MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC

Ústav informatiky

Miroslav Hanák

# Softwarové pirátství v České republice

Software piracy in the Czech Republic

Bakalářská práce

Vedoucí práce: Dr. Jiří Dostál, Ph.D.

Olomouc 2010

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a použil jen uvedené informační zdroje.

Olomouc 27. 10. 2010 ……

Na tomto místě bych rád poděkoval panu Dr. Jiřímu Dostálovi, Ph.D. za příkladné a odpovědné vedení mé bakalářské práce a za poskytnutí odborných rad. Rovněž bych chtěl také poděkovat panu Mgr. Janu Lavrinčíkovi, DiS za jeho cenné rady, které jsem také použil ve své bakalářské práci.

Miroslav Hanák

**Obsah**

# Úvod

Inspirací k napsání této bakalářské práci mi byl článek na internetu. Zde jsem se setkal s informací, že v roce 2010 je 37 procent softwaru nainstalovaného na počítačích v České republice nelegálně. Chtěl jsem o problematice softwarového pirátství vědět více, a tak jsem se rozhodl seznámit se s problematikou pirátství blíže, přičemž při své práci jsem se zaměřil jak na softwarové piráty a jejich práci a organizaci ve skupinách, tak na běžné uživatele, protože vím, že softwarové pirátství není jen o pirátech, ale i o lidech, kteří si softwarové produkty stahují například z internetu. Při získávání informací jsem využíval odborné knižní publikace a také internetové zdroje. Díky těmto získaným informacím jsem získal přehled o problematice, o které pojednává má bakalářská práce. Ta je rozdělena do pěti částí. V první části se zaměřují na historii a vývoj počítačové kriminality, na začátky softwarového pirátství, je zde také vysvětleno, přes jaké technologie se šíří pirátský software, a v neposlední řadě se zde zmiňuji o warez skupinách, o jejich práci, organizovanosti a motivaci. Ve druhé části se naopak zaměřuji na samotné uživatele, protože i oni mají své důvody k tomu, proč stahují software nelegálně. Dále vysvětluji pojem software, jeho rozdělení a také ve své práci přiblížím základní typy ochran a v neposlední řadě se také budu věnovat licenčním smlouvám. Jeden z cílů mé bakalářské práce je poukázat na to, že softwarové pirátství má vliv na ekonomiku v České republice. Na tento fakt poukazuji díky analýzám, které každoročně zveřejňuje proti pirátská organizace BSA za pomoci analytické společnosti IDC.

Popisuji zde i další věci, například co hrozí firmám za užívání pirátského softwaru a také zde uvádím, díky čemu se těmto nepříjemnostem vyvarovat, nabízím zde také srovnání analýz v roce 2008 a 2009 s tím, že shrnuji klíčové poznatky těchto analýz. Třetí část mé bakalářské práce je, co se týče rozsahu, ta nejobsáhlejší. Ve čtvrté části popisuji, jakých trestných činů se dopouští ten, který se dopouští softwarového pirátství, přičemž vycházím z trestního a autorského zákona. V samotném závěru své bakalářské práce navrhuji řešení, jak snížit softwarové pirátství. Také jsem vytvořil příručku pro vývojáře a manažery, ve které radím manažerům, co by měli udělat, aby snížili nebo v lepším případě zamezili výskytu pirátských programů ve svých firmách. V neposlední řadě jsem provedl průzkum, ve kterém se ptám občanů města Přerova na to, zda jsou tresty za softwarové pirátství podle nich adekvátní, zda se softwarovým pirátstvím již setkali nebo také zda je podle nic pirátství omluvitelné.

Důkazem toho, že se v naší zemi softwarové pirátství ve firmách, ale i v domácnostech řeší, je i tento případ[1], ve kterém se uvádí, že policie České republiky provedla prohlídku v menší společnosti, ve které se zjistilo užívání nelegálního softwaru. Majitelům společnosti bylo následně sděleno obvinění z porušování autorských práv. Je zde nutno připomenout, že případné finanční postihy ze strany poškozených výrobců softwaru mohou zcela ohrozit existenci malé firmy. V České republice se však dějí zátahy i na běžné uživatele. Důkazem toho je i tento článek[2], ve kterém se píše, že bylo při domovních prohlídkách zabaveno čtrnáct počítačů a obviněno čtrnáct běžných uživatelů. Stalo se tak v roce 2007 a zátah byl největší svého druhu. Záměrně zde uvádím jeden příklad za firmu a jeden za běžného uživatele, aby bylo jasně vidět, že si nikdo nemůže být jistý tím, že na něj nepřijde policejní kontrola. Dalším cílem této práce je také ukázat, že softwarové pirátství se dá také řešit, tak jako každý problém, i zde lze nalézt řešení, které sice softwarové pirátství zcela nezastaví, ale myslím si, že bude mít za výsledek snížení tohoto druhu pirátství v České republice. V praxi by se mohla využít řešení, která v této bakalářské práci navrhuji.

[1] Dostupnost na World Wide Web: http://www.legalne.cz/nightmare/ 1.6. 2010

[2] Dostupnost na World Wide Web: http://www.lupa.cz/clanky/v-cr-probiha-rozsahly-zatah-proti-uzivatelum-p2p-siti/ 1.6.2010

# 1 Softwarové pirátství

V souvislosti s vývojem počítačových technologií nastal i vývoj počítačové kriminality a tím i softwarového pirátství. Zde bych chtěl podotknout, že k rozmachu počítačové kriminality došlo na počátku 80. let 20. století, tedy v době, kdy se počítače masivně rozšiřovaly mezi jednotlivé uživatele.

Definice tohoto pojmu není zcela jednoznačná, ale například v publikaci Vladimíra Smejkala[3] se uvádí, že jde o útoky proti autorskému právu související s počítačovými programy k získání prospěchu pro sebe nebo jiného. Samozřejmě kromě knižních publikací můžeme nalézt definice i na internetových stránkách[4], které se zabývají softwarovým pirátstvím, kde je napsáno, že jde i o útoky na právo autora. U těchto zdrojů je však ta nevýhoda, že u nich není uvedený autor.

## 1.1 Nejčastější případy počítačového pirátství

Mezi nejčastější[5] případy počítačového pirátství se řadí[6]:

**a) Používání nelicencované kopie počítačového programu –** použití softwarového programu bez zakoupení platné licence. Toto jednání je časté mezi koncovými uživateli, jako jsou například fyzické osoby nebo malé firmy. Podle zjištění analytické studie IDC[7] z roku 2008 si řada těchto malých firem není vědoma toho, že by ve své firmě používala nelegální software.

**b) Pronájem a půjčovaní software bez souhlasu autora** – „Pronájmem originálu nebo rozmnoženiny díla se rozumí zpřístupňování díla ve hmotné podobě za účelem

[3] Srov. SMEJKAL, V., *Právo informačních a telekomunikačních systémů.* Praha : C. H. Beck, 2004.

[4] Dostupnost na World Wide Web: http://www.dolphin.cz/policie/brezen98/piratisoftwaru.html, 1.6.2010

[5] Srov. SUCHA, P., *Preverovanie a vyšetrovanie počítačovej kriminality*. In Zborník referatov "Medzinárodna konferencia Počítačová kriminalita", Bratislava : Bussines Software Aliance SR, 2000, str. 36

[6] Srov. FEDEROVIČOVÁ, I., *Kriminalistická stopa a softvérové pirátstvo*. In Zborník referatov "Medzinárodna konferencia Počítačová kriminalita", Bratislava : Bussines Software Aliance SR, 2000, str. 40

[7] Dostupnost na World Wide Web: www..idc.com, 1.6.2010

přímého nebo nepřímého hospodářského nebo obchodního prospěchu poskytnutím originálu nebo rozmnoženiny díla na dobu určitou."[8]

„Půjčováním originálu nebo rozmnoženiny díla se rozumí zpřístupňování díla ve hmotné podobě zařízením přístupným veřejnosti nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu poskytnutím originálu nebo rozmnoženiny díla na dobu určitou."[9]

**c) Internetové pirátství –** pod tímto pojmem se rozumí stahování softwaru z internetu bez platné licence a souhlasu držitele autorských práv.

**d) Falešné kanály –** situace, při které je software distribuován jako speciální zlevněná licence (například zákazníkům nakupujícím ve velkém). Problém však nastává tehdy, je- li tento software redistribuován dalším uživatelům, kteří tyto licence nevlastní.

## 1.2 Historie počítačové kriminality

Než se začnu věnovat této kapitole, chtěl bych zde podotknout, že různé zdroje si zavádějí svou vlastní etapizaci vývoje, neboť u počítačové kriminality můžeme pozorovat určitá vývojová stádia, která odpovídají právě souvisejícímu vývoji počítačové technologie. Je zde třeba zmínit, že v některých publikacích rozdělení na etapy chybí, jako je tomu například v knize od Paula Craiga[10]. Osobně se přikláním k rozdělení, které ve své publikaci popisuje Michal Matějka[11].

Podle tohoto autora lze počítačovou kriminalitu rozdělit do tří etap:

- pravěk, což je období do uvedení prvního počítače na trh v roce 1981
- středověk, tak nazýváme období od roku 1981 – 1994,
- novověk je období od roku 1994 – dodnes.

---

[8] § 15 AutZ

[9] § 16 AutZ

[10] CRAIG, P., *Softwarové pirátství bez záhad. 1. vyd.* Praha: Grada Publishing, 2008

[11] MAŤEJKA, M., *Počítačová kriminalita*. Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 17

## 1.3 Počítačový pravěk

Nabízí se zde otázka, jestli v tomto období můžeme mluvit o počítačové kriminalitě, jelikož se stále pohybujeme v době, kdy výpočetní technika nebyla mezi uživateli vůbec rozšířena. Avšak i v tomto období docházelo k jednání, ve kterém lze náznaky „počítačové kriminality“ vysledovat.

Jak se v publikaci[12] uvádí, za první „počítačový zločin“ je považován případ, který se udál ve Francii v roce 1801, je to tedy skoro 150 let před vznikem prvního skutečného počítače. Tehdy jistý Joseph Marie Jacquard sestrojil zařízení, které dovolovalo automatizovat a opakovaně provádět jednotlivé úkony používané při tkaní speciálních látek. Problém byl ovšem ten, že zaměstnanci pana Jacquarda jeho „vynález“ nepřijali, protože se báli, že by mohli přijít o své zaměstnání. Ze strany zaměstnanců pak přišla série sabotáží a tyto sabotáže zapříčinily, že Jacquard od dalšího vývoje upustil. O zrodu počítačového věku lze mluvit od data 14. února 1946, neboť na pensylvánské univerzitě byl sestrojen první elektronkový počítač, který je znám jako ENIAC[13]. Avšak v té době počítače zabíraly skoro celou místnost a vzhledem k tomu, že byly velice drahé, staly se doménou hlavně pro velké firmy. V souvislosti s touto skutečností není podstatné mluvit o možnostech jejich kriminálního využití.

Chtěl bych se však zmínit o dvou výrazných momentech, které se v tomto období staly. Pro programátory byla tehdejší doba taková, že byli nuceni při práci se sálovými počítači pracovat s nepříliš fungujícími programy, to je vedlo k tomu, že si tyto programy sami upravovali. Zásahy do programu za účelem lepší funkčnosti se označovaly termínem „hack“ a tak i programátoři, kteří upravovali programy z toho důvodu, aby lépe fungovaly, byli označováni jako hackeři.

Druhým momentem je případ, který je znám jako Cup n Crunch[14] [15]. Tento moment dostal pojmenování podle značky cereálií, které se vyznačovaly tím, že kromě samotných cereálií do nich výrobce přidával píšťalku.

---

[12] Dostupnost z World Wide Web: www.making-a-difference.oorg/computer-crime-chronicles.html. 1.6.2010

[13] Dostupnost z ftp.arl.mil/mike/comphist/eniac-story.html. 1.6.2010

[14] Matějka, M., *Počítačová kriminalita.* Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 21

Pan Draper si všiml, že tato píšťalka vydává zvuk o frekvenci 2600Hz a tato zvuková frekvence je používána telefonní společností, která má název AT&T a používá tento signál k vnitřní signalizaci v síti a která ve spojení se zařízením nazvaným Bluebox mu dovolí uskutečňovat hovory zdarma. Díky tomuto se velmi rozmohl phone phreaking[16].

I u nás se z této doby najdou případy, které řeší počítačovou kriminalitu. Vůbec prvním takovým je případ, který se odehrál v sedmdesátých letech, kdy nespokojený zaměstnanec, který pracoval v úřadu důchodového zabezpečení, poškozoval magnetem záznamy na magnetických páskách.

## 1.4 Počítačový středověk

Po počítačovém pravěku přichází počítačový novověk a začala se psát zcela nová kapitola počítačového věku, jelikož byl na trh uveden první počítač typu IBM, a to přesně dne 12. 8. 1981. Velice brzy se pak počítač rozšířil mezi běžné uživatele, objevuje se zde i systém BBS[17]. V této době se také objevují lidé, pro které je vlastnictví počítače vším a s jeho pomocí si zdokonalují své dovednosti.

## 1.5 Počítačový novověk

Počítačové pirátství v době „středověku“ zažilo svůj vzestup, avšak v době „novověku“ je dovedeno k dokonalosti. V této době byl vymyšlen zcela nový přístup ke sdílení dat.

---

[15] Dostupné z World Wide Web: http://www.webcrunchers.com/crunch 1.6.2010

[16] Phone phreaking je nabourání se do telefonní sítě pomocí počítače tak, že je možné provozovat dálkové telefonní hovory zdarma. Nyní se phone phreaking začíná vracet díky internetu, a cílem je pak ne ani tak hovor, jako spíše připojení k internetu zdarma.

[17] Bulletin Board System jsou systémem elektronických nástěnek, které jsou rozděleny podle témat, do kterých mohou uživatelé přispívat.

Tento nový způsob spočíval v tom, že se data mohla sdílet pomocí peer-to-peer[18], tedy rovný s rovným. Pomocí těchto technologií, jako je například síť Bittorrent,[19] se můžeme připojit ke konkrétnímu uživateli, který sdílí daný obsah. V současné době jsou tyto sítě velice populární díky své jednoduchosti, avšak někteří uživatelé si neuvědomují možná rizika s nimi spojená.

## 1.6 P2P sítě

Úloha těchto sítí během posledních deseti let vzrostla, a to především díky velkému pokroku v oblasti informačních technologií. Člověk díky internetu dnes nejenže data přijímá, ale také vytváří a myslím si, že je to právě velký pokrok ve světě informačních technologií, který umožnil vzestup počítačového pirátství. Díky možnostem, které v současné době máme, lze různými způsoby sdílet data s ostatními uživateli. Dnes lze poměrně jednoduše poskytnout neurčenému množství uživatelů dílo, které je chráněno autorským zákonem. Bohužel vše má své pro a proti, neboť právě díky těmto technologiím mají velké starosti majitelé autorských práv.

Uživatelé internetu, kteří stahují a poskytují data ostatním uživatelům, se ve většině případů nemusejí obávat, že budou odhaleni, na druhou stranu i v České republice lze nalézt případy, kdy se provádí policejní razie proti uživatelům, kteří sdílejí data chráněná autorským zákonem[20]. První velký zátah na piráty v České republice se odehrál v roce 2006[21] v Kadani a Klášterci nad Ohří, kdy policisté provedli domovní prohlídky a zabavili čtrnáct počítačů, z jejichž pevných disků bylo sdíleno velké množství dat prostřednictvím P2P sítí.

---

[18] peer-to-peer - Znamená jakoukoliv síť, kde probíhá nějaká symetrická komunikace či interakce mezi počítači (každý z nich umí iniciovat či naopak na základě vnější iniciace/požadavku vykonat potřebné transakce a operace).

[19] BitTorrent je v informatice nástroj pro peer-to-peer (P2P) distribuci souborů, díky čemuž jsou datové přenosy rozkládány mezi všechny klienty, kteří si data stahují.

