Informačná spoločnosť

1. Autorský zákon a licencie

Autorský zákon
- chráni vlastnícke práva autora na akýkoľvek produkt. Autorské práva sú predmetom dedičstva.

Autorské práva pre zdroje na webe.

- pre nekomerčné použitie (vlastnú potrebu !!!), je možné bezplatné sťahovanie – **Neplatí pre programy !!!**
- pri šírení zdrojov je nutný súhlas autora
- pri použití v **nekomerčnej** práci – uviesť ako citáciu resp. presnú URL adresu zdroja

    - **http://www.jaknainternet.cz/page/1191/autorska-prava/**
    - **http://www.zive.cz/clanky/myty-a-povery-rozplette-sit-autorskeho-zakona-ii/sc-3-a-146422/default.aspx**
    - **www.zive.cz**

- pri práci na PC sa používajú rôzne programy pričom každý z nich je chránený **autorským zákonom**. Autorský zákon určuje práva a povinnosti autora programu. Podľa autorského zákona je právom autora rozhodovať o tom ako sa bude jeho dielo používať alebo šíriť.
Pri kúpe programu (keďže program je nehmotný) sa predávajú licencie na použitie. **Licenčná zmluva** určuje podmienky za akých môžeme program používať. Ak tieto podmienky dodržiavame *vlastníme legálny software.*

Licenčná zmluva
Program môžeme inštalovať iba vtedy, ak súhlasíme so všetkými podmienkami zmluvy (najčastejšie potvrdzujeme súhlas v dialógovom okne)

- určuje na koľkých počítačoch môžeme program používať (licencia alebo multilicencia ?)
- určuje za akých podmienok (a či vôbec) môžeme program ďalej šíriť
- určuje čo smieme resp. nesmieme s programom robiť napr. meniť
- upozorňuje za čo preberá a za čo nepreberá zodpovednosť tvorca programu.

Licencie rozdeľujeme na komerčné a nekomerčné. Účelom komerčných licencií je zaviazať používateľa k tomu aby používal program len spôsobom, ktorý si zaplatil. Nekomerčnými licenciami chránia autori svoje programy proti plagiátorstvu a zneužitiu.

multilicencia – môže byť určená počtom alebo miestom
Školské (študenské) licencie – sú lacnejšie, ale zakazujú použiť program na komerčné účely

Druhy programov

Komerčný software
- programy vytvorené profesionálnymi firmami a musíme si ich zakúpiť
Firmware – programy priamo od výrobcu

- **„Krabicová licencia“ Retail** – najštandartnejší typ licencie, zakupujeme u predajcu SW. SW môže byť nainštalovaný na ľubovoľnom počítači pričom počet inštalácií je určený typom licencie.
- **OEM licencia –** špeciálny typ licencie, ktorá sa kupuje s novým PC. Štandardne je lacnejšia a je viazaná na licenčnú nálepku (ak sa nenalepí je licencia neplatná)
- **Licenčný program -** dohoda so zákazníkom napr. nižšia cena pri odbere väčšieho počtu licencií

Shareware
- programy použiteľné za určitých podmienok napr. manipulačný poplatok za nakopírovanie, obmedzená doba používania, menej funkcií a pod.(**TRIAL, DEMO, adware**, **beta verzie** ...)
Aby sa takýto program mohol používať komerčne je nutné si zakúpiť licenciu.

