VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O.P.S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

2010 **MICHAL ZAPOMĚL**

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O.P.S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

PRÁVNÍ ASPEKTY POUŽITÍ SOFTWARU, PIRÁTSTVÍ

Autor práce: Michal Zapoměl

Studijní obor: Bezpečnostně právní studia ve veřejné správě

Forma studia: Kombinované studium

Vedoucí práce: Mgr. Čížek Vladimír, DiS.

Mgr. Et Dr. Lubomír Pána, Ph.D.

Katedra: KESVS

2010

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s využitím uvedených pramenů a literatury.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna ke studijním účelům.

.....

vlastnoruční podpis autora bakalářské práce

Děkuji vedoucímu bakalářské práce Mgr. Vladimíru Čížkovi, DiS. za cenné rady, připomínky a metodické vedení práce.

Obsah:

Abstrakt

Zapoměl, M. *Právní aspekty použití softwaru, pirátství : bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, o. p. s., 2008. 48 s. Vedoucí bakalářské práce Mgr. Vladimír Čížek, DiS.

Klíčová slova: počítače, počítačový program, softwarové pirátství, duševní vlastnictví, warez, softwarové licence, padělky, sdílení, rozmnožování, stahování, internet, modifikace programu, autorské právo, trestní právo, občanské právo, záložní kopie, spam, infoware, sajty

Bakalářská práce „Právní aspekty použití softwaru, pirátství“ pojednává o problematice tíkající se softwaru a jeho nelegálního šíření z pohledu práva. Hlavním obsahem práce je vymezení pojmů týkající se kybernetické kriminality a popis současné právní úpravy autorského zákona. Dále se v práci nachází počátky softwarové pirátství, z něhož vznikly nové typy protiprávního jednání. Předposlední část práce se zaměřuje na internetové škůdce a ochranu počítače proti jejich šíření. V závěrečné části je uvedena míra pirátství v České republice a ve světě, zaměřuje se na konkrétní případy spojené s pirátstvím, které se dostali až před soud.

Abstrakt

Zapoměl, M. *Legal aspects of the use of software porady : Bachelor thesis.* České Budějovice : The College of European and Regional Studies, o. p. s., 2008. 48 p. Supervisor: Mgr. Vladimír Čížek, DiS.

Keywords: computers, software, software piracy, intellectual property, warez, software license, counterfeits, sharing, copying, downloading, internet, program odification, copyright law, criminal law, civil law, backup copy, spam, infoware, sajts

Thesis "Legal aspects of the use of software piracy" is about ticking the issue of illegal software distribution from the perspective of law. The main content of this work is the definition of terms related to cyber crime and a description of the current legislation of copyright law. Further work is software piracy, which has created new types of infringement. The last part focuses on the internet pests and protect your PC against their spread. The final section is given piracy rate in the Czech Republic and abroad, focusing on specific cases related to piracy, which went to court.

1. Úvod

Dnešní svět si snad již nikdo z nás nedokáže představit bez výpočetní techniky. Využíváme ji každý den ať už k práci, komunikaci, učení, nebo pro zábavu. Setkáváme se zde s názvy, které se staly běžnou součástí informační techniky, avšak mnoho lidí ani netuší, co který název znamená, jeho význam a jaká rizika v některých případech přináší. I v tomto světě výpočetní techniky platí zákony dané společností a i zde platí úsloví „neznalost zákona neomlouvá“.

V této práci se tedy pokusím objasnit některé nejznámější a nejpoužívanější výrazy, s kterými se člověk může na internetu i mimo něj setkat. Budu se snažit přiblížit složitou problematiku týkající se porušování autorských práv a proč k němu v takové velké míře dochází. Uvedu příklady, jak se na danou problematiku dívají softwarové společnosti na straně jedné a piráti na straně druhé. Popíši zde začátky počítačové války mezi těmito dvěma stranami a její postupný vývoj. Dále zde uvedu příklady, jakým způsobem vzniká pirátský software a jak dochází k jeho šíření.

2. Softwarové pirátství

Pojem softwarové pirátství je často milně zaměňováno s warez. Softwarové pirátství označuje útoky proti autorskému právu z hlediska počítačových programů k získání komerčního obohacení, pro sebe nebo někoho jiného.

2.1 Historie softwarového pirátství

Pirátství je v dnešní době v podstatě nová forma padělatelství, představuje elektronickou obdobu jednoho z nejstarších a nejznámějších zločinů v historii naší civilizace. Již římští umělci vytvářeli tisíce padělků podle řeckých uměleckých vzorů, které byly takřka k nerozlišení od originálů. I když existovalo pirátství a padělatelství ve velkém měřítku, naše civilizace stejně vzkvétala. Pirátství je přirozenou součástí evoluce a potřebujeme jej kvůli dalšímu vývoji. Stále musíme být ve střehu a zdokonalovat technologii. [1]

Koncem sedmdesátých let 20. století vstoupily na trh osobní počítače. V této době hrál software zcela jinou roli až do roku 1980, kdy vznikl zákon o autorských právech k počítačovému softwaru, který definoval software jako literární dílo. Do té doby nebyl software uznáván jako duševní vlastnictví, takže ani nemohly existovat zákony proti jeho krádežím, nebo kopírování. [2]

Dobrým příkladem toho, jak se technologie vyvíjí, jsou počítačové operační systémy. Zpočátku byly systémy Windows 95, 98 a 2000 velmi otevřené a komunikativní. Do většiny počítačů se dalo snadno vniknout, a to člověk ani nemusel být s nimi v lokální síti. Zabezpečení pro koncové uživatele před deseti lety neexistovalo a každý počítač se dal lehce zneužít.

Když se v roce 1999 začali objevovat první počítačoví červi, internetové společnosti hned pocítily, jaké následky by rychlé zneužití počítačů mohlo přinést. Microsoft vydal operační systémy s novými bezpečnostními prvky. Firewally a zabezpečovací software zažily nebývalý rozvoj. V polovině roku 2003 již měl každý uživatel doma vlastní antivirový software. I když Internet stále provrtávají počítačoví červi, jejich budoucnost vypadá bledě. Za pár let už bude napadeno jen mizivé procento internetových uživatelů.

---

[1] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 154, ISBN: 978-80-247-1765-4

[2] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 27, ISBN: 978-80-247-1765-4

2.2 Ochrana softwaru proti kopírování

Nejrozšířenější forma, jak získat nelegální software je kopírování. Programy nebo hry uživatelé kopírují od té doby, co se u domácích počítačů objevily disketové, CD, DVD, Blue-ray mechaniky. Vývoj softwaru však jde rychle dopředu. Je čím dál graficky a procesově náročnější. Jeho výrobní náklady stoupají, a tak se výrobci snaží kopírování jejich softwaru předejít. Často to však bývá neúspěšně.

Mezi nejčastější metody zabezpečení softwaru jsou kontroly CD, sériová čísla, hardwarové klíče apod. Tyto metody sice míru pirátství sníží, avšak moc ho nepřibrzdí. Postupem času lze pochopit a následně prolomit každou ochranu. Technologie se však vyvíjí a výrobci nezahálejí při hledání nejlepšího bezpečnostního opatření. Softwary, které jsou nejvíce napadány, ze strany pirátů jsou v prvé řadě počítačové hry. Výrobci těchto her dávají mnoha miliónové náklady právě na zabezpečení jejich produktu.

S rozšířením Internetu do většiny domácností a jeho celosvětovém pokrytí obecně (internetové kavárny, obchodní centra s připojením na internet, apod.), se mnoho vývojářů snaží svůj produkt chránit tím, že raději volí online model prodeje podle služeb, které klient požaduje. Výhodou je, že je velmi těžko napadnutelný piráty. Pro ně je skoro nemožné tuto ochranu prolomit. Jako jedna z prvních firem, která přešla na tento systém ochrany patří asi nejznámější Blizzard Entertainment, inc., který ochranu svých nových produktů dotáhl skoro až k dokonalosti. Jeho nejznámější produkt, kterého tento systém využívá je MMORPG (Massively Multiplayer Online Role Plaing Games) hra s názvem World of Warcraft. Jedná se o online hru (nutnost připojení v době hraní na Internet). Uživatel nemá nainstalovanou celou hru, nýbrž jen její část. Zbytek hry (vytvoření postavy, či mapy), je distribuován na serverech výrobce. Na modelovém příkladě se pokusím blíže objasnit, jak tento systém ochrany na výše zmíněné hře funguje.

2.2.1 Příklad ochrany softwaru

Firma Blizzard nabízí tento produkt hned ve dvou formách, jak si ho zákazník může pořídit. Buď si zakoupí hru na CD, nebo si ji může zdarma stáhnout na stánkách výrobce. Uživatel si hru nainstaluje, avšak bez vytvoření tzv. „accountu“ (uživatelský účet) na stránkách výrobce, hru nespustí. Teprve v něm mu systém vytvoří uměle vygenerovaný kód, který je originální pro daný účet. Hru musí předplatit, aby ji mohl využívat. Při každém spuštění hry, musí následně zadávat svůj login a heslo accountu.

Ochrana produktu se zdála být tímto systémem bezpečná. Ale piráti dokázali vyzrát i na toto.. Jelikož ochrana uživatelského počítače není příliš vysoká, tak se piráti dokázali nabourat do uživatelského accountu a následně si ho přivlastnit. Uživatel se pak musel obrátit na Blizzard, kde doložil svou identitu a na základě této identity mu byl ukradený account vrácen. Blizzard s ochranou svého nejvýdělečnějšího produktu zašel ještě dál. Blizzard vydal tzv. Authenticator. Lze si ho koupit ve formě přívěsku, nebo zdarma stáhnout, jako aplikace pro Iphone. Každý authenticator má své originální výrobní číslo, které uživatel zadá ve svém accountu. Tím dojde ke spárování s accountem a hrou. Authenticator pracuje na principu náhodně generovaných čísel, které se při spuštění každých třicet sekund mění. V konečném výsledku tedy musí uživatel při spuštění hry zadávat svůj login, heslo a vygenerované heslo z authenticatoru. Tímto se jeho účet stává zatím naprosto bezpečným a Blizzard se tak stal průkopníkem v ochraně dat. Toto je přímá ukázka ochrany produktu, jak ze strany výrobce, tak ze strany uživatele.

3. Počítačová kriminalita a společnost

Vnímání počítačové kriminality společností je zatíženo nehmotným charakterem produktů a bezprostřední neviditelností následků trestného činu. Zatímco krádež počítače, tedy fyzického hardwaru, je vnímána jako běžný trestný čin, u věcí, které nemají hmotnou podstatu, se veřejné mínění přesouvá na druhou stranu barikády. Pachatel, který převede několik milionů z účtu svého zaměstnavatele na účet vlastní, je posuzován jinak, než kdyby přišel do banky s pistolí a peníze si vzal násilím. Společnost ho spíše považuje za šikovného a mazaného podvodníčka.

I přesto, že jsou tyto trestné činy společensky velmi nebezpečné a způsobují značné finanční ztráty, odlišují se od klasické představy zločinu s jeho násilnou fyzickou podstatou. Softwarové pirátství je společností vnímáno ještě benevolentněji. Velká část občanů, kteří vlastní počítač, na něm má nainstalováno i nelegální programové vybavení a nepovažuje to za porušení zákona. Vždyť software není žádná hmotná věc.

K obecně laxnímu postoji veřejnosti vede i značná neúspěšnost při vyšetřování a trestání počítačové kriminality. Počítačový útok je daleko závažnější, jelikož vede, pokud se podaří, k daleko většímu zisku pro pachatele. Pachatel zároveň neriskuje fyzické zranění a pravděpodobnost, že bude dopaden a odsouzen je minimální. Všechny tyto okolnosti tedy spíše podporují nárůst a rozvoj počítačové kriminality.

3.1 Výměnné sítě

Velice rozšířené jsou ve společnosti tzv. Peer-to-peer (P2P) sítě. Jedná se o propojení počítačových sítí jednotlivých uživatelů bez nutnosti komunikace se serverem, tyto sítě byli decentralizované (svobodné, bez správce, hůře vystopovatelné). V dnešní době se decentralizované P2P sítě moc nevyskytují. Nahradily je sítě centralizované (pod dohledem, více jak jeden správce). Prostřednictvím této sítě si mohou uživatelé vyměňovat data. Pro příklad uvádím nejpoužívanější programy k P2P komunikaci: Strong DC++, eMule, Shareaza, eD2K (eDonkey)

Na těchto sítích je směsice mnohdy nepřehledných pirátských kopií. Najde se zde v podstatě vše od médiových souborů až po software.

Výhody těchto sítí: jsou snadno dostupné běžným uživatelům.

Nevýhody těchto sítí: obsahují mnohdy záměrně napadený soubor trojskými koni, viry apod..

3.1.1 Napster

Jeden z prvních významnějších pokusů co se počítačů týká, bylo vytvoření systému nazvaného Napster. Vytvořil ho student Bostonské univerzity Shawnem Fawningem. K jeho spuštění došlo 1. června 1999 a jeho cílem bylo snadnější vyhledávání hudebních souborů ve formátu MP3 v komunitě lidí, kteří si navzájem umožní stahovat své soubory. V té samé době došlo díky nástupu vysokorychlostního připojení k Internetu k rozvoji služeb instant messagingu založeného na P2P principech s koordinačním serverem. Napster byl navrhnut podobně jako tyto sítě. Umožňoval vedle komunikace i vyhledávání a sdílení hudebních souborů. Na jeho centrálním serveru byly umístěny seznamy skladeb připojených uživatelů. Nejednalo se tedy o čistou P2P síť, ale o její zprostředkovanou variantu.

Uživatel, který hledal konkrétní soubor, zaslal svůj požadavek na centrální server, a pokud některý z připojených uživatelů požadovaný soubor nabízel, byl k němu zájemce přepojen. Samotný přenos už probíhal pouze mezi počítači těchto dvou klientů na principu P2P bez další účasti serveru. Použití jednoho centrálního serveru bylo samozřejmě slabým místem, neboť jakákoli porucha serveru znemožnila vyhledávání. Napster byl původně vytvořen pro malou skupinu vysokoškolských studentů, idea Shawna Fawninga našla velice rychle mnoho příznivců a za několik měsíců už měla několik milionů uživatelů.