[20] Autorský zákon je zkrácený název zákona číslo 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů

[21] Dostupné na World Wide Web: http://www.lupa.cz/clanky/v-cr-probiha-rozsahly-zatah-proti-uzivatelum-p2p-siti/ 1.6.2010

Zátah samotný překvapil řadu odborníků i osoby, které byly z trestného činu obviněny. V roce 2008[22] se razie opakovala v těchto městech znovu. I když policejní razie u domácích uživatelů, kteří používají výměnné sítě pro sdílení souborů, nejsou tak časté, ani oni si nemohou být jisti, že se u nich neobjeví policie, která bude mít příkaz k domovní prohlídce a obviní dotyčného z porušování autorských práv, zvláště pokud tento uživatel bude sdílet velké množství dat, která jsou chráněna autorským zákonem, například prostřednictvím výměnných sítí. Když mluvíme o P2P, nelze zde nezmínit i to, že se tyto sítě rozdělují na generace, které rozdělujeme následovně:

- **první generace,**
- **druhá generace,**
- **třetí generace.**

Sítě první generace - jsou sítě, ve kterých byly uloženy seznamy a adresy souborů s určitými daty na speciálním serveru. Tyto sítě jsou evolučně nejstarší a používají pro část svých činností centralizovanou strukturu typu klient-server.

Sítě druhé generace - dnes nejčastěji potkáváme právě tento typ sítí, zde už nejsou centrální servery. Výhoda P2P sítí spočívá v tom, že čím více uživatelů daný soubor stahuje, tím větší je přenosová rychlost Nevýhodou u centralizovaných systémů bylo,že s růstem počtu uživatelů přenosová rychlost klesala. U P2P sítí jde tedy o užitečnou vlastnost, kterou ocení především uživatel internetu.

Třetí generace klade důraz na anonymitu a šifrování ( utajení IP adres počítačů – uzlů ). I když třetí generace klade důraz na anonymitu, což je podle mě velmi důležitá věc, přesto si myslím, že uživatelé zůstanou u sítě druhých generací, jelikož záporem třetí generace je menší komfort pro uživatele a pomalost těchto systémů. Samozřejmě bych nechtěl opomenout i užitečnou vlastnost, a to, že sítě třetí generace umožňují výměnu soborů s nulovou mírou odpovědnosti.

Samozřejmě než se dostanou kopie zcela nových programů, her, hudby a filmů na internet, musí je někdo vydat a tohle dělají většinou Warezové skupiny. Zde je nutno také zmínit rozdíl mezi počítačovými piráty a Warez skupinami.

[22] Dostupné na World Wide Web: http://www.dsl.cz/clanek/1070-dalsi-hromadna-policejni-razie-v-domacnostech-kvuli-sdileni-na-dc 1.6.2010

Motivem počítačových pirátů je finanční prospěch, který je dosažitelný pomocí distribuce nelegálních kopií všech kompaktních nosičů, které se tváří jako originální. Naproti tomu Warezové skupiny zpřístupňují audio, software a filmy zdarma. Lidé, kteří jsou součástí těchto skupin, dělají vše pro to, aby získali respekt lidí z ostatních, konkurenčních skupin, nikoli pro peníze. Než se dostaneme k popisu fungování a organizace pirátských skupin, chtěl bych také vyslovit nesouhlas s názorem, že P2P sítě představují hrozbu pro současné pojetí autorského práva[23]. Podle mého názoru uživatelé využili možnosti, které jim tyto systémy nabízejí. Uživatel se tak dostane mnohem snadněji a rychleji ke všem materiálům, které potřebuje. Podle mě by byla situace v České republice jiná, kdyby majitelé autorských práv buď dokázali využít možností P2P sítí nebo byli schopni upravit cenovou politiku svých produktů.

Jak již jsem se zmínil výše, jsou to právě pirátské skupiny, díky kterým se dostávají nové tituly na internet, někdy i před oficiálním vydáním. Ale i tito lidé musí sami najít způsob, kterým by se mohli dostat k novému titulu. Je třeba říci, že pirátské skupiny jsou vysoce organizované, lidé v těchto skupinách využívají plně svých schopnosti, a to samozřejmě i na získávání nových titulů. Pro představu postupu uvádím popis z www stránek.[24]

První důležitou skupinou lidí jsou insideři. Jedná se většinou o pracovníky vývojařských firem, avšak ne vždy to tak musí být. Jeho práce spočívá v tom, že přijde do zaměstnání a čeká na vydání nějakého nového produktu. V okamžiku, kdy se tak stane, tento titul nahraje na přenosný nosič a uploaduje na sajtu své skupiny. Nejenže jsou velice důležití, ale také žádaní, protože tento člověk je ten, který dostává titul mnohem dříve, než je na pultech obchodů. Avšak i práce insidera má svá úskalí, tito lidé se totiž vystavují velikému riziku dopadení. Jak jsem již poznamenal výše, právě oni jsou ti, kteří mají titul dříve, než se objeví v obchodech, a tak pokud se stane, že je produkt na internetu několik dnů či týdnů před oficiálním vydáním, insider je podezřelou osobou číslo jedna. Firmy následně dělají hloubkové kontroly, a v mnoha případech tohoto člověka odhalí. Právě z tohoto důvodu pirátské skupiny vydají titul například den po oficiálním vydaní, a to i přesto, že už jej mají.

---

[23] MINÁRIK, T., *Počítačová kriminalita z pohledu trestního práva hmotného*, Rigorózní práce, Právnická fakulta Univerzity Karlovy 2007, s. 71

[24] Dostupnost na World Wide Web: http://www.warez.cz/clanky/jak-pirati-ziskavaji-nove-tituly/ 1.6.2010

Mezi další způsoby patří například prohledávání FTP[25] serverů. I když to může někoho překvapit, tak právě na těchto serverech vývojových firem se nachází velké množství pirátského softwaru. Na serverech těchto firem jsou umístěny kompletní aplikace, licenční soubory a další informace. Jelikož jsou si pirátské skupiny této skutečnosti velmi dobře vědomy, prohledávají tak denně například až dvacet serverů. Aby si svoji práci usnadnili, využívají svých schopností a naprogramují si různé „webové roboty“[26]. Ti pak kontrolují obsah těchto serverů sami a v případě objevení nového souboru upozorní svého majitele.

Další důležitou činností pro získávání nových titulů je hacking[27].Hacking je činnost, při které dochází k proniknutí do systému té dané společnosti. Člověk, který takové útoky páchá, se nazývá hacker[28].

Práce takového člověka spočívá v tom, že vyčkává, až firma oznámí vydání nového titulu. Poté využije svých schopností, aby se naboural do systému této firmy, a titul „ukradne“, pokud možno i se zdrojovými kódy. Samozřejmě vše má své důvody, piráti velmi dobře vědí, že firmy investují velké částky do ochrany svých produktů, jakmile ale mají piráti originální zdrojové kódy, ochrana jako taková je neúčinná. I když je hacking ojedinělým jevem v získávání titulů, stále je používaný.

Další velice oblíbenou metodou, která je oblíbená jak u pirátů, tak u vývojářů, je metoda licenčních souborů. Vývojáři mají právě díky tomuto souboru zjednodušenou distribuci, protože mohou firmě poslat hotovou verzi produktu s licenčním souborem na třicet dní a nemusejí zasahovat do kódu samotné aplikace, pouze mění licenční soubor, který je ve většině případů malý.

---

[25] FTP (anglicky File Transfer Protocol) je v informatice protokol aplikační vrstvy z rodiny TCP/IP. Je určen pro přenos souborů mezi počítači na kterých mohou běžet rozdílné operační systémy.

[26] Dostupnost z World Wide Web: http://www.symantec.com/cs/cz/norton/theme.jsp?themeid=botnet 1.6.2010

[27] Dostupnost z World Wide Web: www.ijetpack.cz/index.php/clanky/37-hacking/49-co-je-to-hacking 1.6.2010

[28] Hackeři jsou počítačoví specialisté či programátoři s detailními znalostmi fungování systému, dokážou ho výborně používat, ale především si ho i upravit podle svých potřeb.

Pro piráty je tato metoda také oblíbená, protože pokud cracker, což je další velice důležitý člen pirátské skupiny, správně pochopí schéma fungování licenčního souboru, není pro něj problémem vytvořit takovou licenci, která bude omezená, popřípadě licenci takovou, kde se lhůta tohoto produktu bude moci libovolně prodlužovat. Aby však cracker měl co zjišťovat, musí si nejdříve opatřit demonstrační CD. V takovém případě zavolá například do prodejního oddělení vývojářské firmy, a protože tam většinou prodejci firmy pracují za provizi, snaží se samozřejmě vyhovět každému požadavku. Jakmile cracker získá demonstrační CD určitého produktu spolu s trial verzí, není pro něj problémem vytvořit CD s plnou verzí produktu.

Očekávaný titul samozřejmě můžeme získat i pomocí legálně získané kopie. U této metody nepotřebujeme žádné speciální schopnosti a jedná se o nejstarší a nejpoužívanější způsob, jak získat očekávaný produkt. Pirátovi stačí, aby si zjistil, kdy produkt, který chce jeho skupina vydat na internetu, přichází na pulty obchodů. Pirát netrpělivě čeká před nějakou prodejnou, kde je titul k dispozici. Jde však o závod s časem a pirát má na paměti, že jakmile titul získá, musí ho co nejrychleji dodat crackerovi. Pokud skutečně vydá skupina produkt jako první, ostatní ve skupině proplatí dodavateli veškeré náklady, avšak pokud se tak nestane a skupina produkt jako první nevydá, tak ztrácí prestiž a dodavatel nedostane nic.

Zde je zřejmé, že každý, kdo je členem nějaké pirátské skupiny, se musí plně soustředit na svůj úkol a vložit do tohoto úkolu maximum sil.

Pokud zde mluvím o tom, jak pirátské skupiny vydávají své tituly, nelze se nezmínit také o tom, jak tyto skupiny fungují a v čem spočívá práce každého člena. Chci zde upozornit na to, že nejsem příznivcem toho, jaké činy tyto skupiny páchají, cílem této bakalářské práce není obhajoba pirátských skupin, jelikož se dopouštějí svým jednáním trestného činu, ale spíše bych chtěl popsat pirátství z té druhé strany.

Když jsem se seznamoval s problematikou počítačového pirátství, setkal jsem se s velkým množstvím informací, čerpal jsem jak z knih, tak i z internetových zdrojů a nemohu tuto část opomenout. Tyto skupiny jsou dobře organizované, každý člen, který je v určité skupině, má své postavení. Toto postavení mu zajišťují schopnosti, kterými vyniká nad ostatními. Ač se to zdá být jakkoli zvláštní, jedná se zde o velice inteligentní

a talentované lidi, kteří mají zápal pro to, co dělají. Jsou hrdí na to, že mohou být členy pirátských skupin, a pro každého z nich je to velká výzva.

Jsou to lidé, kteří se spoléhají na své schopnosti. Leader skupiny vyžaduje po každém členovi maximální úsilí, přesnost a preciznost. Jak už jsem se zde zmínil, warezové skupiny nemají ze svého počínání žádný zisk, jde jim pouze o prestiž, o to být první. Každý z těchto členů chce být respektovaný a mít uznaní od ostatních. Pro všechny je to koníček, kterému věnují maximum svého času, oni sami svádějí závod s časem, protože konkurence je vždy velká. Tyto pirátské skupiny rovněž dodržují svá pravidla, například to, že člen té dané skupiny nesmí být ve skupině konkurenční anebo dodržují také zásadu, že nikdy nevydají produkt, který byl již vydaný konkurenční skupinou.

Opět uvádím popis převzatý z www stránek[29]. Jak jsem již zmínil, nejvyšší postavení má leader, který má na starosti chod skupiny a snaží se najít nové členy. Na svoji práci však leader není sám, pomáhají mu councils. Dalším důležitým článkem ve skupině je zásobovač. Tento člen naopak shání zcela nový, nevydaný software pro svoji skupinu. V okamžiku jeho získání ho nahraje na server té dané skupiny – DUMP. Často se může jednat o mocné lidi z nějaké veliké společnosti. Velice důležitým článkem ve skupině je také cracker. Jedná se o člověka, který má znalosti systému, tudíž jeho práce spočívá v překonání ochran, do kterých softwarové společnosti investují nemalé peníze. Myslím si, že tyto ochrany ztráta času a peněz, jelikož skutečně dobrému crackerovi netrvá příliš dlouho, aby takovou ochranu prolomil. V okamžiku, kdy se na DUMPu objeví nový software od zásobovače, cracker se dá do práce. Dalším členem skupiny je carder. Je to tajemná postava, která napadá nedostatečně zabezpečené databáze serverů a krade databáze kreditních karet. Vytvořený release pak ještě otestuje tester. Samozřejmě, že členů ve skupinách je mnohem více, ale myslím si, že tohle pro základní přehled stačí.

Samotný release pak putuje na Pre-server, následně na TOPSITE – jedná se o servery s vysokou přenosovou rychlostí, nutno také dodat, že na tyto servery mají přístup jen někteří členové skupiny. Skupiny mají s některými servery zvláštní ujednání, které jim zajišťuje, že jejich release bude vydán jako první, což je samozřejmě klíčová věc

[29] Dostupnost na World Wide Web: www.warez.cz 1.6.2010

v celém procesu. Následně se release s prolomenou ochranou kopíruje i na ostatní servery. Skupina, která to stihne nejrychleji, je skupinou vítěznou.

Jak bylo řečeno dříve, pirátské skupiny svádí každý den souboj nejen s konkurenčními skupinami, ale také s časem, který je neúprosný. I když skupina už má vyhráno, cesta k uživateli teprve může začít. Zde mají prostor kurýrské skupiny. Tyto skupiny mají za úkol co nejrychleji šířit data mezi servery. Vrcholový kurýři pak mají za úkol vytvářet hodnocení serverů. Dostat se mezi takové kurýry je prakticky nemožné. Každý server má svá pevně stanovená pravidla, která se musejí striktně dodržovat. Zde se také vedou statistiky, které zaznamenávají, kolik bylo kterým kurýrem nahráno dat. To je pravý důvod, proč kurýři dělají svoji práci, opět se jedná o prestiž. Mezi ostatní důvody patří například ten, že kurýr se dostane okamžitě ke všemu warezu. Software se mezi obyčejné uživatele šíří pomocí tzv. PUB FTP serverů, v tomto případě se jedná o server s anonymním přístupem a právy pro zápis. Dále se tento materiál šíří mezi běžné uživatele pomocí boardů. Dále se tyto produkty šíří pomocí P2P sítí, o kterých se zmiňuji výše. Snad jen pro úplnost bych chtěl dodat, že pro snadnější šíření bývá například software uložen jako CD obraz a dále bývá často nahrán na specializované servery, a to v zabalených a zaveslovaných kusech. Takto je to udělané záměrně, protože správci tak mají ztíženou možnost kontroly obsahu. Pirátské skupiny si velice střeží své soukromí, a to z toho důvodu, že svým počínáním provádějí trestnou činnost. Pirátské skupiny také ke svým „produktům“ přidávají malý soubor, který má označení .nfo. V tomto souboru lze nalézt informace o daném programu a nechybí zde ani pokyny, jak s tímto programem pracovat, popřípadě pokyny pro jeho spuštění.

V první části své bakalářské práce jsem se zaměřil na historii počítačové kriminality a softwarového pirátství, dále na technologie, přes které se šíří pirátské kopie softwaru, a popsal jsem i způsob práce a fungování pirátských skupin. V této druhé části bych se rád zaměřil na samotný software a jeho rozdělení, vysvětlení tohoto pojmu, objasním zde některé důvody, proč se software používá nelegálně. Uvedu zde také, jak firmy chrání svůj software před zneužitím softwarových pirátů, to znamená některé typy ochran, a budu se také věnovat problematice licenčních smluv.

# 2 Software

Podle Petra Koláře[30] je software v informatice definován jako sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost. V publikaci Petra Koláře lze software rozdělit na systémový a aplikační. Software systémový zajišťuje chod samotného počítače a jeho styk s okolím. Naproti tomu software aplikační je software, se kterým buď pracuje uživatel počítače, nebo zajišťuje řízení nějakého stroje. Definice softwaru se samozřejmě různí. Avšak podle samotného autora není možné zcela přesně definici určit, protože existuje velmi mnoho pohledů na to, jak by měla být provedena. Definice, které lze nalézt na internetu,[31] [32] se shodují v tom, že tento pojem označuje programové vybavení počítače.

