**Počítačový vírus** v oblasti počítačovej bezpečnosti označuje 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. (Pri jednoduchších vírusoch dochádza ku kopírovaniu jeho samotného viackrát na disk poprípade premenovanie kópií.) Takýto program sa teda chová podobne ako biologický vírus, ktorý sa šíri vkladaním svojho genetického kódu do živých buniek. Analogicky sa proces šírenia vírusu nazýva *infekcia* a napadnutému súboru sa hovorí *hostiteľ*. Vírusy sa rozširujú v rámci jedného počítača, ale i medzi viacerými počítačmi. Existuje viacero spôsobov, ako sa môžu počítače infikovať cez rôzne médiá ako je disketa, CD, sieťové linky, výmenné pevné disky, ale najmä cez internet. Vplyv vírusu je ľahko badateľný na spomalení a nestabilite systému, časté je poškodenie dokumentov, zmena veľkosti alebo obsahu súborov, úbytok kapacity pevného disku. Vírusy sú iba jedným z druhov zákerného softvéru tzv. malware. Vo všeobecnosti sa ako vírusy označujú napríklad aj počítačové červy a iné druhy malware. Zatiaľ čo niektoré vírusy môžu byť cielene ničivé (napr. mazať súbory na disku), mnoho iných vírusov je relatívne neškodných, poprípade iba obťažujúcich. Pri niektorých vírusoch sa ničivý kód spúšťa až s oneskorením (napr. v určitý deň či po nakazení určitého počtu iných hostiteľov), čo sa niekedy označuje ako *logická bomba*. Ďalší negatívny vplyv vírusov je ich samotná reprodukcia, ktorá zaťažuje počítačové systémy a obsadzuje ich zdroje.

**Delenie počítačových vírusov**

* podľa umiestnenia v pamäti:

1. *rezidentné* (po infikovaní ostávajú v operačnej pamäti)
2. *nerezidentné*

* podľa cieľa infekcie:

1. *bootovacie*
2. *súborové*
3. *clustrové*

* podľa spôsobu infekcie:

1. *predlžujúce*
2. *prepisujúce*
3. *adresárové*
4. *kombinované*

* podľa deštrukcie:

1. *deštruktívne* (prepisujú náhodne vybraté sektory a formátujú pevný disk)
2. *nedeštruktívne* (ich aktivita sa prejavuje vizuálne (zobrazovanie textových správ))

* podľa správania:

1. *stealth* (schovávajú sa a kódujú)
2. *polymorfné* (menia svoj kód a ním sa ďalej rozširujú)
3. *tunelujúce* (oklamú bezpečnostné prvky BIOSu (Výrobca BIOSu ukončil softvérovú podporu v roku 2007 a v súčasnosti budú hovoriť o témach "Windows 8 bez BIOS".) a získajú tak kontrolu nad hardvérom.)

**Činnosť vírusu**

1. Prevzatie kontroly nad procesorom
2. Riadenie stavu prostredia
3. Inštalácia do pamäte
4. Testovanie na spustenie škody
5. Záškodnícka činnosť
6. Vytvorenie svojej kópie na nájdenom mieste
7. Zakódovanie

V súčasnosti (2014) sú klasické počítačové vírusy na istom ústupe oproti červom a spyware, ktoré sa šíria prostredníctvom počítačových sietí, najmä internetu. Niektoré antivírusové programy, ako aj iné špecializované programy sa preto snažia chrániť počítač aj pred inými, nevírusovými hrozbami.

**Antivírus**, alebo **antivírusový softvér** je počítačový program, ktorého cieľom je identifikovať a eliminovať počítačové vírusy.

Ďalšie spôsoby ochrany: -Firewall

-Heslo

-WPS pin

