INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Název projektu: ICT jako nástroj inovace výuky

Reg. č. projektu: CZ.1.07/1.3.00/51.0040

Legislativní zázemí využívání digitálních technologií, ochrana duševního vlastnictví a bezpečnost na Internetu

Autor: RNDr. Tomáš Sochor, CSc.

Obsah

1. Autorský zákon ... 2
   1.1. Úvod do právního rámce regulujícího používání informační a komunikační technologie v ČR ... 2
   1.2. Autorské právo v zákonech ČR ... 2
      1.2.1. Autorské dílo ... 3
      1.2.2. Autor ... 6
   1.3. Obsah autorského práva ... 7
   1.4. Licenční smlouva ... 8
      1.4.1. Školní dílo ... 9
      1.4.2. Zaměstnanecké dílo ... 10
      1.4.3. Zvláštní druhy vymezení autorských práv ... 11
   1.5. Kolektivní správa autorských práv ... 13
2. Aplikace autorského zákona v oblasti digitálních technologií ... 15
   2.1. Úvod ... 15
   2.2. Úplatná zákonná licence ... 16
   2.3. Aplikace autorského práva na databáze ... 18
   2.4. Porušení ustanovení autorského zákona ... 19
3. Licenční podmínky počítačových programů ... 20
   3.1. Pojem počítačový program ... 20
   3.2. Typy licencí počítačových programů ... 21
      3.2.1. Licenční podmínky ... 21
   3.3. Distribuce počítačových programů ... 25
4. Zásady bezpečného používání Internetu ... 28
   4.1. Společné zásady bezpečnosti ... 28
      4.1.1. Ochrana hesel ... 29
      4.1.2. Zásady bezpečné práce s elektronickou poštou ... 32
   4.2. Rodičovská ochrana ... 33
5. Hrozby z Internetu a možnosti ochrany před nimi ... 35
   5.1. Škodlivý kód a jeho druhy ... 35
      5.1.1. Viry ... 35
      5.1.2. Červi ... 35
      5.1.3. Trojský kůň ... 36
   5.2. Napadení počítače – Hacking ... 36
   5.3. Phishing ... 37
   5.4. Ochrana před hrozbami ... 38
      5.4.1. SPAM a jiné nežádoucí zprávy ... 38
      5.4.2. Antivirus, antispyware ... 38
      5.4.3. Firewall ... 38
      5.4.4. Další opatření pro ochranu před riziky ... 39
6. Použité zdroje ... 43

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

1. Autorský zákon

1.1. Úvod do právního rámce regulujícího používání informační a komunikační technologie v ČR

Zákony a nižší podzákonné normy a jiné obecně závazné předpisy každého státu, Českou republiku nevyjímaje, ovlivňují fungování mnoha součástí společnosti. To platí samozřejmě také pro oblast informačních a komunikačních technologií (ICT), které spolu s tím, jak se počítače, mobilní telefony, tablety a čerpání informací z Internetu stává čím dále tím běžnější a dostupnější pro běžné občany, hrají v našem životě stále významnější roli. Toto zásadní ovlivnění funkcí společnosti samozřejmě platí i pro Českou republiku, na jejíž legislativní prostředí se tato kapitola zaměřuje především. Protože většina právních předpisů ČR v této oblasti je harmonizována v právem EU, lze do jisté míry očekávat, že obdobná právní úprava bude platit i v jiných členských zemích EU, případně i jinde v Evropě. Přesto na to nelze automaticky spoléhat, protože řada oblastí práva členských zemí EU náleží do výlučné pravomoci národních zákonodárců, popř. též není vyloučena špatná implementace práva EU, takže i v této oblasti mohou existovat značné rozdíly mezi právními úpravami jednotlivých zemí.

Významnou překážku při analýze právního prostředí ČR z hlediska fungování IT představuje skutečnost, že zákonná opatření, která regulují fungování ICT, jsou dosud rozptýlena do poměrně velkého množství předpisů, a to nejen zákonů, ale i vyhlášek apod. Kromě zákona o elektronických komunikacích a od roku 2015 platného zákona o kybernetické bezpečnosti (zákon 181/2014 Sb.) totiž neexistuje v ČR zákonná norma, která by se komplexněji věnovala oblasti fungování ICT. V této kapitole se zaměřujeme především na autorský zákon, který do oblasti ICT a jejich aplikace má velmi výrazný přesah.

1.2. Autorské právo v zákonech ČR

I když autorské právo není na první pohled přímo svázáno s používáním počítačů, Internetu a obecně ICT, pak nahlédnutím do zpráv běžných sdělovacích prostředků nabydeme dojmu, že opak je pravdou. Snad nejčastější zprávy týkající se porušení zákonů a předpisů v souvislosti s informačními technologiemi souvisejí právě s porušováním autorských práv.

Na úvod této kapitoly je na místě vymezit samotný pojem **autorské právo**. Jako i v jiných právních odvětvích lze na autorské právo nahlížet v objektivním slova smyslu a v subjektivním slova smyslu.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

V objektivním slova smyslu lze autorské právo definovat jako soubor právních norem, jejichž předmětem je úprava vznikajících při tvorbě a uplatňování autorských děl. V subjektivním slova smyslu se pak autorské právo definuje jako soubor daných oprávnění ke konkrétnímu dílu náležejících jejich autorovi – tedy osobě, která svou duševní činností dílo vytvořila.

Právní rámec autorského práva je na území České republiky stanoven zejména zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorských a o změně některých zákonů, ve znění pozdějších předpisů (dále též autorských zákon).

Věcně jsou tímto zákonem konkrétně upraveny:

- právo autora k jeho dílu;
- právo výkonného umělce k jím vytvořenému uměleckému dílu;
- právo výrobce zvukového záznamu k jeho záznamu;
- právo rozhlasového nebo televizního vysílatele k jeho vysílání;
- právo výrobce zvukově obrazového záznamu k jeho záznamu;
- právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv;
- právo nakladatele na odměnu v souvislosti se zhotovením rozmnoženiny jím vydaného díla pro osobní potřebu;
- právo zveřejnitele k jím pořízené databázi;

Současně je autorským zákonem rovněž řešena úprava ochrany všech výše uvedených práv a úprava kolektivní správy autorských práv a práv souvisejících s autorským právem.

1.2.1. Autorské dílo

Ve smyslu ustanovení § 2 odst. 1 autorského zákona lze konstatovat, že autorským dílem je *„dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam.“*

Jak z výše uvedeného plyne, o autorské dílo se bude jednat v případě, že konkrétní dílo bude splňovat zároveň všechny následující pojmové znaky:

1) umělecké nebo vědecké dílo – dílo musí být vyjádřeno takovým způsobem, aby bylo objektivně vnímatelné jako literární, umělecké nebo jiné vědecké dílo;

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

2) jedinečný výsledek tvůrčí činnosti autora – takový výsledek musí vzejít z autorovy duševní činnosti;
3) vyjádření díla v jakékoliv objektivně vnímatelné podobě v daném čase a na daném místě.

Dále podle ustanovení § 2 odst. 2 autorského zákona platí, že za (autorské) dílo *„se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným… Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické.“*

Dále tímto ustanovením autorský zákon výslovně stanovuje ohledně počítačových programů a databází, že jiná kritéria pro určení způsobilosti počítačových programů a databází se k jejich ochraně neuplatňují.

Autorskoprávní ochrana stanovená autorským zákonem se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav, avšak za současného splněné výše uvedených pojmových znaků autorského díla.

Autorskoprávní ochrana stanovená autorským zákonem se dále vztahuje také na dílo vzniklé tvůrčím zpracováním díla jiného, včetně překladu díla do jiného jazyka – tímto současně nedochází k omezení práv autora díla, které bylo následně zpracováno nebo přeloženo.

Za autorské dílo se však výslovně nepovažuje námět díla sám o sobě, denní zpráva nebo jiný údaj sám o sobě, myšlenka, postup, princip, metoda, objev, vědecká teorie, matematický a obdobný vzorec, statistický graf a podobný předmět sám o sobě.

Pro úplnost je potřeba dále dodat, že některá díla jsou z autorskoprávní ochrany autorským zákonem vyloučena. Jedná se o úřední díla (právní předpisy, veřejně přístupné rejstříky, obecní kroniky, státní symboly, atp.), a díla tradiční lidové kultury, jestliže jejich autor není znám (folklórní díla).

Co do druhů lze autorské dílo klasifikovat na:

- dílo slovesné – např. kniha
- dílo hudební – např. hudební skladba
- dílo dramatické – např. činohra
- dílo hudebně dramatické – např. muzikál, opera

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

- dílo choreografické a pantomimické – např. pantomimické (bezeslovní) vystoupení
- dílo fotografické a dílo vyjádřené postupem podobným fotografii
- dílo audiovizuální – např. film
- dílo výtvarné
- dílo architektonické
- dílo užitného umění – např. umělecký nábytek
- dílo kartografické – např. mapa

Jak již bylo uvedeno výše, autorskoprávní ochrana se vztahuje rovněž na počítačové programy. Není-li zákonem stanoven specifický režim, je obsah uvedené ochrany shodný s ochranou v případě (výše vymezeného) literárního díla. Jelikož nelze počítačový program a software považovat za pojmy se shodným obsahem (software kromě počítačového programu v sobě zahrnuje i související dokumentaci), je na místě předně uvést, že režim autorského zákona se uplatní pouze ve vztahu k počítačovému programu. Autorskoprávní ochraně tak nepodléhají myšlenky a principy, na podkladě kterých počítačový program, popř. jeho část byly vytvořeny, dále pak algoritmy, programovací jazyky, atp.

Naopak autorským zákonem je chráněna vnitřní struktura počítačového programu, která tvoří jeho kostru skládající se z jednotlivých po sobě následujících příkazů a modulů. Vyjádření počítačového programu v materiální podobě pak představuje zdrojový kód programu. Ohledně autorskoprávní ochrany vztahující se k počítačovému programu je pak rovněž na místě doplnit, že autorský zákon obsahuje speciální úpravu omezení práva autora k počítačovému programu ve prospěch oprávněného uživatele rozmnoženiny počítačového programu tak, že právě oprávněnému uživateli jsou zaručena oprávnění k využití rozmnoženiny programu alespoň v minimálním rozsahu. Přesná specifikace uvedeného oprávnění je obsažena v ustanovení § 66 odst. 1, 2 autorského zákona, podle kterého platí, že:

„(1) Do práva autorského nezasahuje oprávněný uživatel rozmnoženiny počítačového programu, jestliže

a) rozmnožuje, překládá, zpracovává, upravuje či jinak mění počítačový program, je-li to nezbytné k využití oprávněně nabyté rozmnoženiny počítačového programu, činí-li tak při zavedení a provozu počítačového programu nebo opravuje-li chyby počítačového programu,

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

b) jinak rozmnožuje, překládá, zpracovává, upravuje či jinak mění počítačový program, je-li to nezbytné k využití oprávněně nabyté rozmnoženiny počítačového programu v souladu s jeho určením, není-li dohodnuto jinak,

c) zhotoví si záložní rozmnoženinu počítačového programu, je-li nezbytná pro jeho užívání,

d) zkoumá, studuje nebo zkouší sám nebo jím pověřená osoba funkčnost počítačového programu za účelem zjištění myšlenek a principů, na nichž je založen kterýkoli prvek počítačového programu, činí-li tak při takovém zavedení, uložení počítačového programu do paměti počítače nebo při jeho zobrazení, provozu či přenosu, k němuž je oprávněn,

e) rozmnožuje kód nebo překládá jeho formu při rozmnožování počítačového programu nebo při jeho překladu či jiném zpracování, úpravě či jiné změně, je-li k ní oprávněn, a to samostatně nebo prostřednictvím jím pověřené osoby, jsou-li takové rozmnožování nebo překlad nezbytné k získání informací potřebných k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu s jinými počítačovými programy, jestliže informace potřebné k dosažení vzájemného funkčního propojení nejsou pro takové osoby dříve jinak snadno a rychle dostupné a tato činnost se omezuje na ty části počítačového programu, které jsou potřebné k dosažení vzájemného funkčního propojení.

(2) Za rozmnožování počítačového programu podle tohoto zákona se považuje i zhotovení rozmnoženiny, je-li nezbytná k zavedení a uložení počítačového programu do paměti počítače, jakož i pro jeho zobrazení, provoz a přenos.“

Je však na místě doplnit, že ustanovení § 66 autorského zákona obsahují rovněž další povinnosti, které je oprávněný uživatel povinen splnit, aby nedošlo z jeho strany k porušení autorského zákona ve vztahu k autorovi počítačového programu.

