

# Právo a bezpečnost v IT

## Duševní vlastnictví

Obecně se duševním vlastnictvím myslí výsledky lidského tvoření.

Duševní vlastnictví se v právním světě dělí do dvou kategorií:

- Autorské právo - vztahuje se na umělecká díla (literaturu, fotografie, filmy,...), není u něj nutnost nikde ho registrovat, vzniká automaticky při vytvoření díla (udělání fotky, natočení filmu, napsání na papír,...)
- Průmyslové vlastnictví - vztahuje se na veškeré vyráběné zboží, pokud jej chceme uplatňovat je potřeba jej registrovat v podobě patentů

## Softwarové licence

Softwarové licence jsou právní nástroje, kterými autor softwareu určuje práva a povinnosti uživatele softwareu.

Za nejznámější licence by se asi daly považovat: licence BSD a licence GNU/GPL.

Důležité je uvědomit si, že licence není kupní smlouva, tím pádem si dané dílo nekupuji, ale dostávám právo s ním pracovat.

### BSD licence

BSD licence je licence pro svobodný software (tzn. software, který má zveřejněný svůj kód a umožňuje jej plně využívat nebo modifikovat). Tato licence umožňuje volné šíření softwareu a žádá pouze uvedení autora, informace o licenci a zřeknutí se práv za jakékoliv škody způsobené tímto softwarem.

### GNU/GPL licence

licence GNU/GPL je také licence určená pro svobodný software. Jedná se o takzvanou copyleftovou licenci, což je licence, která vyžaduje po člověku, který software modifikuje a použije, aby jej dále šířil pod stejnou licenci. Tato licence je známa hlavně kvůli tomu, že ji Linus Torvalds aplikoval na linuxové jádro.

## Hacking X Cracking

Pojem hacker je velmi nejednoznačně určený. Jako hacker může být označený člověk, který má rozsáhlé znalosti v oblasti počítačové bezpečnosti a používá je v praxi k zajištění bezpečnosti (může

být označený také jako etický hacker nebo whitehat hacker). Dále však může být jako hacker označen člověk, který má znalosti v oblasti bezpečnosti, ale zneužívá je k získání uživatelských dat nebo k vyřazení systémů z provozu (může být označován také jako blackhat hacker nebo také cracker).

## Techniky útoku v počítačových sítích

### Distribute denial of service (DDos)

DDos je takový útok, při kterém útočník nebo útočníci pomocí sítě botnetů (viz. [Viry a malware](#)) posílají na server tolik požadavků, že se server přehltí a může tak dojít i k jeho pádu. Problém s tímto útokem při ochraně proti němu je v tom, že se nedá poznat jestli jde opravdu o útok nebo pouze o spoustu uživatelů, kteří chtějí svá data.

### Man in the middle

Man in the middle je útok při kterém se útočník stává aktivním prostředníkem při komunikaci mezi účastníky. Příkladem může být [Pineapple](#), toto zařízení se chová tak, že kopíruje SSID wi-fi sítě a to vede k tomu, že komunikace mezi zařízením a wi-fi routeru běží přes Pineapple.

### Port scanning

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

## Techniky získávání dat z počítače



Dělení útoků - sociální inženýrství a zneužívání systémů

### Keylogger

Virus nebo červ, který zachytává cokoli píšete na klávesnici a odesílá to útočníkovi. To může vést k ukradení hesel.

### Phishing

Jedná se o techniku, při které jsou rozesílány uživatelům maily vydávající se za maily příchozí z nějaké instituce (banka, facebook,...). Většinou vás buď přesměřují na podvrhnutou stránku, která vypadá stejně jako Facebook, ale je na jiném serveru a po zadání hesla si ho útočník uloží a může s ním dále nakládat, nebo žádají o zaslání hesla nebo čísla karty mailem zpátky.

[Ukázka phishingového mailu](#)

## Firewall

Firewall je síťové zařízení, které odděluje dvě sítě s rozdílnými úrovněmi zabezpečení (typicky lokální síť a internet). Firewall má možnosti nastavení různých bezpečnostních pravidel (blokování určitých portů, blokování konkrétních ip adres,...).

From:

<https://wiki.gml.cz/> - **GMLWiki**

Permanent link:

<https://wiki.gml.cz/doku.php/informatika:maturita:4a?rev=1427551762>

Last update: **28. 03. 2015, 15.09**