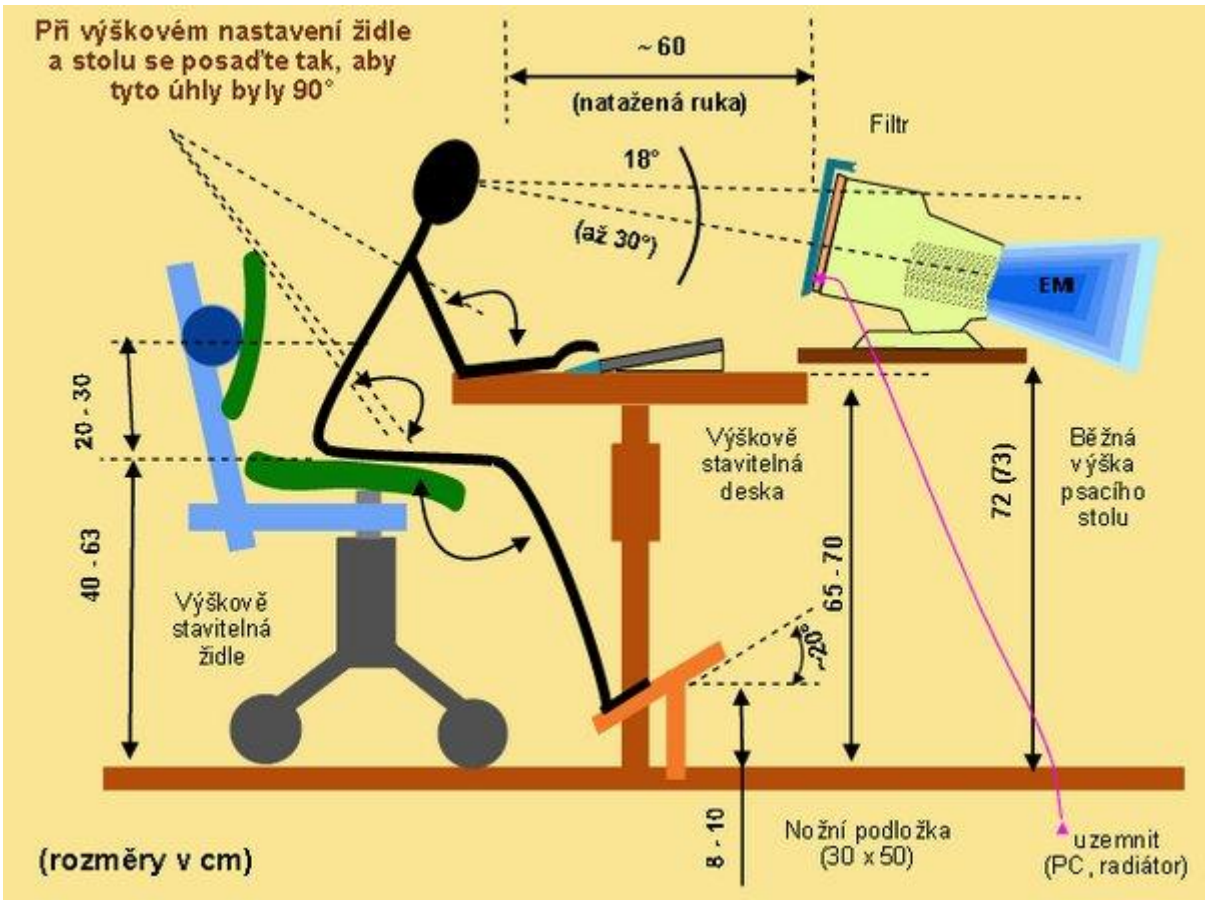
Freeware
- voľne šíriteľné programy, ktoré používateľ môže používať bez nároku na finančné vyrovnanie a autorské práva.

- **GNU/GPL –** nekomerčná licencia určená na ochranu SW. Autor dáva svoj program k dispozícií pričom môže vyžadovať odmenu (väčšinou dobrovoľnú resp. žiadnu). SW dáva k dispozícií spolu so zdrojovým kódom programu a ktokoľvek môže jeho program upraviť, ale musí ho dať k dispozícií ďalším používateľom spolu so zdrojovým kódom. Autor dáva možnosť s programom obchodovať. Predaný SW však musí byť ďalej šírený pod licenciou GNU/GPL. Vzhľadom k voľnému šíreniu kódov sa často používa aj **Open Source SW**
    - výhody open source – bezplatnosť, decentralizovaný vývoj, prístupné zdrojové kódy, môžeme modifikovať program (ak vieme ako), relatívne vysoká stabilita (len pri populárnom sw ako napr. Linux)
    - nevýhody: žiadna podpora (technická, servis výrobcu), náročnejšie konfigurácie zvládne len profesionál, nik negarantuje bezpečnosť programu, často nie je dostupná dokumentácia resp. len v elektronickej podobe.
- **Artistic licencie** – licencia určená na ochranu programov a programových komponentov, ktoré majú charakter umeleckého diela (napr. grafické pluginy do prehrávačov audia a grafické demá)
- **Public domain** – verejné resp. voľné dielo (CC-) – dielo, ktorého autorské práva nie sú chránené,

