|  |
| --- |
|  |
| Seminární práce |
| Seminář z informatiky |
|  |
| **Právo ve výpočetní technice** |
|  |

|  |
| --- |
|  |

1. část

# Autorské právo

Jako u všeho, co se určitým způsobem setkává s filmy, hudbou a dalšími podobnými věcmi, i ve výpočetní technice je důležité autorské právo a vše s ním spojené. Je to odvětví práva, které se zabývá právními vztahy mezi uživateli a držiteli „autorských práv“ k danému dílu. Stát tímto poskytuje autorům určité zajištění návratnosti vynaloženého úsilí, kterého bylo třeba pro vytvoření tohoto díla. Toto právo nechrání samotné myšlenky či ideje, ale pouze konkrétní díla, tudíž umožňuje jeho interpretaci, která se může následně stát novým autorským dílem. V České republice je udáno autorským zákonem (zákon č. 121/2000 Sb.). Základním označením, že je dílo chráněno, je symbol © (z anglického „copyright“), který bývá následován rokem a jménem autora (či společnosti, která drží autorská práva) – toto označení ale není nutné a v mnoha zemích (například v ČR) plní spíše informativní význam. Ve výpočetní technice se autorské právo týká hlavně hudby, filmů a softwaru.

Jako u všeho zde můžeme rozlišit nelegální a legální přístup. Kromě těchto základních 2 opačných stran můžeme samozřejmě vyčlenit i něco mezi, což se většinou označuje jako „šedé jednání“ (případně „šedá zóna“).

Nelegální je hlavně šíření a obcházení ochran, které mají právě šíření zabránit. Do zmíněné „šedé zóny“ by se poté řadilo hlavně podporování a využívání těchto nelegálních praktik, což samo o sobě není nelegální, ale dalo by se přirovnat (při lehkém zveličení) ke koupi ukradeného auta.

## Filmy

Pokud se podíváme na nelegální činnost konkrétně s filmy, tak narazíme přesně na to, co říká obecná definice autorského práva – tedy šíření a obcházení ochran, které tomu mají zabránit. Jednou z těchto aktivit je tedy například natáčení filmů přímo v kině a jejich následné šíření. Takto získané filmy se většinou označují jako „kinoripy“ a bývají zpravidla horší kvality. Dotyčný se kromě porušení autorského práva zároveň proviňuje i proti smlouvě s pořadatelem kina, kterou uzavřel koupením lístku. Další aktivitou je poté obcházení ochran disků, jejich kopírování a šíření. Těmto filmům se poté většinou říká jednoduše „ripy“ a bývají většinou lepší kvality než „kinoripy“. Kromě nelegálních metod kopírování, které ochranu disku odstraňují (jako například nástroj AnyDVD), existují ale i legální řešení získání kopie, které jí pořizují tak, že ochranu neodstraňují, ale pouze ukládají vše, co se zobrazuje na obrazovce a co vychází ze zvukové karty. Následné šíření jiným osobám je ale nelegální vždy.

Do „šedé zóny“ v oblasti filmů můžeme zařadit samotné stahování filmů ze serverů jako například Ulož.to či Rapidshare.cz , kde právě většinou výše zmíněné „ripy“ či „kinoripy“ najdeme. Dále by se sem dal zařadit částečně i všem známý Youtube, kde můžeme rovněž nalézt mnoho nelegálně získaných a šířených kopií. A takto se dají najít i nejnovější filmy, kam spadá například server www.dlouhefilmy.com, který je zároveň příkladem serveru, který umožňuje puštění filmů online. Nevýhodou takovýchto serverů je většinou ale nízká přenosová rychlost (často v řádech stovek kilobitů za sekundu). Kromě samotného podporování nelegálních praktik využívání těchto serverů přináší i určité riziko, jelikož poměrně často využívaným prostředkem pro šíření malwaru.

Na internetu najdeme ale i legální filmy a videa, většinou se ale nejedná o žádné novinky či je potřeba za přístup k nim zaplatit. Příkladem jsou například archivy českých televizí (konkrétně například www.ivysilani.cz , http://archiv.nova.cz , www.iprima.cz/videoarchiv ), kterým se televize snaží o svou další reklamu a o zisk příznivců i na jiném médiu.

## Hudba

U hudby je to velice podobné, jak je zmíněno výše u filmů a obecně autorského práva, princip je stejný. Za porušení autorského práva se opět považuje hlavně nahrávání muziky na internet tak, aby si jí další uživatelé mohli stáhnout, případně jiné další nelegální šíření. Kromě tohoto je také protizákonné odstraňovat ochrany z digitálních médií (ač zakoupených zcela legálně).