1.2.2. Autor

K samotnému vzniku autorského díla je potřeba mimo jiné konatele – osobu autora. Podle ustanovení § 5 autorského zákona je autorem autorského díla „*fyzická osoba, která* (autorské) *dílo vytvořila.“* V souvislosti s předchozí větou je nutné zdůraznit, že autorem může být vždy pouze fyzická osoba, nikoliv právnická osoba.

Pro další výklad k osobě autora je potřeba uvést, že autor je subjekt autorského práva, jehož autorskoprávní vztah je původní (originární). Druhou kategorií autora je subjekt autorského práva, jehož autorskoprávní vztah je odvozený.

Jednoznačné určení osoby autora může být v praxi leckdy složitý problém. Autorský zákon na takto předvídanou situaci reaguje v ustanovení § 6 autorského

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

zákona stanovením tzv. zákonné domněnky autorství, podle které platí, že *„autorem* (autorského) *díla je fyzická osoba, jejíž pravé jméno je obvyklým způsobem uvedeno na díle nebo je u díla uvedeno v rejstříku předmětů ochrany vedeném příslušným kolektivním správcem …; to neplatí v případech, kdy je údaj v rozporu s jiným údajem takto uvedeným.“* Jedná se však o domněnku vyvratitelnou, což jinými slovy znamená, že autorství určené na základě domněnky podle předchozí věty může být na základě příslušných důkazů určeno i podle skutečného stavu.

O autorství jakožto o autorskoprávním vztahu autora k autorskému dílu lze konstatovat, že je výlučným a nepřevoditelným právem absolutní povahy, kterého se nelze vzdát, a které současně působí vůči všem osobám.

1.3. Obsah autorského práva

Práva (a s těmito právy související povinnosti) vyplývající z autorského práva (tedy v souhrnu obsah autorského práva) lze rozdělit na dvě podstatné skupiny, a sice výlučná osobnostní práva a výlučná majetková práva.

Výlučná osobnostní autorská práva jsou práva, která jsou spojená výlučně s osobou autora – smrtí autora osobností autorská práva zanikají. Po smrti autora je zapovězeno, aby si autorství k dílu osobovala jiná osoba – stane-li se tak, autorský zákon obsahuje ustanovení umožňující domáhat se ochrany osobám blízkým ve smyslu občanského zákoníku, právnické osobě sdružující autory nebo příslušnému kolektivnímu správci (tzv. postmortální ochrana díla).

Výlučná majetková práva jsou pak práva, která umožnují dispozici s autorským dílem – pro společnost mají především ekonomický význam.
Doplňující skupinou k výše uvedeným skupinám obsahu autorských práv jsou pak ještě tzv. jiná majetková práva.

Majetková práva trvají po dobu autorova života a 70 let po jeho smrti. Po uplynutí této doby se dílo stává tzv. volným dílem, což znamená, že může být volně užito bez svolení a bezúplatně

Výlučnými osobnostními právy jsou:

- právo autora na zveřejnění díla – obsahem tohoto práva je právo autora rozhodnout o prvním zpřístupnění díla veřejnosti, a to jak co do okruhu osob (všem osobám, určitému okruhu osob, atp.), tak i co do způsobu zveřejnění (předvedení, přednesení, vystavení, prostřednictvím internetu, atp.);
- právo autora osobovat si autorství – obsahem tohoto práva je právo oprávněné osoby označit se za autora autorského díla, jakož i související

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

práva, která je autor oprávněn realizovat v případě, že se neoprávněná osoba (plagiátor) označí za autora díla;

- právo autora na nedotknutelnost díla – obsahem tohoto práva je právo autora na celistvost díla, jakož i na další změny díla dle vůle autora (autorský zákon v tomto smyslu uvádí právo autora udělit svolení se změnou díla při splnění zákonem stanovených podmínek, právo autora na to, aby jeho dílo, je-li užíváno jinou osobou, nebylo užíváno způsobem snižujícím jeho hodnotu, právo autorského dohledu, atp.).

Výlučnými majetkovými právy jsou:

- právo autora dílo užít – obsahem tohoto práva je právo autora použít dílo v původní anebo změněné podobě, samostatně nebo s jiným dílem, v hmotné nebo nehmotné podobě, veřejně či neveřejně;
- právo autora nechat dílo užít - obsahem tohoto práva je právo autora nechat zákonem stanoveným postupem použít dílo třetí osobou, a to na základě uzavřené smlouvy (viz dále).

Jinými majetkovými právy pak jsou například:

- právo autora na odměnu při opětovném prodeji originálu uměleckého díla;
- právo autora na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu;
- právo autora na odměnu za půjčování originálu nebo rozmnoženiny vydaného díla.

Za součást obsahu autorského práva je možné rovněž považovat oprávnění autora vztahující se k ochraně autorských práv. Ochrana autorského práva je takto realizováno jednak tradičními soukromoprávními nároky, tj. nárokem zdržovacím, odstraňovacím a satisfakčním, a dále pak i pro autorský zákon specifickými nároky spočívajícími v nároku na určení autorství a nároku na sdělení údajů a uveřejnění rozsudku vztahujícího se k autorskoprávnímu sporu. Těchto nároků je možno se domáhat v příslušném soudním řízení. Autorskoprávní ochrana je pak rovněž zajišťována v případě intenzivnějších porušení autorského zákon i prostředky veřejného práva – dle rozsahu takového porušení lze rozlišovat mezi správně-právní ochranou a trestněprávní ochranou.

1.4. Licenční smlouva

Jak již bylo výše naznačeno, licenční smlouva se vztahuje k případům, kdy autor využije svého výlučného majetkového práva nechat dílo užít třetí osobou.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Na základě licenční smlouvy tedy autor jakožto poskytovatel licence poskytne nabyvateli oprávnění k výkonu práva užít dílo (licenci), a to buďto k jednotlivě určeným způsobům užití anebo všem způsobům užití, přičemž rozsah užití může být smlouvou omezen či nikoliv. Není-li smlouvou sjednáno jinak, je nabyvatel povinen platit autorovi odměnu.

Účastníky licenční smlouvy jsou:

a) poskytovatel licence – zpravidla autor; může se však jednat i o dědice autora, kolektivního správce, anebo zaměstnavatele v případě zaměstnaneckého díla,

b) nabyvatel licence – kterékoliv právnická či fyzická osoba (i stát), pokud má jak způsobilost k právům a povinnostem, tak i způsobilost k právním úkonům.

Licenční smlouva může být sjednána jako výhradní anebo nevýhradní. Jedná-li se o výhradní licenční smlouvu, zavazuje se autor, že právo dílo užít neumožní další osobě, a současně (není-li sjednáno jinak) se zdrží rovněž výkonu práva dílo užít. Není-li sjednán obsah uvedený v předchozí větě, jedná se o licenci nevýhradní. Pokud smlouva výslovně neuvádí, zda se jedná o licenční smlouvu výhradní nebo o licenční smlouvu nevýhradní, stanovuje legislativní úprava právní domněnku, podle které se má vždy za to, že se jedná o licenci nevýhradní.

Pro výhradní licenční smlouvu (a některé licenční smlouvy k užití díla určeného podle druhu) je zákonem požadována písemná forma, jinak postačí ústní forma. Lze jen doporučit, aby účastníci zamýšleného autorskoprávního vztahu vždy svá vzájemná práva a povinnosti z licenční smlouvy upravili písemně.

Pro úplnost je však potřeba dodat, že třetí osoba může užít dílo autora i v některých, zákonem (nikoliv pouze autorským zákonem) stanovených případech – jedná se o případy tzv. zákonné licence. Jedná se např. o případy knihovní licence, licence pro sociální zařízení, úřední licence, zpravodajské licence. Do této kategorie spadají např. i případy citací v bakalářských, diplomových, rigorózních a disertačních.

1.4.1. Školní dílo

Autorský zákon upravuje zvláštním způsobem případ tzv. školního díla. Jedná se o případy, kdy **autorem díla je žák nebo student**, a dílo vzniklo při plnění školních nebo studijních povinností žáka nebo studenta uložených mu na podkladě jeho právního vztahu ke škole nebo školskému, popř. jinému vzdělávacímu zařízení. V takovém případě má škola nebo školské, popř. jiné vzdělávací zařízení na základě autorského zákona právo k užívání tohoto díla bezplatně v rozsahu tzv. zákonné licence.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Škola nebo školské, popř. jiné vzdělávací zařízení je však oprávněno požadovat po autorovi školního díla i licenční smlouvy v širším rozsahu, než je předpokládáno tzv. zákonnou licencí. Požadavek na uzavření licenční smlouvy v širším než zákonném rozsahu není autor oprávněn odmítnout, ledaže ho k tomu vedou závažné důvody. Při absenci závažných důvodů se škola nebo školské, popř. jiné vzdělávací zařízení může domáhat nahrazení projevu vůle autora soudním rozhodnutím.

Výslovně je pak v ustanovení § 35 odst. 3 autorského zákona stanoveno, že *„do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacímu zařízení (školní dílo).“*

Současně je však na místě uvést, že škola má na základě autorského zákona nárok na nevýhradní licenci ke školnímu dílu, a tedy autor školního díla své dílo užít či poskytnout jinému licenci, pokud takové jeho jednání není v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

V souvislosti se školními díly je potřeba rovněž upozornit na úpravu zákona č. 111/1998 Sb., O vysokých školách, v.z.p.p., podle jehož ustanovení § 47b odst. 1 platí, *„že Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a záznamu o průběhu a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje.“* Se zveřejněním závěrečné práce se nevyžaduje souhlas autora, jelikož platí, že odevzdáním práce autor souhlasí se zveřejněním své práce.

1.4.2. Zaměstnanecké dílo

Dále autorský zákon upravuje rovněž specifický případ tzv. zaměstnaneckého díla. Jde o zvláštní typ díla (odlišný od školního), neboť ve smyslu ustanovení § 58 autorského zákona platí v případě, že nebude dohodnuto něco jiného, že *„**zaměstnavatel vykonává** svým jménem a na svůj účet **autorova majetková práva k dílu**, které autor **vytvořil ke splnění svých povinností** vyplývajících…“* z právního vztahu zaměstnance a zaměstnavatele.

K postoupení práv vyplývajících z tzv. zaměstnaneckého díla třetí osobě však může zaměstnavatel přistoupit pouze se svolením autora díla (tedy zaměstnance), ledaže se tak děje prodeji závodu (dřívější právní terminologií podniku) nebo jeho části. Vykonává-li zaměstnavatel majetková práva k zaměstnaneckému dílu,

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

konstruuje autorský zákon při současné absenci obsahově odlišné dohod vyvratitelnou právní domněnku, podle které se má za to, že autor svolil ke zveřejnění, úpravám, zpracování včetně překladu, spojení s jiným dílem, zařazení do díla souborného, jakož i k tomu, aby uváděl zaměstnanecké dílo na veřejnost pod svým jménem, ledaže je sjednáno jinak.

V případě, že zaměstnavatel nevykonává majetková práva k zaměstnaneckému dílu vůbec nebo je vykonává nedostatečně, má autor právo požadovat, aby mu zaměstnavatel za obvyklých podmínek udělil licenci, ledaže existuje na straně zaměstnavatele závažný důvod k jejímu odmítnutí. Osobnostní práva autora k zaměstnaneckému dílu pak zůstávají nedotčena. Příkladem takové situace může být poměrně známý případ vynálezce kontaktních čoček prof. Wichterleho, který jako zaměstnanec tehdejší Československé akademie věd (ČSAV) vynalezl kontaktní čočky, avšak ČSAV se neměla k dalšímu šíření. Proto se prof. Wichterle jako autor domáhal toho, aby mu byla udělena licence[1].

V případě úmrtí zaměstnavatele anebo zániku zaměstnavatele bez právního nástupce nabývá oprávnění k výkonu těchto práv autor. Autor zaměstnaneckého díla má vůči zaměstnavateli právo na přiměřenou dodatečnou odměnu, jestliže se mzda nebo jiná odměna vyplacená autorovi zaměstnavatelem dostane do zjevného nepoměru k zisku z využití práv k zaměstnaneckému dílu a významu takového díla pro dosažení takového zisku, ledaže autor a zaměstnavatel mezi sebou sjednají odlišný režim. Je třeba upozornit na to, že specifický právní režim platí pro počítačové programy a databáze, jakož i kartografická díla, která nejsou kolektivními díly, když tyto se považují za zaměstnanecká díla i tehdy, byla-li autorem vytvořena na objednávku. (tedy mimo pracovní poměr).

Do roku 2013 byla zákonná ustanovení o licenční smlouvě obsažena v autorském zákoně, s účinností od 1. ledna 2014 pak upravuje licenční smlouvu zákon č. 89/2012 Sb., Občanský zákoník, v.z.p.p. (veřejně známý a dále zde též označovaný jako tzv. nový občanský zákoník).