S rostoucím objemem přenášených hudebních dat se však začal projevovat pokles celkového množství prodejů zvukových nosičů. Výrobci a distributoři nosičů argumentovali, že tento pokles přímo souvisí velkým nárůstem stahování hudby pomocí Napsteru. Poprvé se tak objevil problém se sdílením autorských děl v podobné síti bez souhlasu jejich autorů. Organizace RIAA (Recording Industry Association of America) zastupující americké nahrávací společnosti podala v prosinci 1999 proti Napsteru žalobu na náhradu škody. Jako první z interpretů podala na Napster 12. června 2000 žalobu na náhradu škody skupina Metallica, následovaná záhy několika dalšími. Součástí žaloby byl i návrh na předběžné opatření, který obsahoval požadavek na odpojení konkrétních uživatelů a odstranění chráněných skladeb dotčených interpretů ze systému.

Při projednávání případu porušení autorských práv a stanovení případné spoluodpovědnosti Napsteru za toto porušování bylo nejprve nutné stanovit, zda k takovému porušení autorských práv vůbec došlo. Vzhledem k objemu stažených dat bylo zřejmé, že nemohly být splněny podmínky institutu Fair Use, což je americká obdoba našeho volného užití díla, a k porušení práv autorů tímto jednáním došlo. Na

základě toho bylo rozhodnuto o spoluodpovědnosti Napsteru za chování jeho uživatelů. Podstatným argumentem soudu bylo, že Napster si byl nejen vědom protiprávnosti nabízeného obsahu a jednání, ale také toto jednání otevřeně podporoval.

Soud předběžným opatřením uložil Napsteru povinnost dohlížet na systém a odstraňovat obsah s názvem shodným s chráněnými díly. Následně však bylo shledáno, že použitý způsob filtrace obsahu nefunguje na 100%, a bezúplatná výměna souborů byla zcela zastavena. Napster ve své původní podobě zanikl v roce 2001, když se společnost ocitla v konkurzu. V současnosti je pod známou doménou provozován placený server poskytující hudbu, jehož provoz byl zahájen s poměrně velkou prodlevou, takže původní uživatelé Napsteru přešli na jiné druhy sítí další generace.[3]

3.1.2 BitTorrent

Mezi nejpopulárnější rozšířené sítě patří jednoznačně BitTorrent. Nejenže tuto síť používají obyčejní uživatelé za účelem stáhnutí pirátského softwaru, ale používají jej i organizace, jako spolehlivý způsob šíření velkých souborů.

BitTorrent funguje na jedinečné filozofii, která mu pomohla tak k rychlému růstu. Každý uživatel, který si nějaký soubor stáhne, může ho zároveň i sdílet s ostatními uživateli. Proto čím více uživatelů si soubory stahuje, tím rychleji se rozšíří ke všem. Uživatel si tak například může stáhnout první dvě procenta souboru od jednoho uživatele a posledních deset procent od jiného. Každý uživatel nabízí jiný úsek souboru, a všechny úseky se nakonec spojí v jeden celek. Uživatel s jedním procentem staženého souboru dopomůže jinému uživateli s 99 procenty daného souboru dokončit stahování doplněním chybějících a potřebných bajtů. Existuje bezpočet webových stránek s BitTorrentem, které uživatelům umožňují prohledávat vše, co rozličné BitTorrenty nabízejí. Čím více lidí si soubor stáhne, tím lépe. Jediným požadavkem BitTorrentu je sledovací soubor (tracker file), což je jedinečný soubor URL (Uniform Ressource Locator), se kterým pak počítač komunikuje. Trackery slouží jako prostřednící, kteří předávají požadavky na datové balíky, nebo nabízejí sdílení kusu souboru ostatním.

Technologie BitTorrentu se dá nejlépe popsat jako hybridně centralizovaný distribuční server. I když dostává každý klient data přímo od dalšího klienta, je stále

[3] Robert Šustr, Napster P2P, [online] Dostupný z WWW: <http://p2p.chytrak.cz/> [10.dubna 2010]

zapotřebí onen zprostředkující centrální server a ten je právě slabinou BitTorrentu. Zprostředkující server je totiž zodpovědný za data a obsah, který poskytuje ostatním.[4]

3.2 Diskusní skupiny

Diskusní skupiny patří mezi nejstarší a zároveň nejznámější internetovou službu. V minulosti se tyto skupiny řadily mezi nejvyužívanější možnosti k získání pirátského softwaru. Později se na scéně objevily výměnné sítě a diskusní skupiny se stáhly do pozadí. Nyní si diskusní skupiny na pirátské scéně znovu našly své místo. Na diskusní skupiny se pohlíží jako na méně střežené oblasti internetu. Zde nalezneme více pirátských filmů dříve, než-li se objeví na výměnných sítích. Skupiny nesou jen malou zodpovědnost za produkt, který se na nich nachází. Hlavním faktorem na neutuchajícím úspěchu diskusních skupin je anonymita. Zdrojové IP adresy těch, kteří si něco nahrávají nebo stahují, se nikde neukazují. Navíc se data ukládají na vzdálené servery, takže klienti nenesou právní zodpovědnost za šíření pirátských dat. Z právního hlediska jsou diskusní skupiny pro konečného uživatele mnohem lepší.

3.3 Důvody používání pirátského softwaru

Hlavním důvodem, proč je softwarové pirátství tak rozšířené, je to, že je snadno dostupné. Pirátství škodí softwarovému průmyslu, o tom není pochyb. Softwarové firmy musí tvrdě zapracovat na tom, aby vylepšily bezpečnostní a ochranné technologie svých produktů. Softwarové firmy už zjistily, že když se podívají, jak piráti crackují jejich programy, odhalí tak nejlépe klíčové informace, jak jim čelit. Na softwaru se neustále pracuje, stále se vydávají nové a upravené verze již existujících programů. Aktualizace a upgrady se někdy dávají registrovaným vlastníkům zdarma nebo se slevou.

Proč lidé používají pirátský software? Obrovskou motivací je úspora peněz. Originální software stojí až několik tisíc korun za kus, kdežto pirátský software je zadarmo. Ušetřit peníze je pro lidi v dnešní době důležité, takže pokud se jim dá možnost volby, mnozí si vyberou raději pirátský software. Většina uživatelů domácích počítačů, kteří si pirátský software stahují, si ho nejdříve chtějí vyzkoušet, zda jim bude vyhovovat a většinou si ho koupí, pokud jim vyhovuje. Obdobně jsou na tom hráči počítačových her, když se jim nějaká hra zalíbí, mnohdy rádi podpoří jejího tvůrce a hru si koupí.

[4] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 117, ISBN: 978-80-247-1765-4

3.3.1 Přístupy k pirátství

Nově vyvinuté ochranné prostředky, které vznikají díky vynaložení obrovských nákladů, jsou často prolomovány a někdy dokonce ještě před uvedením produktu na trh. Když už firmy (ať softwarové či jiné) unaví veškeré jejich pokusy chránit svůj produkt, a jejich veškerou ochranu proti kopírování piráti s lehkostí překonávají, řada z nich se obrací o pomoc na policii. Dokázat vinu je ve virtuálním světě velmi obtížné, protože porušení právních předpisů musí orgány činné v trestním řízení dokázat konkrétní osobě.

4. Kybernetická kriminalita

Softwarové pirátství se považuje za organizovaný zločin (a v USA jako federální delikt). Poruší-li někdo americké federální zákony, nemá šanci na podmínečné propuštění a nepomůže mu ani jeho dobré chování během trestu. Tak to platí v USA od 1. listopadu 1987 (po reformě amerického trestního zákoníku).[5]

4.1 Hacker

Pojmenování „hacker“ vznikl zhruba v padesátých letech minulého století v komunitě radioamatérů, kde se jím označoval technicky šikovný jedinec, schopný hledat nová zapojení a metody ke zlepšení výkonu a dosahu svého vysílače.[6]
Hacker je odborník na zpracování dat využívající svých znalostí a prostředků k získání neoprávněného přístupu k chráněným datům nebo programového vybavení.

4.1.1 Hacking

Přes veškeré a někdy oprávněné výhrady, však nelze hackerům upřít znalosti a schopnosti. Díky tomu se vyvíjejí silný tlak na zlepšování bezpečnosti sítí a kvality programů. Možná je způsob vynucování nápravy, který zvolili, nekorektní a v některých případech i nezákonný. Nikdo nemůže popřít, že bez hackerů a jejich veřejných útoků bychom dnes neměli k dispozici mnoho service packů a bezpečnostních záplat. Naše počítače by byly mnohem otevřenější, méně chráněné a snadno zranitelné. Nevznikl by ani tržní úsek bezpečnostních technologií, který je nemalým zdrojem příjmů pro mnohé technologicky vyspělé firmy. [7]

Kolem hackerů, kteří něco umí, není nutno dělat zbytečný rozruch. Je to období růstu a později své aktivity převedí na legální platformu prospěšnou společnosti. Stanou se z nich bezpečnostní odborníci, nebo se uchytí u firem, které se počítačovou bezpečností, pokud si takovou firmu sami nezaloží. Tento trend již můžeme pozorovat u některých hackerských serverů, ze kterých se pomalu stávají servery komerční, transformují se a nabízejí produkty související s počítačovou bezpečností. Základním

[5] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 136, ISBN: 978-80-247-1765-4
[6] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 47, ISBN: 978-80-247-1561-2
[7] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 50, ISBN: 978-80-247-1561-2

motivem hackera je přijetí výzvy k souboji s technologickým problémem, nikoliv zisk, který z jeho vyřešení plyne.

Hacker nejdříve zjistí (většinou z firemního bulletinu nebo z webové stránky firmy), kdy softwarová firma hodlá vydat nějaký nový produkt. Pak se vkrade do dotyčné firmy s jediným cílem: ukrást poslední verzi softwaru, a s ním pokud je to možné, i zdrojový kód.

Vývojářské softwarové společnosti kladou velký důraz na ochranu své práce proti kopírování. Pokud hacker získá zdrojový kód k nějaké aplikaci, ochrana ztrácí význam. Zdrojový kód k aplikaci totiž každému umožňuje, aby si zjistil, jak přesně ochrana funguje a kterou její část aplikace používá. Pokud se tedy skupině dostane zdrojový kód do spárů, stačí jí pár minut na to, aby ochranu proti kopírování prolomila, a ušetří si tak plno času a úsilí, které by museli piráti na překonání ochrany věnovat.

Zaměřený hacking odstraňuje spoustu prvků, které pomáhají hackery chytit. Většinu hackerů nechytí, když se pokouší systém napadnout, protože u málokterého z nich jsou k vidění předběžná bezpečnostní opatření jako např. IDS (Instrusion Detection Systems). Provede-li hacker svou akci během 8 hodin, je pravděpodobnost, že si ho někdo všimne nízká. Pokud se hacker chová diskrétně, nikdo nemá důvod si myslet, že je systém pod „hackerskou palbou“. Softwarové firmy většinou nemají ani potuchy, že si z jejich serveru vytvořený software někdo zkopíroval. [8]

4.2 Cracker

Motivací kriminálních crackerů je zisk za každou cenu. Jedná se o organizované a izolované skupiny spojené s kriminálním podsvětím. Jejich cílem je dostat se na servery velkých firem nebo institucí. Do této skupiny můžeme zařadit hackery najímané korporacemi s cílem provádět průmyslovou a obchodní špionáž u konkurence. Cracker skutečně škodí, pozměňuje nebo maže data, neoprávněně získává informace (čísla kreditních karet), rozšiřuje viry apod. [9]

[8] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 47, ISBN: 978-80-247-1765-4
[9] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 56, ISBN: 978-80-247-1561-2

4.2.1 Cracking

Crackeři dokáží ochranu proti kopírování překonat, a to vše i několik hodin před tím, než se tituly dostanou na prodejní regály obchodů. Pirátství by bez pomoci crackerů nemohlo existovat. Jde o souboj mozků: softwaroví vývojáři vytvářejí složité zámky, jež se crackeři snaží co nejrychleji odemknout.

Při crackování jde o vysoce nelogický, a takříkajíc zpětný způsob uvažování. Proces je to tak zmatený, že i nejzkušenější programátoři nemusí pochopit jeho zásady. Je běžné, že úspěšní crackeři bývají poloviční autisté. Nedá se to naučit, nedá se tak začít přemýšlet, jako cracker se člověk musí narodit.

Na scéně se pohybuje jen hrstka vysoce schopných crackerů, avšak ti, co se tam pohybují, jsou dobří. Zvažte kupříkladu následující: Cracker tráví svůj volný čas, aby prolomil protipirátskou ochranu proti kopírování, kterou vymýšlejí týmy nesmírně zkušených programátorů, a to není nijak řídký jev. Nemálo nadaných crackerů je ve věku něco před dvacítkou, nebo lehce po ní.