Stejně jako u filmů můžeme opět vymezit určitou „šedou zónu“, která je na hranicích zákona, ale ještě není označená jako přímo nelegální. Jednou z věcí, které sem určitě patří, je opět využívání či podporování cest, které jsou povětšinou založené právě na nelegálním šíření – samotné stahování je ale v mezích zákona. Další věcí, která stojí za zmínku, jsou programy a nástroje, které umožňují stahování hudby z Youtube či jiných koutů internetu, jako například „Free Youtube to MP3 Conventer“ (který, jak již napovídá název, vytahuje z videí na Youtube zvuk a ukládá jej ve formátu MP3), propracovanější a šikovnější „aTube Catcher“ (který umí již ukládat v mnoha různých formátech… a poradí si i s videem) nebo „AudialsOne“ (který umožňuje nahrávání z internetových rádií, a to až ze sedmi najednou).

Mezi legální zcela legální způsoby pak můžeme zařadit veškerá internetová rádia, která jsou buď spojená s nějakým rádiem klasickým, jako třeba http://www.radiocity.cz/, a nebo jsou čistě internetová, jako například http://www.play.cz/ nebo http://www.koule.cz . Legální je samozřejmě i šíření vaší vlastní hudby, kde stojí za zmínku stránka http://bandzone.cz/ , která nabízí prostor právě začínajícím a amatérským talentům. A legální je samozřejmě i online nakupování, pokud k tomu využijeme autorizovaných obchodů či serverů.

## Obrázky a fotografie

U obrázků a fotografií tomu je obdobně jako u hudby či filmů. Oproti předchozím dvěma zde ale budeme více řešit jejich použití například při výrobě vlastní internetové stránky či prezentace. Prvním problémem ale je, že se mnohdy velice těžko poznává, kdo je autorem obrázku a jaký má vlastně autor postoj k jeho šíření. Pokud byste chtěli postupovat dokonale podle autorského práva, tak obrázek či fotografii můžete využít jen tehdy, když autor uvádí souhlas s jeho půjčením. U tohoto souhlasu může autor i definovat určité podmínky, které jsou poté nutné splnit. V zásadě zde ale platí jedno základní pravidlo, že musí být uveden autor fotografie či obrázku.

Přesto, že se tato oblast tolik neřeší a není tolik kontrolována, tak za porušení licenčních podmínek hrozí sankce v řádu až desítek tisíc korun.

## Softwarové právo

Poslední, ale asi největší, částí, která by se dala zařadit mezi autorské právo, je softwarové právo. Je to soubor norem udávající vztahy mezi autory, výrobci, prodejci a uživateli při tvorbě, výrobě, prodeji a užívání softwaru.

Co se týče softwaru, tak bez svolení autora lze pořídit pouze bezpečnostní kopie za účelem archivace. Dále lze bez svolení užívat tzv. volná díla, což jsou díla, která z nějakého důvodu nejsou chráněna autorským právem.

Na rozdíl od hudby a filmů není legální pořizovat kopie ani pro svou vlastní potřebu, výjimkou je pouze pořízení kopie na druhý vlastní počítač (např. při vlastnictví stolního domácího PC a notebooku). Neoprávněné používání softwaru je považováno za trestný čin a je posuzováno jako krádež, která poškozuje autora programu (odměna za využívání programu), distributora (zisk) i stát (daně). I přesto je zde však samozřejmě mnoho praktik, které nelegální využití podporují, jako například různé cracky, patche či generátory sériových čísel – všechny tyto praktiky jsou samozřejmě také nelegální.

I u softwaru lze vytyčit určitá pomyslná „šedá zóna“. Zde je to hlavně takzvaný abandonware, což je obecné označení pro starý komerční software, na kterém již nemá výrobce jak vydělávat. Právě kvůli tomu, že již pro výrobce neznamenají potencionální zisk, tak je jejich šíření tolerováno a mnohdy i podporováno, jelikož jim slouží jako bezplatná reklama.

Legální cestou využívání softwaru je poté prosté – jeho zakoupení. Ale i zde si člověk musí dávat pozor, kde a co nakupuje, jelikož by velice snadno mohl pokus o legální zakoupení softwaru skončit nehezky. Dále je legální také osobní používání tzv. freewarových či open-sourcových nástrojů a programů, kterých na internetu najdete také dost. U těchto souborů jen musí být člověk obezřetný, aby si s ním nenatáhl do počítače i nějaký škodlivý program, a tudíž je doporučeno využívat jen software z ověřených zdrojů, jako jsou například CD/DVD vydávané s časopisy (CHIP, Level, …) či servery, které při stažení kontrolují obsah antivirem (Stahuj.cz , Slunecnice.cz). Kromě tohoto je však nutné si dát pozor i na případné omezení, která mohou být autorem určená a jsou vždy zapsaná v licenčních podmínkách. Nejčastější podmínkou bývá nevyužívání programu komerčně, což většinou vyžaduje zakoupení licence (které ovšem nebývají drahé).

Tak trochu nejasnou složkou u softwarového práva jsou e-booky, jelikož nejsou ještě plně uvedeny v českém právním systému. Prozatím pro ně platí stejné podmínky, jako pro audio a video – tedy možnost bezplatného využívání pro osobní použití, například v USA spadají e-booky plně pod práva softwarová a i za osobní používání je nutno zaplatit.