1.4.3. Zvláštní druhy vymezení autorských práv

Existuje poměrně mnoho pokusů o sjednocení přístupu k autorské ochraně děl, která se snaží umožnit k dílům přístup na nekomerční bázi, tedy většinou zdarma. Některé z nich zde stručně popíšeme.

[1] Zde je namístě poznamenat, že jde pouze o příklad inspirovaný zmíněnou událostí, k níž sice došlo, ale jejíž právní rámec byl poněkud odlišný, a aplikovala se tam odlišná zákonná ustanovení.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Creative commons

Zvláštní případy licence pak představují tzv. Creative commons (CC). Jedná se o soubor veřejných licencí rozšiřujících možnosti v oblasti publikování autorských děl, resp. přesněji řečeno vymezují status autora při jeho rozhodování o podmínkách zpřístupnění autorského díla.

Licence Creative commons jsou založeny na tom, že autor jejich prostřednictvím plošně uzavírá se všemi potencionálními uživateli díla smlouvu, kterou jim poskytuje některá svá práva k dílu a jiná nikoliv.

Obsah licence Creative commons se pak určuje mezinárodně srozumitelnými piktogramy- Creative commons obsahují řadu možných omezujících podmínek, která může autor díla k dílu šiřitelnému podle CC připojit.

Piktogramy (prvky) určující podmínky, které je nutno při nakládání s dílem respektovat:


Právo dílo šířit

Tento symbol je společný pro všechny typy Creative commons licencí. Vyjadřuje, že licencovaného dílo je možné šířit, tzn. kopírovat, distribuovat a sdělovat veřejnosti. Zároveň lze dílo zařadit do souborného díla (např. sborníku či časopisu) a jako jeho součást jej v nezměněné podobě šířit dál.


Právo dílo upravovat

Licence s tímto symbolem opravňuje uživatele k pozměňování či doplňování díla. Umožňuje také celé licencované dílo nebo jeho část zpracovat s jiným dílem. Příkladem úprav může být např. dramatizace, překlad, úprava digitálních fotek, zhudebnění nebo remixování hudebních skladeb.


Uveďte autora

Jedná se o společný prvek pro všechny licence. Kdykoliv je licencované dílo nebo jeho úprava dále šířena, je nutno uvést údaje a autorovi a dílu, a to způsobem, jaký autor stanovil. Pokud autor způsob uvádění těchto údajů nespecifikoval, je nutné minimálně uvést jeho jméno (nebo pseudonym, pokud pod ním vystupuje), název díla a odkaz na původní licenci Creative commons. Pokud dochází k šíření upraveného díla, je třeba také uvést způsob, jakým způsobem bylo dílo upraveno.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Zachovejte licenci

Dojde-li k jakékoliv úpravě licencovaného díla, je povinností výsledek provedených úprav díla vystavit pod stejnou nebo slučitelnou licenci.

Neužívejte dílo komerčně

Toto omezení umožňuje nakládat s dílem pouze pro nekomerční účely. Tím se rozumí, že při šíření díla nesmí autorovi plynout žádný finanční zisk. Za nekomerční využití se považuje výměna díla za jiné (např. prostřednictvím výměnných sítí).

Nezasahujte do díla

Toto omezení zakazuje jakkoliv dílo upravovat (tzn. dílo pozměňovat či doplňovat, nebo ho jako celé či jeho část zpracovat s dílem jiným). Jedná se o opak licenčního prvku „právo dílo upravovat", který úpravy díla naopak právě povoluje (proto se v žádné licenci Creative commons neobjevují tyto dva prvky společně).

Bližší informace o licencích Creative commons lze nalézt na webových stránkách příslušné střešní organizace (https://creativecommons.org/). Protože jsou zde uvedené texty převážně v angličtině, která nemusí být pro všechny čtenáře zejména v právnických výrazech dostatečně srozumitelná, existuje i český výtah (http://www.creativecommons.cz/).

General Public License (GPL)

GNU General Public License, GNU GPL je licence pro svobodný software. Obecně se dá říci, že pokud autor označí svoje dílo jako dílo podléhající licenci GPL, zříká se tím všech majetkových práv s dílem spojených. Neznamená to ovšem, že by se zřekl všech práv autora. Především výlučná osobnostní práva autora tím zůstávají nedotčena. Protože je tato problematika úzce spojena s výše zmíněnými Creative commons, ale díky své historii mají GPL své samostatné licenční podmínky, odkazuji zájemce o tuto problematiku na podmínky licence GPL (http://www.gnugpl.cz).

1.5. Kolektivní správa autorských práv

Autorský zákon rovněž v ustanovení § 95 a násl. autorského zákona upravuje kolektivní správu autorských práv. Obecně lze konstatovat, že kolektivní správou je zastupování předem nekonkretizovaného většího okruhu osob, kterým náležejí oprávnění vzešlá z autorského zákona, a to k jejich společnému prospěchu.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Zmíněné zastupování je realizováno ve vztahu k výkonu majetkových autorských práv a majetkových práv souvisejících s právem autorským a umožnění zpřístupňování předmětů těchto práv veřejnosti.

V současné době působí na území České republiky mimo jiné následující správci kolektivních práv:

OSA – Ochranný svaz autorský pro práva k dílům hudebním;

INTERGRAM – Nezávislá společnost výkonných umělců a výrobců zvukových a zvukově-obrazových záznamů;

OOA-S – Ochranná Organizace Autorská – Sdružení autorů děl výtvarného umění, architektury a obrazové složky audiovizuálních děl;

GESTOR – Ochranný svaz autorský.

Problematika kolektivní správy autorských práv je poměrně rozsáhlá a poněkud komplikovaná, a přitom se přímo netýká většiny běžných aplikací ICT, proto zde nebude podrobněji rozebírána. Pro zájemce odkazuji na Hlavu IV. autorského zákona [4] (§95-104).

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

2. Aplikace autorského zákona v oblasti digitálních technologií

2.1. Úvod

Autorský zákon v platném znění obsahuje zvláštní ustanovení (viz §65 a §66), která upřesňují jeho aplikaci na počítačové programy. Základním principem je, že počítačový program požívá stejné ochrany jako literární dílo, Zcela v souladu s tímto principem pak zákon stanovuje, že chráněn je konkrétní program, nikoli myšlenky a principy, na nichž je založen.

Je třeba podotknout, že zejména autorské ochrany počítačových programů, zejména jejich licenčních smluv, se týká také část občanského zákoníku (zákon 89/2012 Sb.), konkrétně jeho oddíl 5, pododdíl 2, který se nazývá Zvláštní ustanovení pro licenci k předmětům chráněným autorským zákonem.

Na úvod je třeba uvést, že přes rozšířené přesvědčení běžné veřejnosti se počítačové programy neprodávají jako běžné zboží, ale zaplacením získává zákazník pouze svolení k jeho užívání za podmínek stanovených licenční smlouvou.

Paragraf 66 autorského zákona pak výslovně uvádí některé činnosti, které vlastník licence k používání počítačovému programu (v zákoně označený výrazem „oprávněný uživatel“) smí provádět, aniž by tím porušoval autorskou ochranu programu.

Pro účely zabránění nejasnostem zde uvádím plné znění odstavců 1 - 4 §66, které vymezují tyto činnosti.

„*(1) Do práva autorského nezasahuje oprávněný uživatel rozmnoženiny počítačového programu, jestliže*

a) rozmnožuje, překládá, zpracovává, upravuje či jinak mění počítačový program, je-li to nezbytné k využití oprávněně nabyté rozmnoženiny počítačového programu, činí-li tak při zavedení a provozu počítačového programu nebo opravuje-li chyby počítačového programu,

b) jinak rozmnožuje, překládá, zpracovává, upravuje či jinak mění počítačový program, je-li to nezbytné k využití oprávněně nabyté rozmnoženiny počítačového programu v souladu s jeho určením, není-li dohodnuto jinak,

c) zhotoví si záložní rozmnoženinu počítačového programu, je-li nezbytná pro jeho užívání,

d) zkoumá, studuje nebo zkouší sám nebo jím pověřená osoba funkčnost počítačového programu za účelem zjištění myšlenek a principů, na nichž je

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

založen kterýkoli prvek počítačového programu, činí-li tak při takovém zavedení, uložení počítačového programu do paměti počítače nebo při jeho zobrazení, provozu či přenosu, k němuž je oprávněn,

e) rozmnožuje kód nebo překládá jeho formu při rozmnožování počítačového programu nebo při jeho překladu či jiném zpracování, úpravě či jiné změně, je-li k ní oprávněn, a to samostatně nebo prostřednictvím jím pověřené osoby, jsou-li takové rozmnožování nebo překlad nezbytné k získání informací potřebných k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu s jinými počítačovými programy, jestliže informace potřebné k dosažení vzájemného funkčního propojení nejsou pro takové osoby dříve jinak snadno a rychle dostupné a tato činnost se omezuje na ty části počítačového programu, které jsou potřebné k dosažení vzájemného funkčního propojení.

(2) Za rozmnožování počítačového programu podle tohoto zákona se považuje i zhotovení rozmnoženiny, je-li nezbytná k zavedení a uložení počítačového programu do paměti počítače, jakož i pro jeho zobrazení, provoz a přenos.

(3) Za pronájem či půjčování podle tohoto zákona se nepovažuje pronájem nebo půjčování rozmnoženiny počítačového programu, kde samotný program není podstatným předmětem pronájmu nebo půjčování.

(4) Informace získané při činnosti podle odstavce 1 písm. e) nesmějí být poskytnuty jiným osobám, ledaže je to nezbytné k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu, ani využity k jiným účelům než k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu. Dále nesmějí být tyto informace využity ani k vývoji, zhotovení nebo k obchodnímu využití počítačového programu podobného tomuto počítačovému programu v jeho vyjádření nebo k jinému jednání ohrožujícímu nebo porušujícímu právo autorské.“ [4]

Po prostudování je vidět, že zákon vlastníkovi umožňuje, aby prováděl činnosti směřující k řádnému využívání programu včetně jeho napojení na jiné programy, k jeho zálohování apod., ale že mu neumožňuje program např. dále šířit či k takové činnosti napomáhat jiným.

2.2. Úplatná zákonná licence

Paragraf 72 autorského zákona vymezuje tzv. úplatnou zákonnou licenci, která se týká zvukových záznamů uměleckých děl a dotýká se také problematiky

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

kolektivní správy autorských práv zmíněné v závěru první kapitoly. Úplné znění příslušného paragrafu zde opět uvádíme:

„§ 72 Úplatná zákonná licence

(1) Do práva výkonného umělce nezasahuje, kdo užije umělecký výkon zaznamenaný na zvukový záznam vydaný k obchodním účelům vysíláním rozhlasem nebo televizí, přenosem rozhlasového nebo televizního vysílání; výkonnému umělci však přísluší právo na odměnu za takové užití. Toto právo může výkonný umělec vykonávat pouze prostřednictvím příslušného kolektivního správce.

(2) Zvukovým záznamem vydaným k obchodním účelům pro účely tohoto ustanovení se rozumí zvukový záznam, jehož rozmnoženiny jsou rozšiřovány prodejem, nebo který je oprávněně veřejnosti sdělován podle § 18 odst. 2.

(3) Do práva výkonného umělce však zasahuje ten, kdo před užitím způsobem uvedeným v odstavci 1 neuzavře s příslušným kolektivním správcem smlouvu, kterou se stanoví výše odměny za takové užití a způsob jejího placení.

(4) Do práva výkonného umělce zasahuje i ten, komu příslušný kolektivní správce zakázal další užití výkonu způsobem uvedeným v odstavci 1, protože je vůči němu v prodlení se zaplacením odměny za takový způsob užití a tuto odměnu nezaplatí ani v dodatečné třicetidenní lhůtě za tím účelem mu kolektivním správcem poskytnuté. Neomezí-li kolektivní správce takový zákaz na kratší dobu, trvá zákaz až do doby, kdy bude závazek zaplatit odměnu splněn nebo jinak zanikne; dojde-li k porušení zákazu, neskončí však bez souhlasu kolektivního správce trvání zákazu dříve, než budou vypořádány i nároky z takového porušení vzniklé.“ [4]

Z textu tohoto paragrafu plyne, že autorské právo připouští veřejné provozování zvukových záznamů, nicméně obecně řečeno toto podléhá placení poplatku, a to podle odst. 1 **výlučně kolektivnímu správci** autorských práv, v tomto případě zpravidla OSA (půjde-li o hudební dílo).

Je třeba poznamenat (viz §18), že sdělování zvukového záznamu se nemusí dít pouze tradičními cestami, tedy např. rozhlasem apod., ale rovněž pomocí ICT. Znamená to, že ustanovení §72 se vztahují také na provozovatele služeb typu Youtube, ale podle ustanovení §72 především na ty, kteří takové dílo zde zveřejní.