Crackeři obvykle pochází z programátorského prostředí a mívají rozsáhlé znalosti v detailních programátorských činnostech, jako je programování hardwaru a programování na úrovní jádra operačního systému. Crackovací techniky nejsou nijak jednoduché. Jsou potřeba léta zkušeností a studia, než cracker vše v pohodě zvládne. [10]

4.3 Warez

Warez, neboli výroba a rozšiřování pirátského software, je trestná činnost. První pirátské kopírování hudby umožnily již audio kazety, technologie videa zase umožnila pirátské šíření filmů na videokazetách. Prvním masivně šířeným pirátským software byly hry na osmibitových počítačích. Zdálo se, že se warez vytratí s nástupem nových technologií, které se nedají přepisovat „CD-ROM a DVD“, ale netrvalo dlouho, než se objevily vypalovací zařízení, a proto je dnes pořízení digitální pirátské kopie mnohokrát levnější, než originál. Opravdový nástup warezu nastal až s rozvojem rychlého Internetu, odkud je možné stáhnout pirátské kopie programů, filmů, nebo hudby již několik dnů po jejich oficiálním vydání. [11]

[10] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 56, ISBN: 978-80-247-1765-4

[11] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 68 ISBN: 978-80-247-1561-2

4.3.1 Warez společenství

Warez je uzavřené společenství lidí, jejichž koníčkem je zpřístupňování pirátských kopií na internetu ve formě tzv. „release.“ Toto společenství se nazývá „warez scéna“ a je velmi dobře organizované. Její členové jsou z celého světa a osobně se nikdy nesetkali. Znají se jen přes internet pod přezdívkami a jejich komunikačním jazykem bývá angličtina. Nejčastěji se jedná o studenty, programátory a pracovníky hudebních nebo filmových vydavatelství. [12]

Warez komunita je poměrně uzavřená okolnímu světu a je obtížné se do ní dostat. Nové členy oslovují pomocí: .nfo souborů. Většinou vyžadují mimořádné schopnosti (cracking, hacking), přednostní přístup k produktům (supplier) nebo možnost poskytnutí hardware či rychlého internetového připojení (siteop). Členové nemají žádný zisk z toho, co pro scénu udělají a toto pravidlo dodržují. Jedním z nejpřísnějších tabu warez scény je vypalovat a prodávat release nebo prodávat či pronajímat získané účty na sites cizím osobám. Za takový přestupek je zjištěný viník bez milosti vyloučen, dostane zákaz přístupu na IRC kanál své skupiny a jsou mu odstraněny možnosti přístupu na FTP servery (File Transfer Protocol – protokol pro přenos souborů). Navíc se informace o viníkovi rozešle ostatním skupinám.

Motivace každého příslušníka warez scény, může být odlišná, avšak lze nalézt společné prvky. Jednou z motivací je rychlý přístup ke všem releasům ve scéně bez složitých hledání a čekání ve frontách. Uživatelé releasů jsou v první řadě členové warez scény. Druhou motivací je touha po uznání a respektu. Tedy být členem této skupiny a sdílet spolu s ostatními trochu uznání, které se mu v reálném světě nedostává. Celá warez scéna připomíná týmové sportovní zápolení, kde vítězí ten nejrychlejší, nejaktivnější. Člen, který má slabé výsledky je nahrazen novým, který je přijat pouze na zkušební dobu, během této zkušební doby musí prokázat své schopnosti.

4.3.2 Boj s warez

Uveřejňování nelegálních kopií uměleckých děl a programů dělá starosti zejména organizacím na ochranu autorských práv. Je zřejmé, že aktivity warez scény jsou vesměs ilegální, a tak logickou reakcí je aktivita represivních složek dotčených států projevující se v zatýkání a odsuzování členů warez scény k vězením nebo

[12] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 71, ISBN: 978-80-247-1561-2

pokutám. Vzhledem k povaze a dokonalé organizaci warez scény to ale není jednoduché. Uzavřenost skupin, jejich globální působnost a příslušnost jejich členů k různým státním jurisdikcím znesnadňuje jak získávání důkazů, tak i možnosti reakce orgánů činných v trestním řízení. Zásahy proti warez scéně jsou proto zřídkavé, ale dlouho připravované a rozsáhlé. K účinnému zásahu je nutná přesná koordinace policejních složek v několika státech; ojedinělá akce jen utlumí na několik dní aktivity warez scény.

4.4 Sajty

Sajty užívané pro warez se už dlouho ztotožňují se světem pirátství. V počátcích pirátské scény se k distribuci informací používaly systémy BBS (Bulletin Board Systems), jenže analogové telefonní linky se brzy přežily, a rozvíjející se internetová technologie nabídla pirátům větší šířku pásma a nové možnosti. Dnes zvládnou warez sajty najednou i padesát uživatelů, kde každý má přinejmenším 100 Mb připojení. Ve světě technologií se toho hodně změnilo, a zároveň s tím se změnilo také pirátství. Pokud se připojíte na skutečnou warez sajtu, je to, jako kdybyste dostali klíč k tajemné komnatě. V digitálním světě umožňuje a zpřístupňuje cokoli. Jsou tu filmy, hry, aplikace, knížky apod.. [13]

Warez skupiny a sajty se potřebují navzájem. Správci sajt chtějí tituly skupin jako první v pořadí; potřebují, aby skupiny předvydávaly své tituly na jejich sajtě, a tím pádem sajtě roste popularita a prestiž. Skupiny oproti tomu potřebují sajty ze dvou důvodů: za prvé potřebují možnost vydat své zboží, a za druhé ho potřebují bleskově rozšířit po sajtách scény. Jako odměnu za neutuchající a namáhavou dřinu odměňují skupiny své členy neomezenou možností stahovat vše, co je napadne. Sajty na scéně jsou báječné a bezpečné datové sklady, kde se na nějakou tu chybičku nehledí, a proto je piráti využívají. [14]

4.4.1 Druhy sajt

Sajty na scéně se objevují v nejrůznějších podobách, a každá se zabývá jinou oblastí zájmů. Faktorem, bývá rychlost, která rozhoduje o úspěchu či neúspěchu sajty. Čím má sajta větší šířku pásma, tím rychleji na ni mohou její kurýři nahrávat tituly.

[13] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 88, ISBN: 978-80-247-1765-4
[14] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 87, ISBN: 978-80-247-1765-4

Hodnocení sajty je důležité, protože piráti hledají sajty s nejlepším hodnocením. Takových sajt (tj. s hodnocením 3,0 až 3,5) je ovšem málo. Na internetu existuje asi patnáct sajt s hodnocením 3,0 a lépe. Platí, že v této významné skupině se udrží jen ty nejbezpečnější a nejuznávanější z nich. Mají obrovské archivy softwarových a jiných titulů. S velkými paměťmi a skoro nulovými prodlevami nabízí pirátům vše, co si přejí. Na skladě mají všechno od hudby, filmů, elektronických knížek až po software pro konzole.

Nejlepší sajty se nacházejí na hlavních páteřních linkách internetu, nebo u velkých poskytovatelů internetu, kteří oplývají impozantním hardwarem. Jejich největším rizikem je to, že se na ně zaměřuje největší pozornost policie, ačkoli se jí prozatím nepodařilo odhalit těchto sajt příliš mnoho. Špičkové sajty a jejich správci si zakládají na své výlučnosti a nadřazenosti. Abyste na některé z nich dostali účet, musíte mít na scéně už nějaké jméno a musíte patřit do známé skupiny s dobrou pověstí. Jejich uživatelské skupiny jsou malé, nečítají často ani sto uživatelů. Pokud už vám účet přidělí, stane se z vás skutečná elita.

Sajty s hodnocením 2,5 až 3,0 patřívají k nejvýznamnějším z obyčejných sajt. Bezpočet skupin, pokud nemají povolené účty na sajtách s hodnocením 3,0 až 3,5, posílají své tituly právě sem.

Na horších sajtách, které mívají jako základnu asi 200 až 300 účtů, se účet shání snáze. Jenže abyste si sehnali účet na sajtě s hodnocení 2,5 až 3,0, musíte mít na scéně slušnou reputaci nebo se přidružit k nějaké známé a velké pirátské skupině.

Na těchto sajtách jsou většinou stejná množství dat jako na exklusivních sajtách s hodnocením 3,0 až 3,5 s jediným rozdílem: mají horší šířkové pásmo a podporují je méně kvalitní skupiny.

Aby sajta dosáhla hodnocení 2,5 až 3,0, musí mít čisté a nezaplněné připojení s rychlostí přinejmenším 100 Mb. Šířku pásma má zpravidla v Evropě nebo na některé z nových vysokorychlostních lokací v Americe.[15]

Sajt s hodnocením 1,5 až 2,5 je mnoho. Na nich má své účty většina členů scény. Dostávají aplikace, obrazy ISO a filmy až několik hodin poté, co vyjdou oficiálně. Než se titul rozšíří celosvětově, uplyne jedna až dvě hodiny, takže tato skupina se stává méně zajímavá. Jestliže nějaká skupina nedokáže protlačit svůj titul na kvalitnější sajtu, musí se spokojit s vydáním právě zde. Většina sajt začíná s hodnocení 1,5, ale jak sajtě

[15] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 90, ISBN: 978-80-247-1765-4

narůstá její reputace a skupina přívrženců, tak roste i její prestiž. Protože mívají takové sajty až jeden tisíc uživatelských účtů, musejí mít něco extra, aby se odlišily od ostatních.

Nejnižší hodnocení je 0,5 až 1,5. To zahrnuje připojení z domu kabelem s rychlostí nějakých 10 Mb a omezeným prostorem ke skladování dat. Tyhle sajty na scéně převažují a rychle se šíří. Každý týden se objeví zhruba dvacet nových sajt, přičemž následující týden z nich deset až patnáct zmizí. U těchto sajt nehraje až tak významnou roli kvalita, protože většinou běží na domácích počítačích.

Existuje spousta druhů sajt. I když je hodnocení důležité, uživatelé oceňují sajty, které nabízejí něco neobvyklého. Rychlost je k ničemu, jestliže sajta nezaujme něčím, po čem uživatel touží.[16]

4.5 Definice počítačové kriminality

Počítačová kriminalita, označovaná v anglické literatuře mnohdy jako „IT crime“, „cybercrime“ nebo „computer crime“ může znamenat, jakýkoliv čin směřující k narušení, zneužití počítače, nebo počítačového systému a informací v něm obsažených. Oficiálních definicí počítačové kriminality existuje celá řada, většina z nich vychází z podstaty uvedené výše. Podle materiálu OSN, zabývající se počítačovou kriminalitou je obsahem:

„Tradiční zločinné aktivity jako krádež, podvod nebo padělání, tedy činy trestné ve většině zemí na světa. Počítač rovněž tvoří prostředí pro nové činy spočívající ve zneužití počítačů, které jsou nebo by měly být ve své podstatě trestné.“/U01/. Ve stejném materiálu se UN snaží odlišit dva základní případy – náhodné a neúmyslné použití počítače, které vede ke vzniku škod, a úmyslné použití počítače jako nástroje nebo předmětu kriminálního deliktu.[17]

Česká Republika nemá žádnou instituci, která by se počítačovou kriminalitou systémově zabývala. Řeší se pouze vzniklé trestné činy, které má na starosti policie.

[16] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 94, ISBN: 978-80-247-1765-4
[17] Václav Jirovský, Kybernetická kriminalita,[citace] Grada Publishing, a.s., první vydání Praha 2007, str. 91, ISBN: 978-80-247-1561-2

4.5.1 Třídění podle mezinárodní dohody

Dohoda je určena pro řešení problémů spojených s mezinárodním charakterem počítačového zločinu. Text dohody dělí jednotlivé skutkové podstaty a obsahu takto:

Zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, **jež se dále dělí na:**

- nezákonný přístup,
- nezákonné odposlouchávání,
- narušování dat,
- narušování systémů,
- zneužití prostředků.

Zločiny se vztahem k počítači, které jsou děleny na:

- počítačové padělání,
- počítačový podvod.

Zločiny se vztahem k obsahu počítače, což je především dětská pornografie.
Zločiny se vztahem k autorským nebo obdobným právům.[18]

4.5.2 Třídění podle eEurope+

Rovněž akční plán eEurope+ zdůrazňuje velkou důležitost bezpečnosti počítačových struktur a boje proti kybernetickému zločinu. Klade si za cíl zvýšit bezpečnost a zajistit, aby orgány činné v trestním řízení měly veškeré přiměřené prostředky k činnosti. Jednotlivé počítačové zločiny dělíme na:

- *zločiny porušující soukromí (ilegální sbírání, uchovávání, modifikace, zveřejňování a šíření osobních dat)*
- *zločiny se vztahem k obsahu počítače (pornografie, zvláště dětská, rasismus, vyzývání k násilí apod.)*
- *ekonomické (neautorizovaný přístup a sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody apod.)*
- *zločiny se vztahem k duševnímu vlastnictví (autorské právo apod.).*[19]

[18] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 91, ISBN: 978-80-247-1561-2
[19] Václav Jirovský, Kybernetická kriminalita,[citace] Grada Publishing, a.s., první vydání Praha 2007, str. 92, ISBN: 978-80-247-1561-2

4.5.3 Třídění podle dopadu konkrétního skutku

Trestný čin proti osobě, kam patří útok proti pověsti, pomluva, vydírání, obtěžování, krádež identity (vydávání se za někoho s cílem ho v první řadě znectít, poškodit ho v rodinném nebo společenském životě), nenáležité nakládání s osobními údaji, atd. Příkladem může být situace, kdy je digitální prostředek využit pro úpravu audiovizuálních projevů, Výsledek může být situace, kdy je projev řečníka upraven tak, že zvuk i obraz plně korespondují, i když se původní projev nesl ve zcela jiném duchu.[20]

Trestný čin proti vlastnictví, kde můžeme dále rozeznat případy:

- Kdy je přímým dopadem činu další obohacení se na úkor poškozeného (odčerpávání majetku z účtu nebo využívání služby na účet poškozeného. Škoda může být i značně vysoká, pokud je platba vázána na objem dat nebo čas.
- Kdy je následkem činu „úspora“ nákladů útočníka, jenž by jinak byl ziskem postiženého (investice do koupě software, audiovizuálních nahrávek, atd.); sem patří případy porušení autorských práv, defraudace dat, atd.
- Kdy zisk útočníka a ztráta poškozeného spočívá v dalším nezákonném šíření neoprávněně získaných dat: software, audiovizuálních nahrávek, atd., ať již za úplatu nebo bez ní; do této oblasti spadá i průmyslová špionáž uskutečněná prostřednictvím informatických prostředků (krádež výsledků výzkumu, patentů, marketingových strategií apod.).
- Kdy je škoda napadeného subjektu odvozena od vratného či nevratného zničení, poškození či pozměnění jeho dat (sabotáž, vandalismus viz např. „defacement“); informace tak nemůže být spolehlivě použita pro účel, ke kterému je určena; často jsou přitom změněna pouze některá dat a to v obtížně rozlišitelných detailech, útok se tedy projeví až s určitým zpožděním.
- Kdy je škoda napadeného subjektu založena na tom, že jeho služba není dostupná. Útok zabrání autorizovanému přístupu ke zdrojům, nebo způsobí zpoždění časově kritických operací. Tento typ útoku je používán např. pro potlačení konkurenčních serverů a provedení vyžaduje široce koordinovanou akci většího počtu počítačů.

