Antiviry

Hlavní druhy ochrany proti malwaru

- Antivir
- Firewall
- AntiSpyware
- ZDRAVÝ ROZUM!

Jak bojovat proti virům

- Mějte nainstalovaný kvalitní antivirový program
- Udržujte antivirový systém aktualizovaný (databázi i program)
- Mějte v antivirovém systému zapnutou rezidentní ochranu
- Každý neznámý disk (flashka, externí HDD…), který vkládáte do svého počítace, nejprve otestujte

  antivirovým programem.
- Nepouštějte ke svému počítači nedůvěryhodnou cizí osobu
- Pravidelně zálohujte svá data. Pokud totiž vir zlikviduje celý disk, nic až tak vážného
- se nestane, jestliže máte důležitá data zálohována.
- Buďte obezřetní. Většina viru se nějak projevuje. Ať je to delším zavaděním systému,
- podezřelým padáním programu, nebo jiným „neobvyklým“ chováním.
- Soubory stažené z internetu před spuštěním zkontrolujte antivirovým programem.
- Podezřelou či nevyžádanou e-mailovou poštu ani neotevírejte a ihned
- mažte.
- Otevřete-li e-mail a zjistíte, že obsahuje soubor, který by tam být nemel nebo má
- „divný“ název či koncovku, zavřete tento e-mail a smažte jej.

Hlavně tedy…

- používat šedou kuru mozkovou
- používat antiviry, antispyware, anti…..,
- používat alternativní prohlížeče, OS
- nechodit na stránky s podezřelým obsahem (nelegální SW, pornografie, cracky, ...)
- být přiměřeně paranoidní

Cože je ta rezidentní ochrana?

- **Rezidentní ochrana** je většinou součástí antivirového programu, nepřetržitě kontroluje a vyhodnocuje provoz počítače a chrání jej tak v reálném čase před průnikem počítačových virů a dalšího malwaru.

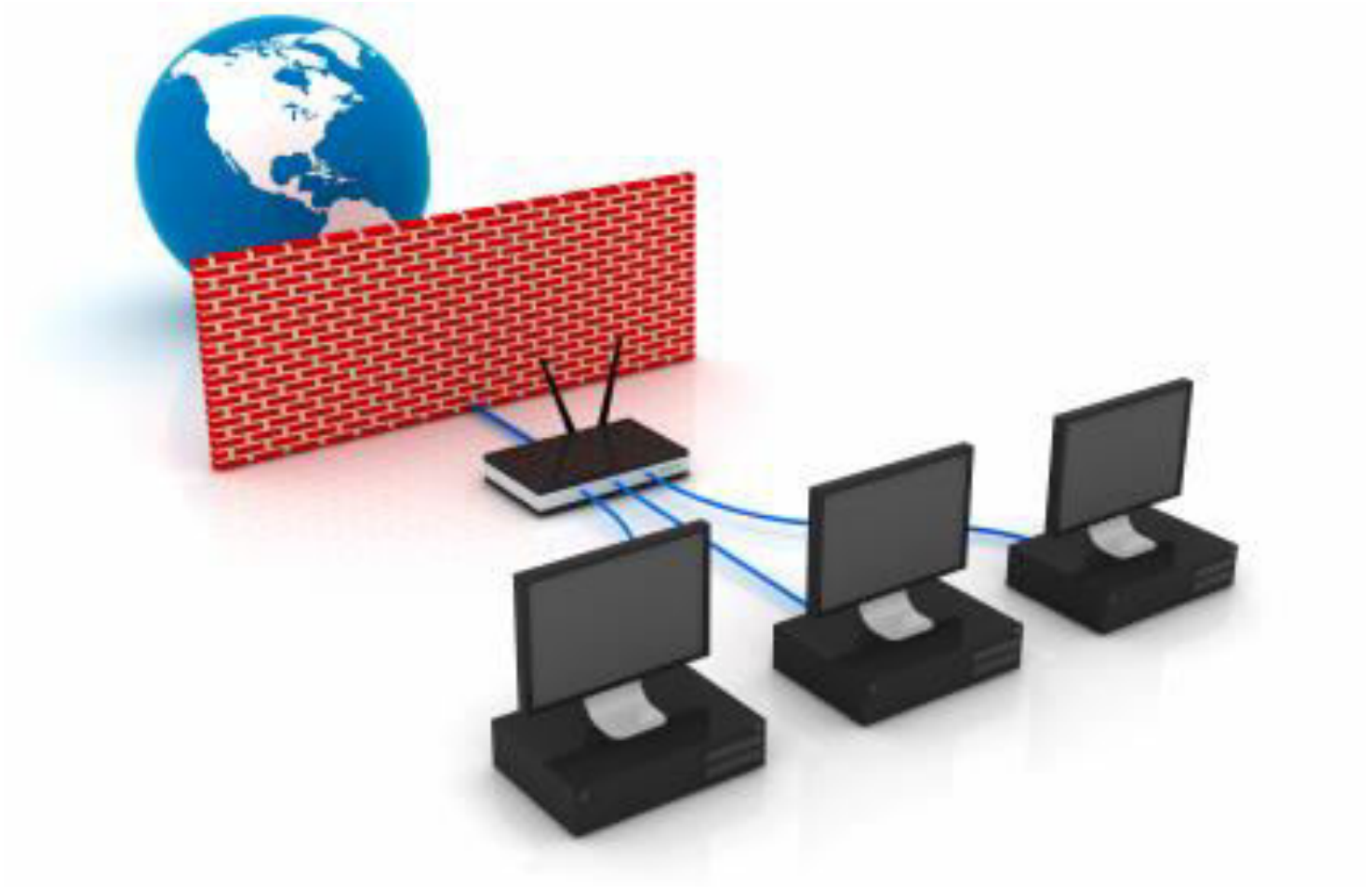
- Rezidentní ochrana antivirového programu se někdy také označuje jako rezidentní štít. Rezidentní ochranou se rozumí funkce antivirového programu, která neustále na pozadí systémových úloh kontroluje a monitoruje všechny spouštěné soubory a složky systému.