Někdy se však pojem úplatná zákonná licence používá i v souvislosti s počítačovými programy, nicméně z hlediska autorského zákona jde o nepřesné použití tohoto pojmu.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

2.3. Aplikace autorského práva na databáze

Zcela specifickou problematikou, která je autorským zákonem upravena v samostatné Hlavě III, konkrétně v paragrafech 88-94. Důvodem pro samostatné vymezení ochrany je odlišný charakter databáze a jejího používání od počítačových programů či literárních děl.

Databáze je autorským zákonem chráněna pouze tehdy, pokud „*pořízení, ověření nebo předvedení obsahu databáze představuje kvalitativně nebo kvantitativně podstatný vklad*“, a to bez ohledu na to, zda „*databáze nebo její obsah jsou předmětem autorskoprávní nebo jiné ochrany*.“[4] §88a.

Vlastník (podle zákona „pořizovatel“) databáze má právo převádět (v praxi často za úplatu, tedy de facto prodávat) právo pro přístup do databáze pro účely vyhledávání podstatných částí v databázi jiným subjektům, zákazníkům. Pokud je databáze zpřístupněna veřejnosti, je zde podobně jako u literárních děl poskytována vědecká a vyučovací licence (zákon pro splnění podmínek vyžaduje uvedení pramene a nevýdělečný účel použití), a licence pro osobní potřebu bezplatně. Toto blíže specifikují § 90 a 91, které opět cituji v plném znění:

*„**§ 90***

Obsah zvláštního práva pořizovatele databáze

(1) Pořizovatel databáze má právo na vytěžování nebo na zužitkování celého obsahu databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva.

(2) Vytěžováním podle odstavce 1 se rozumí trvalý nebo dočasný přepis celého obsahu databáze nebo jeho podstatné části na jiný podklad, a to jakýmikoli prostředky nebo jakýmkoli způsobem.

(3) Zužitkováním podle odstavce 1 se rozumí jakýkoli způsob zpřístupnění veřejnosti celého obsahu databáze nebo jeho podstatné části rozšiřováním rozmnoženin, pronájmem, spojením on-line nebo jinými způsoby přenosu.

(4) Půjčování originálu nebo rozmnoženiny (§ 16) databáze není vytěžování podle odstavce 2 ani zužitkování podle odstavce 3.

(5) Opakované a systematické vytěžování nebo zužitkování nepodstatných částí obsahu databáze a jiné jednání, které není běžné, přiměřené a je na újmu oprávněným zájmům pořizovatele databáze, není dovoleno.

(6) Právo pořizovatele databáze je převoditelné.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

§ 91

Omezení zvláštního práva pořizovatele databáze

Do práva pořizovatele databáze, která byla zpřístupněna jakýmkoli způsobem veřejnosti, nezasahuje oprávněný uživatel, který vytěžuje nebo zužitkovává kvalitativně nebo kvantitativně nepodstatné části obsahu databáze nebo její části, a to k jakémukoli účelu, za podmínky, že tento uživatel databázi užívá běžně a přiměřeně, nikoli systematicky či opakovaně, a bez újmy oprávněných zájmů pořizovatele databáze, a že nezpůsobuje újmu autorovi ani nositeli práv souvisejících s právem autorským k dílům nebo jiným předmětům ochrany obsaženým v databázi.“ [4]

Další podstatnou odlišností autorskoprávní ochrany databází je výrazně kratší délka období ochrany, která činí 15 let (viz §93).

2.4. Porušení ustanovení autorského zákona

Ustanovení autorského zákona jsou často porušována, a to jak fyzickými osobami, tak i společnostmi. V případě autorského zákona nejsou stanovena žádná jednání jako přestupková, což znamená, že porušení autorského zákona je sankciováno pouze v rovině soukromého práva (nejčastěji ve formě žaloby o náhradu vzniklé škody), a v případech stanovených trestním zákonem pak jako trestné činy.

Nicméně přesto existují zákony, které mají aplikaci i do oblasti ICT, z nichž vyplývá možné spáchání přestupku. Proto zde uvádíme základní informace o přestupcích, abychom si uvědomili, jakým sankcím jsou případní narušitelé vybraných zákonných ustanovení vystaveni, uvádíme zde základní informace o přestupcích.

Přestupek je zaviněné jednání osoby, která porušila příslušné ustanovení zákona. Přestupkem může být jen takové jednání, které je společensky nebezpečné. Posouzení toho, které jednání takové je, a které ne, však je vždy na posouzení příslušného orgánu (u přestupků zpravidla obecního úřadu), proto nedoporučujeme, aby se o laický výklad tohoto pravidla pokoušeli sami potenciální pachatelé.

Podobně jako v případě trestných činů nejsou za přestupková jednání odpovědné osoby mladší 15 let. To ovšem neznamená, že za takové jednání nemůže nést odpovědnost někdo jiný, komu byla taková nezletilá osoba svěřena do péče.

Přestože se řada přestupků často projednává ve zjednodušeném režimu tzv. blokového nebo příkazního řízení, v případě porušení autorského zákona to stěží

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

přichází v úvahu. Půjde tedy zpravidla o správní řízení před místně příslušným obecním úřadem.

Možné sankce za přestupek jsou tyto:

- napomenutí,
- pokuta,
- zákaz činnosti,
- propadnutí věci.

Zejména poslední dvě sankce mohou na pachatele dopadnout velmi citelně, a proto je třeba vždy posuzovat případné jednání, u něhož si nejsme jisti jeho přípustností, velmi obezřetně.

Navíc podobně jako v případě trestného činu, o jehož spáchání rozhoduje vždy soud, může i v případě spáchání přestupku vzniknout škoda jiné osobě nebo organizaci (poškozenému). Poškozený se pak může v doprovodném (adhezním) řízení domáhat náhrady škody. Přitom je třeba mít na paměti, že až do nedávna bylo zcela běžné, že soudy v případě řízení o náhradu škody z titulu porušení autorských práv stanovovaly náhradu škody velmi výrazně ve prospěch poškozených. Typické bylo (a dosud někdy je) například počítat ušlý výnos z prodeje jako součin prodejní ceny jedné licence a počtu stažení neoprávněně zpřístupněných dat (například programu). (podle [5]).

Rozhodně se nevyplatí spoléhat na to, že řada přestupků nebude potrestána třeba proto, že uplyne lhůta 1 roku pro jeho projednání. Navíc řízení o náhradě škody není tímto „promlčením“ potrestání za přestupek dotčeno.

3. Licenční podmínky počítačových programů

3.1. Pojem počítačový program

Program je posloupnost instrukcí, které má program provádět. Tvůrce programu program vytváří pomocí některého programovacího nástroje či integrovaného prostředí (IDE) v některém z programovacích jazyků. Příkazy programovacích jazyků jsou však zpravidla komplexní (vyžadující řadu elementárních operací procesoru počítače), proto je nutné program z podoby zápisu v programovacím jazyce převést do podoby spustitelné na konkrétním procesoru (tzv. binární kód). Tento proces se nazývá kompilace nebo překlad. Je třeba upozornit na to, že binární kód je možno spustit jen na procesorech, pro které byl vytvořen. Navíc každý program využívá specifických služeb operačního systému, které jsou v každém operačním systému

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

odlišné, takže proto například není možné spustit programy pro OS Windows a procesory Intel ani na počítači s jiným operačním systémem (např. MacBook, i když má také procesor Intel), ani na počítači s jiným procesorem (např. na tabletu s Windows, protože nemá procesor stejného typu).

Tvůrce programu zpravidla dává k dispozici svůj program (bezplatně či za úplatu) v podobě binárního kódu pro určitý konkrétní procesor a operační systém. Protože součástí zprovoznění programu na počítači obvykle bývá ověření podmínek (přítomnost dalších programů, například určitého www prohlížeče), či služeb apod., jsou programy často distribuovány v podobě tzv. instalačního balíčku. Instalační balíček obsahuje kromě potřebných dat instalační program (opět spustitelný pouze na určitém OS a procesoru), který provede kontrolu podmínek pro spuštění samotného programu, případně sám doplní potřené komponenty nebo o to požádá uživatele, a teprve po splnění technických podmínek samotný program nainstaluje (zpravidla jde o extrakci z archivu, zapsání potřebných informací do systémové databáze – registry ve Windows, apod.). Teprve po instalaci je možno program spouštět. Součástí instalace bývá úkon uživatele vyjadřující souhlas s licenčními podmínkami, který podle zákona nahrazuje podpis licenční smlouvy.

3.2. Typy licencí počítačových programů

3.2.1. Licenční podmínky

Licence v oblasti užívání softwaru znamená oprávnění (povolení) dané uživateli programu k používání počítačového programu za daných podmínek podle tzv. licenční smlouvy. To je smlouva, kterou uzavírá kupující programu s autorem (výrobcem) při legálním nabytí programu. Ve velké většině případů se programy neprodávají, ale se pouze propůjčují k používání (tzv. licencují). Pojem licencování pochází z toho, že se uživatel programu s autorem nebo distributorem uzavírá smlouvu o povolení používání programu, která se i podle českých zákonů označuje jako licenční smlouva. Licencovaný program není možno např. dále prodávat či jinak šířit (to zakazuje přímo autorský zákon, viz §6 citovaný výše), a je možné jej používat jen za dodržení podmínek uvedených v licenční smlouvě.

Je třeba poznamenat, že omezení pro užívání programu stanovená autorským zákonem (viz výše citovaný §66) samozřejmě platí v každém případě a pro všechny programy bez ohledu na licenci, pod kterou jsou šířeny. Autor zpravidla

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

ani nemůže rozsah těchto omezení zmenšit, pokud mu to formulace zákona výslovně neumožňuje. Nejběžnější typy licencí, se kterými se při pořizování programového vybavení můžete setkat:

Demoverze

Program s licencí Demo (Demoverze) verze slouží především k předvedení schopností daného programu, ale ne k jeho běžnému používání. Funkčnost demoverze programu bývá nějakým způsobem výrazně omezena, např. je omezeno nebo zakázáno ukládání dat, jejich zobrazování nebo zpracování. Demoverze bývá často také omezena časově. Bývá zvykem označovat funkčně omezenou verzi Demo a časově omezenou verzi Trial, i když u některých výrobců nalezneme odlišnosti.

Freeware

Autor poskytuje program pro vlastní uspokojení nebo pro prosazení pokrokového nápadu k volnému šíření. Stále se však jedná o autorsky chráněný software, tj. můžete s ním dělat jen to, co bylo výslovně autorem povoleno. Obvykle autor souhlasí s bezplatným používáním, nikoliv však s prodejem či jeho pozměňováním. Jinak však jde o plnohodnotný program bez omezení funkčnosti či doby fungování.

Plná verze (komerční software)

Kompletní program bez jakéhokoli omezení funkčnosti. Omezení týkající se nakládání s programem (např. ta již zmíněná výše) obvykle zůstávají v platnosti.

Public Domain

Uvedením této licence se autor vzdává kontroly nad publikovaným software - můžete jej volně šířit a používat, ale i měnit či zahrnout do svých aplikací. I přesto je obvykle nějaká licenční smlouva definující povolené a nepovolené způsoby nakládání s programem přiložena. Pozor, nezaměňujte s licencí Freeware. U Public domain programů je zpravidla k dispozici i zdrojový kód programu. Někde mezi těmito dvěma licencemi stojí časté modelu licencování označované jako GPL (viz níže).

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Shareware

Produkty jsou pod touto licencí šířeny zdarma, obvykle jsou však funkční jen po nějakou omezenou dobu, nebo s omezenými funkcemi. Autor obvykle požaduje zaplacení finanční částky (obvykle dosti nízké) až v případě, kdy se uživateli produkt líbí a běžně jej používá. V takovém případě pak program ztratí vestavěná omezení, pokud nějaká má.

Zaplacením této částky se stává registrovaným uživatelem, může dostávat aktualizace, případně je mu k dispozici on-line podpora. Shareware býval v počátcích velmi levný – byl většinou produktem jednoho vývojáře a byl distribuován přímo klientům. Díky značnému rozšíření Internetu se z této licence stal naprosto obvyklý způsob distribuce software, který využívají i dříve typické „krabicové“ produkty z oblasti komerčního software.

Start

Zvláštní případ licencování produktu. Je to plně funkční verze omezená pouze např. počtem záznamů do databáze. Lze ho používat bezplatně i několik let, včetně upgrade. Přechod na placenou a počtem záznamů neomezenou verzi bývá zpravidla bezproblémový a bez ztráty dosavadních dat.

Další typy licencí, pro běžného uživatele méně časté:

Adware

Užívání software šířeného pod touto licencí je bezplatné, ale v programu se zobrazuje reklama, ze které je jeho vývoj placen. Odstranění reklamy je nemožné a ani není v souladu s licencí. Reklama bývá většinou stahována z Internetu.

