Právo v IT

Duševní vlastnictví

Práva k nakládání s díly, vynálezy a jinými nehmotnými předměty. Mělo by se jednat o výsledky tvorby nebo výzkumu, které jsou dostatečně originální.

Dělí se do dvou celků:

1. Autorské právo
    - Nabýváno automaticky
    - Vztahuje se na autorská díla
2. Průmyslové vlastnictví
    - Jde o imateriální vlastnictví
        - Topografie polovodičových výrobků
        - Patenty a vynálezy (počítačový program není v ČR vynález)
    - Pokud jej chceme uplatňovat, je nutné jej registrovat u Úřadu průmyslového vlastnictví

Autorské právo

Autorské právo získává autor díla v okamžik jeho vytvoření v jakékoliv objektivně vnímatelné podobě.

Toto právo **není vázáno na předmět kterým je dílo vyjádřeno** - jeho zničením nedochází k zaniknutí autorských práv a nabytím vlastnických práv k tomuto předmětu se nenabývají autorská práva, ani právo díla užít.

Autorským dílem není: námět, zpráva, informace, metoda, graf, ani výstup počítačového programu.

V ČR **není možné vzdát se autorských práv**, a převedení práv na jinou osobu nebo subjekt je možné až po autorově smrti. Ve většině států světa, je toto převedené právo platné 70 let od úmrtí autora.

Pokud se na tvorbě podílí více autorů, všichni získávají stejné nároky na vlastnictví díla, veškerá rozhodnutí musí být společná.

V případě, že je autorem díla zaměstnanec firmy, který vývoj provádí jako plnění svých povinností k zaměstnavateli, získává majetková práva firma, nepředává se však autorství.

Musíme rozlišovat chybné užití a úmysly. Pokud je software autora použit chybně, nemůže za to autor. Pokud je ovšem software vyroben se špatnými úmysly (např. hra ‘Zastřel si svého cikána’), je za to autor zodpovědný.

Autorské právo (copyright) je právo autora nakládat se svým dílem podle libosti. Pro software to znamená, že autor může program upravovat a distribuovat jak uzná za vhodné.

Pokud chce autor umožnit uživateli se softwarem nakládat podle jeho svolení, dělá tak pomocí

licence.

Softwarové licence

Licence je právní dokument, kterým autor určuje podmínky použití jeho softwaru uživatelem.

Free and Open Source software (FOSS/FLOSS)

Free, Libre and Open Source Software

Jde o software který má veřejně dostupný zdrojový kód a tento kód lze upravovat a redistribuovat.

Pod FOSS/FLOSS spadají dvě označení softwaru.

- **Free Software**
- **Open Source software**.

Definice k termínu Free Software (svobodný software) od Free Software Foundation:

Free software lze svobodně:

1. používat jak uživatel uzná za vhodné
2. upravovat
3. distribuovat kopie
4. distribuovat upravené kopie
    - Jak zdarma tak za úplatu

Definice Open Source software od Open Source Initiative:

- 10 bodů, vedou k téměř stejnému závěru

Obě definice vedou v téměř úplné většině případů ke stejně volnému a svobodnému softwaru. Liší se pouze ideologií. Zastánci free softwaru tvrdí, že tento název je jediný správný, protože dává jasně důraz na svobodu uživatele, zatímco open-source klade důraz pouze na možnost kolaborace větší skupiny lidí díky dostupnému zdrojovému kódu, což je výhodné pro firmy, které proto používají tento název.

Uživatelé FOSS softwaru mohou nabízet placenou technickou podporu, nebo další placené služby. Např. Red Hat Enterprise Linux.

Pod jedním názvem je často zahrnuta skupina licencí, většinou různých verzí původní licence. Je proto důležité dávat pozor která verze licence je použita.

Některé verze jedné licence mohou například vyžadovat uvedení jména autora původního softwaru, zatímco jiné verze tento požadavek mít nemusí.

Copyleft licence

Copyright většinou omezuje svobodu uživatelů produktu, zatímco copyleft omezuje omezování svobody uživatelů.

Licence tohoto typu zaručují uživateli produktu možnost kopírovat, upravovat a redistribuovat tento produkt s podmínkou **zachování stejné licence** jako u originálního produktu.

Dále se dělí na strong copyleft a weak copyleft. Kde **strong copyleft** zaručuje nutnost zachování licence u všech kopií, a **weak copyleft** umožňuje v některých případech (například používání knihovny) použití kopie softwaru v softwaru s jinou licencí. Nesmí ovšem dojít k úpravě kódu softwaru s weak copyleft licencí.

