Kapitola sedmá

Bezpečnost, ochrana dat a autorských práv

Mgr. Radek Hoszowski

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
logistiky a chemie
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnost, ochrana dat a autorských práv

Bezpečnost počítače

Za bezpečný počítač považujeme ten počítač, který neobsahuje žádný nežádoucí software a je zabezpečený proti útokům z internetu. Na bezpečnosti se podílí jak technika, tak uživatel.

Nemůžeme pochybovat o tom, že velký podíl na zabezpečení počítače nese samotný uživatel. V této části kapitoly si představíme technické způsoby ochrany počítače a seznámíme se zásadami bezpečné práce na počítači.

*Abychom měli bezpečný počítač, musíme pravidelně **aktualizovat** systém i programy, které používáme. Aktualizace můžeme provádět manuálně, ale mohou být nastaveny automaticky.*

AKTUALIZACE

Nikdo není neomylný, a tak i programátoři a autoři počítačových programů občas udělají někde chybu. Nemůžeme se jim divit, protože počítačové programy jsou velmi složité. **Bezpečnostní chyby** neboli **díry** se objevují v programech velmi často. V současné době jsou to především chyby v internetových prohlížečích, díky kterým je náš počítač snadným cílem hackerů.

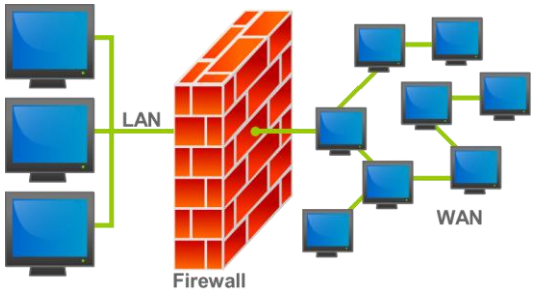
K čemu jsou aktualizace?

Aktualizace systému a programů slouží k „záplatování“ děr a chyb, které se objevují. Oprava systému se nazývá **patch**. Pomocí aktualizace se oprava nainstaluje do našeho počítače.

Daleko častěji chybuje v počítačích lidský faktor než technika, proto je vhodné, nastavit si **automatické aktualizace** programů a systému. Počítač si zjišťuje, zda jsou dostupné nějaké opravy, sám si je stahuje a instaluje. Následně nám dá zprávu, že byla provedena aktualizace.

FIREWALL

Firewall je síťové zařízení, které kontroluje bezpečnost různých sítí na různých úrovních. Kontroluje různé sítě a především kontroluje cílovou IP adresu. **IP adresa**



je jedinečná pro každý počítač. Kontroluje také **porty**, přes které počítač komunikuje s ostatními sítěmi. Různé aplikace používají různé porty, kterých je nepřeberné množství. Můžeme také říci, že firewall je jakási zeď mezi naším počítačem (nebo sítí

počítačů) a okolním světem – Internetem.

Existují dva typy firewallu – **osobní firewall**, který je součástí operačního systému a hlídá data, která proudí do počítače a z něj. **Síťový firewall** kontroluje také data proudící uvnitř místní sítě LAN a hlídá komunikaci s vnější sítí WAN. Většinou bývá součásti **routeru** (směrovače). Router spojuje vnitřní a vnější síť a směřuje data k jejich cíli. LAN sítě spojuje tzv. **switch**.

Kromě firewallu si můžeme zakoupit také další nástroje, které budou hlídat náš počítač. Tyto nástroje mohou kontrolovat odkazy na web a upozornit nás na nebezpečný odkaz, mohou hlídat stránky, které jsme již navštívili a také nám mohou poskytnout zvýšené zabezpečení osobních údajů (hesel, přístupových jmen, aj.). Další důležitou součástí bezpečnosti počítače je antivirový program ochraňující nás před škodlivým softwarem a počítačovými viry.

Antivirový program

Co víme o těchto programech, jaké antivirové programy jsou hodnoceny jako kvalitní a jak vlastně fungují? To vše se dozvíte v následující podkapitolce.