Artistic License

Software šířený pod touto licencí umožňuje volné používání, modifikování i šíření za předpokladu, že budete šířit software bezplatně nebo zamezíte možnosti záměny mezi vlastní verzí a standardní verzí. Licence nevylučuje využití softwaru v komerčních projektech. Licence je schválená sdružením OSI a plně odpovídá Debian Free Software Guidelines.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Cardware

Software je možno neomezeně užívat v případě, že autorovi zašlete skutečnou pohlednici. Autor si tak zajistí nejen přísun pošty do své schránky, ale i přehled o místech, kde se jeho program užívá. Pro tuto licenci se někdy také používá název Postcardware.

Donationware

Volně šiřitelný software, u nějž zaplacení za jeho používání je čistě dobrovolné a autor k němu nenutí. Pokud má uživatel dojem, že by bylo vhodné ocenit kvalitu autorovy práce, může zaslat na jeho konto, zpravidla uvedené v samotném programu, libovolný příspěvek.

GPL

GNU General Public License. Software šířený pod licencí GPL je možno volně používat, modifikovat i šířit, ale za předpokladu, že tento software bude šířen bezplatně (případně za distribuční náklady) s možností získat bezplatně zdrojové kódy. Toto opatření se týká nejen samotného softwaru, ale i softwaru, který je od něj odvozen. Na produkty šířené pod GPL se nevztahuje žádná záruka. Licence je schválená sdružením OSI a plně odpovídá Debian Free Software Guidelines.

MPL

Mozilla Public License. Základním elementem pokrytým licencí je každý jednotlivý zdrojový soubor. Autor takového souboru umožňuje komukoliv používat, měnit a distribuovat jeho zdrojový kód (i jako součást většího díla). Každá změna původních souborů je krytá licencí, tzn., musí se zveřejnit. Totéž platí, pokud přenesete část původního souboru do nového souboru, tj. celý nový soubor je pak nezbytné zveřejnit. Pokud vytváříte nový produkt přidáním nových souborů, můžete pro tyto nové soubory použít libovolnou licenci. Binární verze lze licencovat libovolně, pokud to není výslovně v rozporu s MPL (zákaz distribuce zdrojů). Produkty pod touto licencí jsou distribuované, jak jsou ("as is"), tj. bez záruk libovolného druhu.

Vim's license

Licence kompatibilní s GPL (tedy je software šířený pod touto licencí považován za volně šiřitelný software) použitá pro editor Vim. Umožňuje šířit nezměněné dílo bez jakýchkoliv omezení, jen musí být přiložen text licence. Pokud chcete šířit

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

pozměněné dílo, musíte dodržet několik nepříliš omezujících podmínek uvedených v textu licence.

Orphanware

Jde o spíše neformální označení programu, který byl zpravidla šířen pod nějakou licencí umožňující volné šíření programu. ale program již není samotným autorem podporován nebo nabízen veřejnosti. Lze ho získat pouze z pořízených kopií. Funkčnost ani podpora tohoto programu není zaručena. Jako orphanware může být označen také freeware program, u kterého je jasné, že jeho vývoj byl ukončen a nebude další nová verze.

SGSL - Sun Community Source License.

Pod touto licencí byla šířena především Java 2 (tedy JDK a JRE verze 1.2 a výš). Poměrně problematická licence - především nemáte (až na omezené případy) právo dále distribuovat dílo šířené pod SCSL. Licence není schválená sdružením OSI, neodpovídá Debian Free Software Guidelines.
V textu byly použity informace z [6] a [7].

3.3. Distribuce počítačových programů

Počítačové programy jsou mezi uživatele distribuovány řadou cest a v řadě různých forem. Ty nejobvyklejší jsou popsány dále.

Krabicový prodej

Tradiční způsob „krabicového prodeje“, kdy uživatel dostal datový nosič (např. CD nebo DVD disk) v krabici spolu s návodem k použití (v dnešní době bývá v tištěné podobě nanejvýš návod k samotné instalaci programu) postupně mizí, přesto se s ní stále setkáváme. Její výhodou je, že při prodeji této „krabice“ zpravidla obdržíme doklad o zakoupení produktu, kterým se můžeme později prokázat, pokud by někdo (například policie) prověřoval řádné nabytí programu (resp. práva k jeho používání). Dříve často bývaly součástí krabice různé zabezpečovací prvky (například registrační kódy, licenční štítky apod.).

Zatímco smysl licenčních štítků je v praxi (zejména pro prokazování oprávněného nabytí programu) spíše omezený, registrační či podobné zabezpečovací kódy, bez jejichž znalosti program nelze instalovat nebo aktivovat jeho funkce, se používají i pro jiné způsoby distribuce. Zde je namístě připomenout,

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

že na technické prostředky ochrany před porušováním podmínek pro šíření počítačových programů, ale i jiných digitálních dat, pamatuje i autorský zákon, konkrétně §43, jehož první odstavec zní:

„(1) Do práva autorského neoprávněně zasahuje ten, kdo obchází účinné technické prostředky ochrany práv podle tohoto zákona.“[4]

V praxi to znamená, že například neoprávněným předáním registračního kódu k programu jiné osobě se dopouštíme neoprávněného zásahu do autorského práva (protože i registrační kód je dosud považován za účinný technický prostředek ochrany autorských práv tvůrce daného programu). Takové jednání může být následně vyhodnoceno jako přestupek či dokonce trestný čin, a podle toho i potrestáno.

Elektronická distribuce programů

Mnoho firem dnes dává přednost elektronické distribuci programů. Existuje celá řada způsobů, jak program je možné elektronicky distribuovat, od vystavení na webu s následnou samostatnou distribucí registračních kódů, až po sofistikované způsoby šíření pomocí speciálních úložišť.

Tento způsob se dříve používal především pro volně šiřitelné (bezplatné) programy, dnes je však již zcela běžný i pro komerční software, Rozdíl je často pouze v tom, že bezplatný software zpravidla nepoužívá registrační kódy nebo je jejich získání snadné a rychlé, zatímco u komerčního software je používání registračních či bezpečnostních kódů pravidlem a jejich získání je obvykle podmíněno předchozí úhradou ceny za licenci. Distribuční kanál pro registrační kódy je u komerčního software zpravidla volen tak, aby poskytoval vyšší úrove zabezpečení (například SMS zprávy, papírová distribuce apod.).

V případě **elektronické distribuce** programů existuje jedno **riziko**, které v případě krabicové distribuce prakticky nehrozí. Toto riziko spočívá v tom, že pokud program získáváme (zpravidla „stahujeme“) z veřejně dostupného úložiště (např. webu firmy výrobce), nemáme záruku, že nám nějaký útočník nepodstrčí ke stažení mírně modifikovanou verzi programu doplněnou o nějaký škodlivý kód. V takovém případě by se nejspíše jednalo o tzv. trojského koně, který bude podrobněji popsán v následující kapitole. Proto doporučujeme vždy program stahovat pouze z oficiálních úložišť, a v případě stažení z webu si po stažení ověříme podle dostupných pomůcek (např. MD5 otisku) neporušenost (integritu) staženého programu. Zvlášť velké je toto riziko v případě aplikací pro mobilní telefony a tablety.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Zde důrazně doporučujeme programy stanovat pouze z oficiálních úložišť výrobců (např. Android Market), která jsou pod kontrolou výrobce příslušného operačního systému a riziko jejich napadení je velmi malé. V případě běžných operačních systémů pro počítače (zejména Windows) bohužel takové zabezpečené úložiště neexistuje.

On-line (webové) služby

V poslední době je řada programů poskytována formou tzv. cloudové služby. V takovém případě používáme pouze služby programu, který běží ne serveru v Internetu, a na našem počítači k jejich využívání potřebujeme pouze vhodný www prohlížeč. Přesto i v takovém případě pro nás platí autorský zákon. V takovémto případě by připadalo porušení autorských práv mohlo spočívat především v poskytnutí přístupu ke službě osobě, která k ní nemá oprávněný přístup.

V každém případě (ať licenci k programu získáme jakýmkoli způsobem a pod jakoukoli licencí, placenou či bezplatnou), je v zájmu uživatele programu ponechat si veškeré doklady dokládající způsob získání programu, zaplacenou cenu, identifikaci prodávajícího, licenční podmínky apod. V budoucnu se může stát, že budeme potřebovat doložit tyto údaje například policii (v případě vyšetřování možné trestné činnosti), finančnímu úřadu (jako organizace nebo živnostník) apod. a bez uchování dokladů to může být obtížné.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

4. Zásady bezpečného používání Internetu

4.1. Společné zásady bezpečnosti

Služby Internetu vznikaly v době, kdy počet jejich uživatelů dosahoval nejvýše několika tisíc. Proto u původních služeb nebyl kladen důraz na zabezpečení, a původní služby nebyly vybaveny žádnými bezpečnostními mechanismy (např. služba www), nebo jsou zde používané bezpečnostní mechanismy z dnešního pohledu nedostatečné (např. autentizace jménem a heslem zasílaným po síti v nešifrované podobě, například v případě elektronické pošty, FTP či telnetu).

V reakci na prudký nárůst uživatelů Internetu, který započat v devadesátých letech 20. století díky vzniku služby www a jejího pronikání do komerční sféry, začaly vznikat bezpečnější alternativy k původně nezabezpečeným službám. Proto dnes můžeme pro zabezpečený šifrovaný přístup k webovým stránkám používat protokol HTTPS, do schránky elektronické pošty můžeme přistupovat zabezpečeným přenosem využívajícím protokol SSL/TLS, samotné zprávy elektronické pošty můžeme podepisovat a šifrovat pomocí certifikátů, pro terminálový přístup a přenos souborů můžeme používat protokol SSH.

Rozhodnutí o tom, jakou službu bude používat (zda původní bez zabezpečení, nebo zabezpečenou), je na každém uživateli. Pro některé účely postačí nižší účely zabezpečení (například ne vždy je nutné šifrovat obsah přenášených zpráv), ale základní zabezpečení chránící přístupové údaje bychom měli aplikovat prakticky vždy. Je to z toho důvodu, že sofistikovanější útočníci často sbírají přístupové údaje k nejrůznějším účtům, které však nemusí zneužít okamžitě (například v případě e-mailových účtů obvykle jednotlivý účet ani moc snadno zneužít nejde), ale mohou buď čekat na shromáždění potřebného počtu, nebo na to, až se objeví vhodná příležitost.

Velmi důležitou součástí bezpečnostních zásad je dbát na aktuálnost používaného programového vybavení. V dnešní době se nové hrozby z Internetu objevují prakticky denně. Na tyto nové hrozby pak reagují výrobci software včetně operačních systémů tím, že zamezují těmto novým hrozbám v síření a provádění škodlivých činností. Pokud však ponecháme své programové vybavení (zejména operační systém) bez instalace aktualizací, ponecháváme tím útočníkům možnost nadále náš počítač napadnout, či v případě, že již k napadení došlo, v pokračování škodlivé činnosti. V nedávné výzkumné studii [9] jsme například ukázali, že velké množství serverů po celém světě ještě pořád napadá síťový červ Conficker, který se

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

poprvé objevil v listopad 2008, tedy před více než 6 lety. Přitom pokud by byly na všechny počítače instalovány aktualizace operačních systémů, které byly dány k dispozici již před koncem roku 2008, tento červ by již dávno vymizel. To jen dokumentuje zásadní důležitost aktualizací operačního systému jak na serverech, tak na osobních počítačích či jiných personálních zařízeních.

4.1.1. Ochrana hesel

K nejdůležitějším zásadám bezpečné práce s Internetem patří správná a bezpečná práce s hesly. Tento aspekt práce je o to důležitější, že dnes prakticky nenajdeme uživatele Internetu, který by neměl nikde v Internetu žádný uživatelský účet, k němuž se přihlašuje pomocí autentizace heslem. Navíc s tím, jak uživatelé svěřují on-line službám stále více dat včetně důležitých až kritických, nabývá správná práce s hesly stále větší důležitosti.

Obecně platí, že každé heslo by mělo být co nejodolnější proti uhodnutí i proti tzv. útoku hrubou silou, který spočívá ve vyzkoušení všech kombinací. Zatímco odolnosti proti uhodnutí se dosahuje tím, že jako hesla zásadně nikdy nepoužíváme své osobní údaje (například datum narození či rodné číslo), ani známá jména z našeho okolí (jména dětí, manželky, psa, vnoučat) či jiné údaje, které může potenciální útočník zjistit z jiných zdrojů, odolnost hesla proti útoku hrubou silou závisí především na jeho délce (počtu znaků) a množství znaků, z nichž se heslo tvoří.