[20] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 93, ISBN: 978-80-247-1561-2

- Kdy je škoda založena na zneužití informace, která byla neoprávněně získána z informačních a komunikačních sítí v reálném světě (např. informace o trase přepravy velkých finančních prostředků).

Další možnosti, kterými je např. klamavá reklama, nebo naopak, šíření nepravdivých informací poškozujících protivníka mohou využít jak veřejně přístupné mediálními prostředky, tak i přímo protivníkův informačním systému, který byl jinými prostředky předem kompromitován:

- Trestný čin proti veřejnému zájmu, veřejnému pořádku nebo mravnosti, kam můžeme zahrnout pobuřování, šíření poplašné zprávy, kybernetický terorismus, politicky motivovaná špionáž, šíření nelegální pornografie, šíření nenávist, schvalování zločinu a nabádání k němu nebo propagaci toxikomanie, atd.

Je zřejmé, že jednotlivé skupiny uvedené klasifikace se v detailech navzájem prolínají, avšak je to jedna z možných klasifikací, která není sama o sobě vyčerpávající.

5.5.4 Třídění z hlediska skutkových podstat

Základním ustanovením platného trestního zákona, které se týká kybernality, je **§ 257 a „Poškození a zneužití záznamu na nosiči informací“**. Jeho znění popisuje, i když jen ve vztahu k informacím, co není dovoleno s daty dělat. Paragraf je jediným ustanovením, které je určeno pro informační technologie jako také a postihuje vysoce kvalifikovanou trestnou činnost. Zákon se zaměřuje na tři formy činnosti, kterými jsou:

- Neoprávněné užití informací: často je rovněž uváděno do souvislosti s **§ 105 „Vyzvědačství“, § 106 „Ohrožení utajované informace“, § 107, který postihuje vyzrazení utajované informace z nedbalosti, § 128 „Zneužívání informací v obchodním styku“ nebo § 239 či § 240, které postihují porušování tajemství dopravovaných zpráv**. Vlastní podstatou incidentu je prozrazení resp. Jakákoli forma zneužití získaných informací, nacházející se na nosiči informací, např. zkopírování seznamu zákazníků a jeho předání konkurenci.
- Zničení, poškození nebo učinění informací neupotřebitelnými; často rovněž jako

„Poškozování cizí věci“ podle § 257.

- Zásah do technického nebo programového vybavení počítače; často rovněž ve spojitosti s **§ 257 „Poškozování cizí věci“.**

Řadu dalších jednání lze postihnout samostatně, případě v rámci jednočinného souběhu s trestným činem podle § 257a. V trestním zákoníku lze nalézt následující případy v členění podle dotčených paragrafů. [21]

§ 178 „Neoprávněné nakládání s osobními údaji“ – podstatou činu může být prozrazení osobních údajů jiné osobě nebo umožnění jiným osobám, aby se s nimi seznámily.

§ 124c postihující použití nepravdivého nebo neúplného údaje v¨pro vydání dokladu potřebného pro orgány kontrolující zboží a technologie podle zvláštních předpisů, § 125 „Zkreslování údajů o stavu hospodaření a jmění“ a § 148 „Zkrácení daně, poplatku a podobné povinné platby“. Podstatou uvedených činů jsou různé varianty zásahů do technického nebo programového vybavení počítače, resp. Úprava účetních záznamů v informačním systému podnikatele, např. s cílem zatajení příjmů a tím snížení daňové povinnosti.

§ 150 „Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu“, § 151 „Porušování průmyslových práv“ a § 152 „Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi“. Podstatou těchto činů jsou různé formy porušování autorských práv kopírováním cizích autorských děl (distribuce programů, kopírování stránek, umísťování cizích autorských děl na vlastní stránky a na servery), neoprávněné užívání počítačového programu, což lze chápat jako užívání autorského díla bez souhlasu autora (počítačové pirátství).

§ 247 „Krádež“, § 248 „Zpronevěra“ a § 249 „Neoprávněné užívání cizí věci“. Jedná se zejména o případy, kdy pachatel pomocí počítače převede finanční prostředky z účtu jednoho vlastníka na svůj vlastní účet nebo na účet jiného subjektu. Takový převod prostředků může být proveden jak úmyslně tak i z nedbalosti.

§ 250 „Podvod“ a § 250c „Provozování nepoctivých her a sázek“. Záměrem pachatele je uvedení někoho v omyl, což umožní jeho vlastní obohacení, a to nikoliv pouze informacemi, ale přímo materiálně, např. podvodné transakce s podvodným

[21] Václav Jirovský, Kybernetická kriminalita, [citace] Grada Publishing, a.s., první vydání Praha 2007, str. 93 - 95, ISBN: 978-80-247-1561-2

zbožím, penězi či falešnými identifikacemi při nákupu a prodeji. Sem patří i páchání podvodů spočívajících v zadávání nepravdivých čísel nebo čísel cizích platebních karet při nákupu v internetovém obchodě, internetová „letadla“ či jiné internetové pyramidové hry, jejichž podstatou je přerozdělování finančních prostředků vložených hráči do hry zejména ve prospěch pořadatele. Zvláštností dokazování v tomto případě je, že účastníkům není zaručena objektivnost hry, v čemž spočívá podvodné jednání ze strany organizátorů hry.

§ 93 „Teror“, § 95 „Teroristický útok, § 96 „Záškodnictví“, § 97 „Sabotáž“, trestné činy obecného ohrožení shrnuté v hlavě čtvrté TZ pod § 179, § 180 a zejména pro oblast útoků na telekomunikační zařízení § 182 „Poškozování a ohrožování provozu obecně prospěšného zařízení z nedbalosti“. Jedná se o případy, při nichž jsou prostřednictvím nelegálních operací v rámci informačních a komunikačních technologií ohroženy životy a zdraví lidí, dopravní systémy, letecký provoz, nemocnice apod. Nezáleží na tom, zda je či není v takových situacích deklarována politická motivace útoku, resp. Zda se jedná o úmyslnou aktivitu, nebo nedbalost.

§ 176 „Padělání a pozměňování veřejné listiny“, § 209 „Poškozování cizích práv“ a § 249b „Neoprávněné držení platební karty“. Pozměňování počítačových nebo jiných dokumentů je prováděno prostřednictvím úpravy dokladů, ze kterých jsou zaváděna data do počítače, úpravou dat uložených v počítači, úpravou dat v průběhu počítačové operace nebo úpravou dat na výstupní počítačové sestavě. Tyto skutky mohou často být spáchány v jednočinném souběhu s jinými hospodářskými trestnými činy. [22]

[22] Václav Jirovský, Kybernetická kriminalita, [citace] Grada Publishing, a.s., první vydání Praha 2007, str. 93 - 95, ISBN: 978-80-247-1561-2

5. Autorský zákon

Autorské právo je v České republice ošetřeno autorským zákonem č. 121/2000 Sb., který vychází z několika mezinárodních úmluv, zejména tzv. Bernské úmluvy z roku 1886 a Všeobecné úmluvy o autorském právu uzavřené v Ženevě v roce 1952 (World Intellectual Properte Organization – WIPO – světová organizace duševního vlastnictví vznikla v roce 1967, směřující k ochraně tohoto vlastnictví). Zákon 121/2000 Sb. Přesně specifikuje předmět autorského díla v § 2, kde v odstavci 1 je uvedeno: „Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno a v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam.“ Zároveň podle odstavce 2 téhož paragrafu se za autorské „dílo považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Za dílo souborné se považuje databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem“.[23]

5.1 Obsah autorského práva

Autorská práva, která vznikají okamžikem, kdy je dílo vyjádřeno ve smyslu autorského zákona, lze rozdělit do dvou základních skupin – výlučná práva osobnostní a výlučná práva majetková. Mezi práva osobnostní patří zejména právo autora rozhodnout o zveřejnění díla a právo osobovat si autorství (rozhodovat jakým způsobem má být autorství uvedeno při zveřejnění díla). Jinými osobnostními právy jsou práva na nedotknutelnost díla a udělení souhlasu k jakékoli změně nebo jinému zásahu do díla (toto právo je zejména důležité v oblasti počítačových programů, kde by každý, kdo chce upravit cizí autorské dílo, měl nutně získat autorův souhlas). Základním znakem osobnostních práv je, že autor se jich nemůže vzdát, jsou nepřevoditelná a smrtí autora zanikají (§ 11 odst. 4 AZ).

Majetková práva poskytují autorovi výlučné právo na rozhodování o užívání jeho díla a zároveň mu umožňují udělit jiné osobě, ať už právnické nebo fyzické, oprávnění k výkonu tohoto práva. Poskytnutím oprávnění k užití díla majetková práva autorovi nezanikají, vzniká mu pouze povinnost strpět zásah do práva dílo užít jinou

[23] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 96, ISBN: 978-80-247-1561-2

osobou v rozsahu vyplývajícím ze smlouvy. Smlouvou s autorem získává nabyvatel pouze oprávnění k výkonu majetkového práva.

Na rozdíl od práv osobnostních, jsou majetková autorská práva předmětem dědictví a získají je dědici po autorově smrti v běžném dědickém řízení. Majetková autorská práva trvají, podle současného znění zákona, po dobu autorova života a 70 let po jeho smrti.

U děl spoluautorů se počítá doba trvání ochrany od smrti posledního spoluautora. Dílo, u kterého uplynula doba ochrany majetkových práv, se nazývá volné dílo a každý ho může volně užít.

Podstatným institutem v oblasti autorského zákona je „právo dílo užít“, k čemuž dochází v případě, kdy autor k takovému užití svolil. Do rozsahu tohoto práva na užití díla patří:

- právo na rozmnožování díla,
- právo na rozšiřování díla či jeho rozmnoženiny,
- právo na pronájem díla či jeho rozmnoženiny,
- právo na půjčování díla či jeho rozmnoženiny,
- právo na vystavování díla či jeho rozmnoženiny,
- právo na sdělování díla veřejnosti (provozování živě či ze záznamu, přenos provozování díla, vysílání rozhlasem či televizí apod.).

Kromě těchto práv do majetkových autorských práv patří také právo na odměnu, a to jak při prodeji nebo opětném prodeji díla, tak právo na odměnu v souvislosti s rozmnožováním díla.

Autor se může svých práv domáhat občanskoprávní žalobou, která může směřovat k určení svého autorství, zákazu ohrožení svých práv (např. požadavek na zákaz neoprávněné výroby, obchodování, dovozu či vývozu, sdělování veřejnosti apod.), odstranění následků zásahu do práva včetně poskytnutí přiměřeného zadostiučinění omluvou či finančním odškodněním. Autor také může vyžadovat náhradu škody a vydání bezdůvodného obohacení.

5.2 Porušování autorského práva

Otázku postihů za porušení autorského zákona řeší § 152 trestního zákona o porušování autorského práva, práv souvisejících s právem autorským a práv k databázi následovně: „Kdo neoprávněně zasáhne do zákonem chráněných práv

k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci“. [24]

Trestné činy proti duševnímu vlastnictví se velmi rozšířily zejména s rozmachem internetu. Mezi faktory, které k tomu přispěly můžeme zařadit:

- Dostupnost nelegálních kopií autorských děl, kdy kopie díla je pořízena během pár minut a s nízkými náklady.
- Specifika autorských práv spočívající v jejich nehmotné podstatě. Pohled na autorská práva a duševní vlastnictví vyžaduje jiné chápání veřejností, než je běžné pro většinu ostatních trestných činů.
- Vysoká cena softwarového vybavení, vycházející z faktu, že ceny za software se výrazněji ve světě neliší, a tak vzniká mnohdy nepoměr mezi cenami software a kupní silou obyvatel.

Mezi nejčastější činnosti, kdy je porušován autorský zákon, patří kopírování díla. Zdánlivě, vzhledem k nehmotné podstatě duševního vlastnictví, nevzniká žádná přímá škoda, protože vlastník neutrpí žádnou újmu, jeho dílo není nijak poškozeno.

5.3 Piráti a autorská práva

Pro mnoho lidí jsou drobná porušování práv zcela běžná – nahrávají si televizní pořady, kopírují noty nebo kamarádovi nahrají hudbu – ani si neuvědomují, že tím někoho nevědomě okrádají. Stejně je na tom i stahování hudby na MP3 nebo kopírování sharewarových aplikací. Spousta lidí si navykla z internetu běžně kopírovat soubory, ale věci se v našem současném elektronickém světě rychle změnily v jednom, a sice, že digitální kopie kopírováním je stejně kvalitní jako originál. Jedna digitální kopie se rozmnoží na deset, pak na tisíc a nakonec třeba na milion kopií. Skutečnou škodu nadělá právě digitální pirátství. Tyhle kopie už nejsou repliky nebo padělky originálů, to jsou originály.

Vlastníci autorských práv věří, že pokud si něco zkopírujeme bez zaplacení, je to krádež. Zábavní průmysl se snaží pirátství v médiích vyobrazit jako zločin rovnající se

[24] Václav Jirovský, Kybernetická kriminalita, [citace] Grada Publishing, a.s., první vydání Praha 2007, str. 100, ISBN: 978-80-247-1561-2

krádeži auta nebo loupeži. Chtějí okolí a nás přesvědčit, že kopírováním připravujeme jejich zaměstnance o výdělek, a v důsledku i o práci.

Piráti naopak nevěří, že jde o krádež, protože majitele o jeho majetek nepřipravují. Krádež znamená, že někdo někomu něco vezme, pirátství znamená, že dotyčný něco zkopíruje. Piráti argumentují, že majitele připravují jen o potenciální příjmy, jejichž hodnota je pochybná, protože se nedá odhadnout, kolik lidí by si jejich výrobek zakoupilo.[25]

Autorská práva porušují lidé každého věku ze všech možných profesí, oborů, od organizovaného zločinu až po vzdělané profesionály. Liší se jenom motivy pirátství: může jít o finanční zisk, nebo třeba touze po vzrušení ze zločinu. Pro někoho může být pirátství jen hlas spotřebitele, který ovlivňuje cenu a kvalitu, jiný tím vlastně pomáhá podnikům, neboť pro jejich výrobky vytváří trh.