Uvědomme si, že antivirový program **není dokonalý!!**

Co víme o antivirech?

Antivirus **stále běží** v paměti počítače a kontroluje vše, co na počítači dělám – všechny otevírané soubory a programy. Kvalitní antivir: by měl zachytit většinu škodlivých souborů.

V případě, že máme podezření na napadení počítače, můžeme zadat pokyn a antivirus tak **na náš pokyn otestuje** soubory v počítači – všechny, nebo jen vybrané.

V případě antivirů nás zajímají hlavně dvě funkce:

1. **Vyhledává a kontroluje** data na základě své **virové databáze** – výrobce musí reagovat na nové viry téměř okamžitě.
2. **Sleduje podezřelé aktivity** na pozadí počítače. Pokud něco neobjeví, tak si toho ani nevšimneme.

Stejně jako u programů a systému jsou důležité pravidelné aktualizace virových databází. Antiviry si databáze aktualizují automaticky bez nutnosti zásahu uživatele někdy i několikrát denně.

Je také nesmírně důležité, abychom nenechali propadnout licenci či registraci antivirového programu. **I několik hodin bez ochrany počítače může mít fatální důsledky** pro naše data a náš systém.

Jak odvirovat nakažený počítač??

Tato činnost není vůbec lehká. V současné době existuje velké množství virů, které se dokáží před antivirovým programem velmi dovedně schovat. Musíme tedy **nabootovat** jiný systém (např. z USB disku) a vir v původním systému pak najít pomocí skenovacího systému antivirového programu. Pokud je virus obsažen na HDD můžeme jej

z počítače vyjmout a vyzkoušet v jiném počítači – zde se virus jistě objeví.

ANTISPYWARE

Speciálním typem programu je tzv. **antispyware**, který

v počítači pomáhá odhalovat přítomnost spywarových programů, některé spywary umožňují kontrolu počítače proti veškerým druhům malware.

O typech malware a škodlivého softwaru se dozvíte v následující podkapitole.

ANTIVIRY NA TRHU

V současnosti je na trhu nepřeberné množství antivirových programů. Při zkouškách antivirů pravidelně vítězí antivir **ESET NOD32** od slovenské firmy ESET, spol. s r.o. (logo vidíte na předchozí stránce). Cena licence se pohybuje okolo 1000 Kč na jeden počítač na rok.

Dalším známým antivirem je **Norton** od společnosti Symantec. Licence na jeden rok stojí 930 Kč pro jeden počítač.

V našich podmínkách mezi nejčastěji používané antiviry patří **Avast!** Bez omezení jej můžete používat zdarma, podmínkou je každoroční registrace. Podle testů není tak spolehlivý jako předchozí dva, ale jeho cena je okolo 666 Kč 1 počítač / 1 rok.

Avast Software, a. s. sídlí v Praze. Další široce užívání je antivirus **AVG** má rovněž bezplatnou licenci. Zakoupit si můžeme verzi na 1 rok pro 1 počítač za 749 Kč.

Samozřejmě existuje velké množství antivirových programů. Zmínili jsme pouze ty nejznámější a v ČR nejpoužívanější.

Škodlivý software

Proti jakému softwaru je potřeba chránit náš počítač? V této části kapitoly se blíže podíváme na typy škodlivého softwaru.

Z názvu je jasné, že škodlivý software nám nějakým způsobem škodí. Software je vyvíjen proto, aby umožnil uživatelům vykonávat určité činnosti. V případě, že se jedná o nezamýšlenou činnost jakéhokoliv programu, hovoříme o škodlivém softwaru. Z možností nezamýšlené činnosti programů nyní vynecháme programátorské chyby či chyby hardwaru. Druhy škodlivého softwaru si velmi stručně představíme v následujících odstavcích.

MALWARE

Počítačový program, který byl vytvořen, aby poškodil operační systém jiného programu nebo aby do něj vnikl. Česky bychom mohli říct, že se jedná o takový zákeřný software (z angl. *malicious*). Do malwaru, v podstatě, patří všechny ostatní části škodlivého softwaru – počítačové viry, trojské koně či spyware a adware.

