## Kriminalita

1. ***útok na počítač, program, údaje, komunikačné zariadenie:*** fyzické útoky na zariadenie výpočtovej techniky, magnetické médiá, vedenie počítačovej siete alebo elektrického rozvodu a pod., vymazanie alebo pozmenenie dát, formátovanie pamäťových médií nesúcich dáta, pôsobenie počítačových infiltrácií, nelegálna tvorba a rozširovanie kópií programov, získanie kópie hospodárskych dát, databáz zákazníkov, v štátnych orgánoch únik informácií o občanoch a pod. Z hľadiska rozsahu najväčších škôd pravdepodobne najväčší podiel patrí nelegálnej tvorbe a predaju autorsky chráneného programového vybavenia v počítačovom slangu označovaná ako [Warez](http://sk.wikipedia.org/wiki/Warez%22%20%5Co%20%22Warez).

***\*Vírusy, warez –*** použitie bez autorských práv

1. ***neoprávnené užívanie počítača alebo komunikačného zariadenia:*** využívanie počítačovej techniky, faxov, prostriedkov počítačových sietí, databáz a programov zamestnancami firiem a organizácií na vlastnú zárobkovú činnosť.

***\*Školské počítače na môj zárobok***

1. ***neoprávnený prístup k údajom, získanie utajovaných informácií (počítačová špionáž) alebo iných informácií o osobách, činnosti a pod.:*** prenikanie do bankových systémov, systémov národnej obrany, do počítačových sietí dôležitých inštitúcií a pod. Niekedy táto činnosť spôsobuje priame škody veľkého rozsahu, napr. nelegálne bankové operácie, ako aj nepriame škody spôsobené únikom informácií. V súvislosti s týmto trestným činom môže byť aj súbežný trestný čin ako napr. vydieranie, nekalá súťaž, ohrozenie hospodárskeho tajomstva, vyzvedačstvo, ohrozenie štátneho tajomstva.

***\*špionáž, ohrozenie štátneho tajomstva, únik informácií***

1. ***krádež počítača, programu, údajov, komunikačného zariadenia***

**\*Krádež údajov**

1. ***zmena v programoch a údajoch (okrajovo i v technickom zapojení počítača resp. komunikačného zariadenia):*** zmena programov a údajov inými programami alebo priamymi zásahmi programátora, úprava v zapojení alebo inom atribúte technického vybavenia počítača.

***\*hacker –*** zásah programátora

1. ***zneužívanie počítačových prostriedkov k páchaniu inej trestnej činnosti:*** manipulácia s údajmi ako napr. zostavy v skladoch, tržby, nemocenské poistenie, stavy pracovníkov, stav účtov a pod., patria sem aj krádeže motorových vozidiel, falšovanie technickej dokumentácie, priekupníctvo, daňové podvody, falšovanie a pozmeňovanie cenín, úradných listín a dokladov, dokonca aj peňazí.

***\*krádež mot.* vozidiel, falšovanie dokumentácie, daňové podvody, falšovanie**

1. ***podvody páchané v súvislosti s výpočtovou technikou:*** využitie niečieho omylu vo svoj prospech (hry s vkladom finančnej čiastky a rozosielaním listov “následníkom” so sľubom zaručeného zisku). Tento druh trestnej činnosti možno vykonávať aj bez použitia výpočtovej techniky, ale s jej použitím je táto činnosť efektívnejšia.

***\*pyramídové hry, ťaženie z cudzieho omylu***

1. ***šírenie poplašných správ:*** vytvorenie poplašnej správy upozorňujúcej na fiktívne nebezpečenstvo. Najčastejším motívom páchateľov tejto trestnej činnosti je pobaviť sa na nevedomosti ostatných, no môže ísť i o správy spojené s páchaním inej trestnej činnosti. Tieto správy sú v počítačovom slangu označovaná ako [Hoax](http://sk.wikipedia.org/wiki/Hoax%22%20%5Co%20%22Hoax).

***\*Hoax, pobavenie, iná trestná činnosť***

## Warez

* **aplikácie** – aplikácie: vo všeobecnosti maloobchodné verzie softvérových balíkov
* **cracky** – cracky: záplaty určené na pozmenenie skúšobnej verzie programov na plné alebo na obídenie protipirátskej ochrany
* **keys/key generators (skrátene keygens)** - inštalačné a registračné kľúče: kľúče k inštalačným programom alebo ich generátory, ktoré umožňujú nelegálne nainštalovať program alebo odstránia obmedzenia skúšobnej verzie programu
* **games** – počítačové hry: počítačové hry a hry pre hracie konzoly
* **movies** – filmy: pirátske filmy
* **music/mp3** – hudba: pirátske albumy, single alebo iné hudobné formáty distribuované vo forme hudobného formátu MP3
* **E-Books/Tutorialy** – knihy: do tejto kategórie spadajú pirátske eknihy, naskenované knihy a návody k programom.

## Detekcia vírusov

**Konkrétne antivírové techniky** vyhľadávajú iba známe vírusy podľa vírusovej databázy, ktorú je nutné aktualizovať. Väčšinu takto nájdených vírusov je možné zo súborov alebo z boot sektorov tiež odstrániť, a to buď s použitím informácií o víruse, ktorý príslušný súbor infikoval, alebo s použitím pôvodných informácií o súbore, ktoré popisujú, ako vyzeral pred infekciou. Najväčšou výhodou tejto metódy je jej rýchlosť, táto metóda sa teda používa pre pravidelné kontrolovanie pevného disku. Známe vírusy je tiež možné vyhľadávať v každom spúšťanom, kopírovanom, otváranom súboru a v zavádzacích sektoroch všetkých diskiet, ktoré do počítača vkladáme. K tomu je určený rezidentný ovládač, ktorý možno zavádzať vždy po spustení počítača. Tento ovládač sa zavádza v config.sys a je teda v pamäti ešte skôr, než sa načíta command.com (čo je obvyklá základňa väčšiny vírusov). Samozrejme nechýba možnosť prehľadať pamäť? na prítomnosť rezidentných vírusov.