Většině uživatelů je známo, že například 5 znakové číselné heslo nabízí pouze 10^5=10 000 možných kombinací, což je počet, který dovede vhodně naprogramovaný robotický software vyzkoušet během několika sekund, stejně dlouhé heslo tvořené malými a velkými písmeny anglické abecedy a číslicemi umožňuje vytvořit $(2*26+10)^5$=916 132 832 různých hesel, což pro robota sice není neřešitelné, ale představuje to téměř 10 000 krát větší výpočetní čas. Pokud bychom délku hesla zvýšili na 8 znaků, dostáváme při stejné množině znaků více než 216 miliard možných hesel, což dnešní roboty ani při zapojení mnoha výkonných počítačů nedovedou dostatečně rychle[2] vyzkoušet. Odolnost hesla můžeme dále zvýšit tím, že množinu znaků rozšíříme o speciální znak (např. $, &, @) anebo o české znaky. Nicméně zde je třeba zvažovat vhodnost použití takových znaků, neboť

[2] Útok na heslo (např. hrubou silou) nemůže trvat příliš dlouho, protože jinak se jeho případný úspěch může ukázat jako opožděný. Pokud by vyzkoušení všech kombinací trvalo například 1 měsíc, je při vynucené obměně hesel každých půl roku již poměrně vysoká pravděpodobnost (cca 17%), že původní heslo bylo mezitím změněno, a útok tedy nemusí být úspěšný i přesto, že byly všechny kombinace vyzkoušeny.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

v případě potřeby zapsání hesla na jiné klávesnici může s některými méně frekventovanými speciálními znaky a zejména s českými znaky být problém kvůli jiného „rozložení“ klávesnice. Osobně doporučuji ze speciálních znaků používat pouze mezeru a zavináč a české znaky nepoužívat vůbec. Jak bylo ukázáno výše, je účinnější cestou zvýšení odolnosti hesle prodloužení jeho délky. Rozhodně se v dnešní době nedoporučuje používat hesel kratších než 6-7 znaků. Obecně platí, jak bylo výše vysvětleno, že čím je heslo delší, tím je „silnější“, tedy odolnější vůči útokům. Proto některé služby vyžadují použití hesla o minimální délce 8 znaků a s využitím různých druhů znaků (malých a velkých písmen, číslic atd.).

Potíž s volbou vhodného hesla však spočívá v tom, že heslo musí být nejen odolné proti útokům, ale vedle toho také snadno zapamatovatelné pro uživatele, protože mnohá hesla zadává uživatel i vícekrát denně. Proto je volba vhodného dostatečně odolného hesla poměrně složitá úloha. Nicméně existují některá vhodná doporučení pro jeho volbu. Jedním z nich je vytvoření hesla z vybrané věty, například k nějaké knihy. Z praktických důvodů se doporučuje, aby to byla kniha, kterou vlastníte, nikoli například půjčená. Nicméně zdrojem vhodné věty může být jakýkoli jiný text. Větu si můžete na vhodné (nikoli veřejně přístupné) místo poznamenat, protože sama o sobě heslem není.

Již bylo zmíněno, že heslo by nemělo být tvořeno například jmény osob z Vašeho okolí. Existuje ještě další omezení, a to, že heslo by pokud možno vůbec nemělo obsahovat ani jména, ani jiná celá slovy, alespoň ne v jazycích, které běžně používáte Vy nebo uživatelé ve Vašem okolí. Důvodem je skutečnost, že z důvodu vysoké výpočetní náročnost útoku hrubou silou se mnohem častěji používá jednodušší útok tzv. slovníkový, který spočívá ve vyzkoušení všech známých slov v jazyce či jazycích používaných uživatelem počítače, a jejich kombinací, případně i s doplněním číslic apod. Do slovníků pro slovníkové útoky pak útočníci také zařazují další kombinace znaků, které jsou uživateli často používány (například řetězec 1qaz2wsx), a které proto jsou rovněž považovány za málo bezpečná hesla. V kritických ICT infrastrukturách se dokonce někdy používají k ověření bezpečnosti tzv. penetrační testy, které simulují běžně proveditelné útoky, a které taková slabá hesla dovedou odhalit, nicméně s tím se většina běžných uživatelů v praxi asi nesetká.

Kromě volby vhodného dostatečně silného hesla při jeho nastavení je neméně důležité jejich bezpečné uložení. Často uživatelé stojí před otázkou, kam hesla uschovat, zejména pokud jich používají více. To je přitom dnes dosti časté.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

Určitě nejvhodnějším nástrojem je papír (například menší sešit)ú a pero. Přitom je třeba zdůraznit, že nestačí si poznamenat samotné heslo, ale i uživatelské jméno, které k němu patří, a především aplikaci (například URL webové stránky), na které je toto heslo platné. Bez těchto údajů je samotné heslo zpravidla těžko použitelné. Pokud budeme potřebovat uchovávat větší množství méně důležitých hesel (například pro přístup do elektronických obchodů, pokud tam nemáme zároveň uložené platební údaje), je možné použít ukládání hesel, což je funkce, kterou nabízí v dnešní době většina www prohlížečů. Předtím, než takovou funkci začnete používat, doporučuji si ji vyzkoušet, přečíst si nápovědu k ní a pokud možno nastavit nějaké „hlavní“ heslo, které zde uložená hesla alespoň základním způsobem ochrání. Nedoporučuje se spoléhat na to, že s počítačem pracujete sami, v budoucnu mohou nastat situace, kdy bude mít k počítači (byť třeba jen krátkodobě) přístup jiný uživatel, a nemusí jít přitom jen o možné odcizení.

Často uživatelé zvažují, zda je vhodné použít stejné heslo pro různé služby. Obecně platí, že pro různé služby bychom měli používat odlišná hesla. Toto je třeba striktně dodržovat zejména pro kritické služby, jako internetové bankovnictví. Je totiž zcela běžné, že pokud se útočníkovi podaří získat jméno a heslo k jedné službě, zkouší je použít i k přihlášení k jiných službám. Na druhé straně pokud z důvodu snazšího zapamatování hesla použijete shodné heslo například pro přihlášení do více různých e-shopů (za předpokladu, že tam nemáme uloženy platební údaje), či do jiných méně důležitých webů, asi to lze akceptovat jako málo rizikové chování.

Na závěr této kapitoly se zmíníme o riziku spočívajícím v propojování účtů různých služeb. V dnešní době je běžné, že řada různých služeb nabízí možnost přihlášení prostřednictvím sociálních sítí, tedy namísto abychom si vytvářeni registrací samostatný uživatelský účet, využije příslušná služba autentizace to Facebooku, Google+ apod. Na jednu stranu je to pohodlné, na druhou stranu má tento přístup nejméně 2 rizika. Prvním je to, že se tím zvyšuje citlivost autentizačních údajů do příslušné sociální sítě, a bude, je pak třeba lépe chránit, případně nastavit silnější heslo. Druhé riziko, které si řada uživatelů vůbec neuvědomuje, spočívá v tom, že zejména provozovateli příslušné sociální sítě tím dáváme řadu informací, které možná ani nechceme, aby znal, například naše nákupní zvyklosti apod. Tyto informace pak se mohou ze sociální sítě dostat k příslušnému prodejci. Někdy to nevadí (zejména pokud dbáme na to, abychom na sociální síti o sobě nesdělovali veřejně příliš mnoho osobních informací, jako například přesnou adresu bydliště),

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

nicméně přesto to nelze považovat za příliš žádoucí. Proto je takové propojení účtů vždy pečlivě zvážit.

4.1.2. Zásady bezpečné práce s elektronickou poštou

Při práci s elektronickou poštou je třeba dodržovat několik základních zásad. Lze je shrnout takto:

- nedůvěřovat podezřelým zprávám,
- adresa odesílatele není spolehlivou identifikací,
- přílohy jsou potenciálně nebezpečné,
- aktivace odkazu (kliknutí na odkaz) ve zprávě je velmi rizikové,
- SPAM a Hoax jsou nežádoucí, je třeba se před nimi chránit.

Tyto zásady dále vysvětlíme podrobněji.

Zprávu elektronickou poštou nám může zaslat kdokoli, kdo zná naši adresu. E-mailovou adresu přitom obvykle nijak zvlášť nechráníme, i když již vymizel zvyk uvádět např., na webových stránkách platné e-mailové adresy, a navíc lze snadno rozesílat zprávy „zkusmo“ na všechny možné kombinace znaků jako potenciálně platné adresy. Proto pokud ze samotné zprávy není jasné, že jde o součást nějaké předchozí komunikace s někým, s kým komunikujeme běžně, je na místě obezřetnost. I solidně vypadající zpráva může být podvrhem. Pokud se na takovou zprávu chystáme zareagovat, měli bychom si například ověřit, zda instituce, která je uvedena jako pracoviště odesílatele, existuje, a zda údajný autor zprávy v této organizaci působí. Pokud narazíme ne nesrovnalosti, raději na zprávy nereagujeme, nebo si v odpovědi alespoň vyžádáme důkaz identity odesílatele (třeba telefonické ověření apod.)

Další potíž při používání elektronické pošty představuje skutečnost, že adresa odesílatele sice může být platná, ale zprávu odeslal někdo jiný. Buď mohla být odeslána z jeho počítače bez jeho vědomí (typicky po napadení počítače škodlivým softwarem), nebo mohla být odeslána i z úplně jiného počítače jiným odesílatelem. Adresa odesílatele se totiž na většině poštovních serverů nijak neověřuje, a tedy prakticky každý odesílatel může odesílanou zprávu označit adresou cizího odesílatele.

Dalším rizikovým faktorem jsou přílohy ke zprávám. Nebezpečnost příloh spočívá v tom, že se v nich mohou šířit nebezpečné spustitelné programy. Nejlepší prevencí proti tomuto riziku je používání vhodného antivirového programu. Protože antivirový program nemusí vždycky zachytit všechny rizikové přílohy, doporučuje se mimoto v případě obdržení podezřelé zprávy s přílohou, či e-mailu zdánlivě od

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

známého příjemce, ale s neočekávanou přílohou, tuto přílohy neotvírat. Pokud si nejsme jisti, pak rozhodně lze doporučit nejprve přílohu uložit, poté ji nechat důkladně zkontrolovat antivirovým programem, a teprve v případě nenalezení viru ji otevřít.

Velice nebezpečné mohou být také odkazy zasílané ve zprávách, proto se doporučuje ve zprávách, kde si nejsme jisti identitou odesílatele, na žádné odkazy neklikat. Riziko odkazů může být dvojí: jednak nás mohou zavést na podvrženou stránku napodobující legitimní stránku, která byla vytvořena s podvodným záměrem např. vylákat z uživatelů hesla (viz Phishing), nebo mohou odkazovat na stránku, která má za cíl zavléct do počítače uživatele škodlivý kód. Přestože řada stránek, které jsou takto napadeny, jsou zablokovány buď samotným prohlížečem, nebo nás na pokus o stažení nežádoucího software může upozornit antivirus, nemusí být ani v jednom případě ochrana stoprocentní.

Také nevyžádané zprávy (SPAM a Hoax, které byly popsány výše), jsou potenciálně rizikové, nebo alespoň obtěžující. Proti jejich rozesílání může běžný uživatel bojovat jen obtížně, ale může alespoň pomoci svému přijímajícímu poštovnímu serveru správně na takové zprávy reagovat. Stačí přitom, když správným způsobem takovou zprávu označí jako SPAM. Tím se SPAM filtr na serveru dozví, že se jedná o SPAM, a další podobné zprávy nebude již do schránek uživatelů doručovat.

Z důvodu možné tzv. falešně pozitivní detekce (tedy označení legitimní zprávy za spam) se však doručené nevyžádané zprávy ihned nemažou, pouze se odkládají do speciální spamové schránky, kde je uživatel může vyhledat, a případně označit jako legitimní. I tím uživatelé mohou pomoci přesnější detekci spamu.

4.2. Rodičovská ochrana

Samostatnou kapitolou bezpečného používání služeb Internetu je používání služeb Internetu dětmi a nezletilou mládeží. Protože každá nezletilá osoba v ČR má nejméně jednoho zákonného zástupce (rodiče či jinou osobu), který má dbát mimo jiné na jeho ochranu, leží zodpovědnost především na těchto dospělých osobách. Potíž ovšem spočívá v tom, že tito dospělí často mají sami nedostatečné znalosti o rizicích vyplývajících z používání služeb Internetu. Navíc v mnoha rodinách (nemluvě o dětech a mládeži žijících v jiných prostředích) dospělí nedostatečně dohlížejí na aktivitu svěřených dětí na Internetu.

Technické nástroje pro vynucení ochrany dětí před škodlivým obsahem existují a je jich k dispozici celá řada. Jedná se především o následující:

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

- rodičovské zámky v operačních systémech,
- reputační systémy.