Strong copyleft

- GNU GPL - 3 verze, poslední z roku 2007
  - Linux kernel, VLC, Blender
- AGPL - Affero GPL - podmínka poskytnutí source kódu i u softwaru užívaného přes síť
  - Slic3r, ownCloud

Weak copyleft

- GNU LGPL - často používaná pro knihonvy
  - 7-zip
- MPL - Mozzila Public License
  - LibreOffice

Permissive licence

Permisivní softwarové licence dávají koncovému uživatli ještě více svobody než copyleft licence. Většinou **nevyžadují, aby bylo dílo odvozené od původního software s permisivní licencí vydáno pod stejnou licencí**. Toto platí ve všech případech, bez podmínek, na rozdíl od weak copyleft licencí.

Jednou z nejznámějších skupin licencí tohoto typu jsou **BSD licence**. Proto jsou někdy licence z této skupiny nazývány **BSD-like** nebo **BSD-style**.

- BSD - 4 verze, starší mají více požadavků (4), nejnovější je nejvolnější (0 požadavků)
  - FreeBSD, Go, a další
- MIT - v roce 2015 ji používalo 45% projektů na GitHubu
  - Emmet, Babel
- Apache License
  - Apache HTTP Server

Proprietární licence

Většinou použity pro komerční software. Licence (typicky EULA) zakazuje šíření a modifikace. Uživatel **nemá přístup ke zdrojovému kódu**. Tato licence je s uživatelem typicky uzavřena při **prvním spuštění softwaru** a bez souhlasu s licencí není možné software používat.

Většinou je omezen počet kopií které může uživatel používat, nebo prodejci vydávají verze s menším počtem funkcí které je potřeba dále dokoupit.

Hardwarový klíč

Hardwarové zařízení (v dnešní době většinou flash drive), které dodává výrobce k softwaru. Toto zařízení obsahuje klíč který je spojený s číslem licence SW. Při spuštění si SW ověří přítomnost tohoto zařízení a ověří správnost klíče - až potom umožní spuštění.

Zajímavé linky
https://opensource.org/faq
https://choosealicense.com/
https://www.gnu.org/licenses/license-list.html
https://www.gnu.org/licenses/gpl-faq.html

Bezpečnost v IT

Hacking a Cracking

Hacker

Neznamená pouze člověk který se nabourává do systémů.

Je to označení pro někoho kdo je zvědavý, chce **vytvářet nové věci**, dělat věci **jiným**, nečekaným **způsobem** a ukázat svoji zdatnost v dané disciplíně, např. v programování.

Může být také označením pro zkušeného programátora s detailními znalostmi fungování systému nebo označuje někoho, kdo zkoumá každý detail systému či programu a snaží se jej využít novým, zajímavým způsobem.

Často se ale termínem hacker myslí přímo **security hacker**, neboli člověk snažící se získat neoprávněný přístup k nějakému zařízení či systému nebo v něm najít chyby, bez ohledu na to, k jakému účelu toto provádí.

V mainstream médiích je termín hacker téměř výhradně používán jako označení počítačového zločince, který se nabourává do systémů, krade data nebo nějak jinak škodí uživatelům a jejich zařízením.

Cracker

Cracking je také získávání neoprávněného přístupu k systému, který je využit k další **nelegální činnosti**, např. za účelem krádeže nebo zničení dat.

Někteří lidé s touto definicí a předchozí definicí hackera nesouhlasí, a tvrdí, že všichni kdo se nabourávají do systému za jakýmkoliv účelem by se měli nazývat crackeři a dále se dělit podle úmyslů.

Dělení podle čepic - úmyslů

White hat

- Etičtí hackeři
- zkoumají a testují bezpečnost systému za účelem opravení nebo nahlášení nalezených chyb
  - dělají penetration tests nebo vulnerability assessments
- Společnosti si je najímají aby se s jejich svolením pokusili dostat do jejich systému, nebo aby našli nějakou jinou chybu v jejich softwaru

Black hat

- zločinci
- za účelem **zisku** nebo jen tak

Grey hat

- Něco mezi black hat hackerem a white hat hackerem
- naboural se do systému bez důvodů white hat hackera (není k tomu pověřen výrobcem systému ani pro výrobce nepracuje), ale neprozrazuje nalezené chyby (místo toho např. nabídne správci systému opravení této chyby za určitou peněžní částku)

Script kiddie

- nezkušený hacker bez znalostí, který používá automatické scripty od jiných lidí
- většinou se tak označuje někdo kdo nerozumí jak daný script funguje, pouze se ho naučí používat

Útoky v počítačových sítích

Denial of service útoky

DoS nebo DDoS (Distributed Denial of Service) je typ útoku na internetové služby, jehož cílem je službu shodit a znepřístupnit ostatním uživatelům.