SPYWARE

Spyware [spaiwer] je počítačový program, který pomocí internetu odesílá data z počítače – **bez vědomí uživatele**. Existují různé druhy spyware – od těch, které sledují navštívené stránky a tak tipují cíle pro cílenou reklamu, až po ty, které sledují vaše hesla a odesílají je třetí straně. Mezi nejznámější spyware patří **adware** (vyskakující reklamy), **hijacker** (změna domovské stránky), **KeyLogger** (sledování klávesnice – tedy i hesel).

Jedná se tak o velmi nebezpečný software, který málo uživatelů dokáže odhalit. Spyware můžeme odhalit speciálním antispyware programem.

TROJSKÝ KŮŇ

Trojský kůň je malware, který je velmi podobný spywaru. Zároveň má však velmi blízko k počítačovým virům – s tím rozdílem, že trojský kůň nedokáže sám nakazit další počítače. Trojský kůň využívá toho, že velmi často v nastavení složek nevidíme přípony souborů a vydává se za soubory jiného typu. Jakmile se pokusíme obrázek, hudbu či video otevřít, otevřeme vrátka trojskému koni, který začne v našem počítači úřadovat. Velmi často jich využívají crackeři k prolomení bezpečnosti počítače.

POČÍTAČOVÉ VIRY

Jsou programy, které se v počítači šíří bez vědomí uživatele. Šíří se stejně jako virus v těle, množí se, kopíruje se, přemisťuje se. Pravý virus ke svému šíření využívá **jiné soubory**, do kterých se kopíruje. Spuštěním infikovaného programu spustíme automaticky i virus, který se začne šířit.

Speciálním druhem počítačových virů jsou tzv. **makroviry**, které nejsou součástí programu, ale dokumentu. Nejedná se o jakýkoliv dokument, ale dokument, který může obsahovat **makra** – tj. vložené programové kódy. V dnešní době se jedná o velké množství dokumentů.

Červ je také jedním z tipů škodlivého softwaru, podobný jako virus. Hlavní rozdíl mezi virem a červem je, že červ má vlastní soubor, který se samovolně množí. Pozor! Většina antivirů červa nezachytí, protože nevyžadují spuštění programu.

Napadení počítače

Jak poznáme napadený počítač, jakým způsobem se chovají viry a červi v našem počítači a jakým způsobem náš počítač napadají.

NAPADENÝ POČÍTAČ

Většinu z virů či červů nejde v počítači objevit ihned – šíří se. Teprve po určité době provede nějakou nepříjemnou činnost. Může **ovládnout celý počítač** – tedy umožní vstup k ovládání počítače jiné osobě. Počítač viditelně funguje bez problému, ale vykonává i činnost, kterou mu přímý uživatel nezadal. Viry a červi mohou také zapříčinit **odcizení obsahu počítače** – cizí osoba tak může kopírovat soubory z vašeho počítače, sledovat zadávaná data, aj. Osoba, která takto vnikne do vašeho počítače, však může také data vkládat a mazat. Může navíc váš počítač využít k **nelegální činnosti** – odesílání spamu, přístup na nelegální servery (pornografie, rasistické stránky, aj.) – v tomto případě se navštěvovatel těchto stránek či vykonavatel nelegální činnosti identifikuje podle IP adresy. Některé viry se specializují na **mazání dat z počítače** bez přímého zásahu cizí osoby.

PŘÍTOMNOST VIRU

K podezření, že je v našem počítači přítomen nás můžou dovést některé znaky: pomalý start počítače, dlouhé načítání internetu, nežádoucí změna domovské stránky, chyby OS, záhadně se objevující ikony na ploše, velké množství reklam při surfování po internetu. Musíme pak dále provést různé úkoly k odvirování počítače.

NAPADENÍ POČÍTAČE

Kromě přenosu viru z přenosných médií (dříve disketa, dnes flash disk) jsou nejčastější způsoby útoku na počítač přes webové stránky a přes elektronickou poštu. 60 % škodlivých kódů se šíří přes webové stránky!