Autorská práva jsou výlučná práva, která uděluje vláda tvůrci různých děl. Tato díla musí existovat v hmatatelné a pevné podobě. Autorská práva nezastřešují nápady nebo koncepty, nýbrž jen jejich prezentaci. Například nemůžeme kopírovat a prodávat aplikaci výrobce softwaru, ale můžeme vytvořit vlastní aplikaci, která má stejný účel. Autorská práva chrání práva vlastníka kopírovat a prodávat svá díla, importovat nebo exportovat je, kopírovat a prodávat odvozená díla, veřejně je předvádět a udělovat či prodávat tato práva jiným. Autorská práva by měla lidem umožnit výhradně profitovat ze svých autorských děl, čímž je motivují k jejich tvorbě.

Ústava Spojených států (přesně paragraf 1, hlava 8) uděluje Kongresu Spojených států právo „podporovat rozvoj věd a užitečných umění tak, že, po omezenou dobu budou mít autoři a vynálezci zabezpečena výlučná práva ke svým spisům a objevům“. Je důležité upozornit na to, že ústava stanovuje, že autorské právo platí pouze po omezenou dobu, což znamená, že nakonec pozbude platnosti, a dílo se stane veřejným majetkem.

I když patentový úřad Spojených států přijal registraci počítačových programů už v roce 1964, neuznával se počítačový software jako intelektuální majetek, dokud nebyl v roce 1980 přijat zákon o autorských právech k počítačovému softwaru (Computer Software Copyright Act), který definoval, že odvozenou počítačovou aplikaci lze také nechat autorsky chránit. Před rokem 1980 si mohl vývojář nechat

[25] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 17, ISBN: 978-80-247-1765-4

autorsky chránit zdrojový kód počítačového programu, ale už ne odvozenou aplikaci, protože jen zdrojový kód se dal číst.

Zákon o autorských právech k počítačovému softwaru stál na začátku řady legislativních změn, které daly softwarovým vývojářům stejná práva jako autorům jiných děl a které proměnily odvětví vývoje softwaru za ziskové.[26]

5.4 Organizace BSA (Business Software Aliance)

Business Software Aliance je přední celosvětovou organizací, která se zabývá prosazováním bezpečného a legálního digitálního světa. BSA je mluvčím světového komerčního softwarového průmyslu a jeho hardwarových partnerů směrem ke státním institucím a na mezinárodním trhu. Členské společnosti BSA představují nejrychleji se rozvíjející průmyslové odvětví na světě. BSA podporuje inovace technologií vzděláváním a iniciativami v oblasti ochrany autorských práv, on-line bezpečnosti, obchodování a e-komerce.

5.5 OSA

Ochranný svaz autorský pro práva k dílům hudebním, o.s., je občanské sdružení chránící autorská práva hudebních skladatelů, textařů a nakladatelů z celého světa. Má uzavřeny reciproční smlouvy s obdobnými ochrannými organizacemi z celého světa. Dne 9. 10. 2009 oslavil 90 let od svého vzniku.

OSA zpracovává osobní údaje za účelem výkonu kolektivní správy majetkových autorských práv. V místě svého sídla a v místě regionálních pracovišť zpracovává adresní, identifikační a jiné osobní údaje svých členů i osob s jiným vztahem k OSA. Příjemci jsou fyzické a právnické osoby v České republice a v zahraničí. [27]

- *byl založen již v roce 1919 českými skladateli, textaři a hudebními nakladateli*
- *je občanské sdružení zastupující více než 5800 skladatelů, textařů, hudebních nakladatelů a dědiců autorských práv*
- *na základě recipročních smluv s partnerskými organizacemi zastupuje až milion zahraničních autorů*
- *repertoár OSA tvoří více než 285 000 skladeb*

[26] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 18, ISBN: 978-80-247-1765-4
[27] Home page, Kdo jsme a co děláme?, [online] Dostupné na WWW: <http://www.osa.cz/> [16. dubna 2010]

- *hlavní činností OSA je kolektivní správa autorských práv k hudebním dílům a zhudebněným textům. Jde zejména o udělování souhlasu k užití děl, výběr a výplaty autorských odměn autorům, dědicům a hudebním nakladatelům*
- *umožňuje legální užívání hudebních děl*
- *existence OSA prospívá i uživatelům - pořadatelům koncertů, provozovatelům klubů, vydavatelům CD aj. Prostřednictvím OSA mohou získat souhlas k provozování často všech hudebních děl. V opačném případě by museli oslovit jednotlivé autory, dědice a hudební nakladatele.*[28]

OSA je také členem mezinárodních organizací, které se zabývají ochranou autorských práv:

CISAC - (*Confédération internationale des sociétés d'auteurs et compositeurs*, Mezinárodní konfederace autorů a skladatelů)

BIEM - (*Bureau international des sociétés gerant les droits d'enregistrement et de reproduction mecanique*, Mezinárodní úřad společností spravující práva k mechanickému zaznamenávání a reprodukcí hudebních děl)

GESAC - (*Groupement européen des sociétés d'auteurs et compositeurs*, Evropské sdružení autorů a skladatelů)[29]

OSA je důležitou spojnicí mezi autory hudebních děl a samotnými uživateli, jakými jsou např. vysílatelé rozhlasu a televize, provozovatelé klubů, pořadatelé koncertů aj.. Prostřednictvím OSA mají přístup k celosvětovému hudebnímu repertoáru, který čítá zhruba jeden milion autorů z celého světa.

5.5.1 Uzavření licenční smlouvy s YouTube

První výročí českého video portálu YouTube přináší dobré zprávy pro autory písní, skladatele i celou komunitu. Z nové licence uzavřené mezi YouTube a OSA budou profitovat všichni a zejména uživatelé si budou moci i nadále vychutnávat své oblíbené hudební klipy.

OSA a YouTube oznámily, že uzavřely nové licenční ujednání, které pokrývá hudbu obsaženou ve videoklipech vysílaných prostřednictvím internetové platformy

[28] Home page, Kdo jsme a co děláme?, [online][citace]Dostupné na WWW: <http://www.osa.cz/> [16. dubna 2010]
[29] Home page, Kdo jsme a co děláme?, [online][citace]Dostupné na WWW: <http://www.osa.cz/> [16. dubna 2010]

YouTube. Licence bude platná zpětně od října 2008, kdy český video portál YouTube odstartoval. Textaři, skladatelé i vydavatelé hudby, kteří jsou zastupováni OSA, budou dostávat z vysílaných videoklipů tantiémy.

Roman Strejček, předseda představenstva OSA, ke smlouvě poznamenal: „Je důležité, aby ti, kdo hudbu vytvářejí, tedy textaři a skladatelé, které naše společnost zastupuje, dostali odměnu za používání svých děl na YouTube. YouTube je velice populární video portál a nová licence přispěje k další podpoře hudebních talentů. Jde o velký úspěch pro textaře a skladatele z celého světa, které OSA zastupuje pro území České republiky, jakož i pro komunitu YouTube jako takovou. ”

Kateřina Holcmanová, marketingová manažerka českého Google, dodává: *„YouTube je v České republice nejnavštěvovanějším videoserverem a v průběhu prvního roku si získal mnoho nových českých uživatelů. Jsme rádi, že společně se sdružením OSA jim i nadále budeme přinášet nový prémiový hudební obsah a zároveň podpoříme české autory i nové hudební talenty.“*[30]

5.5.2 YouTube

YouTube je nejpopulárnější video společenství na světě. Umožňuje milionům lidí objevovat, sledovat a vyměňovat si původní video nahrávky. Slouží jako fórum, díky jehož prostřednictvím spolu lidé po celém světě komunikují a vzájemně se inspirují. Rovněž slouží jako distribuční platforma pro tvůrce původního obsahu a inzerenty všech velikostí.

YouTube dává příležitost mladým, nadějným hudebníkům, kteří zde svými doma natočenými videoklipy mohou oslovit celý svět. Na YouTube se můžeme vzdělávat, poslouchat své oblíbené interprety, shlédnout natočená domácí videa apod.. Každý návštěvník si zde určitě najde oblast, která by ho mohla zaujmout. Tento kanál mohou využít i politici ke komunikaci se svými voliči.

5.5.3 Technologie Content ID

Ochrana autorských práv je důležitou součástí YouTube. Vlastníci obsahu mají k dispozici speciální technologii Content ID, tj. nástroj, který umožňuje majitelům autorských práv snáze najít a identifikovat videa s jejich obsahem nahraná na YouTube.

[30] Tisková zpráva OSA o YouTube, [online] [citace]Dostupné na WWW: <http://www.osa.cz/> [15.dubna2010]

Vlastníci práv se pak mohou rozhodnout, zda budou chtít svá videa zablokovat, nechat volně přístupná nebo je zpeněžit, což je nejčastěji preferovaná volba. [31]

[31] Tisková zpráva OSA o YouTube, [online] Dostupné na WWW: <http://www.osa.cz/> [15.dubna2010]

6. Nové typy protiprávního jednání

S nástupem nových technologií se stále častěji objevují i nové druhy trestné činnosti. Existují některé typy jednání, jejichž klasifikace může být obtížnější.

6.1 Hacking

Pronikáním do systémů zneužitím chyb a slabin v programech, nebo operačních systémech prostřednictvím počítačových sítí je hacking. Hacking je vlastně nejstarším deliktem, který v původním pojetí lze těžko označit za trestný čin, neboť nelze vyčíslit škodu, která byla způsobena. Ostatně, někdy ani správce systému neví, že mu do systému hacker pronikl. Motivací nebylo způsobení škody, ale pouze radost z osobního vítězství nad technikou, spolu se získaným obdivem hackerské komunity. Toto lze definovat jako proniknutí do počítačového nebo řídícího systému jinou cestou než standardní – prolomení bezpečností ochrany. Právně postihovat tento hacking je velmi obtížné. Je možné použít ustanovení § 257a TZ, který hovoří o poškození nebo zneužití záznamu na nosiči informací. Zdá se, že pokud nedojde ke škodě, nikomu není způsobena újma, nebo hacker či třetí osoba nemá z průniku do systému neoprávněný prospěch, pak podstata tohoto trestného činu je nenaplněna.[32]

6.2 Cracking

Překonání ochran k programům, DVD disků a vytváření cracků se nazývá cracking. Cracking je často používaná metoda při průniku do systému, kde cílem crackingu není „zprovoznění“ programu chráněného „softwarovým“ nebo „hardwarovým“ klíčem, ale zjištění informací důležitých pro umožnění neoprávněného přístupu do cílového systému.

Nejčastěji se jedná o tzv. „password cracking“ – zjišťování hesla pro přístup do systému. Pasword cracking má širokou škálu metod od snahy uhodnout heslo pomocí slovníku nejčastěji používaných hesel, použití hrubé síly při zkoušení všech možných kombinací znaků přicházejících v úvahu až po sofistikované algoritmy snažící se o zpětnou rekonstrukci odpovídající kombinace znaků ze zakódovaného řetězce hesla, uloženého v systémovém souboru s hesly.

[32] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 102, ISBN: 978-80-247-1561-2

Trestní klasifikace tohoto typu činnosti může být velmi rozličná, a pokud právnické nebo fyzické osobě, která je vlastníkem systému, vůči němuž je útok crackingem prováděn, nevznikla prokazatelná škoda, může být od stíhání zcela upuštěno. V ostatních případech se obvykle jedná o porušení autorského práva (§152 trestního zákona) nebo poškození či zneužití záznamu na nosiči informací (§ 257a trestního zákona). [33]

6.3 Zneužití internetových stránek

Jeden z nejstarších trestných činů „pomluva“ je v našem trestním zákoně označena § 206. Dostala nový rozměr v souvislosti s rozšiřováním elektronické komunikace. Forma spáchání takového trestného činu je při všeobecné dostupnosti internetu jednoduchá a může spočívat třeba v uvedení telefonního čísla spolu s obscénní fotografií (která samozřejmě nepatří dotčené osobě, nebo je výsledkem fotomontáže). Dalším častým případem je vytvoření internetových stránek, vyjadřující názor jejich autora, ale velmi často doplněný smyšlenými komentáři třetích stran. K takové činnosti většinou láká pocit anonymity na internetu, ale nejedná-li se o promyšlený postup, autor může být snadno vysledován. [34]

6.4 Sniffing

Neoprávněné „odposlouchávání“ komunikace na síti, činnost zdánlivě nevinná, může mít rovněž svoji trestní kvalifikaci. Obvykle je předzvěstí nějaké další ilegální činnosti, např. „zachycování hesel pro chystaný průnik do jiného systému, ale samo o sobě je naplněním trestného činu podle § 239 trestního zákona – porušování tajemství dopravovaných zpráv. Za tento trestný čin může být udělen pachateli trest odnětí svobody na 6 měsíců. Jeden rok hrozí pachateli, který je zaměstnancem provozující telekomunikační služby. Pokud dojde ke zneužití či prozrazení takto získané informace třetí straně, je na řadě § 240 trestního zákona. [35]

[33] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 106, ISBN: 978-80-247-1561-2
[34] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 103, ISBN: 978-80-247-1561-2
[35] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 106, ISBN: 978-80-247-1561-2

6.5 Antispamový zákon

Skoro každý uživatel internetu má neblahé zkušenosti s nevyžádanou poštou, která někdy doslova zaplavuje jeho e-mailovou schránku. Pro nevyžádanou poštu se používá označení spam. Provozovat spaming znamená zaplavovat internet mnoha exempláři jedné a téže zprávy, ve snaze vnutit ji lidem, kteří by jinak takovouto zprávu přijmout vůbec nechtěli. Většina spamů jsou obchodně zaměřené nabídky, často jde o nabídky pochybných produktů, postupů na rychlé zbohatnutí či o nabídky pololegálních služeb. Odesílatele přijde rozeslání takovýchto zpráv velmi lacino, většinu nákladů totiž platí příjemci a poskytovatelé přenosových služeb. Od roku 2004 je v účinnosti zákon č. 480/2004 Sb., o některých službách informační společnosti, neboli také tzv. antispamový zákon, který danou problematiku upravuje. Antispamový zákon se, ale nevztahuje pouze na spam.

