Antivírová a antispamová ochrana

Vírus

- program alebo kód, ktorý sa dokáže sám šíriť bez vedomia používateľa
- aby sa mohol rozmnožovať, vkladá kópie svojho kódu do iných spustiteľných súborov alebo dokumentov, ktoré sa tak stávajú prostriedkom na aktiváciu ďalšieho vírusu
- pamäťové médium, internet

História

- Brain (1986)
- označoval sektory disku za chybné, spomalenie pc
- bratia Basit a Amjad Farooq Alvi z Pakistanu
- vírus bránil nelegálnemu šíreniu medicínskeho programu

Rozdelenie

- vírus – spustiteľné súbory na pevnom disku
  Obťažujúci, Deštrukčný, Ostatné

- trojan – obecný pojem. Program ktorý sa vydáva za iný – neškodný

- backdoor – škodlivý kód, ktorý umožňuje prevziať vzdialene kontrolu nad takto infikovaným pc

- downloader – škodlivý kód, ktorý z Internetu sťahuje ďalšiu háveď

- dropper – škodlivý kód, ktorý prenáša ďalšiu škodlivú háveď a túto po spustení vypusti do PC
- worm, červ
- adware – aplikácia, ktorá má obvykle za následok to, že vyskakujú reklamné okna
- spyware – špionážny software

- ransomware – je typ škodlivého softvéru, ktorý zablokuje počítačový systém alebo šifruje zapísané dáta, a potom požaduje od obete výkupné za obnovenie prístupu.

Antivírusový program

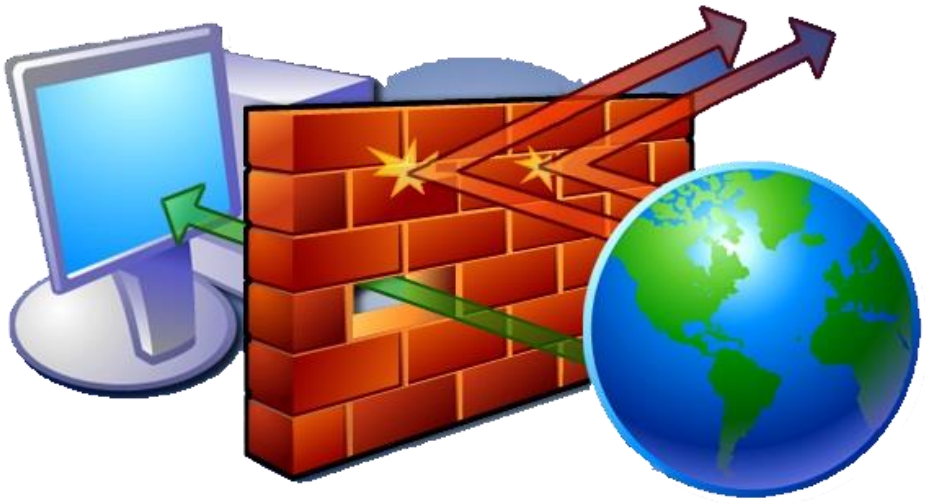
- je program, ktorého cieľom je identifikovať a eliminovať počítačové vírusy
- História antivírusov sa začala písať spolu so vznikom prvých počítačových vírusov. Spočiatku šlo najmä o antivírusy jednoúčelové, ktoré sa sústredili len na jeden konkrétny vírus
- r. 1988 vznikol prvý antivírusový systém, schopný ničiť viacero vírusov

- Jednoúčelové antivírusy – Sú to antivírusové programy, ktoré sa zameriavajú na detekciu, príp. aj dezinfekciu jedného konkrétneho vírusu

- Antivírusové systémy – Najčastejšia forma antivírusových programov. Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupné miesta, ktorými by sa prípadná infiltrácia mohla do počítačového systému dostať (e-mail, www, ...)

  Samozrejmosťou býva aj aktualizácia

- Komplexné antivírusové riešenia ("balíky") – Obvykle sú to balenia niekoľkých produktov od rovnakého výrobcu, ktoré sú určené pre podnikové siete. Často sa v balení vyskytuje:
  - Antivírusový systém pre stanice
  - Antivírus pre poštové servery – antispam
  - Antivírus pre súborové servery
  - Firewall
  - Antispyware



Súčasti antivíru

- nepretržitá kontrola
- test na vybrané oblasti
- zaisťuje sťahovanie aktualizácií z internetu
- automatická kontrola prijatej a odoslanej elektronickej pošty
- plánovač akcií (scheduler)
- karanténa (quarantine)
- monitorovací program


VIPRE
TREND MICRO
pctools
McAfee
KASPERSKY lab
ca
eset
AVG
G DATA
PANDA
AhnLab
avast!
Norton
from symantec
F-Secure
Microsoft
Security Essentials
webroot
Quick Heal
bitdefender
Windows Defender
Avira

Ochrana

- 100% ochrana proti vírom neexistuje
- rozumné chovanie

  najbezpečnejšie weby sú z USA, EU, Austrálie

  najnebezpečnejšie sú z Ázie, Južnej Ameriky, Afriky a cca 70% webových stránok z Ruska
- lokálne nainštalovaný a pravidelne aktualizovaný antivírový program
- pravidelná aktualizácia OS

Ďakujem za pozornosť