Mohou se šířit následujícími způsoby:

- umístění infikovaného souboru na web – umístění do důvěryhodného programu, většinou však na web s nelegálním obsahem (cracky, warez),
- umístění na web, který je důvěryhodný, ale byl napaden hackery,
- umístění skriptu (programu) do kódu webové stránky – využívá chyby prohlížeče,
- vytvoření zavirovaného **plug-inu** pro prohlížeč,
- využití podvržené stránky – přesměrování na falešnou stránku (internet banking!)

Tyto způsoby se však dále vyvíjejí.

Dalším způsobem napadení počítače je napadení přes **elektronickou poštu**. V minulosti to byl hlavní přenašeč, dnes již pouze 10 % napadení.

O tomto způsobu útoků se nejvíce mluví, proto statistiky stále klesají. Uživatel musí kliknout na soubor, který mu přišel, aby se mohl jeho počítač infikovat. Ve většině e-mailových serverů jsou již integrovány antivirové systémy. Ty vyblokují zprávy s podezřelými přílohami. Proto již útočníci posílají mailem pouze odkazy na infikované weby.

Méně agresivní útoky

V této části se zaměříme na méně agresivní útoky. Tyto pokusy o útok jsou sice méně agresivní, za to však jsou daleko vychytralejší a podlejší.

SPAM

SPAM neboli nevyžádané, hromadně rozesílané zprávy většinou obsahující reklamu. Problematika spamu je v současné době jedním z největších problémů e-mailové pošty. Velmi zřídka objevíme uživatele e-mailu, kterému nepřijde žádná spamová pošta v jednom dni. Uživatelé uvádějí, že v průběhu dne maží 5 – 10 spamů. Šiřitelům spamu se říká **spameři** a získávají adresy k rozesílání mnoha způsoby:

- roboti (specializované programy) procházejí internet a hledají adresy, např. na diskuzních fórech,
- viry, které jim odešlou celý váš adresář,
- kupují databáze od jiných spamerů,
- generují náhodné adresy podle seznamů jmen a nejrozšířenějších poštovních serverů

Většina právě těchto poštovních serverů již poskytuje do svých mailů tzv. **antispamový filtr**. Do tohoto filtru si můžeme zadávat adresy, ze kterých nebudeme maily dostávat, popřípadě napíšeme seznam slov, která bude mail automaticky blokovat (např.

porno, viagra, gay…). Občas se nám však do spamové pošty připlete nějaký mail, který potřebujeme, měli bychom tedy občas kontrolovat i tuto složku.

TSI a HOAX

Mezi zvláštní formu spamu patří tzv. **techniky sociálního inženýrství.** Jedná se o metodu podvodu – metodu jak získat finanční prostředky od uživatelů. Jak říkají odborníci: *„Největší bezpečností problém je mezi počítačem a židlí."*

Tyto útoky využívají psychologii člověka. Jak fungují?

- Nabízejí zdarma erotický, pornografický nebo tajný obsah.
- Nabízejí velký finanční zisk při malém úsilí a zaplacení „malého" poplatku.
- Hrají na city.
- Vzbuzují strach.
- Tváří se důvěrně.
- Vydávají se za někoho jiného.
- **Nutí jednat okamžitě!!!**

V těchto případech může dojít k tzv. **phishingu** – ukradení identity. Dostanete zprávu, že se ihned musíte někam přihlásit, kliknete na odkaz, který je na falešnou stránku – ta však vypadá jako stránka původní (i-banking).

Jak se bránit?

Mějte neustále na paměti, že **internet je nebezpečný** a útok může přijít odkudkoliv. Můžeme tak internet přirovnat k divočině.

HOAX

Falešná zpráva, která k něčemu nabádá (rozeslání mailů, potvrzení, smazání viru). Viz stará známá štěňata zlatého retrívra.

Zásady ochrany dat

Jak správně chránit svá data před přístupem jiných uživatelů internetu. Správný postup při vytváření hesla.

