**Datová a informační bezpečnost – základní pojmy**

Informační bezpečnost chápeme jako zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.

Bezpečný informační systém definujeme jako systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti.

Možnosti aplikování bezpečnostní politiky informačního systému:

* Paranoidní - absolutní zabezpečení, téměř vše je uživatelům zakázáno, z důvodů bezpečnosti neexistuje žádné spojení lokálního informačního systému s okolním světem.
* Přísná - všechno, co není výslovně dovoleno provádět, je zakázáno.
* Povolná - co není zakázáno, je povoleno.
* Promiskuitní - vše je dovoleno, tedy i to, co by mělo být z důvodů alespoň základní ochrany zakázáno

Základní pojmy v oblasti informační bezpečnosti:

* **Důvěrnost (confidentiality):** zajištění, že jakékoli nakládání s informacemi/službami/systémem je umožněno pouze oprávněným subjektům,
* **celistvost (integrity):** zajištění, že informace nemohou být neoprávněně pozměněny nebo zničeny,
* **dostupnost (availability):** zajištění, že oprávněné subjekty mají adekvátní a ničím nerušený přístup k informacím nebo službám,
* **autentizace (authentication):** ověření, že subjekt je ten, za koho se vydává **autorizace (authorization):** ověření, zda má příslušný subjekt právo provést operaci, kterou vyžaduje (vystřelit rakety),
* **nepopiratelnost (non-repudiation):** zajištění, že subjekt, který inicioval nějakou operaci, nebude moci tuto skutečnost popřít (rozkaz byl prokazatelně podepsán prezidentem, vlastní rukou),
* **certifikát**: je digitální potvrzení totožnosti připojené k digitálnímu podpisu, použitelné pro ověření pravosti podpisu podepsaného uživatele (u certifikační autority),
* **certifikační autorita**: je instituce, vydávající certifikáty k digitálním podpisům na základě ověřených údajů o žadatelích s mírou odpovědnosti vyplývající z požadované úrovně – třídy certifikátu (Class 1-5),
* elektronický podpis je obdoba písemného podpisu v digitální podobě. (Digitální podpis je speciální případ elektronického podpisu, kdy k ověření původu dochází na bázi šifrování. Digitální podpis je také dále definován jako krátká datová položka pevné délky vytvořená pomocí kryptografické transformace z elektronické zprávy nebo datového souboru a ze soukromého klíče podepisujícího subjektu. Digitální podpis slouží k ověření identity podepisujícího a rovněž stvrzuje, že zpráva nebyla změněna, tzv. ověření integrity zprávy.)

**Cíle informační bezpečnosti:**

Základním cílem je ochrana a eliminace hrozeb četně jejich dopadů. Hrozbami jsou například:

* kompromitace
* nedovolená modifikace (změna hodnot)
* destrukce části, nebo celého informačního systému
* zneužitím citlivých informací
* použití klamných dat, ze kterých budou odvozeny chybné výsledky a závěry
* špatná interpretace hodnot
* neoprávněný přístup k hmotným (hardware) i nehmotným (data, informace) hodnotám
* únik informací (kopie, krádež, odvození požadovaných údajů ze získaných zdrojů dedukcí)

Informační systém se před působením hrozeb brání řadou protiopatření. Ta pak mohou mít různé podoby:

* administrativní (zákaz přístupu, či manipulace s daty …)
* logická (nastavení přístupových práv)
* fyzická (zabránění přístupu nepovolaných osob, ochrana objektů …)
* technická (disková pole, šifrovací a kryptografické systémy …)

**Použitá literatura:**

BRECHLEROVÁ, Dagmar. *Řešení informační bezpečnosti (1. část)* [online]. 2005 [cit. 2013-02-02]. Dostupné z: <http://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm>

JAŠEK, Roman. *Úvod do informační bezpečnosti*. Zlín, 2002.

ŠTÍPEK, Petr. *Základní atributy informační bezpečnosti* [online]. [cit. 2013-02-02]. Dostupné z: http://stipek.wordpress.com/slovnik/