**\*Pravidelná kontrola, vyhľadávanie známych vírusov, podľa databázy**

**Všeobecné antivírové techniky** sa snažia nájsť a pokiaľ je to možné i odstrániť neznámy vírus. Prvou metódou, ako nájsť neznámy vírus je tzv porovnávací test. Pri prvom spustení tohto testu si program zapíše dôležité informácie o súboroch (veľkosť, dátum, čas, atribúty a kontrolné súčty). Pri ďalších spusteniach porovnáva tieto informácie s aktuálnym stavom. Pokiaľ v týchto údajoch došlo k zmene väčšieho rozsahu, je pravdepodobné, že počítač bol napadnutý vírusom. Antivírusový program AVG obsahuje i heuristickú analýzu. Heuristická analýza je všeobecne fungujúca metóda, nie je teda závislá na vírusovej databáze. Automaticky sa pri tejto metóde robí test i na známe vírusy. Pokiaľ je teda súbor označený za napadnutý, prehľadáva sa v databáze vírusov a meno vírusu je vypísané, v opačnom prípade je vírus označený ako neznámy. Program obsahuje tzv plnú heuristickú analýzu (heuristická analýza s emuláciou kódu), kedy sa antivírový program priamo pokúša emulovať činnosť počítača pri spustení programu. Nevýhoda metódy je v tom, že často dochádza k falošným poplachom, kedy niektoré súbory sú označované ako napadnuté. Avšak vzhľadom k zväčšovaniu počtu stále zložitejších vírusov, bude v budúcnosti táto metóda najčastejšie používaná.

**\*Heuristická analýza, porovnávanie stavu súborov a detekcia neznámych vírusov.**

Test prostredia na súborové vírusy (**bezpečnostná ochrana**) spočíva v tom, že program vygeneruje na disk súbory typu .com a .exe, potom ich kopíruje a prevádza s nimi rôzne operácie, pričom vždy kontroluje ich obsah. Ak sa pri manipulácii s nimi zmení ich obsah, je veľmi pravdepodobné, že sa na návnadu práve chytil vírus. Obdobne je program schopný vygenerovať na disketu prázdny zavádzací sektor a potom kontrolovať, ak bol nejako zmenený. Preventívne antivírové techniky sa odporučí využívať pokiaľ možno ešte predtým, než sa vírus v počítači usídli. Spočívajú v zálohovaní niektorých dôležitých informáciách o počítači, podľa ktorých bude v prípade potreby možné obnoviť pôvodný stav. Pomocou programu si môžeme uložiť obsah pamäti CMOS, tabuľku rozdelenia pevného disku apod Po napadnutí počítača možno tieto informácie spätne obnoviť.

**\*.com a .exe súbory, testuje, ak sa zmenia „chytilo na návnadu“ vírus, zálohuje a obnoví**

## Delenie vírusov

**1. Deštruktívne vírusy**- najčastejšie **formátujú** pevný disk, **prepisujú** náhodne vybrané sektory
(náhodnými dátami, menia obsah súborov, mažú súbory, zašifrujú dáta, atď.).
**2. Nedeštruktívne** - **vizuálne prejavy**, zobrazovanie rôznych textových správ, (grafické prejavy nie sú časté)  - akustických prejavov
Každý z prejavov je vyvolaný podmienkou, čo väčšinou býva konkrétny časový moment, aktuálny dátum, prípadne vstup z klávesnice

**Delenie počítačových vírusov podľa umiestnenia v pamäti:**
1. **nerezidentné** - po spustení infikovaného programu sa **replikujú**, najčastejšie do súborov v danom adresári, a predajú riadenie infikovanému programu
2. **rezidentné** - **ostávajú v operačnej pamäti počítača aj po ukončení vykonávania infikovaného programu použitím mechanizmu TSR** (terminate and stay resident)

**Delenie podľa cieľa infekcie:**
1. **bootovacie** - infikujú partition table (tabuľku rozdelenia), alebo častejšie boot sector (zavádzací sektor), čím si zabezpečia **spustenie ešte pred zavedením samotného operačného systému**. Originálny boot sector (ktorý musí byť zachovaný pre korektné zavedenie operačného systému) ukladajú buď na niektorý voľný sektor na 0. stope pevného disku, alebo na ľubovoľný iný sektor z dátovej oblasti pevného disku, pričom ho označia za vadný, aby nedošlo k jeho prepísaniu.
2. **súborové** - je to najrozšírenejšia skupina vírov. Infikujú EXE, COM, OVL, BIN, STS, OBJ, DLL súbory a niekedy aj keď sú uložené v komprimovaných archíve.
Súborové sa ďalej delia podľa spôsobu infekcie na:
    a) **predlžujúce** - **pripoja sa** **na koniec súboru a na začiatok pridajú inštrukciu skoku na telo vírusu**.
    b) **prepisujúce** - **nenávratne prepíšu úvod súboru, ktorý sa potom ako program stáva nefunkčný**.
    c) **adresárové** - **na disku sú uložené len raz**, infikujú prepísaním odkazov priamo vo FAT tabuľke, pričom vzniká tzv. cross - referencing **(prekrývanie     súborov**), ktorý však zväčša **maskujú**.
    d) **multipartitné** - častá skupina vírusov - **infikujú boot sector a zároveň aj súbory.**