HESLA

Hesla jsou jedna z nejkradenějších na internetu. Zároveň také spousta uživatelů chybuje při vytváření hesla a tak je možno je snadno odhadnout. Nejčastější chybou je zadat stejné heslo jako **login** (uživatelské jméno), popřípadě mít stejná hesla na různých místech. Zmíníme si tedy obecné zásady platné pro vytváření hesel. Bezpečné heslo se také nazývá **silné heslo**.

SPAM

Název pochází ze značky amerických konzerv lančmítu. Slovo vzniklo jako zkratka ze slov spiced ham - okořená šunka a tyto konzervy se vyrábí od 30. let 20. století dodnes. V současnosti ale výrobce trvá na psaní velkým písmem - SPAM. V období 2. světové války byla hojně rozšířená a stále méně oblíbená ve Velké Británii.

Proto se spam objevuje v závěrečném skeči 25. dílu seriálu *Monty Pythonův létající cirkus*, kde všechny položky jídelního lístku v restauraci obsahují spam, i mnohokrát opakovaně, a spory zákazníků s číšnicí o objednávky přerušuje skupina Vikingů zpívajících „Spam, spam, spam…"

ODKAZ:

Monty Python - Spam

Označení tak bylo přijato nejprve pro praktiku mnohonásobného rozesílání téže zprávy na Usenetu, ale pak se význam posunul pro zneužívání skupin k šíření různých nepřípadných textů a přímo reklamy a zachoval se i poté, co se těžiště takových aktivit přesunulo do e-mailu.

V jiných výkladech je uváděn výraz SPAM jako zkratka z anglického *Shit Posing As Mail*, což v nevulgárním překladu znamená *Odpad jevící se jako zpráva*

1. Obsahuje **minimálně 8 znaků** – čím víc znaků, tím víc kombinací.
2. **Nedává smysl** v žádném jazyce.
3. Obsahuje **různé znaky** – velká a malá písmena, číslice, speciální znaky.
4. Dá se **dobře zapamatovat!** Hesla bychom si neměli zapisovat, hlavně **NE v blízkosti počítače**.

Jak může být heslo odcizeno?

Existuje poměrně velké množství možností odcizení hesla. Výše jsme si zmínili **sociotechnické prostředky** – podvody, kterými se velmi často podaří hesla získat. Dále je využíváno **neopatrnosti uživatele** – napsaná hesla. Zkušenější a trpělivější útočníci využívají tzv. **keylogger** – tzn. spyware, který sleduje v počítači zapisovaná písmena na klávesnici. V neposlední řadě se využívá **stejných hesel** – stejné heslo jako login, případně stejné heslo na několika místech.

Jak je možné na mé heslo útočit?

Existují dva způsoby. Prvnímu z nich se říká **Útok hrubou silou** – výkonný počítač zkouší všechny možné kombinace hesel. Zde platí, že čím více znaků má vaše heslo, tím je bezpečnější. Druhý způsob je tzv. **Slovníkový útok**, kdy si útočník zjistí jazyk, který používá počítač uživatele. Zkouší slova běžně užívaná slovníkem daného jazyka. Běžně užívaných slov je v každém jazyce přibližně 10 000, takže se tento útok velmi často povede.

ZABEZPEČENÍ POČÍTAČE

V některých případech musíme zabezpečit také fyzickou manipulaci s počítačem a jeho užívání cizí osobě. Tohoto můžeme dosáhnout následujícími způsoby:

- Ochrana místnosti proti vniknutí.
- Spouštění počítače na heslo – nechrání při krádeži.
- Spuštění operačního systému na uživatelské jméno a heslo.
- Přídavné zařízení, do kterého musíme vložit identifikační kartu nebo flash disk (tzv. **token** – zařízení s kódem) – kvalitní zabezpečení počítače.
- Biometrické metody – založeno na fyzických parametrech uživatele – otisk prstu, scan oční duhovky

ZABEZPEČENÍ DŮVĚRNOSTI DAT

V případě, že se někomu podaří zmocnit se našich dat, měli bychom využít další způsoby jejich zabezpečení. **Softwarové** zabezpečení pomocí **šifrování** – šifruje se zápis na disk a dešifruje čtení z něho. **Hardwarové zabezpečení** – pomocí výše zmíněných tokenů.

