁ, L. Analýza a vývoj počítačové kriminality v USA. Plzeň: Fakulta ekonomická ZČU v Plzni, 64 s., 2012

Klíčová slova: Internet, informační technologie, informační kriminalita, rizika, hrozby, hacking, SPAM, kyberkriminalita

Bakalářská práce vyzdvihuje problém současné společnosti týkající se zneužívání informačních technologií a je věnována analýze počítačové kriminality v USA. Tento dokument popisuje historický vývoj počítačové kriminality včetně současné situace. Stručně definuje trestné činnosti, které jsou páchány na Internetu, anebo za jeho využití, a také je rozděluje do různých podskupin. Práce se zabývá vývojem kriminality spáchané v průběhu let 2001 – 2010 a zároveň popisuje a analyzuje její vývoj. Závěrečná část práce obsahuje zajímavá fakta o počítačové kriminalitě ve světě a dává rady o zásadách bezpečnosti práce s PC a na Internetu.

Abstract

TENKOVÁ, L. Analysis and development of computer crime in the U. S. Pilsen: Faculty of economics WBU in Pilsen, 64 p., 2012

Key words: Internet, information technologies, information criminality, risks, threats, hacking, SPAM, cybercrime

Bachelor thesis highlights problem of nowadays society, which is abusing of information technologies. Thesis is devoted to analysis of computer crime in U.S. and it is dedicated with historical development of computer criminality together with description of current situation. It briefly defines criminal activities, which are committed on Internet or via it. Thesis also divides these activities into different subgroups. It deals with development of criminality committed in the years 2001 – 2010 and it describes and analyzes its development. The final part contains interesting facts about computer crime in whole World and it gives advices about safety principles - how to work with computer and with Internet.