### Licence

Se softwarovým právem bezprostředně souvisí licence. Licence je určitá dohoda mezi poskytovatelem softwaru a jeho uživatelem a určuje veškeré podmínky, které musí uživatel při užívání splňovat. Licencí je mnoho typů a druhů. Jedním z dělení licencí je podle počtu možných uživatelů (resp. instalací), kde v jádru rozlišujeme licenci na jednu instalaci, multilicenci na maximální specifikovaný počet nebo neomezená multilicence.

Jedna z nejužívanějších komerčních licencí je EULA (End User License Agreement = licence koncového uživatele). Tato licence určuje koncovému uživateli softwaru, co smí a nesmí dělat.

Další poměrně běžnou licencí je GNU GPL (GNU General Public License = všeobecná veřejná licence GNU), která umožňuje volné šíření, používání i upravování softwaru. Důležitou podmínkou ale je, že tento software bude šířen bezplatně či pouze za distribuční náklady, s možností bezplatně získat zdrojové kódy. Jeho upravená verze byla poté použita například v projektu Wikipedia (GNU Free Documentation License).

Podobnou licencí jako GNU GPL je například licence BSD (Barkeley Software Distribution). Tato licence umožňuje volné šíření, využívání i upravování softwaru, přičemž vyžaduje pouze uvedení autora a informací o licenci. BSD licence však již moc (oproti třeba právě GNU GPL) neřeší ochranu těchto svobod při změnění softwaru či při jeho přidání k softwaru jinému.

Dále jsou poměrně známé a používané OEM licence, které umožňují levnější nákup softwaru při současném zakoupení hardwaru. Typickým příkladem užití této licence je prodej operačních systémů spojený s prodejem stolních počítačů a notebooků.

Posledním typem licencí, kterou zde zmíním, je Creative Commons, která je jedna z nejvyužívanějších u amatérských prací napříč všemi obory. Je to licence, která umožňuje poměrně snadné licencované šíření svého vlastního díla. Tato licence se označuje CC a vznikla díky stejnojmenné americké neziskové organizaci. Licence Creative Commons vznikají kombinací několika základních vlastností, které popisují základní možnosti ponechání či vzdání se autorských práv v určité oblasti. Tyto vlastnosti jsou v jádru 4 a to: nutnost uvedení autora, zákaz využití pro komerční účely, zákaz úpravy díla a nutnost šířit pouze za podmínek původní licence (vzniká nám tedy 11 možných kombinací – z celkových 16 je jich 5 nesmyslných). Povětšinou jsou používány pro „klasická autorská díla“, tedy fotografie, obrázky, zvuk, video apod., nikoliv pro software.

Kromě samotných licencí rozlišujeme i samotný software, podle toho, s jakou licencí se váže. V tomto dělení se zohledňuje hlavně volnost užití a délka platnosti softwaru.

První skupinou, kterou takto můžeme vydělit, je adware. Tento software je šířen bezplatně, ale v programu se zobrazuje reklama (mnohdy více než by bylo uživateli příjemné). Tato reklama poté přináší autorovi žádaný zisk.

Další skupinou je freeware. Tento software je šířen bezplatně a umožňuje plné využívání, autorovi jsou však ponechána všechna autorská práva. Jediné, co takto šířený software nenabídne, je zdrojový kód, což souvisí se zákazem program měnit.

Podobnou skupinou freewaru, avšak přesto jinou, je Public domain licence. Tato licence umožňuje software volně šířit, používat i upravovat (čímž se liší právě od výše zmíněného freewaru).

Další zdarma šířenou skupinou je shareware, který je možné volně užívat, ale autor obvykle požaduje zaplacení malé částky ve chvíli, kdy se uživateli produkt líbí a chce ho běžně využívat. Zaplacením tohoto malého poplatku se člověk stává registrovaným uživatelem a mnohdy se mu tak i dostane aktualizací či online podpory.

Předposlední typ, který bych zde rád zmínil, je demo (či demoverze). Tyto programy slouží k předvedení programu a možnosti vyzkoušení základního obsahu. Takto šířený software má zpravidla značně omezenou funkčnost a slouží pouze pro reklamní účely (nalákání ke koupi plné verze).

Posledním typem je poté trial (či trial verze). Jedná se o software, u kterého je časově omezena funkce či je časově omezen celý. Toto omezení může být udáno reálným časem od jeho stažení, dobou využívání programu či počtem spuštění. Účel je obdobný jako u demoverze, tedy nalákat či definitivně přesvědčit potencionální zájemce ke koupi plné verze, hlavní rozdíl mezi těmito dvěma skupinami je zpravidla odlišnost omezení (u trialu omezení délky možného využívání, u demoverze funkčnosti).

### Softwarové patenty

Další věc, která souvisí se softwarovým právem. Jedná se o patenty na vynálezy realizované počítačem. Oproti patentům klasickým bývají poměrně triviální a často se týkají dílčích součástí programů. Pro ukázku je na stránce http://webshop.ffii.org/ ukázána stránka s vyznačenými porušeními různých softwarových patentů a jejich patřičné okomentování.