Ochrana autorských práv

V současné situaci informačních technologií a internetu jsou nejporušovanějšími právy práva autorská. V neposlední řadě se seznámíme s citační normou.

AUTORSKÝ ZÁKON A CITOVÁNÍ INFORMACÍ[1]

Použití cizích autorských děl pro naše vlastní školní materiály, tedy pro naše vlastní autorská díla, upravuje § 31 Autorského zákona s nadpisem Citace.

Do práva autorského nezasahuje ten, kdo

a) **cituje ve svém díle v odůvodněné míře výňatky** ze zveřejněných děl jiných autorů,
b) zařadí do svého samostatného díla vědeckého, kritického, odborného nebo do

[1] Tato část kapitoly byla převzata z knihy Informatika a výpočetní technika pro střední školy, Roubal Pavel, C-Press.

díla určeného k vyučovacím účelům, pro objasnění jeho obsahu, **drobná celá** zveřejněná díla,

c) užije zveřejněné dílo v přednášce **výlučně k účelům vědeckým nebo vyučovacím či k jiným vzdělávacím** účelům;

vždy je však nutné uvést:

- **jméno autora**, nejde-li o dílo anonymní nebo jméno osoby, pod jejímž jménem se dílo uvádí na veřejnosti, a dále
- **název díla a pramen.**

Co z toho vyplývá:

- Pokud užíváme díla **při výuce ve škole** (tj. výlučně k vyučovacím účelům), můžeme užít **celé dílo** (viz bod c).
- Pokud vytvoříme dokument (prezentaci, text), který vystavíme na webu, jedná se o **zveřejnění** (našeho) samostatného díla a cizí díla můžeme použít pouze **v odůvodněné míře** (viz bod a). Co je tato míra, zákon nespecifikuje. **Vždy musíme uvést** jméno autora, název díla a pramen.

Obrázky používáme vždy celé, těžko obhájit nějakou odůvodněnou míru. Můžeme je tedy bez ohledu na práva autora užívat pouze pro vyučovací účely.

Obrázky v dílech, která zveřejníme (web apod.) je tedy možné použít:

- **Své vlastní** kresby či fotografie (pozor na práva osob a značek).
- **Z volně dostupných zdrojů**, u kterých je užití výslovně povoleno.
- **Po zajištění souhlasu autora** (případně majitele autorských práv).

Užití a šíření hudby a videa

Autorský zákon v § 30 v odstavci 1 a 2 stanovuje:

1) Za užití díla podle tohoto zákona **se nepovažuje užití pro osobní potřebu fyzické osoby**, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak.
2) Do práva autorského tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.
3) Nestanoví-li tento zákon dále jinak, užitím podle tohoto zákona **je užití počítačového programu či elektronické databáze i pro osobní potřebu** fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby včetně zhotovení rozmnoženiny takových děl i pro takovou potřebu.

Z toho plyne, že zákon v ČR rozdílně upravuje stahování hudby a videa na jedné straně a počítačových programů na straně druhé:

- **Hudbu a video** *můžete* získat a užít pro osobní potřebu. Nesmíte je ale šířit, a to ani zdarma. Zakázána je také veřejná produkce.
- **Software (komerční)** *nesmíte* ani ukládat na disk počítače. Nelegální je samozřejmě také odstraňování ochran proti kopírování programů.

Odkazy na jiné weby jsou samozřejmě legální, u částí webů (obrázků, videa) je to sporné, načíst do svého webu cizí obrázek nebo video je nelegální, pokud to licenční podmínky webu nepovolují (jako např. u **youtube.com**).

CITACE

Abychom dostáli Autorskému zákonu, musíme citovat zdroje – knižní i online. Nemůžeme to však dělat, jak se nám zachce. Existuje citační norma. Některé důležité prvky si projdeme:

- Citaci musíme jasně odlišit od vlastního textu.
- Musíme správně uvést bibliografické údaje (podle normy ČSN ISO 690).