Při útoku dojde k přehlcení serveru požadavky a server není schopný vyhovět novým požadavkům od skutečných uživatelů.

- Při DDoS je použita síť botů - velké množství počítačů, které společně napadnou daný server
- Při tomto útoku **nezíská** útočník přístup k žádným datům z napadeného serveru

Amplification útoky

Například DNS Amplification útoky.
Jsou zasílány DNS dotazy z podvržené IP adresy, která je stejně jako u ostatních amplification útoků zároveň IP adresou oběti. Díky značnému množství DNS odpovědí, které si ve skutečnosti oběť nevyžádala, může být její zařízení vyřazeno z provozu. Útočník posílá na DNS servery malé DNS dotazy a na IP adresu oběti jsou zasílány několikanásobně větší odpovědi.

Man in the middle

Útok při kterém se útočník dostane ‘doprostřed’ datového přenosu mezi dvěma počítači (uživatel a webová stránka).

- Je pak schopný odposlouchávat přenesená data, nebo tato data i měnit.
- může dojít k záměně uživatelem vyžádané stránky za utočníkem vytvořenou podvodnou, kam uživatel zadá osobní data

nebezpečné jsou zejména veřejné wifi

Obranou proti tomuto útoku jsou např. certifikáty

ARP spoofing

Zneužití Address Resolution Protocolu (ARP), umožňující útočníkovi vydávat se v místní síti za jiný počítač podvržením odpovědi na ARP dotaz. ARP dotaz slouží k překladu IP adresy příjemce paketu na jeho MAC adresu. Podvržením odpovědi může útočník pakety určené oběti nasměrovat na vlastní MAC adresu.
Může tak dojít k MITM útoku, i když útočící počítač není přímo uprostřed komunikace, ale stačí když je na stejné síti.

Port scanning

Port scanning je útok při kterém se útočník snaží zjistit, které porty jsou na vzdáleném zařízení zranitelné (otevřené) a poté se přes ně pokusí zaútočit.

Získávání dat z počítače

Data ze systému můžeme získat buď díky hlouposti lidí kteří jej vytvořili, nebo díky hlouposti lidí kteří jej používají.

Tedy pomocí:

1. Zneužívání chyb a slabin systému
2. Sociálního inženýrství

Keylogger

Program nebo **hardwarové zařízení** které zaznamenává interakci s **klávesnicí** a data může odesílat útočníkovi.

Phishing

Jde o metodu **sociálního inženýrství**, kdy jsou rozesílány **podvodné emaily** (mohou být použity například i SMS a telefonní hovory), které se **vydávají** za emaily od **legitimních** společností a snaží se přesvědčit uživatele k poskytnutí **citlivých informací**.

Mohou například obsahovat odkaz na stránku napodobující pravou stránku společnosti, která ovšem zasílá všechna zadaná hesla nebo čísla karet útočníkům.

Firewall

Firewall je síťový bezpečnostní systém, který odděluje dvě sítě. Řídí a zabezpečuje síťový provoz mezi těmito sítěmi nebo zařízeními

- Network firewalls
  - odděluje sítě s rozdílnými úrovněmi zabezpečení (typicky lokální síť a internet)
- Host-based firewall
  - řídí provoz do a z počítače na kterém běží

Firewall má možnosti nastavení různých bezpečnostních pravidel, která zahrnují zdrojovou a cílovou **IP adresu**, zdrojový a cílový **port**, informace o stavu spojení, atd. Na základě těchto pravidel pak **blokuje podezřelé** a propouští pouze důvěryhodné připojení z obou směrů komunikace.

Zajímavé linky
https://en.wikipedia.org/wiki/Hacks_at_the_Massachusetts_Institute_of_Technology
https://en.wikipedia.org/wiki/Hacker
https://en.wikipedia.org/wiki/Security_hacker
https://en.wikipedia.org/wiki/DSniff
https://en.wikipedia.org/wiki/Firewall_(computing)#History