Softwarové patenty jsou dodnes místo sporu mezi jednotlivými zeměmi, které na ně mají odlišné názory a některé země je vůbec neuznávají. V USA či Japonsku jsou softwarové patenty běžně, v Indii či ČR naopak vůbec. V Evropě se názory poměrně liší a v Evropské unii jsou předmětem sporu, který stále není rozhodnut.

V zemích, kde je softwarové patentové právo uznáváno, občas dochází k tzv. patentovému vydírání. Toto vydírání je v jádru o tom, že velké firmy, které jsou i vlastníky patentů, si mezi sebou uzavírají dohody a získávají tak větší možnost kontroly trhu. Toto umožní těmto firmám zbavit se dalších konkurentů, které by je jinak mohli potenciálně na trhu ohrozit.

## Pirátské kopie a plagiátorství

V oblasti výpočetní techniky se za „pirátství“ či „plagiátorství“ obecně označuje pořizování nelegálních kopií a jejich následné šíření. Tyto činnosti nejen obírají stát a autory o jejich zisk, ale občas bývají využívány přímo komerčně jako obživa těchto „pirátů“ či „plagiátorů“.

### Pirátské kopie ve světě

Pro dokonalou představu je vhodné asi uvést pár čísel. Následující informace jsou získány autory časopisu CHIP a můžete je naleznout v květnovém vydání roku 2012, uvedené data jsou poté za rok 2011 (tudíž se nejedná o žádné „historické údaje“).

Téměř polovina softwaru užívaného na celém světě je užívána v rozporu s jeho licenčními podmínkami – konkrétně zhruba 47%. Nejrozšířenější forma pirátských kopií je nelegální instalace programu na více PC. Celková roční celosvětová ztráta autorů a států kvůli pirátskému kopírování činí kolem 59 miliard amerických dolarů ročně.

Pokud se podíváme na země s největším podílem „pirátského softwaru“, tak narazíme hlavně země Latinské Ameriky, Afriky a Asie – tedy země, které mají povětšinou opravdu slabé právní ochrany, co se této technologie týče. Na prvním místě je Gruzie s 93%, následuje jí Zimbabwe s 91%. Na třetím až pátém místě jsou státy Bangladéš, Jemen a Moldávie shodně s 90%. Desítku poté uzavírá Arménie s 89% společně se čtveřicí Ázerbajdžán, Libye, Venezuela, Bělorusko s 88%.

Procentuální podíl pirátského softwaru ku celkovému počtu ale není jedinou věcí, na kterou se u pirátství hledí. Dalším důležitým údajem je právě množství odhadovaných ztrát v USD. Tento žebříček vede USA, které má pouze 20% podíl pirátských kopií (což je ve srovnání se světem jedno z nejnižších čísel). Ročně se zde odhaduje ztráta kolem 9,5 miliard USD. Za USA je poté Čína s odhadovanou roční ztrátou 7,7 miliard USD. Poté následuje poměrně velký propad, ale v první desítce tohoto žebříčku nalezneme v jádru všechny velké a vyspělé země. Třetí až desáté místo jsou obsazena následovně: Rusko (2,8 miliard USD/rok), Indie (2,7 miliard USD/rok), Brazílie (2,6 miliard USD/rok), Francie (2,5 miliard USD/rok), Německo (2,0 miliard USD/rok), Itálie (1,8 miliard USD/rok), Velká Británie (1,8 miliard USD/rok), Japonsko (1,6 miliard USD/rok).

Pro porovnání, v České republice se udává podíl pirátských kopií 36% s odhadovanou roční ztrátou 195 milionů USD, což se řadí v obou ohledech na žebříčkách na poměrně nízké pozice. V Evropě má nevyšší podíl pirátských kopií Řecko, ztráta ca 301 milionů USD/rok.

### Zajímavosti, které stojí za zmínění

Zde bych rád uvedl několik zajímavostí, které se tohoto tématu týkají – myslím, že je vždy zajímavé nějaké uvést.

Například kolují poměrně přesvědčivé obvinění, že slavný font Arial, které vydal Microsoft v roce 1982, je vlastně napodobeninou fontu Helvetica, který byl vydán již v roce 1957. Tento případ se však nikdy nedostal před soud.

Od roku 1977 se dokonce uděluje negativní cena „Plagiarius Award“ (anticena za padělek). Tato cena se ovšem netýká pouze výpočetní techniky, ale obecně všech produktů prodaných po celém světě.

Pro hledání plagiátorských textů dokonce existují i speciální vyhledavače jako například Theses.cz, což je systém pro odhalování plagiátů mezi závěrečnými pracemi na vysoké škole. Slouží vysokým školám a univerzitám jako národní registr závěrečných prací a jako úložiště prací pro vyhledávání plagiátů.

Jako se liší i jiná práva různých států, tak se liší i toto. U nás není možné volně kopírovat obsah webových stránek, který je chráněn zákonem. Například v Německu bylo ale rozhodnuto, že zdrojový kód i grafika se mohou volně kopírovat.

