# INFORMAČNÍ TECHNOLOGIE PRO E-BUSINESS P10
# 2008-12-04

## BEZPEČNOST ICT:

### Základní pojmy:

- ✓ **Identifikace:**
  - Jednoznačné rozlišení uživatele
  - Osobní číslo, login, uživatelské jméno apod.
- ✓ **Autentizace:**
  - Ověření pravosti identifikace
  - Autentizace znalostí, vlastnictvím nebo vlastností
- ✓ **Autorizace:**
  - Oprávnění ke zvolené činnosti v systému
  - Na základě provedené autentizace a identifikace
- ✓ **Symetrické/asymetrické šifrování** – zabránění čtení dat neautorizovaným osobám
- ✓ **Steganografie** – skrývání dat mezi jiná (běžná) data
- ✓ **Digitální podpis**

### Bezpečnost na Internetu:

- ✓ **Internet neposkytuje žádné zabezpečení:**
  - Routery ve vlastnictví soukromých společností
  - Snadné podvržení falešných dat
  - Není zajištěna identita protistrany
  - Internet může být dokonale anonymní
  - Bezpečnost je řešena nadstavbami (HTTPS, digitální podpis apod.)
- ✓ **Bezdrátová připojení k internetu:**
  - Nešifrovaná spojení lze snadno odposlechnout
  - WEP klíč byl prolomen
  - ...
- ✓ **Bezpečnost Skype:**
  - Není otevřeným protokolem
  - Přenos dat je šifrovaný, ale nikdo neví jak
  - Nody, supernody
  - Má Skype zadní vrátka? Gary Kasparov
- ✓ **Sociální inženýrství:**
  - Získávání informací od důvěřivých nebo nepozorných uživatelů
  - Phishing [fišink] – „podvodné“ maily vyzývající k zaslání přihlašovacích údajů
- ✓ **Řešení bezpečnosti:**
  - **VPN – virtuální privátní sítě**
    - Připojení vlastního počítače do podnikové sítě přes internet
    - Nebezpečí – domácí počítač se stává součástí firemní sítě – nutnost zabezpečení
  - **HTTPS:**
    - Zabezpečený protokol HTTP
    - Používán pro intranetové aplikace dostupné přes internet
- ✓ **Počítačové viry:**
  - Jedná se o škodlivý programový kód
  - OneHalf
  - **Dělení virů:**
    - Rezidentní/nerezidentní:
      - Rezidentní:
        - V dnešní době je většina virů rezidentních
        - Po spuštění počítače nebo aktivaci viru přetrvává v paměti

- Při pokusu o likvidaci se snaží vrátit zpět (klasicky záznam v registru)
- Často se snaží odesílat informace z počítače
- Umožňuje útočníkovi ovládat systém

▪ Polymorfní

- o Bootovací viry – zavádí se před vlastním zaváděním operačního systému
- o Polymorfní – virus neustále mění svůj otisk, je tedy těžko odhalitelný pro antivirové programy
- o Stealth viry – snaží se skrýt před systémem – schovávání procesů, při pokus o čtení souboru s virem systému podvrhne původní obsah
- o Hoaxy – jedná se o poplašné zprávy, není přímo virem, nechá uživatele, aby si škodu způsobil sám
- o Keylogger – programy zaznamenávající stisky kláves, některé dokonalejší zaznamenávají kliknutí myší a okolí kliknutí na obrazovce, k dispozici jsou i hardwarové keyloggery.

**Šifrování dat:**

- ✓ Snaha skrýt data před neautorizovanými uživateli
- ✓ **Symetrické šifrování:**
  - Stejný (nebo snadno odvoditelný) klíč pro šifrování a dešifrování
  - Prvopočátky již v Římě – Cézarova šifra
  - Playfairova šifra (1854)
  - Nejnověji se používá DES, 3DES, AES
- ✓ **Asymetrické šifrování**
- ✓ **Hashování:**
  - Význam má pro ověření integrity dat, pro řazení nebo pro ukládání hesel
  - Základní vlastností je, že malá změna na vstupu představuje velkou změnu na výstupu
  - Původně CRC
  - Pravidla pro hash:
    - o Vstup může být jakékoliv délky
    - o Výstup musí mít pevnou délku
    - o Hodnota hash musí být jednoduše vypočitatelná pro jakýkoliv vstupní řetězec
    - o Funkce je jednosměrná (irreverzibilní)
  - Hashovací funkce je:
    - o Jednosměrná
    - o Slabě bezkolizní
    - o Silně bezkolizní

**Steganografie:**

- ✓ Data jsou pouze schovávaná, nikoliv šifrovaná
- ✓ Historie vznikla opět v Římě
- ✓ Pro schovávání se nejlépe využívají rozsáhlé soubory – obrázky, videa
- ✓ Existují programy pro schovávání dat do obrázků

**Důkaz znalostí:**

- ✓ Nejběžnější způsob autentizace
- ✓ Ověření heslem
- ✓ Náchylné na odposlech (keylogger, termosnímače)
- ✓ Výhodou je možnost sdílení hesla (sdílení hesla ve skupině)

**Důkaz vlastnictvím:**

- ✓ Uživatel se prokazuje vlastnictvím autentizačního prvku
- ✓ OTP (One TIme Password) – jednorázová hesla (nelze je použít opakovaně)

**Důkaz vlastností:**

- ✓ Bimetrické metody autentizace
- ✓ Otisk prstu, oční duhovka, skenery žil, typické chování uživatele (dynamika úhozu na klávesnici, rychlost psaní)

**Digitální podpis:**

- ✓ Využívá asymetrické kryptografie
- ✓ Digitální podpis zprávy