Zákon reguluje nevyžádanou elektronickou inzerci a povoluje zasílat obchodní sdělení pouze podle tzv. systému opt-in, tedy pouze s výslovným souhlasem adresáta. Zákon tedy nezakazuje rozesílání spamu obecně, ale pouze rozesílání tzv. nevyžádaných obchodních sdělení.

Nevyžádané obchodní sdělení je kategorie užší než obecná kategorie „spam“, protože spam samozřejmě může zahrnovat i e-maily, které s podnikáním nemají nic společného. Zákon definuje obchodní sdělení jako všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem. Za obchodní sdělení považuje zákon též reklamu. Zákon dále vymezuje pojem obchodní sdělení i negativně, když stanoví, co se za obchodní sdělení nepovažuje. Za obchodní sdělení zákon nepovažuje údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno, nebo adresu elektronické pošty. Jinými slovy, pokud podnikatel např. změnil adresu, nebo telefonní číslo či email a o tomto informuje své klienty, nebo zákazníky prostřednictvím e-mailu, nebude se jednat o obchodní sdělení a k rozeslání takového e-mailu nebude potřebovat souhlas adresátů. Dále zákon stanoví, že zasílání obchodních sdělení (tedy se souhlasem adresáta) ve formě e-mailu je zakázáno, pokud:

- takového sdělení není zřetelně a jasně označeno jako obchodní sdělení;
- skrývá, nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje;

- nebo je zasláno bez platné adresy, na kterou je možno zaslat informaci o tom, že si adresát nepřeje, aby mu byla obchodní sdělení dále zasílána. [36]

6.6 Pokuty a sankce

Orgánem příslušným k výkonu dozoru nad dodržování zákona je Úřad pro ochranu osobních údajů, který může za porušení zákona (tedy za zasílání nevyžádaných obchodních sdělení) stanovit sankci až do výše 10 miliónů Kč. Právnická osoba ovšem nebude za správní delikt odpovídat, pokud prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení povinností dle zákona zabránila. [37]

[36] JUDr. Bohumír Štědroň, LL.M., Ing. Miroslav Ludvík, Ph.D., Právo v informačních technologiích, první vydání 2008, str. 7 ISBN: 978-80-86686-36-3
[37] JUDr. Bohumír Štědroň, LL.M., Ing. Miroslav Ludvík, Ph.D., Právo v informačních technologiích, první vydání 2008, str. 9 ISBN: 978-80-86686-36-3

7. Kybernetické a informační války

Přesně určit kybernetické války můžeme jako činnosti vedené, nebo koordinované státem, jehož hlavním cílem je získat informační převahu. Informační válku, je možno chápat jako boj o informace, který svádějí lidé pracující s informacemi, případně střet, kde hlavní zbraní je právě informace. Většina států dnes intenzivně pracuje na konceptu informační války. Informační válka je boj velmi specifický a ve svém základě personálně a materiálně poměrně nenáročný. Mnohdy se vyzdvihuje její nesouměrná povaha, kdy nezjištěný nebo překvapivý útok, může podkopat obranyschopnost o poznání silnějšího protivníka a způsobit mu škody, které jsou mnohonásobně větší než náklady na jeho provedení.

Kybernetické střety sebou také nesou nový název válečného arzenálu infoware. Pod tímto termínem se rozumí souhrn všech bojových prostředků zaměřených na zničení informační nebo elektronické infrastruktury protivníka a informatických prostředků k vedení elektronického boje. [38]

7.1 Kybernetický warfare

Válka vedená proti nepříteli v kyberprostoru je součástí scénářů vyspělých vojenských systémů a spojuje v sobě kyberterorismus, útok a simulovanou válku. Cílem útoku jsou telekomunikační systémy. Útok je veden prostřednictvím telekomunikačních kanálů, které nahrazují použití fyzických zbraní. Výsledek je závislý především na správném použití získaných informací, proti nepříteli. Mohou jimi být zveřejnění soukromých informací, záměrné uveřejnění klamných informací, napadení webových stránek nepřítele s úmyslem ho zastrašit. Mezi nejdiskutovanější kybernetické zbraně patří logické bomby, které se mohou po dlouhá léta skrývat v počítači, jen aby ho ve vhodný okamžik ochromily.

[38] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, [citace] str. 152 , ISBN: 978-80-247-1561-2

Je možno vysledovat dva základní trendy v této oblasti:

- *Hackerskou válku, vedenou hackerským warfare a vyvolávající náhlá nebo systematická selhání systémů nebo zabránění v jejich provozu.*
- *Sémantický útok, kdy systém pokračuje v provozu a je vnímán jako správně fungující složka, avšak generuje výstupní informaci rozdílnou od reálné. Možnosti takového útoku závisí na předpokladech a charakteru konkrétního systému a velmi často se sémantické útoky používají pro percepční management.*[39]

K základním pravidlům kybernetické války můžeme zařadit následující prvky:

- Hlavním prvkem je, že se útočník snaží vždy schovat v kyberprostoru. Kyberprostor je natolik rozsáhlý, že vyvolává dojem falešné anonymity, ale není to tak. Jakákoli aktivita se odrazí v přenosu dat, a tak se kybernetický útočník musí snažit schovat své aktivity v existujících tocích dat. Změny vyvolané jeho aktivitou nesmí mít snadno detekovatelný charakter.
- *V kyberprostoru vždy existuje entita, která má povolení a možnost provést přesně tu aktivitu, kterou potřebuje útočník k dosažení svého cíle. Jedním ze základních úkolů útočníka je jakýmkoli způsobem převzít práva této entity.*
- *Kyberprostor není teritoriálně omezen, což je vlastnost reálného světa. Některé přední světové analytické společnosti předpokládají, že neustále rostoucí závislost států na internetu, může vyprovokovat závody v kybernetickém zbrojení. Podle jejich odhadů bude brzy úroveň infiltrace internetových technologií do ekonomického, politického a sociálního života lidstva tak vysoká, že se bude muset zařadit do skupiny „kritické infrastruktury". Internetová síť začne hrát dominantní roli v životě každého státu, proto útok, který bude na ní zaměřen, vyvolá úplné ekonomické a politické ochrnutí státu.*[40]

[39] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, [citace] str. 162, ISBN: 978-80-247-1561-2
[40] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, [citace] str. 162, ISBN: 978-80-247-1561-2

7.2 Informační válka

Zbraně použité v informačních válkách, jsou často podobné zbraním, které se používají ke kriminálním aktivitám na internetu. Je však nutné odlišit informační válku od počítačové kriminality. Vést informační válku není náhodným procesem odděleným od jiných dění a předpokládá se koordinovaná činnost mnoha složek, při použití informace, jako zbraně informační války na dvou úrovních – civilní a vojenské. Vojenské síly nemohou ochránit hospodářství před informačními útoky, což není ani jejich úkol. [41]

Výraznou vlastností u informační války je dosah prostředků, které využívá. Především se jedná o možnou schopnost útočníka, zaútočit z libovolného místa na světě (kde existuje připojení k síti), na jakýkoliv vybraný cíl. Prostředky použité k útoku jsou ve srovnání se škodami, které by mohly napáchat, zanedbatelné. A tak potenciální konflikt je výrazně asymetrický. Útočník si vystačí s minimálním vybavením, zatímco k obraně před ním, je potřeba provést plošné ochranné kroky, což jsou nesrovnatelně vyšší náklady než u útočníka. Obrana před informatickým útokem, je i tak problematická. Je totiž velice obtížné útočníkovi zabránit v dalších akcích a situaci ještě stěžuje i fakt, že útočník se nemusí nacházet na území napadeného státu. To velice omezuje běžné obrané prostředky, které by se proti útočníkovi mohly za jiných okolností využít. Rovněž se ztrácí klasické rozdělení cílů, jelikož se všechny možné cíle útoku musí stejně adekvátně bránit. V tomto smyslu mizí i rozdíly mezi civilními a vojenskými cíli, jelikož civilní cíle jsou daleko snadněji napadnutelné, než vojenské.

Mezi nejnebezpečnější charakteristiky informační války, je čím dál tím větší závislost vojenských informačních struktur na civilních. Armádní systémy totiž používají stejný hardware a software, jako je používán v civilním sektoru.

Informační války mají za hlavní cíl, oslabení pozice jiných států, podkopání jejich státních základů a narušení státního zřízení pomocí informačního působení na politickou, diplomatickou, ekonomickou a sociální sféru společenského života prováděním psychologických operací a jiných demoralizujících a rozvracejících aktivit v kyberprostoru.

[41] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 154, ISBN: 978-80-247-1561-2

7.3 Postupy a účinky informačního boje

Infoware slouží především, jako prostředek k ovlivnění virtuálních cílů. Jeho schopnost na ovlivnění virtuálních cílů mimo síť je značně omezená, jelikož na něj může působit pouze nepřímo. A však to neznamená, že by byl infoware v informačním systému nějak neškodný. Společnost totiž používá počítačové systémy k zajištění mnohých bytostně důležitých funkcí. Jednou z takovýchto funkcí, které bývají napadeny prostřednictvím sítě jsou telekomunikace. Ekonomické škody, způsobené rozsáhlejším výpadkem komunikačních sítí, by byly obrovské. Jejich výpadek by totiž ovlivnil i koordinaci hasičů, nebo lékařské pohotovosti. Součástí telekomunikační sítě je i internet, i když k útokům na klíčová zařízení, zejména TLD servery, příliš často nedochází. Podobně mohou být prostřednictvím telekomunikačních připojení zranitelné i informační systémy sloužící k řízení inženýrských sítí, jako jsou elektrárny nebo vodárny.

Cíle, které bývají nejčastěji napadány jsou banky. Jejich informační systémy jsou velmi rozsáhlé a většina z nich dnes umožňuje vzdálený přístup přes Internet. I když banky ve svých marketingových materiálech vždy velice zdůrazňují, jak dbají na bezpečnost, průzkumy ukazují na některé nedostatky. Navíc, banky v obavě ze ztráty klientů často podobné incidenty spíše utají, nebo dokonce přistoupí na podmínky útočníků nebo kybernetických vyděračů. Slabina bankovních systémů spočívá v počtu připojovaných laických klientů na jejich informační systém. Příčina většiny útoků je napadení počítače klienta banky a zneužití jeho přístupových práv. Jiným případem je medializace nějakého nepodstatného bezpečnostního incidentu konkurencí; ta je téměř častější než skutečně podniknutý útok. Zmíněné slabiny představují civilní cíle útoku, které mohou být zasaženy infoware. Takové útoky nazýváme „útoky na infrastrukturu“ a ty nemusí nutně spočívat v jejím narušení, ale např. ve zneužití pro změny důležitých informací, které následně vedou k nesprávným krokům.[42]

[42] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 152, ISBN: 978-80-247-1561-2

8. Internetoví škůdci

Internet obsahuje mnoho škůdců, které se dají shrnout pod společný název „malware“ což pochází z anglického „malicious software“ čili „škodlivý software“. Tito škůdci se na internetu nacházejí většinou proto, aby znepříjemnili život, poškodili počítač, nebo přinejhorším obojí. Útočí na nás viry, trojští koně, červi a spyware. Riziko nákazy malwarem stoupá zejména, když navštěvujeme nezabezpečené stránky. Naštěstí existují specializované programy, které takovým to útokům dokáží předcházet. Řada z těchto programů se dá stáhnout zdarma. Je nesmírně důležité mít v počítači nainstalovánu účinnou a aktuální ochranu proti virům a spywaru.