## Ochrana

Pokud přejdeme k ochraně, která je užívána za účelem kontrolovat či omezovat používání obsahu digitálních médií, tak by měl zaznít hlavně DRM (Digital rights management = Správa digitálních práv). Je to obecné označení metod, které mají za účel právě kontrolovat či omezovat používání obsahu digitálních médií. Cílem je hlavně podporu ochrany autorských práv a licencí. Pomocí těchto technik jsou chráněny především filmy, hry, hudba, a další. Ani tato ochrana ale není spolehlivá a dá se poměrně snadno odstranit (ač již toto odstranění je považováno za přestupek proti autorskému právu, viz výše). V poslední době se od těchto ochran poměrně opouští, jelikož jsou povětšinou neúčinné a navíc vzbuzují poměrně silnou vlnu kritiky. Tato kritika argumentuje hlavně tím, že samotná technologie poměrně omezuje ty, kteří si danou věc legálně a poctivě zakoupí, a těm, kteří se určitým způsobem angažují v nelegální sféře, v jádru nečiní žádné problémy překonat.

### Krátké zmínění historie

Vývoj samotné technologie provází i právě vývoj ochrany proti kopírování dat a porušování následně ustanovených autorských práv. Asi je jasné, že se tyto snahy nesou v duchu zoufalého boje, který neztěžuje práci jen „plagiátorům“, ale ztěžuje život i poctivému zákazníkovi.

Pokud se podíváme hluboko do minulosti, tak ochranu před zcizením vlastně ani nenajdeme. Jediná věc, která se reálně praktikuje, je pouze používání jakýchsi kleteb, které mají za úkol odradit aspoň ty pověrčivé. Známou „kletbou“ je například „Kdo tuto knihu ukradne, tomu ruka upadne.“, která později našla své místo spíše ve vtipech.

V roce 1837 se objevují reálně první právní úpravy, které hovoří o kopírování uměleckých a vědeckých prací.

V roce 1980 poté přichází textový procesor „Wordcraft“, který běžel pouze ve chvíli, když měl k sobě připojen „hardwarový klíč“. Podobné řešení se dokonce v určité míře využívá doposud.

V roce 1983 představila poměrně revoluční řešení na ochranu proti kopírování videokazet společnost Macrovision. Tato ochrana spočívala ve vložení rušivých signálů.

Následoval rok 1990, kdy se začali objevovat hry, které potřebovali k úspěšnému puštění vložení klíčového slova, které bylo uvedeno v příručce hry.

V roce 1993 se objevuje hra „Rebel Assault“ vydaná na CD. Tato hra nejen že spustila rozmach her na PC, ale také byla svým způsobem revoluční. V tuto dobu totiž hra nepotřebovala žádnou ochranu (ani žádnou neměla), jelikož CD vypalovačky a média byly nákladné.

Dalším důležitým datem je rok 1997, kdy se na evropském trhu objevilo první DVD s ochranou proti kopírování. Tato ochrana byla nazvána CSS – Content Scramble System.

V dalších letech se objevuje například ochrana SecuRom, která jako první mimo jiné vytváří skryté položky v registru. Jednou z prvních her s touto ochranou byla FIFA99. V této době se také objevují CD s hrami, které když někdo zkopíroval, tak obsahovaly záměrné chyby, které sice nezabraňovaly samotnému spuštění hry, ale povětšinou vedli k dřívějšímu nebo pozdějšímu znemožnění ve hře pokračovat. Tato ochrana byla použita například u kopií se hrou Settlers 3.

V roce 2001 přichází revoluční řešení společnosti Microsoft. S operačním systémem Windows XP se totiž objevila i ochrana pomocí aktivace produktu přes internet. Paradoxně za tuto ochranu sklidil Microsoft poměrně silnou kritiku a byl dokonce obviněn ze špionáže údajů.

V roce 2005 se poté objevují první platformy určené k digitální distribuci her, zajištění multiplayerového zázemí a i další snaze k ochraně proti kopírování. První takovou platformou byl Steam od společnosti Valve.

Naopak v roce 2008 přichází poměrně silná rána snahám o zabránění nelegálnímu kopírování. Zasloužila se o to firma SlySoft s programem AnyDVD, který dokáže obejít ochranu proti kopírování Blu-ray disků. Umožňuje tak poměrně jednoduchou možnost vytvářet si vlastní kopie – a to prakticky každému.

V poslední době se pak kvůli vývoji směřujícímu hlavně k smartphonům a tabletům upouští od dříve klasických metod (například výše zmíněné DRM) a přechází se na ochrany jiné. Začínají se používat například vodoznaky u MP3 souborů a jiné.

## Stahování

Jak bylo zmíněno už výše, počítačové právo se v různých zemích velice liší. Za normální situace by to neznamenalo takový problém, ale díky Internetu jsou všechny tyto země spojeny jedním prostředkem a tak se zde běžně úplně legálně vyskytují věci, které jsou jinde protiprávní. Kromě již zmíněného stojí za zmínku samotné způsoby stahování.