Rodičovské zámky umožňují aplikovat omezení přístupu k určitým programům nebo k Internetu, a to v závislosti na denní době, případně i na již vyčerpané kvótě (lze tedy například nastavit omezení nejvýše 2 hodiny používání Internetu denně v pracovních dnech a 3 hodiny v sobotu a neděli). Rodičovské zámky jsou součástí většiny desktopových operačních systémů a k jejich nastavení stačí pouze vytvořit samostatný účet pro dětského uživatele a zajistit neznalost hesla jiných uživatelů s plným oprávněním.

Návod na použití rodičovského filtru ve Windows 7 je k dispozici na adrese http://windows.microsoft.com/enus/windows7/products/features/parental-controls.

Naproti tomu reputační systémy jsou programy, které využívají on-lineové seznamy zařazující webové stránky do kategorií podle obsahu závadného obsahu (např. erotika, porno, násilí apod.). Podle nastavených kritérií pak nainstalovaný reputační program zamezuje přístup ke stránkám, které obsahují nastavený typ nežádoucího obsahu. Příkladem reputačního systému může být http://i-bezpecne.cz.

Při snaze zajistit bezpečnost dětí při práci s Internetem je zcela zásadní složkou podávání vhodných informací. Zde je třeba vždy zvažovat, které informace konkrétní dítě dovede pochopit a aplikovat, a které ne. Zkušenosti ukazují, že jednu z prvních informací, kterou by dítě mělo dostat, je poučení o osobních údajích a o práci s hesly. Dítě si často neuvědomí, že heslo, které jednou někam zadá, si nebude pamatovat navždy, a po jeho zapomenutí bývá někdy velmi obtížné mu vysvětlit, že to, co si vytvořilo v příslušné službě, zkrátka už nemá k dispozici. O obecných doporučených zásadách správy hesel podrobněji pojednává předchozí podkapitola

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

5. Hrozby z Internetu a možnosti ochrany před nimi

Je známo, že největší slabinou ICT jsou uživatelé. Proto také největšího zlepšení bezpečnosti je možné docílit vzděláváním a osvětou uživatelů. Zde je na místě apelovat především na zdravý rozum každého uživatele tak jako při používání jiných nástrojů, zařízení a prostředků. Podobně jako zřejmě málokdo nechá svou plnou peněženku ležet na veřejně dostupném místě či otevřený hlavní vhod do bytu v době své nepřítomnosti, měli bychom i při použití ICT být rozumně obezřetní. Nenechávejme tedy například „otevřené dveře“ do svých počítačů například tím, že umožníme sdílení našich souborů bez omezení apod.

5.1. Škodlivý kód a jeho druhy

5.1.1. Viry

Programový kód, který pro aktivaci vyžaduje spojení s jiným programem, který jej pak aktivuje. Spolu se spustitelným programe se pak také viry obvykle šíří. Rozlišujeme souborové viry napadající programové soubory, makroviry napadající některé typy dokumentů (ty jsou škodlivé pouze tehdy, pokud je otevřeme v programu, který aktivaci maker umožňuje, např. MS Office, a má ji povolenou), a některé další typy, dnes méně významné. Přestože viry stále představují důležité riziko, nejsou dnes považovány za zásadní riziko, zejména proto, že velká většina koncových počítačů je před viry chráněna pomocí vhodných antivirových programů, které jsou často k dispozici i bezplatně (byť stupeň poskytované ochrany u bezplatných verzí je nižní než u placených). Skutečně nebezpečné jsou pouze zcela nové viry (tzv. „zero-day threats” neboli hrozby dne nula), na které výrobci ještě nestačili zareagovat vydáním aktualizace. proto je i při používání antivirového programu potřebná jistá dávka obezřetnosti.

Prevence před napadením virem spočívá v tom, že neotevíráme podezřelé soubory v příloze e-mailových zpráv (a to ani od známých uživatelů), a nestahujeme a neinstalujeme programy neznámého původu.

5.1.2. Červi

Červ (také označovaný jako síťový červ) je na rozdíl od viru programový kód, který je schopen samostatného spuštění a dalších akcí, především šíření. Nepotřebuje tedy žádný hostitelský program. Proto na rozdíl od viru musí šířit jiným způsobem. Obvykle se šíří s využitím chyb operačních systémů, které umožňují uložení kódu na dálku do paměti a jeho spuštění.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

Proti červům se obvykle chráníme pomocí firewallu. Pokud je firewall správně nakonfigurovaný, nepovolí síťovým červům se nepozorovaně připojit a přenést do paměti našeho počítače, a tedy se zde nemůže aktivovat. V případě, že již k infekci došlo, obvykle jej jsou schopné detekovat antivirové programy.

5.1.3. Trojský kůň

Podobně jako dřevěný trojský kůň byl vtažen obránci města dovnitř hradeb, šíří se i digitální trojské koně tak, že se nepozorovaně připojí k instalační sadě nějakého legitimního programu, a poté, co takový modifikovaný instalační program uživatel spustí, naistaluje se zároveň i skrytý program. Nežádoucí činnost takového skrytého programu může spočívat třeba ve skrytém zachycování dat zadávaných uživatelem (například jména, hesla, čísla kreditních karet apod. a jejich odesílání útočníkovi), nebo zejména v případě mobilních zařízení zachycování dat o poloze apod.

Ochranou před trojskými koňmi je zejména instalace programů pouze z ověřených úložišť. V případě nutnosti instalace programu z jiného úložiště (tomu se například v případě počítačů s Windows někdy nevyhneme) doporučuji vždy ověřit integritu instalační sady například pomocí MD5 otisku.

Existují také další jiné typy škodlivého kódu neboli malware, nicméně nebudeme je zde podrobněji rozebírat.

5.2. Napadení počítače – Hacking

V některých případech může dojít k tomu, že útočník se připojí do Vašeho počítače a provádí tam nějakou nežádoucí činnost. Takové napadení se označuje jako hacking. Mnohem častějším případem je sice připojení provedené roboty, ale to na věci nic nemění. Každé skryté připojení je nežádoucí a nebezpečné, proto je třeba mu vždy předcházet. Útočník může do Vašeho počítače například instalovat skryté programy provádějící škodlivou činnost (nejčastěji jde o zapojení počítače do DDoS útoku na cizí servery, kde je napadený počítač pouze nástrojem pro útok na někoho jiného), ale může jít přímo o útok na uživatele počítače, neboť skryté programy mohou slídit v počítači a v zadávaných datech z klávesnice po citlivých údajích, jména, hesla, čísla platebních karet apod.)

Napadení počítače nejlépe zabrání správně nastavený a aktualizovaný firewall aktualizovaný antivirový a antimalwarový program.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

5.3. Phishing

Phishing je velmi nebezpečný druh útoku, který je založen na tzv. sociálním inženýrství neboli zneužití přílišné důvěřivosti nebo nedostatečné informovanosti a kvalifikace uživatelů. Phishing zneužívá důvěry uživatelů, zejména s nižší kvalifikací v oblasti ICT. Nejčastější podoba phishingu spočívá v tom, že útočník pošle oběti (nebo spíše velkému množství potenciálních obětí) zprávu (obvykle e-mailem, ale znám je také telefonický phishing, zejména ve větších společnostech, kde se využívá toho, že se zaměstnanci navzájem neznají osobně). Tato zpráva zpravidla nabádá uživatele k přihlášení do jejich účtu (např. bankovního, ale též např. účtu pro přístup do informačního systému organizace) prostřednictvím přiloženého odkazu. Podstatou útoku je, že odkaz vede na podvrženou stránku, která je podobná té, kterou má zastupovat. Jakmile se oběť přihlásí na podvrženou stránku, budou její přihlašovací údaje odchyceny útočníkem a dále bude přesměrována na skutečnou stránku, která byla podvržena, a tam budou předány i přihlašovací údaje, takže oběť často ani nepozná, že se stala obětí tohoto typu útoku.

Podobnost podvodné stránky může být dosti vysoká, i když zřídka bývá napodobenina dokonalá. Rozpoznání falešné stránky je možné podle URL (pokud tu správnou uživatel zná), a nejspolehlivěji podle chybného certifikátu (pokud se ovšem pro přístup na stránku certifikát používá, a je platný).

Oběť je k přihlášení prostřednictvím zaslaného odkazu nabádána obvykle se zdůvodněním, že došlo k nějaké mimořádné události, a motivována tím, že pokud přihlášení neprovede do určitého času (lhůta bývá poměrně krátká, málokdy je delší než 24 hodin, ale poznávacím znamením může být, že tam nebývá konkrétní časový údaj, ale čas od doručení zprávy), bude účet zablokován.

Spolehlivou prevencí proti tomuto typu útoků bývá dodržování zásad bezpečné práce se zprávami elektronické pošty (zejména neklikat na odkazy v podezřelých zprávách), které jsou popsány v předchozí kapitole, a nezávislé ověřování obdržených informací z jiného zdroje. Zavolání do banky či na IT oddělení pro ověření pravdivosti sdělení nás určitě stojí méně úsilí než odstraňování následných škod. Navíc je třeba pamatovat na to, že prakticky žádná banka ani IT organizace zprávy tohoto typu nikdy nezasílá. Pokud by výjimečně tuto formu oslovení svých zákazníků použila, ve zprávě by nikdy nebyl odkaz na přihlašovací stránku. Proto také v případě pochybností se do příslušné webové aplikace přihlaste běžným způsobem na adrese, kterou běžně používáte. Tím se žádnému riziku nevystavujete.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

5.4. Ochrana před hrozbami

5.4.1. SPAM a jiné nežádoucí zprávy

Spam je označení pro nevyžádané poštovní zprávy, zpravidla šířené hromadně. Každá jednotlivá spam zpráva není sama o sobě nebezpečná, nebezpečné může být to, c s nimi nepozorný nebo neinformovaný uživatel udělá. Zásady správné práce s elektronickou poštou jsou uvedeny v předchozí kapitole. Pomocí spamu se často šíří viry, malware, phishingové zprávy apod.

Dalším typem nevyžádaných zpráv je hoax. Jde o zprávy se sdělením, které má zpravidla alarmující obsah vyzývající příjemce k přeposlání. Tyto zprávy nejsou nebezpečné, ale je lépe se vyhnout jejich přeposílání. Snadné ověření, zda se jedná o hoax, umožňuje seznam na serveru hoax.cz.

5.4.2. Antivirus, antispyware

Antivirus sleduje spouštěné programy a kontroluje, zda není spouštěný program infikován virem. Pokud zjistí virus, zabrání v jeho spuštění a informuje uživatele.

Počítač bez antiviru by vůbec neměl být používán. Antivirus je v dnešní době natolik samozřejmou součástí programového vybavení počítače, že ve Windows 8 je již součástí operačního systému. Přestože jeho spolehlivost nepatří mezi nejvyšší (viz [8]), je bezpochyby lepší mít alespoň tuto ochranu k dispozici. Pokud si však můžete použít jiný antivirový program, vyberte si podle některého důvěryhodného hodnocení. Při výběru pamatujte na to, že spolehlivost samotné detekce virů nebývá rozdíl mezi placenými a bezplatnými verzemi antivirů (ty bezplatné jsou však často vyhrazeny pro nekomerční použití, tedy například v domácnostech), ale rozdíly bývají v dalších funkcích, například firewallu, blokování spamu, blokování podezřelých či závadných webových stránek apod.

Nutnou podmínkou používání antiviru je pravidelná aktualizace virové databáze. Bez ní antivirus velmi rychle zastarává a již po několika týdnech je téměř neúčinný.

Vhodné je mít na počítači také antispywarový program. Ten má za úkol chránit počítač před dalšími typy malware. Antispyware bývá součástí placených antivirových programů.

5.4.3. Firewall

Firewall je v dnešní době součástí každého operačního systému, a to jak desktopového, tak i pro servery. Většina uživatelů využívá firewall, který je součástí operačního systému. Ten bývá v základním nastavení poměrně bezpečný, ale přesto

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání
pro konkurenceschopnost a státního rozpočtu České republiky.