Jak citovat knihu?

Pokud jsme použili citaci z knihy, musíme uvést tyto bibliografické údaje v následujícím pořadí:

- **PŘÍJMENÍ, Jméno.** Příjmení velkými písmeny na prvním místě, odděleno čárkou od jména. Za křestním jménem je tečka.
- ***Název knihy***. Píšeme kurzívou, na konci tečka.
- **Místo: Vydavatel, rok vydání.** Za místem následuje dvojtečka vydavatelství čárka rok vydání.
- **ISBN** – „rodné číslo" knihy.

HRABAL, Bohumil. *Příliš hlučná samota.* Praha: Odeon, 1992. ISBN 80-207-0156-7.

Jak citovat elektronický zdroj?

- **PŘÍJMENÍ, Jméno.** Příjmení velkými písmeny na prvním místě, odděleno čárkou od jména. Za křestním jménem je tečka.
- ***Název článku*** – kurzívou.
- V hranatých závorkách **[online]**. Následuje tečka.
- V hranatých závorkách datum citace ve formátu **[rok-měsíc-den]**, následuje tečka.
- **Dostupný z URL:** vložený odkaz na zdroj – v elektronických dokumentech by měl sloužit jako odkaz

KOPECKÝ, Josef. *Prezidentští kandidáti museli do baru, na univerzitě je nechtěli* [online]. [cit. 2012-11-18]. Dostupný z URL: http://zpravy.idnes.cz/debata-prezidentskych-kandidatu-dienstbier-sobotka-bobosikova-dlouhy-1mp-/domaci.aspx?c=A121118_150616_domaci_kop

Licence

Licence k užívání programů je jeden ze způsobů ochrany autorských práv autorů softwaru. Projdeme si základní typy licencí a pojetí programu jako autorského díla.

LICENCE K UŽITÍ PROGRAMU

Licenci můžeme považovat za jakési oprávnění používat určitý software. Autoři softwaru mají k tomuto dílu autorská práva, chtějí se o ně podělit a tak je software jako každé jiné zboží k prodeji. Nemohou však prodat autorská práva a tak prodávají **licenci**. Dá se říct, že licence je něco jako pronájem na určitou dobu.

Při instalaci programu musíme odsouhlasit licenční smlouvu s koncovým uživatelem (**EULA** – End User License Agreement). Je to obchodní smlouva, která stanovuje práva a povinnosti koncového uživatele programu. Nedodržení smlouvy může mít právní následky, stejně jako nedodržení jakékoliv jiné obchodní i soukromé smlouvy.

Nainstalovaný program musíme **aktivovat** po zadání **licenčního (sériového) čísla** – v angličtině serial key. Licenční číslo můžeme použít na tolik počítačů, na kolik máme licenci.

Samotná **Aktivace** probíhá přes internet nebo telefon a asociuje tak sériové číslo s IP adresou či telefonním číslem. Software nemůžeme pouze zkopírovat, ale crackeři musejí projít jeho ochranou.

Nelegální překonávání těchto zábran se děje především díky **crackům** a **keygenům**. Crack odstraňuje ochranu softwaru a keygen vytváří uměle sériová čísla.

Registrace programu poskytuje uživateli právo na upgrady programy či na jeho aktualizace. Některé programy nabízejí také možnost zavolat na zákaznickou linku v případě problémů.

DRUHY LICENCÍ

Stručně si představíme nejznámější a nejpoužívanější druhy licencí. Licence

k freeware a shareware programům již nebudeme rozebírat.

OEM SOFTWARE

OEM programy jsou klasické programy, které jsou však nabízeny pouze při zakoupení nového hardwaru za sníženou (většinou přibližně třetinovou) cenu. Jsou vázány na díl, se kterým byly zakoupeny. Nedají se upgradovat.

PUBLIC DOMAIN

Skupina programů k volnému užití. Programy můžeme používat, šířit a upravovat. Autoři se totiž vzdali některých svých práv ve prospěch uživatelů. Ze známých produktů uvedeme IM nástroj **ICQ.**

KOMERČNÍ PROGRAMY

U těchto programů platíme za licenci pro koncového uživatele programu. Uživatel neví, jak program funguje, má uzavřený zdrojový kód. Rovněž se nazývají programy **proprietární**.