## 2.1 Rozdělení softwaru

Podle funkce můžeme software rozdělit na tyto skupiny:[33]

- **Systémový software** – Tento software umožňuje efektivní používání počítače.
- **Firmware** – Jedná se o software obsažený v hardware, přičemž hardware definujeme jako technické vybavení počítače.
- **Operační systém** – operační systém vytváří prostředí pro programy.
- **Aplikační software –** aplikační software umožňuje uživateli vykonávat nějakou užitečnou činnost.

Podle finanční dostupnosti pak můžeme software rozdělit následovně:

- **Freeware – Tímto pojmem se rozumí software, který je šířený zdarma34.**
- **Shareware** – Je označení pro software, který je chráněný autorským právem a který je možné volně distribuovat například na internetu nebo v přílohách časopisů[35] .

---

[30] Srov.*KOLÁŘ, P.,* Operační systémy *[online]. Liberec : 2005-02-01, [cit. 2010-06-07].*

[31] Dostupnost z World Wide Web: http://www.adminxp.cz/zaciname/index.php?aid=230, 7.6. 2010

[32] Dostupnost z World Wide Web: www.znamky.szesro.cz/text/Informatika/Informatika.doc, 7.6.2010

[33] Srov. *KOLÁŘ, P.,* Operační systémy *[online]. Liberec : 2005-02-01, [cit. 2010-06-07].*

[34] Dostupnost z World Wide Web: www.ucime-se.kvalitne.cz/obr/mat/Slovnicek%20pojmu.doc, 7.6.2010

[35] Dostupnost z World Wide Web: http://cs.wikipedia.org/wiki/Shareware, 7.6.2010

- **Komerční software** – Je takový software, který je šířen za úplatu. To znamená, že pokud chceme tento software používat, musíme za něj zaplatit jeho tvůrci[36].

Zde jsou vyjmenované jen některé slupiny, najdeme jich samozřejmě více, například podle druhu účelu, vzhledu, funkčnosti, zde jsem uvedl jen základní přehled.

## 2.2 Důvody pro nelegální užívání softwaru

V první části své bakalářské práce jsem se mimo jiné zaměřil na to, jak pracují pirátské skupiny, jak vydávají softwarové programy, a také jsem zmínil důvody, proč to vlastně dělají. V této kapitole bych se naopak chtěl zaměřit na běžné uživatele. Jsem si vědom toho, že každý, kdo užívá nelegální software, má jiné důvody pro své počínání.

Podle knižní publikace od Paula Craiga[37] jsou důvody následující:

- **úspora peněz,**
- **hodnocení softwaru,**
- **kompatibilita,**
- **zábava,**
- **zvědavost,**
- **aktuální verze,**
- **získání znalostí.**

Nyní bych chtěl jednotlivé důvody rozvést. Prvním je úspora peněz. V knižní publikaci, ze které čerpám, je psáno, že právě úspora peněz je obrovskou motivací pro používání nelegálního softwaru. Zřejmě je to tak proto, že uživatel může ušetřit spoustu peněz. Navíc dnes má možnost volby, což je velice důležité. Tito uživatelé se navíc nemusí bát trestního postihu, protože riziko, že budou odhaleni, je takřka nulové. Druhým důvodem je hodnocení. Znamená to, že potencionální uživatel chce zjistit, jestli mu ten konkrétní software vyhovuje, a proto si pořídí jeho kopii nelegálně. Stává se totiž, že zákazníkovi výrobek nevyhovuje a nesplňuje jeho požadavky. Tímto se posuneme

[36] Dostupnost z World Wide Web: http://cs.wikipedia.org/wiki/Komer%C4%8Dn%C3%AD_software, 7.6.2010

[37] Srov. CRAIG, P., Softwarové pirátství bez záhad. 1. vyd. Praha: Grada Publishing, 2008

k dalšímu důvodu a tím je kompatibilita. Kompatibilita je také důležitou součástí hodnocení softwaru. Uživateli samozřejmě záleží na tom, aby byl ten daný software kompatibilní s hardwarem a ostatním softwarem v jeho počítači. V současné době stále ještě není neobvyklou situací, že nově nainstalovaný program je nekompatibilní s programem jiným. Pokud bychom na takovou situaci narazili, doporučuje se, abychom jeden z programů, po dobu používání druhého programu, zavřeli. Zábava je v pořadí další z důvodů. Zde se nám nabízí pohled ze dvou stran. Na straně jedné jsou softwarové firmy snažící se mít své výrobky co nejlépe chráněné. Na straně druhé můžeme vidět, jak se crackeři naopak snaží prolomit ochranu těchto programů jako první. Důvod, pro který to dělají, jsem vysvětloval již v první části této bakalářské práce. U tohoto důvodu nezáleží na tom, zda pirát nějakým způsobem program využije. On se pouze snaží získat kopii tohoto softwaru jako první. Zvědavost je dalším důvodem, proč lidé využívají software nelegálně. Vždy, když jde o pirátský software, tak jsou uživatelé zvědaví. Například taková méně známá aplikace, která by normálně nevzbudila u uživatele zájem, se naopak stává velice zajímavou v případě, že si ji tento uživatel může stáhnout, nainstalovat a odzkoušet. Díky dnešním možnostem, které se uživateli nabízejí, již není problémem si několik takových aplikací stáhnout a následně se rozhodnout, který program si uživatel ponechá. Přecházíme k předposlednímu důvodu, který má název aktuální verze. Tento důvod je zcela prostý. Na softwaru se neustále pracuje, vydávají se stále novější a upravené verze existujících programů, které svému uživateli nabízejí nové vlastnosti a lepší výkon, případně opravují odhalené chyby. Uživatelé si tak díky internetu mohou stáhnout zdarma nové, aktualizované verze. Posledním důvodem pro užívání nelegálního softwaru, který je uveden v této publikaci,[38] jsou znalosti. Jak jsem již napsal výše, i když uživatel pirátský software nijak nevyužije, stále se o něm může něco naučit.

Zde je shrnutí některých důvodů, proč se software užívá nelegálně, a i když se lidé na pirátský software dívají z různých úhlů pohledu, a samozřejmě ho také různě obhajují, nelze zde zapomínat, že jde o krádež. Tudíž žádný z těchto důvodů pro existenci pirátského softwaru tuto skutečnost neobhajuje. V žádném případě se tímto nezastávám uživatelů, kteří užívají pirátský software. Pouze chci poukázat na to, že stejně tak jako je důvodem pirátských skupin získat co nejnovější aplikace a co nejrychleji je vydat, tak i samotní uživatelé mají důvody pro používání nelegálního softwaru.

[38] Srov. CRAIG, P., *Softwarové pirátství bez záhad. 1. vyd.* Praha: Grada Publishing, 2008

## 2.3 Základní typy softwarové ochrany

Vývojáři softwarových firem si jsou plně vědomi toho, že se jejich produkt může ihned po oficiálním vydání šířit díky softwarovým pirátům i prostřednictvím internetu a především pak díky P2P. Na tomto by nebylo zase až tak nic neobvyklého. Problém však nastává v okamžiku, kdy se vývojářům, kteří software vytvořili, nevrátí vložené náklady spojené s vývojem určitého softwarového produktu. Proto se také vytvářejí ochrany, které mají za úkol jednak znepříjemnit uživateli nelegální užívání programu nebo, což je pro softwarové firmy mnohem lepší, zcela zabránit uživateli, aby daný produkt používal, a tímto ho vlastně donutit, aby si zakoupil produkt dané softwarové společnosti legálně. Tím, že si uživatel zakoupí software, který potřebuje, zvyšují se legální cestou zisky společnosti, která tento produkt vydala, a následně se jí tedy vracejí vynaložené náklady na tento produkt. To je další důvod, proč softwarové firmy vynakládají vysoké částky na tvoření proti pirátských ochran, které by dané společnosti zajistily, aby si její produkty kupovali uživatelé legálně. Zde je však nutno dodat, že jsou většinou tyto ochrany u softwarových produktů dříve či později prolomeny. V této kapitole bych se chtěl věnovat základním typům ochran, které používají softwarové firmy. Vycházím z knižní publikace Pavola Červeni[39]. Podle tohoto autora máme tyto základní typy ochrany:

- **registrační číslo ( seriál numer ),**
- **časové omezení ( time limit ),**
- **registrační soubor ( key file ),**
- **hardwarový klíč ( dongle ).**

Nyní si opět jednotlivé druhy ochran blíže popíšeme. Vycházím s popisu, který je dostupný právě v knize tohoto autora[40]. První softwarovou ochranou, kterou bych chtěl přiblížit, je sériové číslo. Tuto ochranu vidíme dnes u softwarových produktů nejčastěji. Celý proces spočívá v tom, že uživatel je při instalaci daného produktu požádán o zadání CD klíče, který bývá nejčastěji uveden na zadní straně obalu, ve kterém se nachází CD. Pokud uživatel zadá platný registrační klíč, instalace se spustí. Pokud se tak

[39] Srov. ČERVEŇ, P., *Cracking a jak se proti němu bránit.* 1. vyd. Praha : Computer Press, 2002.

[40] Srov. ČERVEŇ, P., *Cracking a jak se proti němu bránit.* 1. vyd. Praha : Computer Press, 2002.

však nestane, pak je uživatel vyzván, aby zadal správný registrační klíč. Pokud tak neučiní, pak je instalace tohoto programu ukončena.

Ochranu registračním číslem můžeme rozdělit na:

- **registrační číslo je vždy stejné;**
- **Registrační číslo se mění podle zadaných položek například firma, jméno, atd.**
- **Registrační číslo se mění podle počítače, na kterém je program spuštěn.**
- **Registrační číslo je kontrolováno díky internetu.**

Nyní bych chtěl tyto podskupiny popsat podrobněji. Začneme tedy se situací, kdy je sériové číslo vždy stejné. Ochrana se stejným sériovým číslem má však velkou nevýhodu. V tomto případě stačí, aby cracker zjistil jedno sériové číslo. Pokud se tak stane, cracker pak může šířit tento softwarový titul dál, protože se tohle sériové číslo nemění. Avšak programátor může crackerovi práci velice znepříjemnit. Sériové číslo může být složitě zašifrováno, při zadávání čísla uživatele se kóduje číslo zadané, nemusí se z tohoto důvodu dekódovat číslo skutečné a pro crackera není jednoduché ho odhalit. Jen pro úplnost bych dodal, že tento typ ochrany se doporučuje jen u levnějších aplikací. V případě dražších aplikací se doporučuje kombinace i s jinými typy ochran. Další je sériové číslo, které se mění podle zadaných položek. V současnosti je tato forma ochrany sériovým číslem nejpoužívanější. Její fungování spočívá v tom, že se sériovým číslem musíme zadat také jméno, organizace, popřípadě jiné doplňující údaje. Na základě těchto údajů se kontroluje správnost sériového čísla. Další formou ochrany je, pokud se registrační číslo mění podle počítače uživatele.

Pro útočníka je to velice nepříjemný typ ochrany. Uživatel zaregistruje program jen na svém počítači a pirátskou verzi není možné registrovat. Toto sériové číslo se mění například v závislosti na sériovém čísle harddisku nebo náhodně. Jedna z nejdůležitějších věcí je však toto číslo ukrýt, v případě nalezení tohoto čísla by se dalo jednoduše změnit na jednotné a program by se dal registrovat na jakémkoliv počítači tím samým registračním číslem. Pokud je sériové číslo kontrolováno za pomocí internetu, tak po zadání registračního čísla uživatelem program pošle pomocí internetu registrační číslo na ověření. Server, který má na starosti kontrolu správnosti těchto registrač-

ních čísel, toto číslo otestuje a pošle zprávu, zda se jedná o správné sériové číslo či nikoliv.

Další ochranou, která se stále používá, je časové omezení. Autoři softwarových programů si touto ochranou chtějí zabezpečit to, aby po uplynutí zkušební doby uživatel nemohl tento program dále používat.

Typy ochran s časovým omezením jsou:

- **Časové omezeni se zruší po zadání správného registračního čísla.**
- **Časové omezení se zruší po nahrání registračního souboru.**
- **Časové omezení se nedá zrušit, můžeme pouze koupit originální program bez omezení.**
- **Časové omezení na počet spuštění.**

Pokud jde o první typ ochrany, tedy časové omezení se zruší po zadání správného registračního čísla, v podstatě platí to samé jako v případě registračních čísel. Rozdíl je ovšem v tom, že pokud nebylo registrační číslo zadáno správně, stane se, že se program nezaregistruje, a tak se po určitém čase odmítne spustit. Pokud mluvíme o třetím typu ochrany, tedy o ochraně, kdy se časové omezení zruší po nahrávání registračního souboru, je třeba říci, že podle autora[41] jde o výborný typ ochrany, který se však často nevyužívá. V tomto případě se využívá možnosti zaslání registračního souboru za pomocí internetu. Registrační soubor obsahuje podstatnou část kódu programu, která odblokuje například časové omezení. Další typ ochrany často využívají dema programů. Jedná se o časové omezení, které se zrušit nedá, uživatel má možnost koupit si originální program, který je bez časového omezení.

Uživatel se při tomto typu ochrany nachází v situaci, kdy se softwarový program po uplynutí časového limitu nedá spustit. Poslední typ ochrany s časovým omezením funguje v podstatě stejně jako časové omezení až na to, že program nemůžeme spouštět věčně, ale počet jeho spuštění je omezený.

Nyní bych se chtěl blíže věnovat dalšímu základnímu typu ochrany, a tou je registrační soubor. Tato ochrana je založená na tom, že v adresáři, kde je program nainstalován, je nahrán registrační soubor. Program kontroluje obsah tohoto registračního souboru, a pokud je tento obsah správný, pak se program chová jako registrovaný. Po-

[41] Pavol Červeň – autor publikace s názvem Cracking a jak se proti němu bránit

kud však nastane situace, že registrační soubor není správný, pak program pracuje jako neregistrovaný a v horším případě nepracuje vůbec. Většinou registrační soubor obsahuje informace o uživateli, pro kterého je vytvořen, popřípadě čísla pro odstranění kódu těch částí programu, které jsou zakódované a jsou přístupné pouze ve verzi registrované.

Dalším typem základní ochrany, které bych chtěl věnovat pozornost, je hardwarový klíč. Opět čerpám informace z této knižní publikace[42], kde autor mimo jiné zmiňuje tyto typy ochrany hardwarovým klíčem:

- **Program bez hardwarového klíče nelze spustit.**
- **Program má bez hardwarového klíče omezené některé funkce.**
- **Program má bez hardwarového klíče omezené některé funkce.**

Nyní blíže popíši oba typy ochran. V první případě ochrana funguje tak, že program pošle data na port, kde má být připojen hardwarový klíč, a čeká na odezvu. Pokud program odezvu nedostane, pak program nelze spustit a uživateli se zobrazí chybová hláška. V druhém případě je princip ochrany velice jednoduchý – pokud v programu není zapojen hardwarový klíč, pak v programu nefungují některé důležité funkce. Ovšem po zapojení hardwarového klíče je program plně funkční. Samozřejmě, že v dnešní době existuje mnoho ochran, které mají za úkol zabránit uživateli, aby program užíval nelegálně. Zmínil jsem zde, a také následně blíže popsal některé typy ochran, nepopisoval jsem všechny, protože si myslím, že pro účely této práce to stačí. Ještě než se začnu věnovat následující kapitole, chtěl bych zde zmínit, že každá ochrana má své kladné a záporné stránky.

V poslední době se často mluví o ochraně, kterou proti pirátům vydala firma Ubisoft[43]. Tato ochrana funguje tak, že uživatel musí být připojen neustále k internetu, aby si mohl například hru od této firmy zahrát. I když již je tato ochrana prolomena, na což poukazuje i tento článek[44], je zde otázka k zamyšlení, jestli se nejedná o omezování těch, kteří by si v tomto případě hru koupili, protože i v dnešní době nemusí mít každý

[42] Srov. ČERVEŇ, P., *Cracking a jak se proti němu bránit.* 1. vyd. Praha : Computer Press, 2002.