- Rezidentní ochrana je často posledním i prvním místem, jak lze odhalit virus před jeho spuštěním v operační paměti, při kterém obvykle dochází k poškození počítače a dalšímu šíření viru.

A co je to firewall?

- **Firewall** je virtuální nástroj oddělující provoz mezi sítí (internetem) a počítačem, tak že propouští jedním nebo druhým směrem informace podle předem definovaných pravidel. Brání tak zejména před neoprávněným vniknutím do sítě a odesílání dat bez vědomí a souhlasu uživatele či oprávněné osoby. Ve virtuálním prostředí domácností i firem je instalace brány firewall nejefektivnějším a nejdůležitějším krokem při ochraně a zabezpečení počítače.

- Firewall definuje pravidla, podle kterých může probíhat komunikace mezi počítači či sítěmi, resp. povolí se podmínky a služby, které jsou nutné pro provoz a ostatní jsou zakázány. Firewall nepřetržitě kontroluje dění v domácí či firemní síti a podrobně jej monitoruje. Informuje i o legálních procesech, vzniklých použitím některých aplikací a dovolí tuto činnost povolit či zablokovat.



A jak teda funguje Antivir?

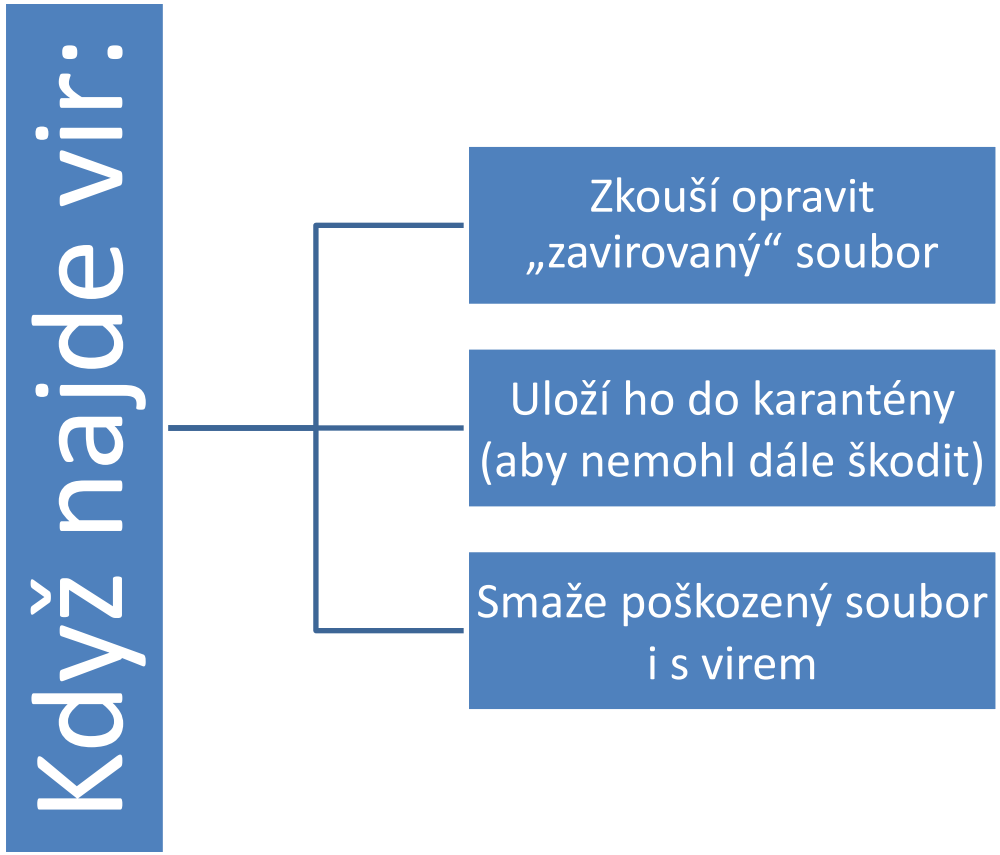
- Antivirový program má několik možností, jak malware najít
- 1) Každý vir má nějakou podezřelou sekvenci počítačového kódu a antivir manuálně projde každý soubor na disku a infikované soubory hledá. Je to velice obtížná procedura hlavně u virů, které program nezná je těžké odlišit kód viru od běžného kódu

A jak teda funguje Antivir?

- 2) **Heuristickou analýzou** – antivor bezpečně emuluje různé funkce PC (předstírá) a zaznamenává jak na to programy zareagují. Na základně toho jak program (nebo vir) zareaguje určí, zda je bezpečný nebo ne.

A jak teda funguje Antivir?