8.1 Viry

Počítačový virus je škodlivý program nebo programový kód, který se dostane na počítač uživatele bez jeho vědomí. Mezi jeho škodlivé účinky patří změna dat, přemazání pevného disku, vypnutí počítače. Virová nákaza se šíří různě, nejčastěji instalací staženého softwaru, nebo otevřením přílohy e-mailu. Viry jsou mnohdy vytvořeny tak, že se samy zkopírují, a automaticky se šíří z počítače na počítač. Jak ví každý uživatel internetu, počet počítačových virů na internetu dosáhl gigantických rozměrů. Počítačové viry nejsou jen chiméra z novinových zpráv, jsou skutečné a je jich hodně. [43]

8.2 Spyware

Spyware, kterému se někdy říká „data miner“ (čili jakýsi „důl na informace“), je škodlivý software, který sbírá informace o tom, jak se uživatel na internetu chová, co dělá apod.. Monitoruje prováděné úkony, spouštěné programy, e-maily, navštívené webové stránky, ale i přihlašovací jména, hesla a čísla kreditních karet To vše bez vědomí uživatele. Nasbírané informace pak odesílá po Internetu. Spyware běží na pozadí, a může uživatelům kvůli němu zkolabovat počítač. Přinejmenším je to narušení soukromí. Ze své podstaty umí spyware sbírat a přenášet osobní informace – například e-mailové adresy, uživatelská jména, hesla a čísla kreditních karet. I když se spyware často spojuje s adwarem (advertising-supported software - označení pro produkty, které

[43] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 182, ISBN: 978-80-247-1765-4

neustále zobrazují reklamy), počítač se jím může nakazit skoro z každého typu webové stránky, a proto se musí odstraňovat. [44]

8.3 Spamming

Pod pojmem spamming se rozumí hromadné zasílání nevyžádané elektronické pošty obvykle s reklamním obsahem. Tento typ nepříjemného přímého marketingu, který obtěžuje zejména tam, kde doba připojení nebo objem přenesených dat je účtováno, je znám již z dob, kdy se začalo využívat e-mailu. Spammeři získávají elektronické adresy nejrůznějším způsobem, kde nejběžnější zdroj jsou různé www shromáždění, IRC, ICQ, registrační stránky pro služby „zdarma“, ve kterých může být elektronická adresa jednou z přenášených informací. Existuje již řada programů, které spam dokáží odfiltrovat, ale ne nastálo. Spameři tento mechanismus znají a pro jeho obejití často mění adresu odesílatele. [45]

8.4 Dialer

Dialery mají nejen podobně škodlivý dopad jako viry nebo spyware: nejdříve nakazí počítač, a pak i navýší telefonní účty. Dialer je škodlivý program, který, když se na počítač nahraje, začne bez jeho svolení vytáčet různá telefonní čísla. Vytáčí číslo s dražší tarifikací za účelem zpřístupnění placeného obsahu. Podvodné dealery toto činí bez vědomí uživatele. Často také přesměruje uživatele na sajty s pirátským warezem, pornografií, nebo třeba někam úplně jinam. Některé dialery při surfování po internetu přeruší spojení, a pak se znovu připojí, ovšem přes jiné telefonní číslo. Jiné dialery se umí připojit na internet třeba ve chvíli, kdy uživatel není u počítače, ba ani jej nepoužívá. Tohoto parazita dokáže odstranit většina antivirových a antispywarových programů. Nejjistější ochranou je nechat si u operátora zablokovat volání na tzv. žluté linky a volání do zahraničí. [46]

[44] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 183, ISBN: 978-80-247-1765-4
[45] Václav Jirovský, Kybernetická kriminalita, Grada Publishing, a.s., první vydání Praha 2007, str. 104, ISBN: 978-80-247-1561-2
[46] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 185, ISBN: 978-80-247-1765-4

9. Ochrana počítače

9.1 Firewall

Je software k ochraně před útoky a únikem dat. Provádí též kontrolu spouštěných aplikací, blokování nežádoucího obsahu např. reklamy atd.. Existují dva typy firewallu – paketové filtry a aplikační servery. U paketového filtru je každý paket zkontrolován, zda vyhovuje bezpečnostním pravidlům správce sítě. Aplikační server rozhoduje na základě rozboru obsahu (např. přenášených webových stránek). Síť může být chráněna oběma typy firewallů. Síťový firewall bývá umístěn na bránu či směrovač, který připojuje chráněnou podsíť k internetu. Existuje i personální firewall např. AlarmZone), který chrání jeden konkrétní počítač. Navíc umožňuje měnit své chování na základě vzájemného působení dvou nebo více činitelů s uživatelem. [47]

Základním úkolem firewallu je řídit přístup mezi počítačem (nebo počítačovou sítí) a internetem. V podstatě jde o miniaturní bezpečnostní systém, který přiděluje práva k vybranému programu, a omezuje přístupová práva ke všemu ostatnímu. Systém kontroluje veškeré příchozí data dříve, než se setkají s programy, a blokuje nevyžádaná data, aby se nedostala dovnitř. Nikdy není zbytečné nainstalovat si firewall, který bude bránit hackerům, aby se nabourali do počítačové sítě, obzvláště pokud je neustále spuštěné vysokorychlostní připojení k internetu. [48]

Ačkoli placené verze antivirových, antispywarových programů a firewallů se za svou cenu určitě vyplatí, většině uživatelů pravděpodobně vystačí verze bezplatné. Ovšem naprosto neomluvitelné je tyto programy vůbec nemít na svém počítači nainstalované.

9.2 IDS (instrusion detection systém)

IDS (systém detekce napadení) je schopen přesně odhalovat cílené útoky a chránit v reálném čase síť před průniky. IDS by měl odrážet běžný typ útoků, jako je zobrazování portů a současně má zabránit i únikům informací. Využívá databázi známých typů útoků, obdobně jako antiviry používají databázi známých virů. IDS mohou být hostované (viz. HIDS), nebo síťové (viz. NIDS). [49]

[47] Antonín Vitovský, Anglicko – český a česko – anglický výkladový slovník Internetu, první vydání, Praha 2004, str. 97 ISBN: 80-901428-7-7
[48] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 185, ISBN: 978-80-247-1765-4
[49] Antonín Vitovský, Anglicko – český a česko – anglický výkladový slovník Internetu, první vydání, Praha 2004, str. 119 ISBN: 80-901428-7-7

IDS může být určen jako soubor nástrojů, metod a zdrojů, které nám pomáhají identifikovat, zpřístupnit a hlásit neautorizované a neschválené síťové aktivity. Část jména „detekce narušení“ v IDS je poněkud zavádějící, neboť IDS neodhaluje narušení. Zjišťuje takové aktivity v provozu, které mohou, nebo nemusí být narušeními. Detekce narušení je jednou částí celkového ochranného systému, který je instalován na nějakém systému nebo zařízení, není to tedy samostatné ochranné opatření. [50]

9.2.1 Typy IDS

HIDS (host-based intrusion-detection systems), vyžaduje určitý software, který je umístěn na tomto systému a může zobrazovat aktivitu všech uzlových zdrojů. Zapíše jakoukoliv událost do bezpečnostní databáze a prověří, zda se tyto události neshodují se záznamy závadných událostí obsažených ve znalostní databázi. [51]

NIDS (network-based intrusion-detection systems) se obyčejně zařazuje do sítě sériově a rozebírá síťové pakety, z čehož se pak usuzuje zda jde o napadení. Přijímá všechny pakety ve zvláštním úseku sítě, včetně přepínaných sítí, pomocí jedné z metod jako například větvení, nebo zrcadlení portů. Pečlivě rekonstruuje provozní proud, analyzuje v něm přítomnost vzorů závadného chování. Většina systémů NIDS je vybavena schopností zaznamenávat součinnost, hlásit nebo vytvořit výstrahu ve sporných případech.

Základním režimem IDS je, že NIDS nebo HIDS pasivně sbírají data, která předzpracovávají a hodnotí. Na základě statistického rozboru lze stanovit, zda informace spadá mimo rámec normální činnosti, a v případě, že ano, je porovnána s databází znalostí. Je-li nalezena shoda, vytvoří se výstraha.

[50] Carl Endorf, Eugene Shultz, Jim Mellander, Hacking detekce a prevence počítačového útoku, Grada Publishing, a. s., první vydání, Praha 2005, str. 36 ISBN: 80-247-1035-8
[51] Carl Endorf, Eugene Shultz, Jim Mellander, Hacking detekce a prevence počítačového útoku, Grada Publishing, a. s., první vydání, Praha 2005, str. 37 ISBN: 80-247-1035-8

9.3 IPS (Intrusion Prevention Systém)

IPS (systém prevence proti narušení) na rozdíl od IDS jsou určeny pro aktivní ochranu před útoky na Internetu. A to nejen proti známým útokům, ale i proti útokům neznámým. Podle stanovených pravidel sledují odchylky od běžného síťového provozu a vyřazují útok již na samém počátku. Existují dva typy IPS – síťové (NIPS) a hostované (HIPS). Firewall může obsahovat IDS i IPS. Rozdíl mezi těmito třemi systémy lze obecně vyjádřit následovně – firewall je ochranný systém, IDS je detekční systém a IPS je prevenční systém. Jejich trendem je sbíhání do všeobecného bezpečnostního firewalu[52]

9.3.1 Detekce a prevence počítačového útoku

Obecně IPS je umístěn v síti a monitoruje ji. Pokud se odehraje nějaká událost, přijme se opatření dle předepsaných pravidel. Je to jiné než v případě IDS, které se neumisťuje sériově do sítě a je pasivní. Někdo považuje IPS za systém IDS příští generace, protože k detekci dochází v dalším kroku. Avšak jiní, uvažující v širších souvislostech, považují IPS za nástroj v bezpečnostní infrastruktuře, který by mohl pomoci v prevenci proti narušení. IPS se sice vyvinulo z IDS, ale ve skutečnosti jsou to odlišné bezpečnostní produkty lišící se ve funkci a síle. IDS a IPS jsou důležité pro mnoho organizací, od malých kanceláří počínaje, až po velké nadnárodní korporace konče. [53]

9.4 Antispywarové programy

Jako existují speciální programy na odstraňování virů, existuje i jejich obdoba na odstraňování spywaru. Mnoho uživatelů je věrno svým oblíbeným produktům, a mezi ně nepochybně patří jeden z nejoblíbenějších Ad-Aware od firmy Lavasoft. Stojí za to stáhnout si byť jen verzi zdarma. Placená verze v sobě obsahuje i modul Ad-Watch, který běží v pozadí počítače, monitoruje průběžně stav počítače a zabraňuje, aby se na

[52] Antonín Vitovský, Anglicko – český a česko – anglický výkladový slovník Internetu, první vydání, Praha 2004, str. 127 ISBN: 80-901428-7-7
[53] Carl Endorf, Eugene Shultz, Jim Mellander, Hacking detekce a prevence počítačového útoku, Grada Publishing, a. s., první vydání, Praha 2005, str. 39 ISBN: 80-247-1035-8

něj nainstalovaly malwarové programy. Knihovny Ad-Awaru se pravidelně a často aktualizují. [54]

9.5 Antivirové programy

Při vybírání antivirového programu musíme dbát na možnosti a kvalitu nastavení aktivního monitoru, nebo rezidentního šítu, který nepřetržitě kontroluje prováděné operace. Dobře nastavený aktivní monitor odhalí počítačový virus dříve, než si ho zkopírujeme do počítače. Naštěstí existují antivirové programy od firem, jako jsou Symantec, McAfee a Grisoft, které počítač proti takovým hrozbám chrání. Některé firmy nabízejí bezplatné verze svých hlavních produktů. Mezi takové platné pomocníky patří asi jedna z nejznámější u nás – AVG software od firmy Grisoft. Placená verze obsahuje samozřejmě více „vychytávek“, ale i na bezplatné verzi je těžké najít chybičku. Jako u všech podobných programů, musí se i zde dodržovat základní pravidla a to pravidelně testovat počítač, často aktualizovat databáze virů, nepoužívat programy z nedůvěryhodných zdrojů. Každý nově příchozí program musíme před otevřením otestovat antivirovým programem, protože jen tak si na počítači udržíme tak zvanou maximální bezpečnost. Stoprocentní bezpečnost nám, ale nezajistí žádná antivirová ochrana, pokud počítač používáme. Dá se říct, že stoprocentní bezpečnost má pouze ten uživatel, který počítač nepoužívá vůbec. Mezi nejdůležitější bezpečnostní pravidla patří používání originálního softwaru**.** [55]

Základním bezpečnostním pravidlem při práci s počítačem je zálohování! Při zálohování je nutné si uvědomit, že diskety mají také jen omezenou životnost. Proto je nejlepší zálohovat si data na více médiích.

[54] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 183, ISBN: 978-80-247-1765-4
[55] Paul Craig, Ron Honick, Mark Burnett (technický redaktor), Softwarové pirátství bez záhad, Grada Publishing, a. s., první vydání, Praha 2008, str. 182, ISBN: 978-80-247-1765-4

10. Míra pirátství v České republice a ve světě

Softwarové pirátství na osobních počítačích v České republice je na ústupu. Mezi roky 2007 a 2008 softwarové pirátství pokleslo o jedno procento. V roce 2008 se v ČR užívalo nelegálně pouze 38 procent softwaru. Ztráty českého softwarového odvětví v důsledku pirátství v roce 2008 stouply o 4 procenta na 3,3 miliardy korun (168 mil. USD). V roce 2007 míra softwarového pirátství naopak stagnovala a držela se dva roky za sebou na 39 procentech. Výsledky dokazují vliv BSA na potlačování softwarového pirátství v České republice. V této ekonomicky krizové době je důležité, aby se firmy bránily proti šíření nelegálního softwaru. Pirátství pro firmy může mít zničující důsledky, ale rovněž jím trpí i tuzemská ekonomika. Pokles pirátství je důsledek odvedené dobré práce policie a protipirátských kampaní BSA, které se zaměřují zejména na firmy. Zatímco firmy se dlouhodobě snaží pirátství potírat, domácí uživatelé rizika plynoucí z užívání nelegálního softwaru stále podceňují a hojně pirátský software užívají. V důsledku toho tuzemská míra pirátství v posledních letech klesá pomaleji.[56]

10.1 Celosvětová bilance pirátství

*Z*e 110 sledovaných zemí zahrnutých do studie v 57 zemích kleslo softwarové pirátství, beze změny zůstalo v 36 zemích a v 16 zemích pirátství vzrostlo.

Celosvětový trh s počítači rostl nejrychleji v zemích s vysokou mírou pirátství, proto v roce 2008 vzrostla celosvětová míra pirátství o tři procenta, tedy na 41 procent.

V rámci Evropské unie byla nejvyšší míra pirátství zaznamenána v **Bulharsku** (68 %), **Rumunsku** (66 %), **Řecku** (57 %), **Polsku** (56 %), **Slovensku** (43 %). Naopak Rakousko s (24 %) a Německo s (27 %) patří mezi země s nejnižší mírou pirátství. Belgie, Dánsko a Švédsko dosáhly (25 %).

Nejméně pirátského softwaru je zaznamenáno ve **Spojených státech** (20 %), v **Japonsku** (21 %), **Lucembursku** (21 %) a na **Novém Zélandu** (22 %).

Největšího meziročního poklesu pirátství z celosvětového pohledu dosáhlo **Rusko**, kde míra pirátství klesla o 5 procentních bodů na 68 %. V průběhu šesti let tak míra pirátství v Rusku klesla o 19 procentních bodů.