[43] Dostupnost z World Wide Web: www.ubi.com, 7.6.2010

[44] Dostupnost z World Wide Web:.http://tn.nova.cz/magazin/hry/novinky/ubisoft-upravil-protipiratskou-ochranu-ta-je-jiz-prolomena.html, 7.6.2010

internet. V článku se mluví o tom, že pokud hráč není připojen k internetu, tak si hru nezahraje. Tomuto článku[45]je věnována také anketní otázka, která se čtenářů ptá na to, co si oni sami myslí o této ochraně, přičemž 90 procent má za to, že ochrana šikanuje poctivé hráče, a 10 procent dotázaných si naopak myslí, že jde o správný krok proti pirátům. Já osobně souhlasím s názorem, že jde o znevýhodnění těch, kteří mají originální hru. Samozřejmě chápu snahu firem, že chtějí ochránit své produkty, ať už se jedná o software, hudbu nebo filmy, ale nemělo by se to dělat takovým způsobem, že budou znevýhodněni ti, kteří si tyto produkty kupují legální cestou.

V této druhé části své bakalářské práce bych se rád zmínil o tom, jak můžeme uzavřít licenční smlouvy a jaké máme druhy těchto smluv. O licenčních smlouvách pojednává ustanovení § 46, následně autorský zákon upravuje, jak lze uzavřít licenční smlouvu.

## 2.4 Způsoby uzavírání licenčních smluv

V první řadě bych rád vysvětlil pojem licence. Tak tedy podle internetové definice[46]je slovo licence právním termínem, kterým vyjadřujeme několik skutečností, které jsou závislé na souvislostech, v jakých je tento termín používán.

Jiná definice[47]zase říká, že v případě pořizování softwarového vybavení si zákazník nekupuje software, ale licenci na používání tohoto softwaru. Může tedy dojít k následujícím situacím[48]:

Kupujícím je nepodnikatel, zákazník, který si pořizuje hotový software. Zákazník si může koupit program na CD a DVD nebo si jej stáhnout i z internetových stránek,

---

[45] Dostupnost z World Wide Web: http://tn.nova.cz/magazin/hry/novinky/ubisoft-upravil-protipiratskou-ochranu-ta-je-jiz-prolomena.html, 7.6.2010

[46] Dostupnost z World Wide Web: http://cs.wikipedia.org/wiki/Licence, 7.6.2010

[47] Dostupnost na World Wide Web: http://www.microsoft.com/cze/licence/ZakladniInformace/CojeLicence.mspx, 7.6.2010

[48] Srov. SMEJKAL, V., *Internet a §§§.* 2. aktualizované a rozšířené vydání Praha : Grada Publishing, 2001, str. 67

kde jej poskytuje výrobce. Pokud se software nachází na CD nebo DVD, tak dochází jak ke koupi tohoto CD nebo DVD, tak i k poskytnutí práva užívat tento program.

- **Kupující** – podnikatel si kupuje hotový program. Zde dochází ke stejné situaci, která je popsána výše.
- **Kupující - podnikatel nebo zákazník** si kupuje software společně s hardware. Tedy jedná se o OEM verzi. Je to druh licenční smlouvy, které se budu věnovat v následující kapitole.
- **Objednatel** – podnikatel si nechá zhotovit software, který mu vyhovuje a který potřebuje.

Objednatel si nechává zhotovit software svým zaměstnancem.

## 2.5 Druhy licenčních smluv

Než se začnu věnovat problematice licenčních smluv, chtěl bych říci, že druhů licencí je opravdu mnoho. V této bakalářské práci proto popíši jen ty nejdůležitější a nejznámější.

**Komerční software** – v tomto případě autor poskytuje pouze právo užívat program podle ustanovení licenční smlouvy. Rozdíl od ostatních druhů licencí je v tom, že tento druh licence je poskytnut za peníze a neumožňuje úpravu softwaru, kromě zákonných výjimek. „Veškerá omezení práva autora k počítačovému programu se týkají takové podoby kódu, v níž byla rozmnožena počítačového programu zpřístupněna veřejnosti, nikoli tedy formy jiné.“[49].

**OEM licence** – u této licence si kupující kupuje software společně s hardware. To znamená, že software může být používaný pouze s hardwarem, ke kterému byl dodán, a nelze ho koupit zvlášť. Jako příklad si zde můžeme uvést Microsoft Windows, kdy je operační systém již nainstalován v době, kdy si zákazník kupuje nový počítač. Software tedy nelze nainstalovat na jiný počítač a při ztrátě nebo poškození hardware, ke kterému

[49] KŘÍŽ, J., a kol. *Autorský zákon – komentář a předpisy související.* 2. aktualizované vydání Praha : Linde Praha, 2005, str. 179

se váže OEM licence, právo užívat software zaniká. Při převodu nebo při prodeji hardware, na který je OEM software vázán, má právo užívat software zákazník, který si jej koupil.

- **Shareware** – program tohoto typu je spjat s licencí, která dovoluje vytvářet a šířit kopie, ale jen určitou dobu, většinou se jedná o časovou lhůtu, nejčastěji v rozmezí 30 – 60 dnů. V případě, že uživatel bude software nadále používat, bude po této časové lhůtě vyzván, aby zaplatil licenční poplatek. Po uplynutí časové lhůty, kterou stanovil autor tohoto softwaru, je nutno tento softwarový program odinstalovat anebo zaplatit licenční poplatek. Takto to například funguje u Total Commander, kdy je uživatel upozorněn na to, že se jedná o shareware, a to znamená, že funkční je tento program po dobu jednoho měsíce, poté ho uživatel musí odstranit z pevného disku. Výhodou těchto licencí je to, že uživatel, který si shareware stáhne například z těchto www stránek, si může bezplatně vyzkoušet vlastnosti a funkce toho daného programu, a to bez jakéhokoliv omezení, protože se jedná o plnou verzi, která má všechny funkce.
- **Adware** – Licence, kdy uživatel, který používá nějaký program, neplatí poplatek za licenci, ale souhlasí, aby se na jeho počítači zobrazovala reklama a tím si jako by „kupuje“ souhlas autora k tomu, aby mohl používat software, který potřebuje. Jako příklad bych uvedl ICQ. Způsoby zobrazování reklamy zde mohou mít různou podobu. Například se v programu samotném může zobrazovat reklamní banner, popřípadě software může zasílat reklamní maily na emailovou adresu, kterou uživatel uvedl při registraci tohoto software, nebo program může sledovat systém počítače a odesílat data od uživatele výrobci programu.
- **Freeware a volný software** – v případě freeware jde o volně dostupný software. Autor, který software vytvořil, nepožaduje za tento program poplatky po uživatelích, kteří jej používají. Je třeba si ale uvědomit, že autor je ten, který má stále autorská práva k tomuto softwaru, a tudíž bez jeho souhlasu není možné program jakkoliv měnit.

Naproti tomu pojem volný software znamená, že jde o program, ke kterému již nikdo nevlastní autorská práva. Jde tedy o program, kdy uplynulo více než 70 let od smrti posledního autora, v tomto případě tomu říkáme volné dílo.

- **GNU/GPL a svobodný software** – je-li počítačový program uveřejněn pod tímto druhem licence, označuje se jako svobodný software, přičemž svobodný software je

definován jako software, ke kterému je k dispozici také zdrojový kód, spolu s právem tento software používat, modifikovat a distribuovat. Naprostá většina svobodného software je zdarma, ačkoliv to není podmínkou. Tato licence je napsaná Richardem Stallmanem, který také definoval tyto čtyři svobody:

- **Svoboda používat program za jakýmkoliv účelem.**
- **Svoboda studovat, jak program pracuje, a možnost přizpůsobit ho svým potřebám.**
- **Svoboda redistribuovat kopie programu.**
- **Svoboda vylepšovat program a zveřejňovat zlepšení, aby z nich mohla mít prospěch celá komunita.**

Pro úplnost bych ještě dodal, že svobodný software můžeme platit nebo jej obdržet zdarma, ovšem uživatel má vždy svobodu kopírovat a měnit software, dokonce může prodávat nebo darovat kopie tohoto softwaru.

# 3 Softwarové pirátství v České republice

Jeden z cílů mé bakalářské práce je ukázat, že softwarové pirátství má vliv na ekonomiku v České republice, což dokazují analýzy, které na svých stránkách prezentuje proti pirátská organizace BSA[52]. V začátcích psaní této bakalářské práce bylo v České republice nainstalováno 38 procent softwaru nelegálně. Tato skutečnost vyplývala též z analýzy, která je uveřejněna zde[53]. Tyto analýzy se uveřejňují vždy v měsíci květnu a proti pirátská organizace BSA si nechává tyto studie zpracovávat analytickou společností IDC[54]. Je tomu tak proto, aby byla zajištěna objektivita zjištěných skutečností. 14. května 2009 vyšla další studie,[55] ze které vyplývá, že softwarové pirátství v České republice pokleslo o jeden procentní bod, tedy na 37 procent. Ze studie vyplývá i několik dalších skutečností, které bych zde chtěl prezentovat. Jelikož zde zmiňuji organizaci BSA a společnost IDC, chtěl bych jen ve stručnosti říci, o jaké organizace se jedná a na co se zaměřují. BSA je tedy proti pirátská organizace, která prosazuje po celém světě práva softwarového odvětví. Tato organizace působí v osmdesáti zemích světa a usiluje o vytváření podmínek pro inovace a růst trhu se softwarem. Členové BSA každoročně investují miliardy dolarů do ekonomik jednotlivých států. Tím přispívají k tvorbě nových pracovních míst a vytvářejí softwarová řešení, která pomáhají lidem po celém světě být produktivnější a lépe a bezpečně navzájem komunikovat. Členové BSA jsou například společnosti Microsoft, Adobe nebo Apple. Tyto a další informace opět nalezneme na www stránkách[56] této společnosti. Musím dodat, že někteří lidé nemají s touto organizací dobré zkušenosti a nelibí se jim praktiky, které jsou lidmi z BSA uplatňovány.

[52] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[53] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[54] Dostupnost z World Wide Web: www.idc.com, 7.6.2010

[55] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[56] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

Důkazem toho je i tento článek[57]. V něm se vyjadřuje Emil Čelustka, mimo jiné zakladatel společnosti ABC systems[58], na adresu BSA a popisuje metody, které tato společnost používá k tomu, aby dosáhla svého. Pro doplnění informací bych chtěl říci, že firma ABC systems je jednou z nejrychleji rostoucích technologických společností, což dokazuje průzkum Technology Fast 50[59]. Tento průzkum je každoročně připravovaný společností Deloitte & Touche[60].

Nyní si ve zkratce představíme společnost IDC[61]. Jedná se o mezinárodní analytickou a poradenskou společnost, která působí na trhu informačních a komunikačních technologií a zároveň organizuje odborné konference, a to v oblasti informačních technologií, telekomunikací a spotřebitelských technologií. Tato společnost napomáhá IT odborníkům, manažerům a investorům rozhodovat o investicích právě do informačních technologií a vytvářet tak vlastní obchodní strategii. Průzkumy zpracovává pro tuto společnost přes tisíc analytiků ve více než 110 zemích. Přes 46 let IDC také poskytuje náhledy, které klientům umožní dosáhnout svých obchodních cílů. Nutno také dodat, že IDC je dceřinou společností IDG[62]. IDG je přední mezinárodní firma se zaměřením na média, výzkum a organizaci různých akcí v oblasti informačních technologií.

Jak už zde bylo řečeno, 14. května vyšla nová analýza[63], která je věnována softwarovému pirátství. V souvislosti s ní vyšlo najevo i několik zajímavých skutečností. Tato analýza je zpracovaná pro rok 2009.

---

[57] Dostupnost z World Wide Web: http://www.e-komerce.cz/ec/ec.nsf/0/7fdcd0dd523a2bf9c1256c7100567eff, 7.6.2010

[58] Dostupnost z World Wide Web: http://www.abcsys.cz/, 7.6.2010

[59] Dostupnost z World Wide Web: http://www.deloitte.com/fast50ce, 7.6.2010

[60] Dostupnost z World Wide Web: www.deloitte.com, 7.6.2010

[61] Dostupnost z World Wide Web: www.idc.com, 7.6.2010

[62] Dostupnost z World Wide Web: www.idg.com, 7.6.2010

[63] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

## 3.1 Škody napáchané v České republice za rok 2009

Jeden z nejdůležitějších bodů této analýzy[64] je zjištění, že meziročně počet instalací nelegálního softwaru v tuzemských osobních počítačích klesl o jeden procentní bod a míra pirátství v České republice tak dosahuje 37 procent.

V roce 2008 to bylo 38 procent. Tato skutečnost též vyplývá ze zveřejněné studie[65], kterou můžeme najít na www stránkách BSA. Studie také tvrdí, že v důsledku pirátství výrobci softwaru v České republice přišli o tržby v hodnotě 3,6 miliardy korun. Opět si dovolím malé srovnání s rokem 2008.

Tehdy přišli v důsledku pirátství výrobci o 3,3 miliardy korun[66]. Na tuto skutečnost taktéž poukazuje analýza, která byla zpracována firmou IDC a lze ji opět nalézt na www stránkách BSA. Studie také poukazuje na to, že v mnoha zemích navzdory hospodářské krizi softwarového pirátství v osobních počítačích ubylo. Míra pirátství podle IDC[67] klesla v 54 státech a vzrostla v 19 zemích. Dále uvádí, že celosvětová míra softwarového pirátství vzrostla o 2 procenta, tedy ze 41 procent na 43 procent. Podle Jana Hlaváče[68] má tato skutečnost svůj důvod „Stalo se tak zejména v důsledku toho, že na globálním softwarovém trhu získaly vyšší podíl rychle se rozvíjející země jako Čína, Indie a Brazílie, v nichž je míra pirátství podstatně vyšší než v ostatních státech.“[69] Studie také podle Jana Hlaváče ukazuje, že je BSA v boji proti pirátství úspěšná. Tvrdí také, že tato organizace hodlá nadále šířit povědomí o rizicích, která zde jsou v případě, že budeme používat nelegální software, a to jak ve firemní oblasti a v domácnostech, tak na vládní úrovni. Zejména tam by chtěla BSA[70] upozornit na to, že pirátství má negativní vliv na ekonomiku v České republice. Podle výzkumu společnosti IDC[71], který

[64] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[65] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[66] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[67] Dostupnost z World Wide Web: www.idc.com, 7.6.2010

[68] Jan Hlaváč – tiskový mluvčí protipirátské organizace BSA

[69] Citace dostupná v analýze, která je dostupná na World Wide Web: www.bsa.org, 7.6.2010

[70] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[71] Dostupnost z World Wide Web: www.idc.com, 7.6.2010

je dostupný na www stránkách, na každých 100 amerických dolarů legálně zakoupeného softwaru připadá dalších 75 dolarů softwaru nelegálního. Hovoříme zde o roku 2009. Jan Hlaváč, mluvčí proti pirátské organizace BSA, také dodal: „Při snížení míry pirátství o deset procentních bodů by si česká ekonomika během čtyř let polepšila o tisíce nových pracovních míst, hrubý domácí produkt by vzrostl o 8,9 miliardy korun a stát by na daních navíc vybral téměř dvě miliardy korun. IT firmy by díky vyšším výdajům za informační technologie zvýšily své příjmy o 6,2 miliardy korun.“[72] Na základě těchto tvrzení můžeme říci, že softwarové pirátství má vliv na ekonomiku v České republice více, než by se mohlo zdát. Pirátství zmenšuje příjmy jak softwarovým firmám, tak se projevuje i ve statním rozpočtu. Snížení pirátství se pak pozitivně projevuje i v ekonomické rovině, na což poukazuje i studie[73], kterou opět vypracovala analytická společnost IDC. Stalo se tak v roce 2008.

