Riziká - Antivírusový softvér (antivírus) a jeho typy, antivírusové techniky :)

Program, ktorého cieľom je identifikovať a eliminovať počítačové vírusy.

Typy antivírusových programov:

- **Jednoúčelové antivírusy** - antivírusové programy, ktoré sa zameriavajú na detekciu, príp. aj dezinfekciu jedného konkrétneho vírusu. Nedajú sa použiť ako plnohodnotná antivírusová ochrana. Používajú sa len ak vieme, že máme v počítači konkrétny vírus. Na rozdiel od plnohodnotného antivírusového systému ponúkajú dôkladnejšiu dezinfekciu a ďaleko väčšiu rýchlosť. Väčšinou vznikajú len na detekciu/dezinfekciu hojne sa vyskytujúcich vírusov.
- **Balík jednoúčelových antivírusov -** ide o obdobu jednoúčelového antivíru, s tým rozdielom, že tento druh antivírusu dokáže nájsť a odstrániť väčšie množstvo obvykle hojne sa vyskytujúcich vírusov.
- **Komplexné 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, média - CD-ROM, DVD, Flash...). Samozrejmosťou býva aj aktualizácia prostredníctvom internetu.

Všeobecné antivírusové techniky:

- **Porovnávací test** - antivírusový program si po inštalácii vytvorí databázu informácií o súboroch uložených na diskoch počítača. Potom porovnáva napríklad veľkosť spustiteľného súboru s údajom naposledy zapísaným do databázy. Pri zmene veľkosti spustiteľného súboru antivírový program upozorní na možnosť vírusovej nákazy. Možno totiž predpokladať, že veľkosť spustiteľného súboru sa nemení. Táto metóda detekcie vírusov nevyvoláva toľko planých poplachov ako napríklad metóda heuristickej analýzy. Na druhej strane autor nového vírusu môže obísť problém databázy informácií o súboroch priamo úpravou zápisu v tejto databáze.
- **Heuristická analýza** - spôsob podrobnej analýzy obsahov súborov na pevnom disku spojenej s vyhľadávaním rôznych podozrivých častí kódu (priame zápisy na disk, prevzatie kontroly nad operačným systémom). Heuristická analýza je všeobecne fungujúca metóda, ktorá nie je závislá na vírusovej databáze. Automaticky sa pri tejto metóde vykonáva test aj na známe vírusy. Ak je niektorý súbor označený ako napadnutý, prehľadáva sa v databáze vírusov a meno vírusu je vypísané, v opačnom prípade je vírus označený ako neznámy. Ak antivírusový program obsahuje tzv. plnú heuristickú analýzu (heuristická analýza s emuláciou kódu), vtedy sa antivírový program priamo pokúša emulovať (schopnosť napodobniť jeden systém iným) činnosť počítača pri spustení programu. Touto metódou môže antivírový program nájsť a odhaliť úplne nový, neznámy vírus, ktorý nie je obsiahnutý v databáze antivírového programu, ktorý prehľadáva súbory metódou skenovania. Táto metóda odhaľovania vírusov môže označiť za nakazené neznámym vírusom aj tie súbory, ktoré sú v poriadku. Stačí, keď vnútorná štruktúra kódovania bude podobná kódovaniu vírusov alebo ich správaniu.
- **Skenovanie** - metóda založená na porovnávaní reťazcov kódov vírusov obsiahnutých v internej databáze antivírového programu s reťazcami v skenovaných súboroch. Ak narazí antivírový program na súbor, ktorý obsahuje kód vírusu zhodný s kódom v internej databáze, ohlási nájdenie vírusu a pomenuje ho menom priradeným kódu v databáze. Takýto spôsob ochrany je veľmi spoľahlivý, na druhej strane úroveň ochrany závisí na aktuálnosti vírusovej databázy. Ak ju užívateľ nebude pravidelne a často aktualizovať, program proti novým vírusom nemá najmenšiu šancu. Najväčšou výhodou tejto metódy je jej rýchlosť, táto metóda sa preto používa pre pravidelné kontrolovanie pevného disku.
- **Rezidentné sledovanie (Rezidentný štít** - pri štarte počítača sa do operačnej pamäte automaticky zavedie rezidentný antivírus, ktorý monitoruje činnosť počítača. V prípade neobvyklých operácií (zápis do systémových oblastí diskov, modifikácie spustiteľných súborov a pod.) antivírový program ihneď upozorní na túto neobvyklú činnosť a čaká na reakciu užívateľa. Táto metóda je využívaná od doby, keď sú počítače dostatočne výkonné a majú dostatočnú operačnú pamäť, takže rezidentný antivírus systém prakticky nezaťažuje.

Zdroje

Prevzaté a upravené z:

Ján Skalka, Cyril Klimeš, Gabriela Lovászová, Peter Švec, *Informatika na maturity a prijímacie skúšky*, Enigma, Nitra 2007, ISBN 978-80-89132-50-8.