



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY



**OP Vzdělávání  
pro konkurenceschopnost**

INVESTICE  
DO ROZVOJE  
VZDĚLÁVÁNÍ

Střední průmyslová škola a Vyšší odborná škola technická Brno, Sokolská 1

**Šablona:** Inovace a zkvalitnění výuky prostřednictvím ICT

**Název:** Základy výpočetní techniky

**Téma:** Ochrana před viry

**Autor:** Ing. Jakab Barnabáš

**Číslo:** VY\_32\_INOVACE\_28–19

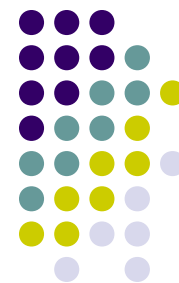
**Anotace:** *Materiál uvádí základní technologie, které používají antivirové programy.  
Je určen pro žáky 1. ročníku oboru strojírenství.  
Vytvořeno: prosinec 2013*

# Antivirové programy



- **Antivirový program** sleduje všechna nejpodstatnější vstupní/výstupní místa, kterými by viry mohly do počítačového systému proniknout.
- Pokud jde o viry samotné můžeme říci, že se jedná o nežádoucí a ve většině případů škodící kód, který se cíleně šíří.

# Rozdělení antivirových programů



- **On-demand skenery** – spouštějí se přes rozhraní OS DOS a jsou určeny pro případ, že systém není z důvodu poškození schopen nastartovat běžným způsobem.
- **Jednoúčelové antiviry** – jde o antivirové programy, které jsou zaměřeny na detekci, popřípadě i odstranění jednoho konkrétního viru, popřípadě menší skupiny virů.

# Rozdělení antivirových programů



- **Antivirové systémy** – jde o komplexní antivirové řešení, které má za úkol ochránit počítač před červy šířící se poštou, škodlivými skripty případně zabránit stažení infikovaných souborů.
- Komplexní nástroj může mít ve výbavě jak firewall tak i další specializované nástroje.

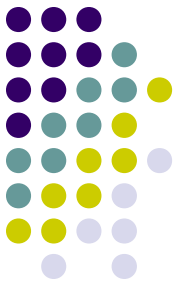


# Antivirové programy

- Kaspersky
- Eset
- AVG
- Avast
- McAfee
- F-Secure
- BitDefender

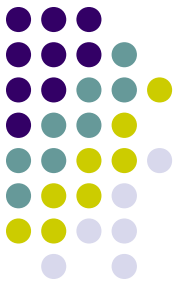


# Způsoby ochrany



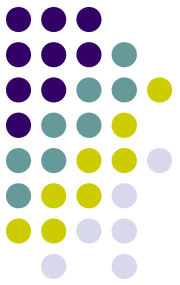
- **Vyhledávací programy** – vyhledávají určité kódy, které obsahují již známé viry.
- Vyhledávací program, využívající tuto techniku je velmi spolehlivý.
- Při dnešním množství virů a jejich variant není možné vytvořit vyhledávací program, který by našel většinu z nich.

# Způsoby ochrany



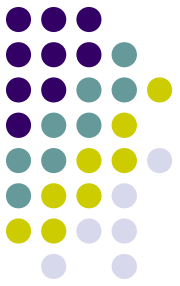
- **Skenovací programy** – vybere z těla virů nějaké charakteristické skupiny instrukcí a takto získané sekvence použije pro hledání napadených programů.
- Tato koncepce vyžaduje pravidelnou aktualizace, ale nabízí za to jedinečnou schopnost rozpoznat napadený program ještě před tím, než ho začneme používat.

# Způsoby ochrany



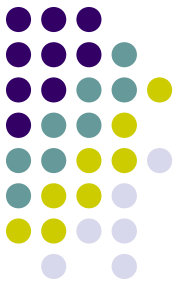
- **Heuristická analýza** – jde o rozbor kódu hledající postupy pro činnost virů typické.
- **Kontrola integrity** – je založena na porovnání aktuálního stavu důležitých programů a oblastí na disku s informacemi, které si o nich kontrolní program uložil při své instalaci.

# Způsoby ochrany



- **Rezidentní kontrola** – počítač je stále pod dohledem, i když nedetekuje tolik virů, jako normální skener.
- **Léčky** – doplňková metoda, která pro hledání nových virů vypouští různé udičky a následuje následná kontrola.

# Použité zdroje



- Kocman, R., Lohniský, J. *Jak se bránit virům, spamu a spyware*. Computer press, 2005
- <http://www.nejlepsi-antivir.cz> [cit. 2013-12-04].
- <http://www.viry.cz> [cit. 2013-12-04].