Z této studie můžeme zjistit, že Česká republika vynaložila v tomto roce 74 miliard korun na informační technologie, například na počítače, příslušenství, síťovou techniku, krabicový software nebo IT služby. Ze studie vyplývá, že tyto výdaje tvořily 2,8 procenta hrubého domácího produktu a podpořily rozvoj více než 7100 IT firem, které zaměstnávaly téměř 73 tisíc lidí a umožnily státu na daních vybrat 51 miliard korun. Na základě této analýzy se také odhaduje, že tuzemské IT odvětví bude v roce 2011 bez ohledu na to, jestli se pirátství sníží nebo ne, poskytovat téměř 90 tisíc pracovních míst. Do ekonomiky díky výdajům za IT přibude 100 miliard korun a stát na daních vybere 25 miliard korun. Dále se posílí český sektor informačních technologií a díky tomu se vytvoří 1194 nových nadprůměrně placených pracovních míst. Proti pirátská organizace BSA kromě potírání softwarového pirátství v České republice také vyzývá vlády, aby učinily například opatření, která by mohla pomoci v boji proti problému, jakým softwarové pirátství bezesporu je, a uskutečnit tak kroky a opatření k tomu, aby vedly ke splnění výše zmíněné studie. Některé z těchto kroků jsou velice zajímavé a myslím si, že by mohly být velice přínosné a mohly by vést ke snížení softwarového pirátství v České republice, proto bych je chtěl ve stručnosti shrnout.

[72] Tvrzení Jana Hlaváče, které je dostupné v analýze IDC z roku 2008 na World Wide Web: http://extrawindows.cnews.cz/piratskeho-softwaru-v-cesku-opet-ubylo-nelegalne-se-ho-uziva-37

[73] Dostupnost z World Wide Web: www.idc.com

V první řadě BSA vyzývá vlády, které chtějí těžit z ekonomických výhod, které plynou ze snížení softwarového pirátství, aby aktualizovaly zákony, které chrání duševní vlastnictví, dále apeluje na to, aby vlády vytvořily účinnější mechanismy práva, a to včetně přísných proti pirátských zákonů. Podle BSA je na řešení tohoto problému třeba vyčlenit patřičné zdroje, dále vytvořit orgány pro ochranu duševního vlastnictví a zajistit vzdělání jak pro úředníky, tak pro veřejnost.

S uvedenými opatřeními bych souhlasil a zvláště potom s opatřením, které se týká vzdělání veřejnosti, neboť je třeba si v první řadě uvědomit, že pirátství je zločin, musím však podotknout, že kromě tohoto bych dal také běžným uživatelům internetu a firmám, které se podle BSA softwarového pirátství dopouštějí, lepší možnosti a cesty k tomu, jak si produkt té dané firmy pořídit legálně a pokud možno i za nižší ceny.

## 3.2 Klíčové poznatky studie v roce 2009

Studie, která byla vydána 14. 5. 2010 a následně uveřejněna na www stránkách proti pirátské organizace, ukazuje, že v roce 2009 došlo k jistému pokroku v boji proti pirátství. Ředitel BSA Robert Holleyman k tomu řekl: „Pirátství brzdí inovace v IT odvětví, brání vytváření nových pracovních míst a vládní rozpočty připravuje o klíčové příjmy z daní. Naše zpráva velice jasně říká, že vlády zemí po celém světě musí zdvojnásobit své snahy v potlačování šíření nelegálního softwaru.“[74]

Studie dále poukazuje na tyto klíčové poznatky:

- Míra softwarového pirátství klesla celkově v 54 ze 111 zemí, avšak celosvětové míra pirátství vzrostla ze 41 procent ( tento údaj byl platný v roce 2008 ) na 43 procent ( tento údaj je platný za rok 2009 ). Má se zato, že celosvětová míra pirátství vzrostla, protože došlo k růstu softwarových trhů v rozvíjejících se zemích.

Globální komerční hodnota nelegálního softwaru dosáhla v roce 2009 hodnoty 51,4 miliardy amerických dolarů. V Česku softwarové firmy postihla ztráta ve výši 3,6 miliardy korun.

[74] Citace z analýzy, která je dostupná na Woeld Wide Web: www.bsa.org, 7.6.2010

Podle této analýzy[75]míru pirátství snižuje hned několik věcí jako například legalizační programy, osvětové kampaně vládních úřadů i softwarových firem, které se pravidelně konají za účelem vysvětlit lidem, co si mohou dovolit a naopak čeho by se neměli dopouštět, kroky orgánů činných v trestním řízení a v neposlední řadě změny technologií jako například ochrana DRM[76]. DMR znamená Digital Rights Management (správa digitálních práv) - je nástroj, který dává poskytovatelům kontrolu nad obsahem digitálních médií. Tato technologie je nejčastěji využívána k šíření souborů s hudbou.

Jako příklad bych uvedl iTunes[77] od společnosti Aplle. Jeho hudební soubory, které jsou ve formátu ACC, jsou DRM „chráněny" například tak, že nejdou přehrát v jiném přehrávači, než je iPod od stejné firmy. Osobně nesouhlasím s tím, že konkrétně tato technologie přispívaje ke snížení porušování autorských práv, naopak právě omezuje ty uživatele, kteří si za hudbu zaplatili. Nemyslím si, že tohle je ten správný směr, kterým by se měli prodejci ať už hudebních souborů, či softwarových produktů ubírat. Jednak je zde jasně vidět, že uživatel, který je legální a ochoten si zaplatit za produkty, které chce nebo je potřebuje, je v nevýhodě a výhodu dostává naopak ten uživatel, který si své oblíbené produkty nebo hudební soubory pořídí například prostřednictvím P2P sítí. Kromě toho ochrana DMR již byla prolomena, což dokazuje i tento[78]článek. Z mého pohledu je investování do těchto ochran zcela zbytečné. Jednak omezují samotné uživatele, kteří mají vše legálně a jsou ochotni zaplatit si za produkty té dané firmy, a druhý důvod je ten, že dříve či později jsou tyto ochrany stejně prolomeny, takže investice je zcela bezúčelná.

- K růstu míry pirátství naopak přispívá rychlý růst trhu s výpočetní technikou a větší užívání starších počítačů, v nichž se vyskytuje největší množství nelegální-

[75] Dostupnost z World Wide Web: www.idc.com, 7.6.2010

[76] Dostupnost z World Wide Web: http://podani.blog.respekt.cz/c/1760/Spoutana-hudba-aneb-je-DRM-spatne.html, 7.6.2010

[77] iTunes je aplikace určená pro organizaci a přehrávání multimediálních souborů. Program je také rozhraním pro správu obsahu přehrávače iPod a multifunkčního mobilního telefonu iPhone společnosti Apple. – www.wikipedia.org

[78] Dostupnost z World Wide Web: http://technet.idnes.cz/konec-placene-hudby-na-internetu-ochrana-drm-prolomena-p1o-/tec_audio.asp?c=A060827_234634_tec_audio_kuz, 7.6.2010

ho softwaru, a v neposlední řadě je to také propracovanější postup pirátů, kteří dokáží softwarové produkty získat.

- Nejnižší míra softwarového pirátství je zaznamenána v USA, kde míra softwarového pirátství činí 20 procent.
- Průměrná míra pirátství v EU činí 35 procent.

## 3.3 Pirátství podniků

Opět vycházím z analýzy[79]BSA, kde se uvádí, že nelegální software se nejvíce šíří v malých firmách, kdy jde nejčastěji o firmy, které zaměstnávají 50 pracovníků. Tyto firmy podnikají ve výrobních oblastech nebo službách. Do další kategorie této analýzy jsou také zahrnuty firmy, které se specializují na různé obory, například architekti, reklamní agentury, designéři nebo inženýrské společnosti. Tato analýza vychází z evidence případů softwarového pirátství za posledních deset let.

Na základě těchto údajů bylo hodnocení následující:

- Softwarového pirátství se nejvíce dopouštějí firmy, které vlastní od pěti do sta počítačů.
- Řada manažerů, kteří působí v těchto firmách, si není vědoma, že u nich docházelo k užívání softwaru nelegálním způsobem.

Podle studie IDC[80] jsou na tom nejlépe firmy s více než 250 počítači. Tyto firmy mají výhodu v tom, že jsou v nich zpravidla dobře zavedeny kontrolní mechanismy. V těchto společnostech mají administrátoři i manažeři přehled o nákupu počítačového vybavení a existují zde i určitá pravidla pro práci se softwarem a poškozování zaměstnanců, v neposlední řadě je také velice důležitá důsledná správa užívaného softwaru. Z této studie tedy jasně vyplývá, že firmy, které mají pravidelný softwarový audit a dbají na dodržování jasně daných pravidel a následně provádějí kontrolu těchto pravidel, se nevystavují rizikům, která jsou spojena s užíváním nelegálního softwaru.

[79] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[80] www.idc.com - je přední mezinárodní analytická a poradenská společnost působící na trhu informačních a komunikačních technologií

A to ať už mluvíme o riziku finančního postihu, které může firmu reálně ohrozit, tak trestního postihu, kde nám hrozí, že bude pošpiněna pověst firmy a také učiněn záznam v rejstříku trestů, což může ohrozit osobu, která byla obviněna.

Z analýzy vyplývá, že pirátství, které se děje ve firmách, je způsobeno chaosem, kdy firma nevěnuje dostatek pozornosti výpočetní technice a nemá vytvořená pravidla, jak pracovat se softwarem. Z analýzy BSA[81] plyne, že nejčastější příčinou pirátství v těchto firmách je nainstalování více kopií softwaru, než kolik povoluje zakoupená licence. Tato analýza také říká, že různé specializované firmy užívají nelegální software úmyslně, a to z toho důvodu, aby ušetřili peníze. Jde například o software pro vytváření a úpravu grafiky, kreslení CAD výkresů nebo projektové dokumentace. Tyto programy cenou odpovídají užitné hodnotě a tak se licenční poplatek za jednu instalaci takového softwaru může pohybovat v řádech desítek tisíc korun. Je samozřejmé, že při tak vysoké ceně hledají někteří lidé, kteří pracují s takovými programy cestu, jak si jej pořídit za nižší cenu, anebo nainstalují software nelegálně. Analýza však poukazuje na to, že v těchto firmách může být pirátské užívání softwaru způsobeno nedbalostí anebo také nezájmem ze strany pracovníka či manažera legalitu softwaru hlídat. Uvádí se také, že nejčastěji nelegálně užívaným softwarem jsou kancelářské balíčky společnosti Microsoft ( jako například Word, Excel , PowerPoint ), dále antivirové programy, které jsou například od společnosti Symantec[82]. Chtěl bych zde podotknout, že k pirátství by nemuselo docházet v takové míře, kdyby si manažeři firem byli vědomi toho, že za kancelářské balíčky společnosti Microsoft lze nalézt náhradu v podobě open office[83], což je také kancelářský balík, který je šířený jako svobodný software pod licencí LGPL. Je komukoliv dostupný zdarma a můžeme ho provozovat například na operačním systému Microsoft Windows. Co se týče antivirových programů, u nich existuje také alternativní náhrada. Můžeme využít například Avast free.

[81] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[82] Dostupnost z World Wide Web: www.symantec.com, 7.6.2010

[83] Dostupnost z World Wide Web: http://cs.wikipedia.org/wiki/Open_Office, 7.6.2010

Tento antivirus vyhoví lidem, kteří odesílají emailovou poštu a navštěvují různé internetové stránky. Princip je takový, že si stáhneme tento antivir například zde[84] a po uplynutí třicetidenní zkušební lhůty se zaregistrujeme na oficiálních stránkách[85]. Po úspěšně dokončené registraci nám bude tento antivir poskytovat kvalitní antivirovou kontrolu, je navržen tak, aby ochránil důležitá data a programy, navíc každý ocení jednoduchost tohoto antivirového programu. Ještě pro upřesnění bych dodal, že po registraci bude tento antivir funkční po dobu jednoho roku.

Mezi další poškozené firmy patří například Adobe[86]a Corel[87]. Tyto společnosti nabízejí grafický software, který lze pořídit mnohdy za desetitisíce korun. Především právě proto lidé, kteří využívají produkty těchto společností, hledají cesty k tomu, aby nemuseli platit licenční poplatek. Další důvod je samozřejmě ten, že by došlo ke snížení nákladů, což je pro některé firmy zcela klíčová záležitost a tak dochází k tomu, že je takový software nainstalován nelegálně. Další poškozovanou společností podle této analýzy[88]je Autodesk[89]. Tato společnost už od roku 1982 představuje špičkové 2D a 3D technologie, díky kterým návrháři analyzují a simulují jejich nápady v praxi. Analýza také apeluje na manažery různých firem, aby neztráceli přehled o užívaném softwaru ve svých firmách. Ztráta těchto důležitých informací totiž může způsobit, že se množství nelegálně instalovaných programů zvýší a společně s ním také riziko finančního postihu, které se může pohybovat až do stovek tisíc korun. V minulém roce provedla organizace BSA anketu[90], které se zúčastnilo 300 manažerů z řad malých firem. Anketa odhalila následující skutečnosti:

[84] Dostupnost z World Wide Web: http://www.stahuj.centrum.cz/utility_a_ostatni/antiviry/kompletni/avast/, 7.6.2010

[85] Dostupnost z World Wide Web: www.avast.com, 7.6.2010

[86] Dostupnost z World Wide Web: www.adobe.com, 7.6.2010

[87] Dostupnost z World Wide Web: www.corel.com, 7.6.2010

[88] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[89] Dostupnost z World Wide Web: www.autodesk.cz, 7.6.2010

[90] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

Více než polovina respondentů, přesněji 53 procent, nevěděla, kdo je ve firmě za software zodpovědný.

Další polovina, přesněji 56 procent, uvedla, že se doposud nezajímala o to, jak se softwarem správně hospodařit.

Vzhledem k těmto údajům, které nám tato analýza nabízí, můžeme usoudit, že někteří manažeři firem nejsou ochotni aktivně kontrolovat, jaký software firma užívá. Záměrně píši slovo někteří, jelikož anketa se zaměřila na manažery z malých firem a já bych nerad říkal, že takový přístup uplatňují všichni. Tito manažeři jsou tak vystaveni riziku postihu, a proto BSA doporučuje všem manažerům těchto firem položit si následující čtyři otázky:

- Kdy byla naposledy provedena kontrola licencí? Zde je třeba říci, že pokud firma provádí pravidelný kontrolní audit, neměl by být problém v doložení těchto údajů.
- Kdo má oprávnění instalovat programy a kdo za případné nežádoucí instalace ponese odpovědnost? Zde bych chtěl podotknout, že toto oprávnění by měl mít pouze administrátor sítě, jelikož právě on je zodpovědný za to, že jsou v počítačích všechny programy nainstalovány legálně, s platnou licencí. Pokud by přišla kontrola, byl by to právě administrátor, který by stanul před soudem.
- Existují závazná pravidla pro využívání výpočetní techniky a internetu?
- Mají zaměstnanci v pracovní smlouvě definovánu spoluodpovědnost za užívání softwaru a výpočetní techniky vůbec?

Pokud na nějakou otázku manažer firmy nebude znát odpověď, BSA doporučuje ve vlastním zájmu vzniklou situaci řešit. Existuje totiž reálné riziko, že je firma v ohrožení. To, že by každý manažer neměl tuto situaci podceňovat, dokládá i prohlášení Jana Hlaváče: „Každým rokem roste počet oznámení na firmy projektující pomocí nelegálně užívaného softwaru. Stojí za nimi většinou firmy, které si naopak licence poctivě kupují.“[91] Slova Jana Hlaváče, který, jak jsem již zmínil, je tiskový mluvčí BSA,

[91] Citace z analýzy, která je dostupná na World Wide Web: www.bsa.org, 7.6.2010

potvrzuje i tento[92] článek, ve kterém se uvádí, že největší obavy mají manažeři firem právě z toho, že budou udáni svými zaměstnanci, které propustili. Manažeři si totiž uvědomují, že pokud se u nich prokáže používání nelegálního softwaru jsou spoluodpovědní za vzniklou dost nepříjemnou situaci.

