**Antivirový software**

Na softwarovém poli působí poměrně velké množství antivirových programů. Antivirový program by měl používat každý, kdo je alespoň částečně nucen komunikovat prostřednictvím flash disků nebo jiného typu média s daty na jiných počítačích a kdo je propojen do sítě s jinými počítači.

Antivirovou kontrolu by měl uživatel provádět v pravidelných intervalech. Důležitá je také aktualizace virové databáze – načtení nově zjištěných virů do databáze antivirového programu je nutné proto, aby antivirový program byl schopen nové viry identifikovat a odstranit. Aktualizace se provádí většinou přes Internet, může být však ještě realizována pomocí disket nebo CD. Slouží k vyhledání a odstranění virové hrozby pro zajištění bezpečnosti používaného PC.

Antivirové programy můžeme rozdělit do několika skupin například následovně od nejednodušších až po nejsložitější:

Jde o antivirové **Jednoúčelové antiviry**

Programy, které jsou zaměřeny na detekci, popřípadě i dezinfekci jednoho konkrétního viru, popřípadě menší skupiny virů. Jednoúčelové antiviry nelze rozhodně použít jako plnohodnotnou antivirovou ochranu.

**On-line skenery**

Obvykle jde o skript, který ve spojení s internetovým browserem dokážou plnohodnotně prohledat na výskyt virů pevný disk uživatele, bez toho, aby tento antivirus získal fyzicky natrvalo.

**Antivirové systémy**

V dnešní době jde o nejčastější formu antivirových programů. Antivirový systém se skládá s částí, které sledují všechny nejpodstatnější vstupní/výstupní místa, kterými by případná infiltrace mohla do počítačového systému proniknout. Mezi tyto vstupní/výstupní místa může patřit například elektronická pošta (červi šířící se poštou), www stránky (škodlivé skripty, download infikovaných souborů), média (cédéčka, diskety apod.). Nedílnou součástí dnešních antivirových systémů je aktualizace prostřednictvím Internetu. Jde o komplexní antivirové řešení v některých případech doplněno i o osobní firewall. Do této kategorie patří takové produkty, jakými jsou: avast!, AVG, Norton Antivirus, Kaspersky Antivirus, NOD32, McAfee Viruscan atd.

## Nástroje pro zjištění ( odstarnění) virů

* Skenování – hlavním cílem bylo vybrat z těla virů některé charakteristické skupiny instrukcí a takto získané sekvence použít pro hledání napadených programů. Pro zvýšení šance zachytit nové varianty virů používají skenery více různých sekvencí pro jeden virus. Tím je také umožněno přesnější rozpoznání konkrétního viru a snížena pravděpodobnost falešného poplachu. Velmi důležitá je zde pravidelná aktualizace.
* Kontrola integrity - Kontrola integrity (integrity checker, CRC checker) je založena na porovnávání aktuálního stavu důležitých programů a oblastí na disku s informacemi, které si o nich kontrolní program uložil při jejich příchodu do systému nebo při své instalaci. Pokud se do tímto způsobem chráněného počítače dostane vir, tak na sebe upozorní změnou některého z kontrolovaných objektů a je záhy detekován. Dají se tak spolehlivě zachytiti nové viry, které nemusí být odhaleny skenováním a heuristickou analýzou.
* Heuristická analýza - jde o rozbor kódu hledající postupy pro činnost virů

**Praktické projevy virů:**

Počítačový vir je program a jako takový se projevuje podle toho, jak byl naprogramován. Existují stovky způsobů, jak se viry projevují, počínaje výpisem nejrůznějších humorných hlášení na obrazovku až po destrukční viry. Obecně můžeme projevy virů rozdělit na:

* obtěžující - příznaky obtěžujících virů spočívají například ve výpisech nesmyslných hlášení na obrazovku. Viry mohou obtěžovat také záměnou kláves na klávesnici atd,
* destrukční - základním úkolem takových virů je zlikvidovat data. Chytré viry pracují tak, že nezničí všechna data na disku, ale postupně zaměňují pouze určité byty nebo řetězce. Uživatel takový vir těžko odhalí a při dlouhodobém působení nakazí i záložní kopie. Jednoduché viry zničí okamžitě po napadení například obsah disku a tím vlastně zničí samy sebe. Destrukční viry, stejně jako obtěžující, mohou být naprogramovány na určitou dobu (například pátek třináctého) nebo v souvislosti s určitou akcí v počítači. Také mohou být zaměřeny pouze na určitý typ dat (např. dokumenty MS Office),
* ostatní - sem se řadí ostatní typy virů. Často se stává, že viry nejsou kvalitně napsané a že se dostávají do kolizí s jinými programy. Pak se z původně neškodného viru klidně může stát destrukční – a to vlastně náhodou. Spousta virů nevykonává žádnou přímo destrukční činnost, ale pouze se snaží dále a dále šířit. I takové viry mohou způsobovat problémy, obsazovat paměť, brzdit síťový provoz a podobně. Další viry mohou rozesílat informace z vašeho počítače na jiné, kde si je může autor viru přečíst, šířit se automatickým rozesíláním elektronickou poštou, nebo třeba šifrovat data na disku.

**Použitá literatura:**

HÁK, Igor. *Moderní počítačové viry* [online]. [cit. 2013-02-03]. Dostupné z: <http://www.cmsps.cz/~marlib/bezpecnost/viry/velka_kniha_o_virech.pdf>

*Počítačové viry* [online]. [cit. 2013-02-03]. Dostupné z: <http://www1.osu.cz/~klimesc/public/files/Pocitacove%20systemy/Prednasky/08_-_Pocitacove_viry.pdf>

*Počítačové viry, antivirová ochrana a bezpečnost na internetu* [online]. [cit. 2013-02-03]. Dostupné z: http://www.ped.muni.cz/wtech/old2012/u3v/iepp/05.pdf