Jako první je nutné zmínit hostování souborů a stahovací servery. Samotné stahování z těchto serverů je čistě legální, ale přesto se tyto servery řadí spíše do tzv. „šedé zóny“. Toto zařazení si vysloužily hlavně tím, že dávají poměrně hodně prostoru pro nahrávání a šíření nelegálních kopií a povětšinou to ani moc nekontrolují. Typickým příkladem jsou servery jako HellShare, Ulož.to, Rapidshare či jiné. Některé servery umožňují stahovat bezplatně, jiné za malý poplatek, některé nabízejí obě možnosti (kde ta bezplatná má povětšinou poměrně omezenou maximální rychlost stahování). Tyto servery jsou také potencionálními šiřiteli virů a dalšího malwaru, právě díky poměrně malé kontrole nahrávaných souborů.

Se zmíněnými stahovacími servery bezprostředně souvisí takzvaná Warez-fóra, která si v jádru slouží jako přehled možných míst, kde stáhnout ten či onen nelegální software. Dříve byla tato fóra provozována stylem spíše „všichni pro všechny“ a byla volně přístupná každému, v dalším vývoji ale tyto fóra začali nejen omezovat registrace, ale často i zavádět nutné zaplacení určitého „vstupního poplatku“. Tyto fóra také často obsahují poměrně velké množství reklam, které slouží provozovatelům (společně s případným vstupním poplatkem) jako zisk.

Najdeme však i čistě legální a bezúhonné servery, které umožňují předávání či ukládání souborů. Zde bych uvedl hlavně Cloudy, jako například Skydrive nebo GoogleDocs. Tyto servery mají zpravidla mnohem přísnější pravidla i ochrany a nedávají šíření nelegálního softwaru velkou možnost je pro svou činnost využívat.

Poslední věcí, která je nutná uvést, je stahování založené na Peer-to-peer síti (označované též P2P případně klient-klient). Jak již vychází z názvu, tak je to systém, kde jsou si všichni rovni a stejně tak je tomu u stahování. Principem peer-to-peer distribuce souborů je to, že každý, který soubor stahuje, zároveň poskytuje (uploaduje) to, co již má stažené. Základní výhodou je poměrně vysoká maximální rychlost, pokud se na tomto stahování podílí dostatečný počet uživatelů. Tento fakt je ale i prvním z mnoha problémů – bez dalších aktivních uživatelů totiž takto nestáhnete nic a s malým počtem budete stahovat jen velmi pomalu. Rychlost stahování je také poměrně kolísavá v závislosti na to, jak se uživatelé odpojují či připojují. Další poměrně zásadní nevýhodou je fakt, že pokud takto budete chtít stáhnout nelegální software, tak se již dopouštíte trestného činu, jelikož současně tento software i nahráváte a poskytujete dalším uživatelům v P2P síti. Nástroje, které se užívají pro P2P distribuci souborů se nazývají obecné „torrenty“ a mezi nejznámnější patří BitTorrent a μTorrent.

# Hacking, cracking a jiné škodlivé aktivity

Jak to již bohužel chodí, vždy se najde někdo, kdo se živí tím, že poškozuje práci jiných – ať už pro zábavu či pro obživu.

Mezi základní věci patří hacking a cracking. Tyto dvě věci jsou sice poměrně podobné a bývají proto poměrně často zaměňovány (nebo chybně obě označovány jako „hacking“), ale hackeři by vás za to asi nepochválili. Hacking i cracking jsou aktivity, které se mají za cíl proniknout do cizího systému. Zde ovšem přichází zásadní rozdíl v účelu. Zatímco hacker tento průnik do systému dělá spíše pro dokázání svých schopností, poukázání na díry v ochraně či pro zábavu, tak cracker má za hlavní cíl někoho poškodit či ukrást důležitá data.

Jeden z nástrojů crackerů a dalších lidí, kteří chtějí působit škodu, je malware. Malware je souhrnné označení pro software, který má za cíl umožnit vniknutí do systému nebo jeho poškození. Podle toho, co daný software dělá, se dají programy i dělit.

V zásadě můžeme vyčlenit počítačové viry, které infikují spustitelný soubor a poté nenápadně infikují soubory další. Zpravidla nebývají tolik škodlivé, ovlivňují spíše výkon počítače.

Další a poměrně nebezpečnější skupinou jsou počítačoví červi. Ti mají za úkol doslova „rozežrat“ cílový systém. Působením červů se může velice docílit nefunkčnost jednotlivých programů, stejně jako celého operačního systému.

Dále jsou zde pak programy, které mají za cíl hlavně utajené dostání se do systému. Toto poté ale bývá využíváno – buď ve spojení s počítačovými viry a červi či pro převzetí kontroly nad celým počítačem. V této skupině v jádru rozlišujeme 3 hlavní skupiny. První jsou Trojští koně, kteří mají za úkol dostat se nepozorovaně do systému. Právě Trojští koně často obsahují viry či červi, které po proniknutí koně do systému začnou pracovat a dělat svou práci. Další skupinou jsou rootkity, které se snaží hlavně o zamaskování práce jiného programu či pohybu fyzického útočníka. Poslední skupinou jsou backdoory, které (jak již vyplývá z názvu) mají za úkol proniknout do systému a otevřít „zadní vrátka“.