Jan Hlaváč také dodal: ”Při vyšetřování dotyční manažeři obvykle tvrdí, že o ničem nevěděli, případně se vymlouvají na pochybení kolegů. To je ale zodpovědnosti nezbavuje.“[93]. Toto jednání svědčí o tom, že jakmile jde o nepříjemnou situaci, manažeři se nebojí svoji vinu přenést na své zaměstnance. Manažer je však právě ten, který úkoly dává a kontroluje. Proto i zaměstnanci by měli být obezřetní, protože trestní stíhání je vedeno i proti tomu, kdo se na pirátství podílel nepřímo. Tuto skutečnost uvádí článek[94], ve kterém se mimo jiné píše také o tom, že o míře, odpovědnosti a výši trestu rozhoduje soud. Jan Hlaváč k tomu dodal: „Ten může uložit vysoké peněžité tresty, nařídit propadnutí věci, či dokonce uložit trest odnětí svobody až do výše pěti let.“[95] Na základě tohoto tvrzení můžeme říci, že užívat nelegální software se skutečně nevyplácí. K výši peněžitých trestů Jan Hlaváč dodal: „Náhrady škod způsobeným výrobcům softwaru se mohou vyšplhat do závratných výší. Poškození výrobci se totiž mohou domáhat vysokých finančních kompenzací až ve výši dvojnásobku ceny nelegálně užívaného softwaru. Velmi často se tak odškodnění vyšplhá i přes milion korun.“[96] Na základě tohoto tvrzení můžeme vidět, že kvůli nelegálně používanému softwaru může jakákoliv firma, která tak činí, mít velké finanční problémy a kromě toho může být pošpiněno její dobré jméno. Od toho se pak odvíjí další skutečnosti, které pak mohou způsobit její zánik nebo krach.

Ideální je podle BSA podniknout technická a administrativní opatření, která nelegální software pomůžou z pracoviště odstranit. Jedna z možností podle BSA, ke které se přikláním také já, je provádět pravidelný softwarový audit, díky kterému můžeme pře-

---

[92] Dostupnost z World Wide Web: http://www.itpoint.cz/zprava/?i=propusteni-zamestnanci-podavaji-udani-na-byvale-zamestnavatele-3831

[93] Dostupnost z World Wide Web: http://www.eprofil.cz/tag/hr/, 7.6.2010

[94] http://www.czechcomputer.cz/art_doc-CFA41FF76D665623C1257520002FE20A.html, 7.6.2010

[95] Citace dostupná z analýzy, která je uveřejněna na World Wide Web: www.bsa.org, 7.6.2010

[96] Citace dostupná z analýzy, která je uveřejněna na World Wide Web: www.bsa.org, 7.6.2010

dejít velkým nepříjemnostem ze strany proti pirátských organizací, a navíc manažeři firem zamezí problémům, které můžou díky častým kontrolám předejít. O tom, co je to softwarový audit, proč ho provádět a jaké výhody z toho plynou, si povíme v následující kapitole.

## 3.4 Softwarový audit

V této kapitole bych se chtěl věnovat blíže softwarovému auditu. Myslím si, že pro firmy, které pracují se softwarovými programy, je softwarový audit záležitostí, která by se neměla podceňovat, a proto této problematice věnuji dostatečnou pozornost.

Na úvod bych začal s vysvětlením pojmu, co je vlastně softwarový audit, přičemž vycházím z definice, která je dostupná na www stránkách. Tak tedy „Softwarový audit znamená, inventarizace veškerého nainstalovaného softwaru a doložení dokladů, které potvrzují jeho legální nabytí“.[97]

Pro přiblížení problematiky softwarového auditu uvádím přepis z těchto www stránek[98]. Dříve či později nastane okamžik, kdy každá firma, která se chce vyhnout případným nepříjemnostem ze strany proti pirátských organizací, začne provádět právě softwarový audit. V počáteční fázi je třeba si uvědomit, že v počítačích té dané firmy se může vyskytovat nelegální software. Jeden z důvodů, proč tomu tak je, může být například ten, že uživatel si software nainstaloval jen z toho důvodu, aby si ho vyzkoušel, a v současné době již tyto programy nevyužívá. V počítači se tak nachází spousty různých souborů, u nichž nemusí být zcela jasné, ke kterému softwarovému programu patří. Tato situace je chaotická, a proto se v takovém případě doporučuje provést kompletní formát disků počítače a provést novou instalaci operačního systému. V okamžiku, kdy na počítač instalujeme nově operační systém a různé další programy, musíme samozřejmě mít patřičné licence. Po splnění této podmínky si můžeme založit evidenci k tomuto počítači.

[97] Dostupnost z World Wide Web: http://www.soom.cz/index.php?name=articles/show&aid=453, 7.6.2010

[98] Dostupnost z World Wide Web: www.soom.cz, 7.6.2010

List, ve kterém máme napsaný soupis všeho hardwaru a dalších aplikací, říkáme pasport. V Paspartu uvádíme soupis a veškerého softwaru, který je na počítači nainstalován. K evidenci můžeme připojit i další důležité náležitosti, jako například kopie pořizovacích dokladů nebo výtisky licenčních smluv. Tímto krokem bychom měli získat přehled o auditovaném počítači. V okamžiku, kdy na tomto počítači dojde k instalaci dalšího softwaru, bychom neměli zapomenout tento software připsat do evidence. Softwarový audit by se měl provádět minimálně jednou do jednoho roku. V další fázi pak stačí jen porovnat aktuálně nainstalovaný software s evidencí námi vytvořenou a dohledáme případné doklady v případě, že se v počítači bude vyskytovat software, který není zapsán v naší evidenci, nebo z počítače odstraníme zjištěné nelegální kopie. Tomuto kroku se říká narovnání licencí. Pokud chceme provést plánovaný softwarový audit, je vhodné to tento audit oznámit zaměstnancům firmy předem.

Samozřejmě i tento krok má své opodstatnění. Mnoho zaměstnanců raději samo před plánovaným auditem odinstaluje všechen software, který se na počítači nachází nelegálně. Samozřejmě, že i na internetu jsou programy[99], které nám mohou softwarový audit usnadnit, a to takovým způsobem, že provedou kontrolu počítače a zinventarizují veškerý hardware a software na auditovaném počítači, nebo na všech počítačích, které jsou v síti.

Co se týče nelegálního softwaru, pokud se stane, že v nějaké firmě dojde k policejní kontrole, je zcela logické, že zaměstnanci firmy neví, jak je možné, že právě na jejich počítači je software nelegálně. Takové situaci se dá samozřejmě předejít a to díky správci sítě. Tento člověk je ve firmě velice důležitý, protože je to právě on, kdo může nastavit oprávnění pro jednotlivé uživatele. Zaměstnanci firmy by v žádném případě neměli mít práva administrátora a díky tomu by ztratili možnost na počítač cokoliv instalovat. Druhou věcí je vlastnictví tajných hesel každého firemního zaměstnance, díky kterým by se dostávali do systému. Po zavedení tohoto kroku ve firmě by se pak zaměstnanci nemohli vymlouvat na to, že mohl software do počítače nainstalovat jiný zaměstnanec. Myslím si, že i zaměstnanci musí mít v tomto směru určitou zodpovědnost a nebrat nic na lehkou váhu. Dalším důležitým krokem je podepsání protokolu o převzetí hardware s nainstalovanými programy. Tento protokol by byl podepsán všemi zaměstnanci. Může jít například o výše zmíněný evidenční list, kde je veškerý software

[99] Dostupnost z World Wide Web: http://global.bsa.org/zeptejtesesam/04_00.cfm, 7.6.2010

i s licenčními čísly uveden. Je velice důležité nezapomenout na to, aby na předávacím protokolu byl vyjmenován i software s free licenční politikou. I toto jednání má svůj důvod. Pracovníci firmy by se mohli vymlouvat na to, že v počítači byl nainstalován i jiný software, než jen ten, který podpisem přebírali. Firmy by také měly trvat na tom, aby byli všichni zaměstnanci proškoleni, co si mohou a naopak nemohou dovolit, a podepsat o provedeném školství protokol. Na řadu tedy přichází samotný softwarový audit, který odhalí případné porušení zákazů ze strany zaměstnanců. Je také třeba říci, že softwarový audit by neměl být pravidelný, například v určité dny nebo měsíce. Mělo by spíše jít o neočekávanou událost. Pokud by se tak nestalo, zaměstnanci si této skutečnosti, že softwarové audity se konají například každý měsíc, brzy všimli a z daného počítače odstranili například nelegálně nainstalovaný software, který by po skončení auditu opět nainstalovali do počítače. V tomto případě by tyto audity ztrácely smysl.

Je také důležité, aby správce sítě měl plnou podporu vedení. Právě vedení musí souhlasit s popsanými kroky a i samo vedení musí tyto kroky dodržovat. Vedení by mělo vyžadovat po každém pracovníkovi ve firmě, aby se dodržovala stanovená pravidla, a pracovníky, kteří se proviní, spravedlivě potrestat. Pokud se firmě podaří tyto kroky využívat efektivně v praxi, nemusí se firma bát postihu ze strany proti pirátských organizací. Mnohem důležitější je ale fakt, že pokud budou pravidla skutečně dodržována, pak si žádný pracovník nedovolí instalovat nelegální software, a tím ohrozit nejen sebe, ale i manažery firmy.

Další výhodou, které používání těchto pravidel přináší, je i fakt, že pokud na nás například bývalý zaměstnanec pošle policejní kontrolu, manažeři firem se jí nemusejí obávat, protože provedli všechny potřebné kroky k tomu, aby zabránili používaní a šíření nelegálního softwaru ve firmě. Díky těmto skutečnostem se z pravidelného softwarového auditu stane činnost, která správci IT nezabere mnoho času.

## 3.5 Čím dokladovat legální nabytí software

Opět zde uvádím přepis z www stránek[100], Nejdůležitějším dokladem o tom, že jsme software nabyli legálně, je faktura nebo jiný doklad, který je vystavený prodejcem toho určitého softwaru. S pomocí tohoto dokladu dokážeme legální nabytí softwaru. Tyto doklady by měly být pečlivě uschovány, protože dokazují, že máme vše legálně. Tohoto by si měli být vědomy jak společnosti, ve kterých se pracuje s výpočetní technikou, tak fyzické osoby, které podnikají na vlastní zodpovědnost. Na tuto skutečnost by také myslet firmy, které mají stanovené, že je povinností uschovávat daňové doklady pouze po dobu pěti let. Po uplynutí této lhůty totiž dochází ke skartaci těchto důležitých dokladů. Pokud se stane situace, kdy by došlo ke skartaci dokladů, díky kterým bychom prokázali jejich legální nabytí, musíme pamatovat vždy na to, že bez nich se nám bude legálnost softwaru prokazovat jen velice těžko, a navíc pokud se stane, že tyto doklady nenajde ani dodavatel, tak firma bude muset zakoupit software podruhé.

Znamená to, že firma přijde o peníze jen proto, že její pracovníci nebyli schopni dohledat důležité doklady. Zcela jiná situace nastane, pokud provedeme upgrade[101]. Definici tohoto slova můžeme najít na internetu, tedy že upgrade je termín, který označuje výměnu výrobku za novější verzi téhož produktu. Jestliže firma pořizuje k některým svým programům upgrade, pak je pro ni důležité uschovat doklady nejen od koupě tohoto upgradu, ale zároveň musí firma dokladovat legální nabytí předchozí verze, kterou v současné době právě díky upgrade nepoužívá, ale díky ní měli například nárok na slevu v rámci upgrade. Pokud se nyní zaměříme na OEM licence[102], které je možné až na výjimky pořídit pouze s novým hardwarem, pak bychom neměli zapomínat na to, aby byl veškerý OEM software uveden na kupním dokladu tohoto hardwaru. Zde je nutné si uvědomit, že nestačí, aby bylo na dokladu například napsáno, že předmětem koupě je například počítač LINX společně s nainstalovaným hardwarem. Pracovník firmy vždy musí trvat na tom, aby byly na dokladu tyto skutečnosti:

---

[100] Dostupnost z World Wide Web: http://www.soom.cz/index.php?name=articles/show&aid=448, 7.6.2010

[101] Dostupnost z World Wide Web: www.wikipedia.org, 7.6.2010

[102] OEM verze je taková verze produktu, která není určená k přímému prodeji

- **přesný název programu,**
- **o jakou verzi tohoto programu se jedná,**
- **jaká je jazyková mutace tohoto programu.**

Správně vypsaný doklad by měl podle článku, který se nachází na těchto www stránkách,[103]vypadat následovně: „Uvedený hardware je dodán společně s nainstalovaným operačním systémem OEM MS Windows XP professional CZ.“[104] OEM verze softwaru jsou vázány na hardware, se kterým byly pořízeny. Často se na skříň počítače lepí štítek, kde je napsáno, že hardware počítače je dodávaný s OEM verzemi programů.

Pokud ve firmě dochází k odpisům tohoto hardware, firma společně s ním musí vyřadit i OEM software, který je uvedený na prodejním dokladu k hardwaru. V žádném případě se ve firmě nemůže stát, že například její pracovník vezme verze OEM programů a nainstaluje je na jiný hardware. Pokud by totiž ve firmě probíhala kontrola o legálnosti a bylo by zjištěno, že OEM verze softwaru jsou nainstalovány na jiném hardwaru, než který je uvedený na nabývacím dokladu s příslušným softwarem, pak by se bohužel pro firmu tato kopie brala jako kopie nelegální. Z této kapitoly tedy vyplývá, že firma by vždy měla trvat na tom, aby byl seznam veškerého softwaru, který je dodán společně s hardwarem, uveden na dokladu o koupi. Toto opatření a pozornost k těmto věcem se firmě vyplatí, protože v případě kontroly nenastanou žádné nepříjemnosti, které by mohly firmu, popřípadě pracovníky ohrozit.

Další věcí, o které se autor zmiňuje v tomto článku,[105]jsou počítače, které čekají na vyřazení, které přestaneme používat. Zde je důležité si uvědomit, že software, který byl používaný na počítači, který čeká na vyřazení, nainstalujeme na počítač nový, nesmíme zapomenout odinstalovat software na starém počítači. Tento krok má zajisté také svůj důvod. Pokud se stane, že přijde kontrola, nebude jí v žádném případě zajímat, že počítač někde v koutě místnosti čeká na vyřazení, a software nainstalovaný v něm bude kontrola považovat za nelegální.

---

[103] Dostupnost z World Wide Web: http://www.soom.cz/index.php?name=articles/show&aid=448, 7.6.2010

[104] Citace dostupná z World Wide Web: www.soom.cz, 7.6.2010

[105] Dostupnost z World Wide Web: http://www.soom.cz/index.php?name=articles/show&aid=448, 7.6.2010

## 3.6 Důvody pro softwarový audit

Softwarový audit je pro firmy, které pracují se softwarem, zcela klíčová věc, která by se neměla nikdy podceňovat. Každá firma by měla myslet na nejhorší a považovat policejní kontrolu za zcela reálnou věc. Pro příklad uvádím jeden z odstrašujících případů, který se odehrál v květnu roku 2006: „Byla uzavřena nová mimosoudní dohoda s jednatelem společnosti užívající nelegální software. Ve středně velké společnosti ze severní Moravy byl v 19 počítačích užíván nelegální software společnosti Microsoft a Autodesk. Jednatel, který byl v této souvislosti obviněn, se na BSA obrátil s prosbou o ukončení případu mimosoudní cestou. Na základě dohody je společnosti povinna zakoupit legální software, který potřebuje pro svou podnikatelskou činnost, v hodnotě 320 tisíc korun. Společnost také nahradí škodu ve výši 250 tisíc korun".[106] Na základě této zprávy můžeme vypozorovat několik skutečností První z nich je například ta, že když už dojde k policejnímu zásahu, tak se dotyčné osoby snaží urovnat celý spor mimosoudní cestou, protože nikdo z nich nechce mít záznam v rejstříku trestů. Druhou skutečnosti je fakt, že firma vždy musí nahradit škodu.

Tato škoda se pohybuje v řádech desítek tisíc korun a poškozené společnosti samozřejmě požadují náhradu v plné výši. Tato finanční ztráta může firmu, která čelí takovému obvinění, zcela odrovnat. Softwarový audit má navíc tu výhodu, že pokud bude provádět preventivní softwarový audit firma sama od sebe, bude vždy na policejní kontrolu připravena a nebude se muset bát případných sankcí, které by ji mohly ohrozit nebo úplně zničit. Zvláště velký pozor by si měli dávat správci IT, protože jsou to právě oni, kdo nesou plnou zodpovědnost za nainstalovaný software ve firmě, a pokud si na své počítače nainstalují nelegální software sami zaměstnanci, s nejvyšší pravděpodobností stane před soudem právě správce informačních technologií. Z mého pohledu jsou výše uvedené důvody dostačující k tomu, aby firmy prováděly pravidelný softwarový audit.

