Bezpečnost informačních technologií

Ing. Bc. Marek Čandík, PhD.

Úvod

- Informační technologie zpracovávají hodně informací s velkou hodnotou.
- Pokud hovoříme v souvislosti s informačními technologiemi o *zpracovávání informací*, pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací.

Bezpečnost informací

musí být chráněny tak:

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly nefalšované informace
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- aby nebyly nekontrolovaným způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřebné.

Narušení bezpečnosti

- narušením soukromí či utajení informací
- vydáváním se za jinou oprávněnou osobu a zneužíváním jejích privilegií
- distancováním se od odpovědnosti nebo od závazků plynoucích z manipulace s informacemi
- tvrzením, že se nějaká informace někam poslala a toto se nikdy nestalo
- tvrzením, že se informace získala od nějakého podvodníka
- neoprávněným zvýšením svých privilegií přístupu k informacím
- modifikací privilegií ostatních osob
- zatajením výskytu důvěrné informace v jiných informacích

Zranitelnost informačních systémů

- Zranitelnost informačních systémů představuje jejich obecnou vlastnost. Jedná se vlastně o zranitelná místa (zranitelné komponenty, prvky) těchto systémů jak z hlediska funkčnosti, tak i správnosti (přesněji, míry záruky za správnost).

Rizika informačních systémů

- Pravděpodobnost, že se uplatní některá z hrozeb nebo zranitelných míst informačních systémů je vyjádřena hodnotou informačního rizika.

Rizika informačních systémů

- nejpravděpodobnější riziko pramení z uplatnění hrozby - systém je dodán, instalován nebo používán způsobem, který není bezpečný.
- Nejčastějšími příčinami tohoto rizika bývají omyly a nedbalost personálu spolu s nesprávnou manipulací

Napadení informačního systému

- **Nedostupnost služby** - tzv. DoS útoky (Denial of Service) - způsobí, že případná služba (http, ftp…), na kterou byl prováděn útok přestane být funkční - může dojít i k "zatuhnutí", případně restartu serveru apod.
- **Neoprávněný přístup** - výsledkem útoku může být to, že útočník neoprávněně získá plný nebo částečný přístup k zařízení, a to mu následně umožní provádět neautorizované změny v konfiguraci, mazání nebo modifikaci souborů apod. Často bývá takto napadený server využíván jako základna pro provádění útoků na další zařízení.
- **Získání důvěrných informací** - výsledkem útoku může být získání citlivých informací - např. seznam uživatelských jmen a hesel apod.

Zabezpečování IT

- Pojmem zabezpečování IT označujeme proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT na přiměřené úrovni.

Závěr

- absolutní bezpečnost je nedosažitelná.
- *bezpečnost je trvalý proces.*

Tento článek byl zpracován v rámci Projektu vědeckovýzkumného úkolu č. 4/4 „Informační bezpečnost a kybernetická kriminalita v organizaci“, který je součástí Integrovaného výzkumného úkolu na léta 2010-2015, realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.