Často používanou technikou je také phishing. Je to aktivita, která se snaží získat důležité údaje (hesla, čísla karet, čísla účtů, apod.). Většinou je k tomu využívána e-mailová komunikace, kde se útočník vydává za důvěryhodnou osobnost a snaží se oklamat důvěřivou veřejnost a donutit je k zadání těchto údajů na stránku, která se sice tváří jako ta správná, ve skutečnosti ale správná určitě není. Tyto techniky se dají poměrně často rozeznat prostým důkladným pročtením a kontrolováním adres, jelikož mnohdy obsahují chyby či nesedí internetové adresy.

Další činností je například skimming, který se snaží využít bankomaty, do kterých instalují tzv. skimmovací zařízení, které jsou schopny zjistit PIN při běžném použití bankomatu.

Šíření malwaru a phishing často využívá elektronické pošty a něčeho, co se označuje jako spam. Obecně to je označení pro nevyžádané sdělení, které je masově šířeno internetem. Rozesílané spamy však nejsou pouze snahou o šíření této nekalé činnosti, ale jsou i (a to hlavně) používány pro reklamu.

## Ochrana

Proti těmto nekalým praktikám byla, je a bude samozřejmě vyvíjena ochrana, která v kombinaci s dodržením určitých zásad dokáže poměrně zaručit neproniknutelný štít. Mnohdy ale stačí i malé pochybení v nepravý čas a předchozí snahy mohou najednou být marné.

Základní ochranou proti virům a dalšímu malwaru je aplikace Firewall. Je to síťové zařízení, které slouží k řízení a zabezpečení sítě a provozu mezi sítěmi. V dnešní době je součástí je v určité podobě obsažena snad v každém operačním systému.

Pro zvýšenou ochranu proti malwaru poté slouží programy, které bývají obecně označovány jako „antiviry“. Tyto programy tiše monitorují systém, umožňují otestovat soubory na přítomnost virů a hlásí veškeré podezřelé činnosti a soubory. Většinou mají několik stupňů ochrany, které jsou patřičně rozděleny cenou. Mnohdy antiviry nabízí i volně stažitelnou základní verzi, která ovšem je osekaná o mnoho funkcí. Příkladem antivirových programů je například AVG, Avast! či ESET.

Poslední důležitou věcí je antispam, který filtruje příchozí elektronickou poštu. Tímto způsobem je většinou odfiltrována většina nevyžádané pošty, může ale vést i k problémům s doručením i pošty vyžádané. Kromě samotných algoritmů mohou antispamy využívat i takzvané „blacklisty“, které podle určitých kritérií označují mail servery za spolehlivé či nespolehlivé. Antispamu poté stačí jen přečíst hlavičku emailu, kde zjistí odchozí mailový server a na základě této informace email pustí či nepustí. Mezi největší blacklisty patří nejspíše SORBS, Spamhaus-ZEN nebo BARRACUDA.

1. část

Můj osobní názor na právo je ten, že určitý řád potřeba je, tak jako u všeho. Myslím si, že je potřeba nalézt kompromis mezi právem, komfortem a spravedlivostí, a to na všechny strany celého systému. Toto vyvážení určitě není nic jednoduchého, a proto se poměrně nedivím, že v jádru neexistuje žádný 100% fungující systém. Myslím si ale, že to možné je a že je to spíše otázkou času, kdy by se celková situace mohla stát vyhovující všem.

Zároveň si myslím, že celkově licence jsou poměrně podceňované a že většina uživatelů standartní licence při instalaci ani nečte. Ač tak většinou činím také, tak mi celá ta věc přijde poměrně paradoxní, jelikož tak dělají i mnozí lidé, které v reálném světě čtou všechny papírové smlouvy, které jsou možné k nahlédnutí, dříve než něco podepíší či odsouhlasí. To mě vede k myšlence, že jsou tyto licence potencionálním nebezpečím, které by mohli firmy a společnosti poměrně lehce minimálně nějaký čas využívat k nekalým účelům – ač je pravda, že je otázkou, jak by to pro ně dopadlo poté, co by se zpráva roznesla do médií a mezi lidi.

Dále bych chtěl zmínit aktuální trendy ochrany počítačových her. Do druhé části jsem toto téma zařadil hlavně proto, že celé téma je psáno čistě ze zkušeností a vlastních pocitů. Navíc je to téma poměrně konkrétní a specifické a tudíž mi přišlo vhodné ho oddělit a dát sem, kde je pro něj dle mého názoru ideální místo.

Dnešní trendem ochrany her je hlavně přechod k systému účtů. Tento systém umožňuje poměrně spolehlivou ochranu multiplayeru hry, avšak většinou tolik neřeší část singleplayerovou, který je většinou poměrně jednoduše k dostání (ač jeho získání a umožnění hraní bezplatně je samozřejmě nelegální). Tento fakt, dle mého názoru, vede společnosti k zaměření právě na multiplayer hry a ponechání singleplayeru spíše jako bonusu či doplnění.