[106] Dostupnost z World Wide Web: na http://www.legalne.cz/nightmare/, 7.6.2010

## 3.7 Policejní zásah

Jestliže se věnujeme problematice softwarového pirátství, nemohu se nezmínit také o tom, jak probíhá policejní zásah ve firmě. K policejnímu zásahu dochází ve chvíli, kdy je podáno trestní oznámení. Trestní oznámení může podat kdokoliv, nejčastěji je to však proti pirátská organizace BSA, a to po obdrženém udaní nebo při podezření na trestnou činnost. V naprosté většině případů se jedná o zásah, který kontroluje legálnost softwarových programů ve firmách. K provedení policejní kontroly je potřeba tolik policistů, kolik je ve firmě počítačů. Příslušník policie odpojí počítač od sítě a za pomoci specializovaného programu začne shromažďovat informace o tom, jaký software je na tom konkrétním počítači nainstalován. Někdy se při policejní kontrole stane, že počítač může být odvezen do kriminalistického ústavu. Stává se tak v případech, kdy kontrola na místě není možná. Z tohoto důvodu se nemusejí policejního zásahu zase až tak bát velké firmy, neboť v těchto firmách se nachází velké množství počítačů. Nejsnadnějším cílem se tak stávají firmy, které mají například dvacet počítačů. Je samozřejmostí, že při těchto kontrolách má policie soudní povolení a na základě tohoto povolení má policie možnost kontrolovat pouze ty počítače, které jsou ve vlastnictví kontrolovaného subjektu. Znamená to, že pokud bych například já měl ve firmě, která je kontrolována policejními orgány, svůj osobní počítač, nemůže policie přistoupit k jeho kontrole. V okamžiku, kdy policie skončí se soupisem nainstalovaného softwaru, je nález předán soudnímu znalci k vyhodnocení. Na majiteli počítačů je, aby doložil legalitu zjištěného softwaru v těchto počítačích.

Pokud nastane situace, kdy se v počítačích najde software, u kterého majitel počítače nedoloží jeho legální nabytí, pak policie vyzývá autory softwaru, aby přistoupili k vyčíslení škody. V tomto okamžiku má pachatel poslední šanci, kterou může využít k tomu, aby se pokusil se mimosoudně vyrovnat s poškozenou stranou. Tato varianta je pro pachatele výhodnější, než soudní spor, který může trvat roky. Očekává se, že v blízké budoucnosti budou moci legalitu softwaru ve firmách kontrolovat i finanční úřady. V současné době probíhají první školení těchto úředníků. Při zpracování této kapitoly jsem vycházel z tohoto článku[107].

[107] Dostupnost z World Wide Web: http://www.soom.cz/index.php?name=articles/show&aid=442, 7.6.2010

## 3.8 Tresty pro firmy s nelegálním softwarem

V únoru v roce 2010, tedy v době zpracovávání této bakalářské práce, vyšel tento článek[108]. V tomto článku se uvádí, že kompenzace, kterou mohou poškození výrobci softwaru vymáhat po pachatelích, činí 240 tisíc korun. Tato výše kompenzace byla platná v roce 2009. Podle informací v tomto článku[109] však v tomto roce, tedy v roce 2010, mohly tyto tresty být až dvojnásobné, tedy kompenzace, které mohou po pachatelích poškození výrobci softwaru vymáhat, by činila 480 tisíc korun. Samozřejmě, že článek se odvolává na to, že takové postihy hrozí všem uživatelům, kteří používají nelegální software proti pirátská organizace BSA. Podle tohoto článku výše kompenzace pravděpodobně vzrostla z toho důvodu, protože výrobci softwaru, kteří stojí na straně poškozených, si chtějí uplatnit své právní nároky v plné výši. Navíc tím, že se firmy vyrovnají s poškozenými, neznamená, že si zaplatili software, který používají, ten musí zakoupit znovu. Kontroly budou probíhat také na internetu, protože internet je místem, kde se softwarové pirátství stalo organizovaným zločinem. Lidé, kteří dělají takové podvody, nabízejí různé možnosti plateb, a to i se zákaznickou podporou.

Tento kradený, nelicencovaný software tito lidé prodávají pomocí falešných internetových obchodů a také přes aukční portály, jako je například eBay[110].To, že si i samotní uživatelé, kteří si software prostřednictvím těchto aukčních síní koupili, neví rady s tím, zda je tento zakoupený software legální, dokazuje i fakt, že počet dotazů na toto téma prostřednictvím proti pirátské infolinky se během roku zvýšil o 27 procent. S tím, že volající se nejvíce táží na to, jak poznat, zda je jejich software legální. Podle BSA[111] se šíří internetem vysoké množství nelegálního softwaru. Například v roce 2009 tato organizace během šesti měsíců identifikovala na výměnných sítích nelegální software v hodnotě 18 miliard korun ( myšleno

[108] Dostupnost z World Wide Web: http://www.businessinfo.cz/cz/clanek/unor-2010/2010-firem-stihanych-software-piratstvi/1001903/56286/, 7.6.2010

[109] Dostupnost z World Wide Web: http://www.zive.cz/bleskovky/bsa-opet-hrozi-pokuty-za-piratstvi-se-vysplhaji-na-dvojnasobek/sc-4-a-150808/default.aspx, 7.6.2010

[110] eBay je nejznámější americká internetová aukční síň. Zdroj www.wikipedia.org

[111] Dostupnost z World Wide Web: www.bsa.org

v celosvětovém měřítku ). Podle tohoto článku[112] se hodnota pirátského softwaru počítá podle následujícího vzorce:

**Hodnota ztrát z pirátského softwaru = (výnosy z legálního softwaru) / (1 - koeficient pirátství) – výnosy z legálního softwaru.**

- Přičemž autor výše zmiňovaného článku, kterým je Jan Handl, tvrdí: „Hodnota ztrát kvůli pirátům by tedy měla reprezentovat ztráty způsobené celému odvětví, mezinárodním i lokálním prodejcům softwaru“[113].

Na základě analýz, které provádí firma IDC[114] a které následně prezentuje každoročně proti pirátská organizace BSA[115], lze jasně vidět, že softwarové pirátství má značný vliv na ekonomiku v České republice, a to více, než by se mohlo zdát. I když se v České republice podařilo za posledních patnáct let snížit míru softwarového pirátství o 29 procentních bodů, na což poukazuje tento článek,[116] stále je před námi ještě dlouhá cesta k tomu, aby se zde situace zlepšila.

[112] Dostupnost z World Wide Web: http://www.lupa.cz/clanky/softwarove-piratstvi-v-cr-problem-ci-prilezitost/

[113] Dostupnost z World Wide Web: http://www.lupa.cz/clanky/softwarove-piratstvi-v-cr-problem-ci-prilezitost/, 7.6.2010

[114] Dostupnost z World Wide Web: www.idc.com, 7.6.2010

[115] Dostupnost z World Wide Web: www.bsa.org, 7.6.2010

[116] Dostupnost z World Wide Web: http://computerworld.cz/aktuality/bsa-podil-piratskeho-softwaru-v-cr-klesl-na-37-6654,7.6.2010

# 4 Softwarové pirátství a právo

Jak jsem se zde již zmínil, softwarové pirátství je zločin, za který mohou být potrestáni ti, kteří se ho dopustí. V této kapitole bych se chtěl jen okrajové dotknout některých zákonů, které souvisejí s touto problematikou, a stručně zde ukázat, jaké tresty hrozí těm, kteří poruší tato práva.

Asi první velikou změnou je, že trestní zákon č.140/1961 Sb. pozbyl účinnosti a nahradil ho trestní zákoník, a to konkrétně 1. 1. 2010. V trestním zákoně č.140/1961 Sb., který tedy již neplatí, řešil věci týkající se trestů za softwarové pirátství paragraf 151 a 152.

V novém trestním zákoníku č. 40/2009 Sb. řeší tyto věci paragraf 270. Tento paragraf říká, že „kdo neoprávněně zasáhne nikoli nepatrně 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, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“[117]

Dále se zde mluví o dalších trestech a o jejich výši za splnění určitých podmínek. „Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo

propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí- li tím jinému značnou škodu, nebo

c) dopustí-li se takového činu ve značném rozsahu.“[118]

[117] Trestní zákoník č. 40/2009 Sb. Dostupnost z World Wide Web: http://www.legalne.cz/zakony/, 7.6.2010

[118] tamtéž., 7.6.2010

„Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu.“[119] Zde je vidět, že v nejhorším možném případě může pachatel dostat až osm let vězení. Nejmírnější trest je tedy dva roky vězení, propadnutí věci nebo jiné majetkové hodnoty.

„V okamžiku, kdy počítačový program splňuje základní znaky autorského díla, podle definice autorského zákona, je autorským zákonem i chráněn.“[120]

Pro upřesnění ještě dodávám, že v licenčních smlouvách nám autor sděluje způsob, jak s jeho programem můžeme nakládat. Pro úplnost dodám, že jde o autorský zákon č. 121/2000 Sb. Ve své bakalářské práci budu řešit konkrétně hlavu VI, kde jsou zaznamenány správní delikty. Blíže se tedy podíváme na paragraf 105 a – 105 c. Paragraf 105 a řeší přestupky fyzických osob a pokuty za tyto přestupky. Paragraf 105 b pojednává o správních deliktech právnických a podnikajících fyzických osob a následně pokuty za tyto správní delikty. Posledním je paragraf 105 c. Zde se pojednává o společných ustanoveních.

## 4.1 Paragraf 105a – Přestupky

„Fyzická osoba se dopustí přestupku tím, že:

a) neoprávněně užije autorské dílo, umělecký výkon, zvukový či zvukově obrazový záznam, rozhlasové nebo televizní vysílání nebo databázi,

b) neoprávněně zasahuje do práva autorského způsobem uvedeným v § 43 odst. 1 nebo 2 anebo v § 44 odst. 1, nebo

c) jako obchodník, který se účastní prodeje originálu díla uměleckého, nesplní oznamovací povinnost podle § 24 odst. 6.

[119] tamtéž., 7.6.2010

[120] http://www.legalne.cz/zakony/, 7.6.2010

Za přestupek podle odstavce 1 písm. a) lze uložit pokutu do 150 000 Kč, za přestupek podle odstavce 1 písm. b) pokutu do 100 000 Kč a za přestupek podle odstavce 1 písm. c) pokutu do 50 000 Kč“.[121]

## 4.2 Paragraf 105b – Správní delikty právnických a podnikajících fyzických osob

„Právnická nebo podnikající fyzická osoba se dopustí správního deliktu tím, že:

a) neoprávněně užije autorské dílo, umělecký výkon, zvukový či zvukově obrazový záznam, rozhlasové nebo televizní vysílání nebo databázi,

b) neoprávněně zasahuje do práva autorského způsobem uvedeným v § 43 odst. 1 nebo 2 anebo v § 44 odst. 1, nebo

c) jako obchodník, který se účastní prodeje originálu díla uměleckého, nesplní oznamovací povinnost podle § 24 odst. 6.

Za správní delikt podle odstavce 1 písm. a) se uloží pokuta do 150 000 Kč, za správní delikt podle odstavce 1 písm. b) pokuta do 100 000 Kč a za správní delikt podle odstavce 1 písm. c) pokuta do 50 000 Kč“.[122]

## 4.3 Paragraf 105c – Společná ustanovení

„Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. Při určení výměry pokuty se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán. Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení

[121] autorský zákon č. 121/2000 Sb. Dostupnost z World Wide Web: http://www.legalne.cz/zakony/, 7.6.2010

[122] autorský zákon č. 121/2000 Sb. Dostupnost z World Wide Web: http://www.legalne.cz/zakony/, 7.6.2010

do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.“[123]

Správní delikty podle tohoto zákona v přenesené působnosti projednává v prvním stupni obecní úřad obce s rozšířenou působností, v jehož územním obvodu byl správní delikt spáchán.

„Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby nebo v přímé souvislosti s ním, se vztahují ustanovení zákona o odpovědnosti a postihu PO. Pokuty vybírá a vymáhá orgán, který je uložil. Příjem z pokut je příjmem rozpočtu, ze kterého je hrazena činnost orgánu, který pokutu uložil.“[124]

[123] Citace dostupná z World Wide Web: http://www.legalne.cz/zakony/, 7.6.2010

[124] autorský zákon č. 121/2000 Sb. Dostupnost z World Wide Web: http://www.legalne.cz/zakony/ 7.6.2010

# 5 Vybrané možnosti omezení softwarového pirátství

Myslím si, že softwarové pirátství je problém, který se řeší velice obtížně. Avšak podle mě existují určitá řešení, která by dokázala snížit míru softwarového pirátství v České republice. V první řadě bych zpřísnil kontroly firem. Kontroly by měly být časté, a měly by probíhat po celé České republice. Tyto opatření by vedly k tomu, že by si uživatelé nelegálních softwarových programů uvědomili, že jim to také nemusí projít a některé z nich by to určitě motivovalo k tomu, aby si legální software pořídili. Samozřejmě, aby myšlenka uvedená výše mohla fungovat, je třeba vytvořit účinné mechanismy vymáhání práva. Dále bych zpřísnil kontroly na tržnicích a trestal prodejce, kteří touto činností získávají peníze na úkor druhých. Také by se měly zpřísnit kontroly na internetu, na různých aukčních portálech typu aukro, Bay podobně. Myslím si, že i vlády, které těží z ekonomických výhod plynoucích ze snižování míry softwarového pirátství, by měly aktualizovat zákony chránící duševní vlastnictví tak, aby reflektovaly standardy Světové organizace pro ochranu duševního vlastnictví. Na řešení tohoto problému je také třeba vyčlenit patřičné peněžní zdroje. V poslední řadě bych organizoval přednášky na základních, středních, ale i vysokých školách, kde by představitelé proti pirátských organizací přednášeli o tomto problému. Vzdělání bych též zajistil i pro veřejnost.

Samozřejmě jsem si vědom toho, že tato opatření nebude možné vytvořit hned, chce to začít postupně a mít dostatek času na to, aby se vše mohlo realizovat. Jak jsem již uvedl, nemyslím si, že se těmito kroky pirátství zcela vymýtí, protože nelegální kopie počítačových programů se šíří přes technologie, které jdou stále dopředu, a lidé jich samozřejmě budou využívat, ale mám za to, že tato opatření by byla mnohem účinnější a efektivnější než investice do různých proti pirátských ochran, které jsou většinou brzy prolomeny pirátskými skupinami.

# 6 Závěr

Softwarové pirátství je problémem naší společnosti a je opravdu obtížné této problém řešit. Vzhledem k tomu, že je možné technologicky sdílet soubory a tyto technologie jdou stále kupředu, myslím si, že je lidé budou využívat. Nakonec z nelegálního materiálu má nejvíce konečný uživatel, který si vše stáhne zadarmo.

Pirátství nahrává i fakt, že mezi mladými lidmi jde o zcela běžnou věc, která se neřeší. Přesto si myslím, že počítačové pirátství bude možné v budoucnu omezit, a to hlavně postupnou osvětou, přístupem držitelů autorských práv a také přístupem lidí samotných, kteří vezmou v úvahu fakt, že pirátství je prostě krádež a že i za software se musí platit. Myslím si, že boj proti pirátství není otázka pouze práva, protože tím se vše nevyřeší. Je třeba si uvědomit, že i majitelé autorských práv by měli hledat cesty k tomu, aby ceny jejich produktů nebyly tak drahé anebo pokud ano, tak aby byly přiměřené vzhledem k platům v České republice. Dále je potřeba, aby se majitelé autorských práv dokázali přizpůsobit dnešní době – musí hledat takové obchodní modely, díky kterým umožní uživatelům rychlý, snadný a hlavně legální přístup ke svým produktům. Mým cílem je ukázat, že i pirátství má vliv na ekonomiku v České republice. Především to dokazují i analýzy proti pirátské organizace BSA a analytické společnosti IDC. Myslím si, že je mnohem lepší hledat nové obchodní modely, díky kterým umožní uživatelům legální přístup ke svým produktům, než investovat velké částky do proti pirátských ochran, které jsou piráty velice brzy prolomeny. Podle mého názoru jsou to vyhozené peníze a tato cesta k ničemu nevede. Na jednu stranu chápu velké počítačové firmy, které se za každou cenu snaží chránit své produkty. Na druhou stranu i ony musí pochopit, že nikdy nezabrání tomu, aby se jejich produkty šířily volně ke stažení na internetu. Pokud výrobci softwarových programů chtějí změnu, myslím si, že je třeba pro ni také něco dělat. Jak už jsem zmiňoval na začátku, výsledek mé práce spočívá v tom, že jsem nastínil konkrétní řešení, která by podle mě pomohla ke snížení softwarového pirátství v České republice. Nepůjde však o jednoduchý proces.

