Riziká - Počítačové vírusy, vírus, makrovírus a červ, spyware, keylogger, rootkit :)

Programy, ktoré niekto vytvoril, aby získal dôverné dáta z vášho počítača (napr. heslá), získal kontrolu nad vašim počítačom (alebo aspoň dokázal využívať jeho zdroje), prípadne zničil vašu prácu.



Vírus

Malý program, ktorý sa dokáže vložiť do iného programu a spolu s ním sa šíriť. Spustením programu teda spúšťate nevedomky aj vírus, ktorý napadne ďalšie programy.

Makrovírus

Vírus, ktorý nie je súčasťou programu, ale dokumentu, ktorý môže obsahovať makrá, ktoré predstavujú v dokumente vložené programové kódy.

Červ

Má vlastný súbor a väčšinou sa snaží presvedčiť užívateľa počítača, aby ho spustil, prípadne využíva bezpečnostnú chybu (poštového programu, prehliadača webových stránok) a snaží sa spustiť sám. Niektoré internetové červy využívajú chyby v zabezpečení sieťového prepojenia operačného systému a šíria sa priamo v paketoch sieťového protokolu. Sú veľmi nebezpečné, pretože ich nezachytí antivírový program a tiež nevyžadujú k napadnutiu počítača aktivitu používateľa (len jeho pasivitu, t.j. nenainštalovanie bezpečnostnej záplaty vydanej tvorcami systému).

Spyware

Program, ktorý zbiera informácie o užívateľovi a jeho aktivitách bez jeho vedomia, t.j. bez jeho súhlasu, a tie následne odosiela napríklad rôznym marketingovým oddeleniam[1].

Rootkit

Škodlivý kód, ktorý beží v jadre operačného systému s právami administrátora počítača. Preto sa zle detekuje a odstraňuje. Ide o zložitý a nebezpečný program, ktorý umožňuje jeho autorovi získať kompletnú kontrolu nad vašim zariadením bez toho, aby ste si to vôbec všimli.

[1] Najnebezpečnejší druhom spyware sú keyloggery, ktoré zaznamenávajú všetky stlačenia kláves a tak dokážu získať napr. prístupové heslá do počítačového systému, čísla kreditných kariet, registračné kľúče. V ojedinelých prípadoch sledujú aj kliknutia myšou či nahrávajú videá činnosti užívateľa.

Copyright © 2013 - 2026 Encyklopédia poznania