- 3) **Kontrola integrity** - Antivirový program s testem integrity hlídá změny v systému, adresářích a systémových oblastech disku a na základe změn detekuje vir. Tato metoda je velmi spolehlivá, ale neumí zjistit konkrétní vir, pouze změnu v systému.
- Každá technika má své silné a slabé stránky. Antivirové programy proto většinou používají kombinaci technik a tím zvyšují svou účinnost.


Když najde vir:
Zkouší opravit „zavirovaný“ soubor
Uloží ho do karantény (aby nemohl dále škodit)
Smaže poškozený soubor i s virem

A Antispyware?

- **Antispyware** program je druh bezpečnostního softwaru jehož pomocí lze zabezpečit PC proti spyware hrozbám. Jelikož spyware pracuje na jiném principu a je tvořen za odlišným účelem než-li klasické **počítačové viry** je jeho přítomnost v PC zpravidla neodhalitelná klasickou antivirovou ochranou. Proto existuje mnoho specifických antispyware programů, jejíchž účelem je tyto aplikace vyhledávat a chránit počítač před jejich negativním dopadem.

- Program na ochranu proti spyware dokáže vyhledat a následně i mazat nevyžádané aplikace, které se již nalézají v operačním systému, ale také je i blokovat v reálném čase. Antispyware software však nezaručuje dokonalou ochranu dat v počítači a ochranu proti malware aplikacím. Pro komplexnější bezpečnost dat a ochranu proti virům je proto nutné využívat i antivirových ochran.

Známé antiviry

- AVAST! Antivirus 
- Avira Antivirus
- AVG Antivirus 
- Ad-aware
- ESET 
- Kaspersky, 
- Microsoft Security Essentials,
- McAfee Antivirus 
- Norton Antivirus

Zdroje

- http://www.ceskatelevize.cz/ivysilani/10121359557-port/208572241900033/obsah/70350-pocitacove-viry-a-jina-havet/
- Dosedla, Architektura počítačů
- http://pc-security.cz/