# ANOTACE

| | |
|---|---|
| **Příjmení a jméno autora:** | Hanák Miroslav |
| **Instituce:** | Moravská vysoká škola |
| **Název práce v českém jazyce:** | Softwarové pirátství v České republice |
| **Název práce v anglickém jazyce:** | Software piracy in the Czech Republic |
| **Vedoucí práce:** | Dr. Jiří Dostál, Ph.D. |
| **Počet stran:** | 70 |
| **Počet příloh:** | 2 |
| **Rok obhajoby:** | 2011 |
| **Klíčová slova v českém jazyce:** | Softwarové pirátství, software, počítačoví piráti, warez, warez supiny, počítačová kriminalita, P2P sítě, bsa. |
| **Klíčová slova v anglickém jazyce:** | Software piracy, software, cybercriminals, warez, warez groups. peer-to-peer, business software aliance. |

Bakalářská práce Softwarové pirátství v České republice pojednává o problematice softwarového pirátství v podnicích a jeho vlivu na ekonomiku v České republice. Obsahem práce je vymezení pojmu softwarového pirátství a popis šíření počítačových programů. Dále je v práci blíže objasněn fenomén označovaný jako „warez“ se zaměřením zejména na historii a způsoby distribuce pirátského software. V další části se práce zabývá tím, jaké škody páchají piráti vydáváním nelegálního softwaru a jaký dopad to má na ekonomiku v České republice.

Bachelor Thesis Software piracy in the Czech Republic is about the problems of software piracy in business and its impact on the economy in the Czech Republic. The thesis is the definition of software piracy, and a description of the distribution of computer programs. The study also describes in detail the phenomenon known as "warez", focusing in particular on the history, methods of distribution of pirated software. In the

next part of the work deals with what kind of damage committed by illegal software piracy issue and what impact it has on the economy in the Czech Republic.

# Literatura a prameny:

1. CRAIG, P., *Softwarové pirátství bez záhad.* 1.vyd. Praha: Grada Publishing, 2008. ISBN: 978-80-247-1765-4.

2. ČERVEŇ, P., *Cracking a jak se proti němu bránit.* 1. vyd. Praha : Computer Press, 2002. ISBN: 80-7226-382-X.

3. FEDEROVIČOVÁ, I., *Kriminalistická stopa a softvérové pirátstvo.* In Zborník referatov "Mezinárodna konferencia Počítačová kriminalita", Bratislava : Bussines Software Aliance SR, 2000, str. 40.

4. KOLÁŘ, P., *Operační systémy* [online]. Liberec : 2005-02-01, [cit. 2010-06-07].

5. KŘÍŽ, J., a kol. *Autorský zákon – komentář a předpisy související.* 2.aktualizované vydání. Praha : Linde Praha, 2005, str. 179. ISBN: 80-7201-546-X

6. MATĚJKA, M., *Počítačová kriminalita.* Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 21. ISBN: 80-7226-419-2.

7. MAŤEJKA, M., *Počítačová kriminalita*. Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 17. ISBN: 80-7226-419-2.

8. MINÁRIK, T., *Počítačová kriminalita z pohledu trestního práva hmotného*, Rigorózní práce, Právnická fakulta Univerzity Karlovy 2007, s. 71.

9. SMEJKAL, V., Právo informačních a telekomunikačních systémů. Praha : C. H. Beck, 2004. ISBN: 80-7179-552-6

10. SUCHA, P., *Preverovanie a vyšetrovanie počítačovej kriminality*. In Zborník referatov "Mezinárodna konferencia Počítačová kriminalita", Bratislava : Bussines Software Aliance SR, 2000, str. 36.

## Internetové zdroje:

Dostupnost z World Wide Web:

http://www.legalne.cz/nightmare/

http://www.lupa.cz/clanky/v-cr-probiha-rozsahly-zatah-proti-uzivatelum-p2p-siti/

http://www.dolphin.cz/policie/brezen98/piratisoftwaru.html

www.making-a-difference.oorg/computer-crime-chronicles.html

ftp.arl.mil/mike/comphist/eniac-story.html

www.idc.com

www.bsa.org

http://www.webcrunchers.com/crunch

http://www.lupa.cz/clanky/v-cr-probiha-rozsahly-zatah-proti-uzivatelum-p2p-siti/

http://www.dsl.cz/clanek/1070-dalsi-hromadna-policejni-razie-v-domacnostech-kvuli-sdileni-na-dc

http://www.warez.cz/clanky/jak-pirati-ziskavaji-nove-tituly/

www.ijetpack.cz/index.php/clanky/37-hacking/49-co-je-to-hacking

http://www.symantec.com/cs/cz/norton/theme.jsp?themeid=botnet

www.warez.cz

www.ucime-se.kvalitne.cz/obr/mat/Slovnicek%20pojmu.doc

http://cs.wikipedia.org/wiki/Komer%C4%8Dn%C3%AD_software

http://cs.wikipedia.org/wiki/Shareware

www.ubi.com

http://tn.nova.cz/magazin/hry/novinky/ubisoft-upravil-protipiratskou-ochranu-ta-je-jiz-prolomena.html

http://tn.nova.cz/magazin/hry/novinky/ubisoft-upravil-protipiratskou-ochranu-ta-je-jiz-prolomena.html

http://cs.wikipedia.org/wiki/Licence

http://www.microsoft.com/cze/licence/ZakladniInformace/CojeLicence.mspx

http://www.e-komerce.cz/ec/ec.nsf/0/7fdcd0dd523a2bf9c1256c7100567eff

http://www.abcsys.cz/

www.deloitte.com

www.idg.com

http://podani.blog.respekt.cz/c/1760/Spoutana-hudba-aneb-je-DRM-spatne.html

www.wikipedia.org

http://technet.idnes.cz/konec-placene-hudby-na-internetu-ochrana-drm-prolomena-p1o-/tec_audio.asp?c=A060827_234634_tec_audio_kuz

www.symantec.com

www.adobe.com

www.avast.com

www.corel.com

http://www.stahuj.centrum.cz/utility_a_ostatni/antiviry/kompletni/avast/

http://cs.wikipedia.org/wiki/Open_Office

www.autodesk.cz

http://www.itpoint.cz/zprava/?i=propusteni-zamestnanci-podavaji-udani-na-byvale-zamestnavatele-3831

http://www.czechcomputer.cz/art_doc-CFA41FF76D665623C1257520002FE20A.html

www.soom.cz

http://www.soom.cz/index.php?name=articles/show&aid=453

http://global.bsa.org/zeptejtesesam/04_00.cfm

http://www.soom.cz/index.php?name=articles/show&aid=448

http://www.soom.cz/index.php?name=articles/show&aid=448

http://www.soom.cz/index.php?name=articles/show&aid=448

http://www.soom.cz/index.php?name=articles/show&aid=442

http://www.businessinfo.cz/cz/clanek/unor-2010/2010-firem-stihanych-software-piratstvi/1001903/56286/

http://www.zive.cz/bleskovky/bsa-opet-hrozi-pokuty-za-piratstvi-se-vysplhaji-na-dvojnasobek/sc-4-a-150808/default.aspx

http://computerworld.cz/aktuality/bsa-podil-piratskeho-softwaru-v-cr-klesl-na-37-6654

http://www.legalne.cz/zakony/

# 7 Seznam příloh

# PŘÍLOHY

**Softwarové pirátství**

Tento průzkum realizuji, abych zjistil, jaký je názor lidí na softwarové pirátství v České republice. Zároveň také zjišťuji, jak lidé v České republice vnímají softwarové pirátství. Všechny respondenty bych chtěl tímto uklidnit a zdůraznit, že se jedná o **anonymní** průzkum, ničeho se tedy nemusíte obávat, za vaše odpovědi Vám nic nehrozí.

1) Setkali jste se někdy ve vaší firmě se softwarovým pirátstvím?

☐ Ano ☐ Ne

2) Jestliže ano, jakou podobu mělo (stručně popište):

……..

……..

……..

3) Domníváte se, že je softwarové pirátství obhajitelné? Souhlasíte s ním (stručně popište)?

……..

……..

……..

4) Jsou dle Vás tresty v souvislosti se softwarovým pirátstvím adekvátní?

☐ Ano ☐ Ne

5) Co by Vás motivovalo k ohlášení softwarového pirátství?

……..

……..

……..

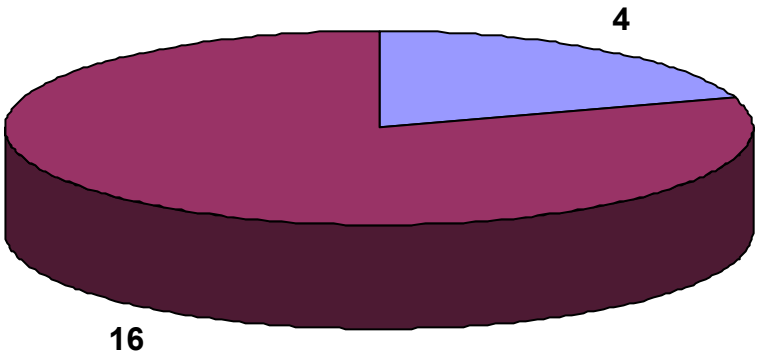
Tímto Vám chci poděkovat za Váš čas a odpovědi, které jsou uvedené v tomto dotazníku. Připomínám, že se jedná o **anonymní** průzkum.

## Výsledky průzkumu:

Tento průzkum, který se týkal softwarového pirátství je dalším z výstupů mé bakalářské práce. Průzkumu se zúčastnilo dvacet lidí a bylo jim položeno pět otázek, na které odpovídali. Průzkum ukázal, že šestnáct lidí z celkových dvaceti se ve firmě, kde pracující se nesetkali se softwarovým pirátstvím. Na další otázku tedy odpověděli čtyři lidé, kteří u první otázky napsali, že se setkali se softwarovým pirátstvím. Všichni čtyři dotázaní vypověděli, že byli svědky softwarového pirátství, které mělo formu nelegálně nainstalovaných softwarových programů s tím, že tyto nainstalované programy byly následně vypáleny na CD nebo DVD. Osmnáct dotázaných z celkových dvaceti nesouhlasí se softwarovým pirátstvím. Jeden z dotázaných si myslí, že pirátství obhájitelné je a poslední dotázaný neví. U Předposlední otázky si sedmnáct dotázaných myslí, že tresty, které souvisí se softwarovým pirátstvím jsou adekvátní, další dva dotázaní nevědí a poslední dotázaný si myslí, že jsou tresty za softwarové pirátství příliš vysoké. U poslední otázky se polovina dotázaných přiznala k tomu, že by je k ohlášení softwarového pirátství nemotivovalo vůbec nic, další dva dotázaní neví a zbylých osm by mělo své důvody, mezi které patří například pomsta zaměstnavateli, strach o ztrátu interních dat anebo si nepřejí, aby konkurenční firma byla ve výhodě jen proto, že si řádně nezakoupila licence daného softwarového produktu na rozdíl od ostatních firem.

1) Setkali jste se někdy ve vaší firmě se softwarovým pirátstvím?

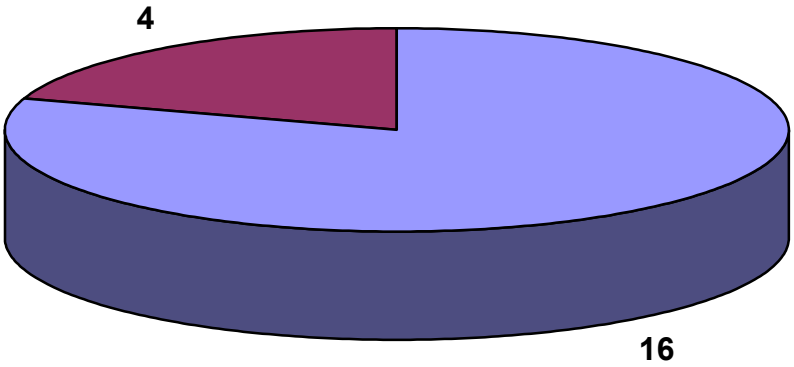
**4 dotázaní odpověděli kladně**




**16 dotázaných odpovědělo záporně**

## 2) Jestliže ano, jakou podobu mělo?

**4 dotázaní se setkali se softwarovým pirátstvím**
**a to ve formě nelegální instalace a následného vypálení těchto softwarových programů na CD a DVD**

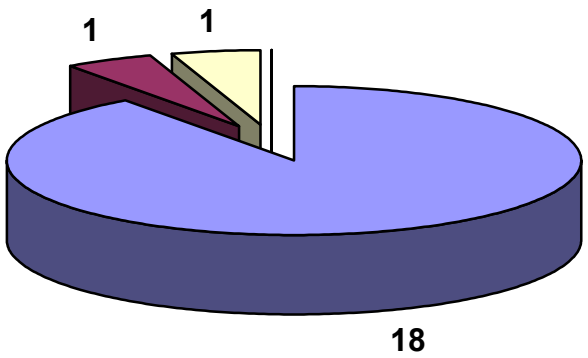



**16 dotázaných tuto otázku nezodpovědělo**

## 3) Domníváte se, že je softwarové pirátství obhajitelné?

**1 z dotázaných odpověděl, že neví**

**1 z dotázaných odpověděl, že softwarové pirátství naopak obhajitelné je**



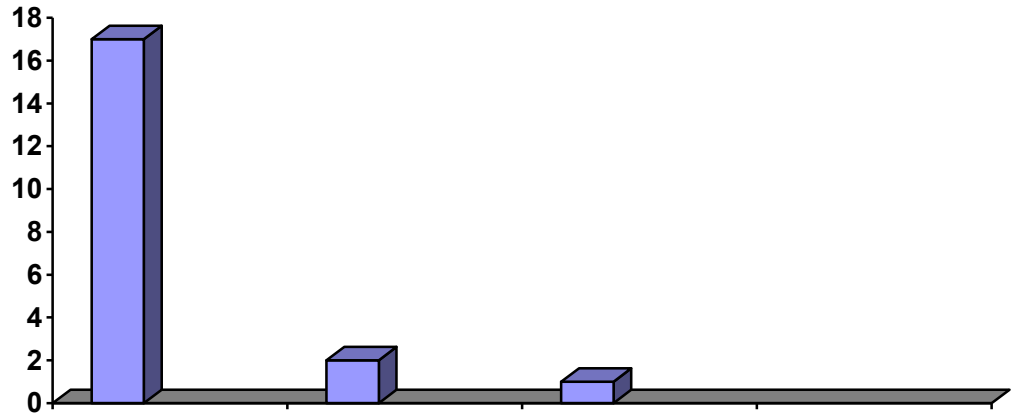

**18 dotázaných odpovědělo, že softwarové pirátství není obhajitelné**

## 4) Jsou podle Vás tresty v souvislosti se softwarovým pirátstvím adekvátní?

**17 dotázaných řeklo ano**

**2 dotázaní odpověděli, že nevědí**

**1 dotázaný odpověděl kladně**



# 5) Co by vás motivovalo k ohlášení pirátství?

**10 dotázaných odpovědělo, že je by nemotivovalo nic**

**2 dotázaní nevědí**

**8 dotázaných má své osobni důvody (např. pomsta zaměstnavateli)**