GNU/GPL LICENCE

Je licence používaná u svobodného softwaru a u opensourcových programů. Tyto programy vytváří alternativu k drahým komerčním programům. Jejich zdrojový kód je otevřený a uživatelé je mohou upravovat za podmínek, které stanovuje tato licence. GPL doslova znamená **General Public Licence.**

Open Source programy vytváří lidé z celé Země a vytváří ji z různých důvodů. Volně dostupné programy vytváří nadšenci, komerční firmy, které je následně předělají a prodávají a také vlády některých zemí podporují vývoj volně šiřitelných programů – např. Čína, Japonsko.

CREATIVE COMMONS

Licencí Creative Commons se neřídí programy, nýbrž zdroje informací. Tyto zdroje jsou legálně a zdarma dostupné. Volná licence však nikdy není úplně volná – může být omezena pouze na nekomerční použití, na určité státy. Může však existovat také podmínka, že nově zveřejněný materiál s touto informací musí být také publikován s volně použitelnou licencí. Otevřených licencí je více – již jsme zmiňovali Public Domain.

Creative Commons jsou licence, které mohou autoři uvést:

- **by)** nebo **[Attribution]** – musíme uvést původního autora materiálu,
- **nc)** nebo **[Noncommercial]** – pouze pro nekomerční využití,
- **nd)** nebo **[No Derivative Works]** – zakazuje změnu původního díla,
- **sa)** nebo **[ShareAlike]** – díla, ve kterých je materiál použit musí mít stejnou licenci.

Autor může omezení libovolně kombinovat, ale nemusí použít žádné. Pokud nepoužije žádné zapíše CC a nic dál, pokud chce všechna omezení, zapíše CC by,nc,nd,sa.

GNU FREE DOCUMENTATION LICENSE

Tato licence je používána u svobodných encyklopedií jako je **Wikipedia**. Autoři textů díky této licenci neručí za zveřejňované údaje. Je možno texty používat, pokud dílo bude mít opět stejnou licenci. Měl by být uveden autor (pokud je znám) a odkaz na stránku.

Použité zdroje

NAVRÁTIL, Pavel. *S počítačem nejen k maturitě*. Praha: ComputerMedia, 2002, ISBN 80-90-2815-9-1.

ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy - Teoretická učebnice*. Praha: Computer Press, 2010, ISBN 978-80-251-3228-9.

Použité obrázky

AUTOR NEUVEDEN. *www.wikimedia.org* [online]. [cit. 1.12.2012]. Dostupný na WWW: http://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png

AUTOR NEUVEDEN. *www.tyden.cz* [online]. [cit. 1.12.2012]. Dostupný na WWW: http://pctuning.tyden.cz/ilustrace3/zombux/ess/nod32-logo.jpg

AUTOR NEUVEDEN. *www.cio.com* [online]. [cit. 1.12.2012]. Dostupný na WWW: http://blogs.cio.com/sites/cio.com/files/u7736/New_Norton_Logo.png

AUTOR NEUVEDEN. *www.careertec-il.org* [online]. [cit. 1.12.2012]. Dostupný na WWW: http://www.careertec-il.org/pages/uploaded_images/AVG_Antivirus_System_logo.jpg

AUTOR NEUVEDEN. *www.creareonline.it* [online]. [cit. 1.12.2012]. Dostupný na WWW: http://www.creareonline.it/wp-content/uploads/2012/10/avast_logo.jpg

AUTOR NEUVEDEN. *www.authworks.com* [online]. [cit. 1.12.2012]. Dostupný na WWW: http://www.authworks.com/images/aut-tokens.jpg

AUTOR NEUVEDEN. *www.lava360.com* [online]. [cit. 1.12.2012]. Dostupný na WWW: http://lava360.com/wp-content/uploads/2010/04/creative_commons_licenses.jpg