S tímto nejspíše souvisí i čím dál větší užití a vývoj vlastních launcherů a platforem, jako například Steam (společnosti Valve... následně jí ale začali využívat i další firmy; fungují přes něj hry jako třeba nové Call of Duty, Dishonored či nový Bioshock), Origin (společnosti EA; příkladem her je tedy například nový Battlefield či FIFA) nebo Uplay (společnosti Ubisoft; zde bych zmínil hlavně zatím poslední díl Heroes of Might and Magic VI či FarCry 3). Bohužel se tyto spouštěče ale stali, minimálně z počátku, z pohledu uživatele spíše noční můrou, jelikož byly poměrně problémové a paradoxně dělaly vrásky na čele právě lidem, kteří měli hru zakoupenou legálně. Mnohdy se stávalo, že člověk musel platformu či hru pouštět naněkolikrát nebo skončil již neúspěšným přihlášením k serveru. Naštěstí tento problém zavnímali i společnosti, které se za tyto platformy zaručily, a tak se tato situace poměrně rychle vylepšila, ač by se stále dalo mnohé vytknout. Jedním z přetrvávajících problém (a zároveň v jádru neodstranitelným) může být samotná podstata platforem, tedy přidání dalšího požadavku na propustnost dalších portů než na hry samotné – pro člověka, který nemá možnost takové kontroly nad správou a nastavením portů, zde může poměrně narazit.

Co se ale týče zabránění nelegálních kopií a hráčů, tak ani tyto platformy nebyly úplně účinné, jelikož se dají buď obejít úplně, nebo se již dají sehnat i upravené verze, které vám žádný problém dělat nebudou, pokud se spokojíte se singleplayerovou částí hry a obejdete se bez různých bonusů, achievementů a podobných věcí, které bývají závislé na spojení na internet a autorizovaným přístupem k serverům hry za pomocí osobního profilu.

Úplně odlišným způsobem, který je poslední dobou také velice rozšířený a využívaný, jsou hry „free to play“. U těchto her vývojáři neřeší zabezpečení vůbec a vydají hru volně ke stažení. Příjem firem je poté činěn nákupy bonusového obsahu či placení „premium profilů“, které většinou přináší nejen přednostní přístup na server nebo urychlení/zjednodušení určitých věcí, ale občas i určité bonusy do hry samotné, které ovlivňují vyváženost hry vůči ostatním – a tak se pak na účet takovýchto her často vznáší kritika a při jejich popisu je označení často rozšířeno na „free to play; pay to win“. Existují ale i hry, které dávají stejné šance na výhru jak „platičům“ tak „neplatičům“ a za peníze spíše nabízí rychlejší postup, bonusové věci, možnost většího přizpůsobení či kosmetické úpravy a skiny. Příkladem těchto her jsou například hry od společnosti WARGAMING.NET. Konkrétně pak hry „World of Tanks“, která by se dala již za právoplatně fungující hru, ač vývojáři je stále označována spíše jako Beta-test, „World of Warplanes“, která je v oficiálním uzavřeném beta-testu, a „World of Warships“, který je zatím ve fázi příprav. Dalším příkladem je poté například „League of Legends“ od společnosti Riot games. Pokud bych měl zmínit nějakou větší a známější společnost, tak by to byla nejspíše společnost Electronic Arts (EA), která plánuje pokračování slavné „Command and Conquer“ série právě jako „free to play“.

Můj osobní názor na tyto hry je poté pouze pozitivní, jelikož pokud hráče daná hra chytne, tak si již cestu, jak přispět na autory najde – zvláště pokud za to něco dostane. Tudíž mi přijde tato cesta poměrně zajímavým řešením.

Co se týče mého obecného přístupu ke kupování či nekupování softwaru, tak jsem zastánce toho, že pokud mě software opravdu zajímá či vím, že ho budu opravdu využívat, tak radši zainvestuji a užívám si plných funkcí plné verze. Občas samozřejmě ale využiji i jiné cesty a možnosti.

Zdroje

## Literatura

* časopis CHIP, konkrétně tato vydání:
  + CHIP 02/10
  + CHIP 07/10
  + CHIP 02/11
  + CHIP 06/11
  + CHIP07/11
  + CHIP 11/11
  + CHIP 05/12
  + CHIP 01/13

## Internet

* <http://cs.wikipedia.org/wiki/Autorské_právo>
* <http://cs.wikipedia.org/wiki/Volné_dílo>
* <http://cs.wikipedia.org/wiki/GNU_General_Public_License>
* <http://cs.wikipedia.org/wiki/BSD_licence>
* <http://cs.wikipedia.org/wiki/Creative_Commons>
* <http://cs.wikipedia.org/wiki/Digital_rights_management>
* <http://cs.wikipedia.org/wiki/Malware>
* <http://www.unium.cz/materialy/0/0/softwarove-pravo-m26833-p1.html>