Počítačové viry, antiviry

1. Počítačové viry

Počítačový vir je malý program (kus programového kódu), který se samovolně šíří bez vědomí uživatele.

1. Charakteristika viru

- Vir může za určitých podmínek vytvářet své „kopie“, připojené k jiným nosičům, které se mohou znovu „kopírovat“ a množit. Kopie jsou vytvářeny bez vědomého zásahu uživatele.

- „Kopie“ viru nemusí být shodná se svým originálem (o to je horší vir rozpoznat a odchytit). Zpravidla však vykonává stejné funkce jako originál.

- Pro část virů je typická škodlivá činnost, která se liší od běžných programů (formátování disk, záměrné provádění náhodné změny dat na disku apod.).

- Viry zpravidla využívají řady technik, které znesnadňují jejich odhalení, následnou analýzu a likvidaci.

2. Jak poznáme, že je počítač napaden

To, že je v počítači virus, poznáme zpravidla až na základě jeho projevů, pokud to není oznámeno antivirovým programem.

Důsledky napadení virem jsou většinou následující :

- Zpomalení načtení programu do paměti. Před provedením programu dojde nejprve ke spuštění viru a teprve po skončení své činnosti předá virus řízení programu, který jste původně spustili. Jiným důvodem zpomalení může být i přímé působení viru, který právě provádí svoji škodlivou činnost. U výkonných počítačů však toto zpomalení nemusíte postřehnout.

- Snížení výkonu počítače (důvodem může být souběžně prováděná činnost viru nebo jde o záměrné zpomalení systému jako součást škodlivé činnosti viru).

- Ubývání volného prostoru na disku – příčinou tohoto jevu mohou být například souborové viry, které prodlužují soubory, nebo vytvářejí soubory nové.

- Úbytek systémové paměti RAM – důvodem je výskyt rezidentních virů v paměti. Projevuje se hlášením o nedostatku paměti při spouštění programů. Jestliže vám program šel dříve spustit a mezitím jste nezměnili nastavení rezidentních programů, pak může jít o napadení virem.

- Poruchy programů – program, který dříve pracoval, nyní nemůžete spustit nebo již není plně funkční.

- Nečekaná hlášení na obrazovce a další speciální projevy. Mnozí tvůrci virů cítí potřebu dát najevo přítomnost viru.To napomáhá odhalení a identifikaci viru. Jsou však aktivovány se zpožděním, aby se virus stihl rozšířit. Patří sem různé výpisy zpráv na obrazovku, grafické „žertovné“ projevy (houkající sanitka přejíždějící přes monitor, padání písmenek) i akustické projevy v podobě melodií.

3. Jaké škody může virus způsobit

3.1 - Přímé škody

- Náklady související s odstraněním viru
- Náklady na kontrolu, opravu nebo obnovení poškozených dat z archivních kopií.
- Náklady na opětovnou instalaci poškozených programů.
- Náklady na znovuvytvoření poškozených nezálohovaných dat.
- Peněžní či materiální ztráty vzniklé v důsledku výpadku výroby nebo prodeje.
- Následky havárie (např. v chemické továrně, kde počítače řídí technologický proces).
- Poškození zdraví v důsledku používání poškozeného programu (diagnostické nebo léčebné programy ve zdravotnictví).

3.2 - Nepřímé škody

- Náklady na nákup a provoz antivirového softwaru a hardwaru.
- Náklady na provádění organizačních opatření proti šíření virů.
- Náklady z omezení provozu dané opatřeními v antivirové ochraně

4. Jak se virus dostane do počítače

- Vnější pamětí: nejčastějším způsobem napadení počítače je disketa, popřípadě CD. V dnešních dobách již skoro nevyužívaná metoda
- Intra/Internetem: viry se přenášejí lokální nebo globální počítačovou sítí za použití různých protokolů, zejména přes e-maily, web, … .

5. Jak se proti nim bránit

- Neotvírat pochybné či nápadně vypadající e-maily, při brouzdání Internetem používat bezpečný internetový browser.
- Používat kvalitní antivirový program

2. Antiviry

Antivirové programy (antiviry) jsou programy vytvořené pro vyhledávání a ničení počítačových virů. Nutností pro správné fungování je vždy aktuální virová databáze, díky které program ví, co je a není virem, následně tím ho může včas detekovat a zamezit jeho dalšímu působení.
Většina antivirových programů obsahuje obnovu napadených souborů. Dříve byl antivirový program určen pouze k jednomu účelu, vyhledat a zničit veškeré viry v počítači. V pozdějších dobách se krom virů zaměřily také na trojské koně a červy.

Moderní antivirové programy mají rezidentní ochranu (umístěna v RAM, kterou také sleduje), standartní štít, webový a e-mailový štít, siťový štít. Veškerá konfigurace záleží na tom, jaký antivirový program používáme. Mezi antivirové programy patří například český Avast,AVG a mezi zahraniční F-Secure, Norton Antivirus, Kaspersky Antivir, ...