[56] Jan Hlaváč, Softwarové pirátství kleslo: v česku se užívá 38% softwaru nelegálně, tisková zpráva BSA. [online] Dostupná z WWW: < http://global.bsa.org/globalpiracy2008/pr/pr_czechrep.pdf> [15.dubna 2010]

Rozšiřování přístupu k internetu zvýší dostupnost pirátského softwaru. Růst bude nejpatrnější mezi domácími spotřebiteli a malými firmami – v jejich případě je míra pirátství vyšší než u větších firem a státních organizací. [57]

Míra pirátství v jednotlivých státech Evropské unie

Pořadí	Země	2007	2008	Rozdíl
1.	Lucembursko	21%	21%	0%
2.	Rakousko	25%	24%	-1%
3.	Belgie	25%	25%	0%
4.	Dánsko	25%	25%	0%
5.	Švédsko	25%	25%	0%
6.	Finsko	25%	26%	1%
7.	Německo	27%	27%	0%
8.	Velká Británie	26%	27%	1%
9.	Nizozemsko	28%	28%	0%
10.	Irsko	34%	34%	0%
11.	**Česká republika**	**39%**	**38%**	**-1%**
12.	Francie	42%	41%	-1%
13.	Maďarsko	42%	42%	0%
14.	Portugalsko	43%	42%	-1%
15.	Španělsko	43%	42%	-1%
16.	**Slovensko**	**45%**	**43%**	**-2%**
17.	Malta	46%	45%	-1%
18.	Slovinsko	48%	47%	-1%
19.	Itálie	49%	48%	-1%
20.	Estonsko	51%	50%	-1%

Tab. 1. [58]

V České republice se podařilo snížit míru pirátství o 28 procent. Při **srovnání s dalšími členskými státy EU je Česko na jedenáctém místě.** Celosvětově je ČR na 22. místě.

[57] Jan Hlaváč, Softwarové pirátství kleslo: v česku se užívá 38% softwaru nelegálně, [online] tisková zpráva BSA. Dostupná z WWW: <http://global.bsa.org/globalpiracy2008/pr/pr_czechrep.pdf> [15.dubna 2010]

[58] Miloslav Fišer, Microsoft bojuje, proti nelegálnímu softwaru, pomáhá mu soud i policie. [online] [citace]Dostupné na WWW: <http://www.novinky.cz/> [14. března 2010]

Tyto závěry vycházejí z Celosvětové studie softwarového pirátství, kterou zveřejnila protipirátská mezinárodní organizace BSA hájící zájmy softwarového odvětví po celém světě. Studie byla provedena nezávisle na BSA respektovanou analytickou společností IDC, zaměřující se na průzkumy a analýzy v oblasti informačních technologií.

10.2 Nejznámější kauzy týkající se pirátství

Uvedu zde nejznámější případy porušení autorských práv, které se dostali až k soudu. Jeden z novějších případů, je kauza týkající se švédského serveru The Pirate Bay, jehož čtveřice zakladatelů si od soudu vyslechla rozsudek, jednoho roku vězení a zaplacení odškodného ve výši 30miliónů švédských korun firmám, které poškodily.

The Pirate Bay je jedním z nejznámějších serverů svého druhu. Denně pomocí něho uživatelé stahují milióny nelegálních dat. Portál v roce 2003 zřídila organizace Piratbyran, v posledních pěti letech ho však provozovali jednotlivci. Samotný server přitom neobsahuje žádná data s ochrannými právy, místo toho odkazuje na jiné servery pro sdílení dat. [59]

Tím že odsoudily zakladatele serveru The Pirate Bay, stejně úřady nedosáhli svého. Tento portál se totiž od doby svého vzniku rozšířil po celém světě. Tyto servery fungují nezávisle na sobě, tudíž zavřením jednoho (švédského) serveru nic nezmění. Jak řekl Magnus Ericsson z organizace Piratbyran "*Stahování zdarma vytváří o hudbu mnohem větší zájem a protože umělci mají mnoho jiných cest k tomu, jak vydělávat peníze, tato cesta jim spíš pomáhá, než škodí.*" [60]

Podobné případy jsou i u nás v České republice například, kdy trojice mladíků v prostorách Akademie věd provozovali počítačový server na sdílení nelegálních kopií filmů, hudby, softwaru a počítačových her. Škoda, kterou tímto sdílením způsobili měla přesahovat částku 37 miliónů korun českých, proto poškozené firmy žádali maximální tresty, aby tato trojice mladíků sloužila, jako exemplární odstrašující příklad, pro všechny piráty v České republice. Trojici mladíků byli prvním soudem uděleny tresty odnětí svobody po dobu jednoho roku s podmíněným odkladem na dva roky. Protože ale s rozsudkem nesouhlasili, zabýval se kauzou pražský soud. Druhý rozsudek zprostil

[59] Tomáš Reiner, Miloslav Fišer, Zakladatelé pirátského serveru Piráte Bay půjdou na rok do vězení, [online] článek ze dne 17. dubna 2009. Dostupné na WWW: <http://www.novinky.cz/> [13. dubna 2010]
[60] Tomáš Reiner, Miloslav Fišer, Zakladatelé pirátského serveru Piráte Bay půjdou na rok do vězení, [online] [citace]článek ze dne 17. dubna 2009. Dostupné na WWW: <http://www.novinky.cz/> [13. dubna 2010]

všechny tři mladíky obžaloby. Rozsudek zatím nenabyl právní moci, jelikož si státní zástupce ponechal lhůtu na odvolání.[61]

Justice se snaží proti pirátství bojovat všemi svými dostupnými prostředky, avšak ne vždy podle mého názoru správnými. Je dobré udržovat a chránit nějaká pravidla, aby nevznikl chaos, ale ne za každých okolností. Například, jak tomu bylo v americkém státě Minnesota, kde soud shledal vinnou 32letou Jammie Thomasovou-Rassetovou, že si z internetu ilegálně stáhla 24 hudebních titulů, které si z jejího počítače mohli stáhnout další lidé, neboť byla napojena na P2P síť Kazaa. Měla na základě porušení autorských práv zaplatit pokutu 1,92 miliónů dolarů, přitom cena jedné stáhnuté písničky činí pouhých 99 centů. Podle nového soudního rozhodnutí má žena zaplatit 54 tisíc dolarů. Výši původní pokuty soud označil za „monstrózní". I tak je to, pro obyčejnou ženu se čtyřmi dětmi nezaplatitelné. [62]

Nemyslím si, že piráti ať úmyslně či neúmyslně poškozují společnosti, tím že jejichž výrobek dále šíří. Klasický spotřebitel si totiž raději stáhne pirátskou kopii, než aby investoval většinou nepřiměřeně vysokou finanční částku. Tímto skutkem nikoho neohrožuje na životě a ani tím nikoho nechce vědomě finančně poškodit. Většinou si chce být jist, že nekupuje tzv. „zajíce v pytli". Ať se jedná o software, film, hudbu či hru, nic z toho není hmotného charakteru. Nedá se osahat, nevidí se do něj, neví se, zda to je přesně to pravé co zrovna ten dotyčný potřebuje. Proto si jej většinou stáhne a vyzkouší. Pokud mu to vyhovuje, tak si software, hru nebo album zakoupí. Pokud mu produkt nevyhovuje, jednoduše ho smaže a je rád, že do toho bezhlavě neinvestoval. Takto to vidí většina spotřebitelů, kteří stahují nelegálně pirátské kopie, ať už z P2P sítí, nebo z warezu. Dalo by se tedy říci, že obyčejný spotřebitel se nechová, jako zloděj, ale chce si být jistý tím, co kupuje. Proto nevidím důvod k tomu, proč by tito spotřebitelé měli být trestáni nesmyslně vysokými pokutami.

Myslím, že jediná schůdná cesta proti nelegálnímu kopírování, nebo jeho zmírnění je plné využití zákonu trhu a aby vydavatelé nabídli uživatelům natolik cenově výhodné produkty, aby se již nelegální kopírování nevyplácelo.

[61] Miloslav Fišer, Kauza počítačových pirátů z Akademie věd nekončí, žalobce se odvolal, [online] článek ze dne 14. srpna 2009. Dostupné na WWW: <http://www.novinky.cz/> [14. dubna 2010]
[62] mif, Soud snížil ženě monstrózní pokutu za stažení 24 písniček z internetu, [online] článek ze dne 26. ledna 2010. Dostupné na WWW: <http://www.novinky.cz/> [26.ledna 2010]

11. Závěr

Cílem této práce má být přiblížení světa pirátství a lidí, kteří se v něm nacházejí. Osvětlení toho, kdo to vlastně je softwaroví pirát a co ho vede k pirátství. Internet je plný nástrah, které běžný uživatel využívá a mnohdy si ani neuvědomí, že jedná protiprávně. Tato problematika, totiž čím dál více zasahuje do běžných životů obyčejných lidí.

S rozvojem počítačové techniky a možností jejího využití se vynořují nové výzvy jak pro softwarové společnosti počítačové piráty, tak i pro zákonodárce a orgány činné v trestním řízení. Ti jsou nuceni neustále zdokonalovat prostředky pro potírání tohoto druhu kriminality. Avšak je to boj, který se nedá vyhrát. Internet se stal samostatným světem, ve kterém není možné tento druh kriminality vymítit. Je to nikdy nekončící bitva, ve které se někdy ocitnou i neviní lidé, kteří bývají často nepřiměřeně potrestáni za věci, které mnohdy neúmyslně spáchaly. Proto by právo mělo být více shovívavé, pro tyto případy a trestat přísněji spíše ty, kteří vědomě páchají trestné skutky za účelem svého obohacení.

Dá se říci že počítačová kriminalita je stále ještě na samém počátku vzniku a ani odborníci se neshodnou ve svých názorech, jak tyto skutky posuzovat. Jak již jsem výše uvedl nechci hájit počítačové piráty, ale pouze obyčejné uživatele. Proto by se zde nemělo uplatňovat pravidlo, že „neznalost zákona neomlouvá“ a vynášet rozsudky z nepřiměřenými tresty.

12. Seznam použité literatury

A. Vitovský, *Anglicko – český a česko – anglický výkladový slovník Internetu*, datum vydání: Praha 2004, ISBN: 80-901428-7-7

A. Harper, S. Harris, Ch. Eagle, J. Ness, M. Lester, *Hacking – manuál hackera*, datum vydání: 28.01.2008, GRADA Publishing, ISBN: 978-80-247-1346-5

JUDr. B. Štědroň, LL.M., Ing. M. Ludvík, Ph.D., *Právo v informačních technologiích*, datum vydání: Praha 2008, Computer Media s. r. o., ISBN: 978-80-86686-36-3

C. Endorf, E. Schultz, J. Mellander, *Hacking – detekce a prevence počítačového útoku*, datum vydání: 02.09.2005, GRADA Publishing, ISBN: 80-247-1035-8

D. Naik, *Internet standardy a protokoly*, datum vydání: Praha 1999, Computer Press, ISBN 80-7226-146-0

J. Čermák, *Internet a autorské právo*, datum vydání: Praha 2003, Linde Praha, a.s., ISBN: 80-7201-423-4

M. Adámek, *Spam jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu*, datum vydání: Praha 2009, GRADA Publishing, ISBN: 978-80-247-2638-0

Ing. M. Ludvík, Ph.D., JUDr. B. Štědroň. LL.M., *Teorie bezpečnosti počítačových sítí*, datum vydání: Praha 2008, Computer Media s. r. o., ISBN: 978-80-86686-35-6

M. Michal, *Počítačová kriminalita*, datum vydání: Praha 2002, Computer Press, ISBN: 80-7226-419-2

J. Scrambray, S. McClure, G. Kurtz, *Hacking bez tajemství*, datum vydání: Praha 2002, Computer Press, ISBN: 80-7226-644-6

P. Craig, R. Honick, M. Burnett, *Softwarové pirátství bez záhad*, datum vydání: Praha 2008, GRADA Publishing, ISBN: 978-80-247-1765-4

P. Svoboda, *Vliv autorskoprávní teritoriality na vývoj evropského práva*, datum vydání: Praha 2001, Karolinum ISBN 80-246-0352-7

S. McClure, J. Scambray, G. Kurtz, *Hacking bez záhad*, datum vydání: 16.02.2007, GRADA Publishing, ISBN: 978-80-247-1502-5

V. Jirkovský, *Kybernetická kriminalita*, datum vydání: 27.11.2007, GRADA Publishing, ISBN: 978-80-247-1561-2

V. Smejkal, *Internet a §§§*, datum vydání: Praha 2001, GRADA Publishing, ISBN: 80-7169-765-6

Elektronické zdroje

Copyright infringement of software, [online] [10.ledna 2010] Dostupné z WWW: http://en.wikipedia.org/wiki/Software_piracy

Home page, *Kdo jsme a co děláme?*, [online] [16. dubna 2010] Dostupné na WWW: <http://www.osa.cz/>

Jan Hlaváč, *Softwarové pirátství kleslo: v česku se užívá 38% softwaru nelegálně*, [online] tisková zpráva BSA. [15.dubna 2010] Dostupná z WWW: <http://global.bsa.org/globalpiracy2008/pr/pr_czechrep.pdf>

Miloslav Fišer, *Kauza počítačových pirátů z Akademie věd nekončí, žalobce se odvolal*, [online] článek ze dne 14. srpna 2009. [14. dubna 2010] Dostupné na WWW: <http://www.novinky.cz/>

Miloslav Fišer, *Microsoft bojuje, proti nelegálnímu softwaru, pomáhá mu soud i policie*. [online] [14. března 2010] Dostupné na WWW: <http://www.novinky.cz/>

mif, *Soud snížil ženě monstrózní pokutu za stažení 24 písniček z internetu*, [online] článek ze dne 26. ledna 2010. [26.ledna 2010] Dostupné na WWW: <http://www.novinky.cz/>

Tomáš Reiner, Miloslav Fišer, *Zakladatelé pirátského serveru Piráte Bay půjdou na rok do vězení*, [online] článek ze dne 17. dubna 2009. [13. dubna 2010] Dostupné na WWW: <http://www.novinky.cz/>

Tisková zpráva OSA o YouTube, [online] [15.dubna 2010] Dostupné na WWW: <http://www.osa.cz/>

Robert Šustr, *Napster P2P*, [online] Dostupné z [10.dubna 2010] WWW: <http://p2p.chytrak.cz/>

Použité právní předpisy

Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů
Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů,
Zákon č. 586/1992 Sb. o daních z příjmů, ve znění pozdějších předpisů
Zákon č. 121/2000 Sb., autorský zákon, ve znění pozdějších přepisů