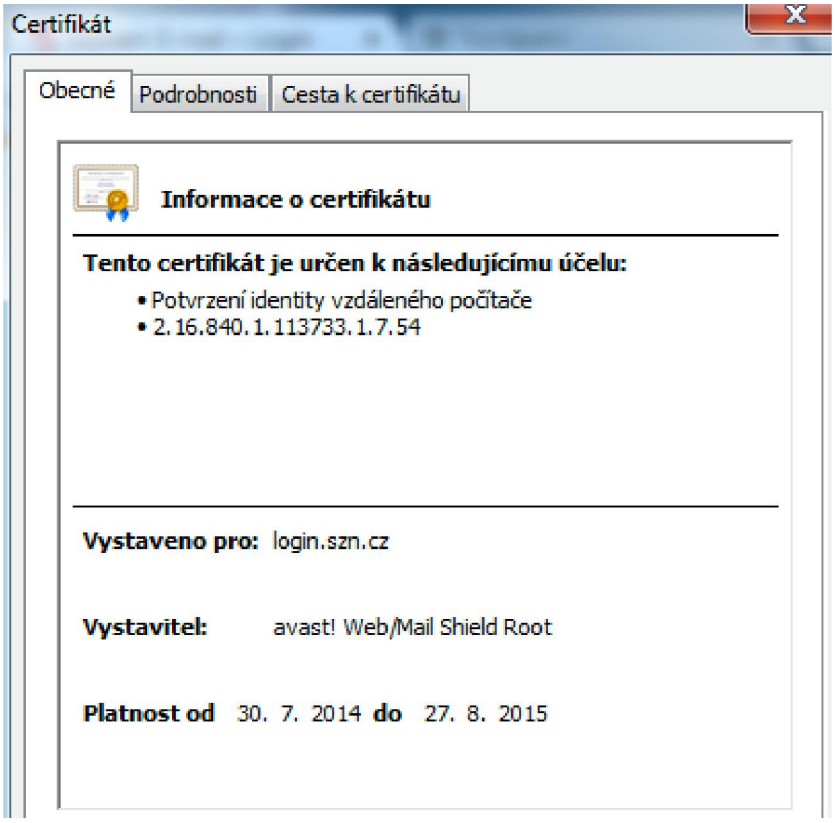
je vhodné se o jeho účinnosti přesvědčit, nejlépe s pomocí zkušeného IT administrátora, případně (pokud byste si byli jisti, že chcete namísto základního firewallu používat nějaký dokonalejší, často placený) si nechat takový program instalovat. Rozhodně nedoporučuji, aby do konfigurace firewallu zasahoval nekvalifikovaný uživatel.

Za zcela nevhodná pak lze považovat místy ještě se objevující doporučení k vypnutí firewallu, pokud zjistíte nefunkčnost určitého programu nebo www služby. Pokud opravdu takovou službu potřebujete využívat, nechte si od IT administrátora doporučit (nebo provést) změnu konfigurace firewallu (podle dokumentace k příslušnému programu či službě je zpravidla snadné takovou úpravu provést a docílit funkčnosti služby. Vypnutím celého firewallu sice docílíte funkčnosti programu také, ale za cenu zásadního oslabení bezpečnosti celého počítače.

5.4.4. Další opatření pro ochranu před riziky

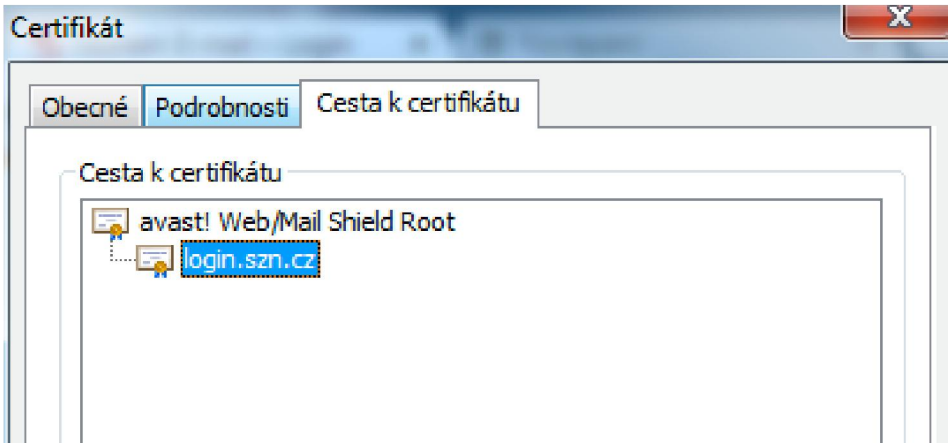
Jak bylo zmíněno výše, existují zabezpečené aplikace, které využívají šifrování přenosu dat, například https apod. Převážná většina šifrování v Internetu se dnes realizuje pomocí tzv. asymetrického šifrování založeného na certifikátech. **Bezpečné použití certifikátů** má jednu principiální podmínku, a to akceptování pouze **platných důvěryhodných certifikátů**. Certifikát je platný pouze ve stanoveném časovém období, pouze pro server či uživatelskou e-mailovou adresu, pro který byl vystaven, a pokud je podepsán důvěryhodným certifikátem (viz obrázek Detaily certifikátu).

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.



Obrázek 1: Detaily certifikátu

To je možné realizovat buď tak, že bude podepsán přímo důvěryhodným kořenovým certifikátem, nebo tak, že bude podepsán jiným certifikátem, který již je podepsán důvěryhodným kořenovým certifikátem. To může být provedeno i zprostředkovaně, tedy řetězec podepisujících certifikátů může být i delší než 1-2 zprostředkující certifikáty (viz obrázek Cesta k certifikátu).



Obrázek 2: Cesta k certifikátu

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

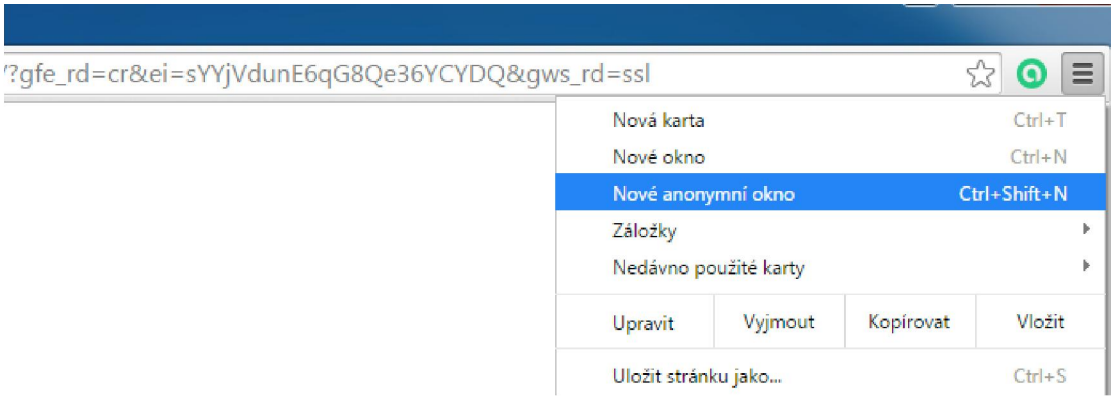
Každopádně na neplatnost či nedůvěryhodnost certifikátu poskytovaného serverem vždy upozorní www prohlížeč či jiná aplikace, která jej používá. V takovém případě je doporučeno v komunikaci nepokračovat, neboť není zaručeno, že komunikace (byť šifrovaná) je navázána s tím serverem, za který se vydává.

Další důležitou zásadou je dodržovat pravidla práce s elektronickou poštou, která byla uvedena v předcházející kapitole. Dalším důležitým pravidlem bezpečnosti je opatrné práce se staženými programy a jinými spustitelnými soubory. Minimem by mělo být důkladné zkontrolování staženého programu před jeho spuštěním. Tím však neodhalíme případné trojské koně a podobný škodlivý kód. Proto se doporučuje používat programy pouze z prověřených úložišť, nebo na základě doporučení důvěryhodných zkušených uživatelů.

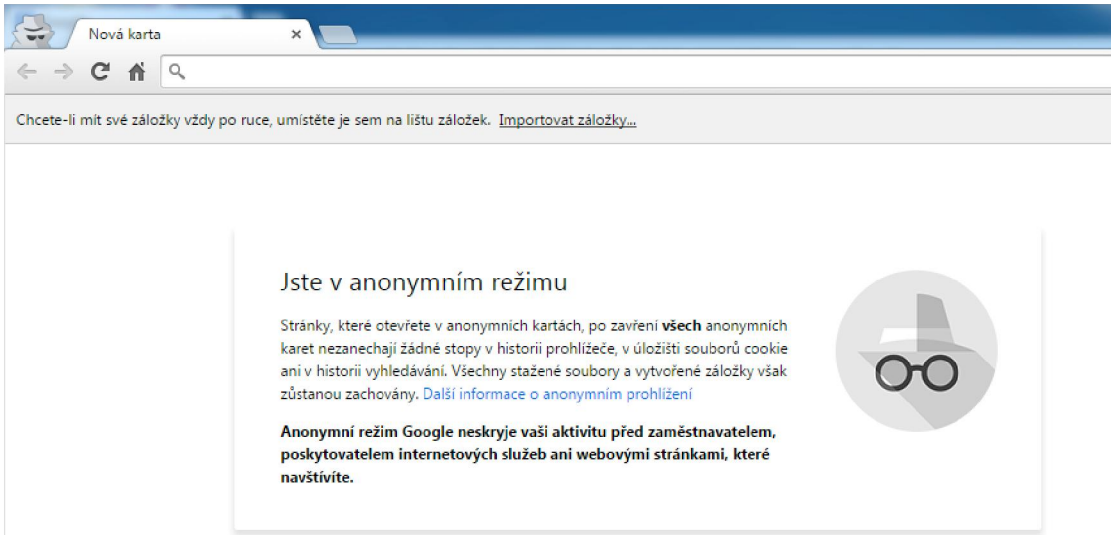
Velmi rozšířenou aplikací posledních let jsou sociální sítě. Protože jde o služby, které uživatele motivují ke zveřejňování osobních údajů, je třeba klást zvýšený důraz na řádnou práci s osobními údaji. Nejdůležitější zásadou je správné nastavení tzv. soukromí, neboli nastavení přístupnosti (resp. nepřístupnosti) osobních údajů pro ostatní uživatele.

Na závěr zmíníme jednu důležitou zásadu pro případ, kdy pracujete na tzv. veřejném počítači, tedy na počítači, k němuž má přístup více uživatelů. Příkladem takového počítače může být veřejný počítač ve studovně, v kavárně apod. Nicméně je třeba upozornit, že velmi podobná situace nastává i tehdy, když pracujete na svém počítači, ale jste připojení do WiFi sítě bez autentizace. V tomto případě prochází veškerá komunikace z Vašeho počítače do sítě (přístupového bodu) bez šifrování. Z toho vyplývá, že kdokoli (třeba uživatel počítače u vedlejšího stolku) může zachycovat veškerou Vaši komunikaci. V takovém případě se rozhodně nedoporučuje přistupovat na stránky vyžadující přihlášení, neboť nezle zabránit odchycení přihlašovacích údajů. Pokud se používá spolehlivé šifrování přihlašovacích dat pomocí https, toto riziko je eliminováno, nicméně zejména na veřejných počítačích je třeba dát pozor na skrytý software, jako např. keyloggery zaznamenávající údery na klávesnici, takže může dojít k prozrazení hesla. Viz obrázky 3 a 4.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.



Obrázek 3: Spuštění anonymního okna v Chrome



Obrázek 4: Anonymní okno v Chrome

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.

6. Použité zdroje

[1] Sochor T. *Bezpečnost v síťovém prostředí*. Ostravská univerzita: Ostrava 2014

[2] Petrovič M., Kostěnec M. *Bezpečnost počítačových sítí*. Západočeská univerzita. Plzeň. 2012. ISBN 987-80-261-0117-8

[3] Doucek P., Novák L., Svatá V. *Řízení bezpečnosti informací*. Professional Publishing Praha 2008. ISBN 978-80-86946-88-7

[4] Česká republika. Zákon č. 121/2000 Sb. o právu autorském ve znění pozdějších předpisů. [online]
Dostupné z: http://business.center.cz/business/pravo/zakony/autorsky/

[5] Iuridictum. Přestupek. [online]
Dostupné z: http://iuridictum.pecina.cz/w/Přestupek

[6] Sochorová H., Materová H. *Informační systémy ve zdravotnictví – praktické aplikace výpočetní techniky*. Ostravská univerzita: Ostrava 2012

[7] Slunečnice.cz. Softwarové licence. [online]
Dostupné z: http://www.slunecnice.cz/licence/

[8] dtest. Ochrana počítače. Základní ochrana Windows zklamala. dtest 2015. číslo 4, str. 42-47

[9] Sochor T., Zuzčák M. *Study of Internet Threats and Attack Methods Using Honeypots and Honeynets Computer Networks A. Kwiecien, P. Gaj and P. Stera (Eds.)*:CN2014, CCIS 431, s. 118–127. Springer International Publishing Switzerland: 2014. ISSN: 18650929 ISBN: 978-331907940-0.

Toto vzdělávání je financováno z prostředků ESF prostřednictvím OP Vzdělávání pro konkurenceschopnost a státního rozpočtu České republiky.