Doplnkové pojmy k téme:
adware – shareware, ktorý obsahuje reklamu
beta verzia – sw v skúšobnej verzii nemusí byť plne funkčný – je zverejnený a šírený na testovanie
upgrade – výmena výrobku za novšiu verziu
update – aktualizácia sw na úrovni opravy chýb
registrácia sw – zaslanie údajov používateľa jeho tvorcovi

2.Počítačová hygiena

- výpočtová technika má svoje špecifiká, ktoré je nutné zohľadniť pri jej umiestňovaní
- dlhodobá fyzicky jednotvárna činnosť ⇒ vhodné umiestnenie počítača (stôl, stolička, podložka po nohy a pod.)



<u>Technické zabezpečenie</u>

- monitor by mal byť mierne pod zorným uhlom
- nikdy neumiestňujeme monitor tak, aby bol za ním silný zdroj svetla alebo okno ⇒ vzniká tzv. fotografické videnie (oči sa prispôsobujú intenzite zdroja a slabo vnímajú obraz na monitore)
- klávesnicu umiestňujeme tak, aby sme mali predlaktia na stole
- základnú jednotku neumiestňovať priamo na podlahu ⇒ ventilátor nasáva rozvírený prach.
- rozmiestnenie počítačov v tvare U alebo L – je možné použiť aj umiestnenie v radoch (LCD monitory a rozvody v lištách)
- laboratórium by malo byť vybavené centrálnym vypínačom PC
- pri voľbe laboratórnych priestorov je potrebné vhodne určiť ich osvetlenie, úpravu (farebnú a akustickú) ako aj ich vhodnú polohu.

3.Riziká informačných technológií.

⇒ *zdravotné ťažkosti*

1. fyzické ťažkosti
   - zlé umiestnenia monitora, nevhodný pracovný priestor ⇒ problémy so zrakom, chrbticou a.pod
2. psychické ťažkosti
   - únik od reality, strata identity vo virtuálnom svete
   - závislosť od počítačových hier
   - celková psychická nepohoda – nervozita, podráždenosť, ...

⇒ *počítačová kriminalita*

Riešením sa zaoberá **počítačové právo.**

1. neoprávnené rozmnožovanie súborov a programov
   - kopírovanie SW – bez platných licencií
2. nedovolená modifikácia, poškodenie a získavanie údajov (súkromné informácie lekárske, policajné záznamy, etické problémy pri el. komunikácii a pod.)
   - hackerstvo
   - počítačové vírusy, spyware a pod.

Počítačová bezpečnosť

Bezpečnostná politika

- Určuje, čo môže užívateľ vykonávať, do akej miery a kto zodpovedá za dodržiavanie bezpečnostnej politiky.
- Koncepcia počítačovej bezpečnosti
  1. prevencia - ochrana pred hrozbami
  2. detekcia - odhalenie neoprávnenej činnosti a slabého miesta v systéme
  3. náprava - odstránenie slabého miesta v systéme

Ochrana zariadení

- prístup k zariadeniam len oprávnené osoby,
- zariadenia chránené heslom – slabé a silné heslo - min. 6 znakov, kombinované, z malých aj veľkých písmen, čísel a znakov
- biometrické snímače

Ochrana dát

- prístupové práva
- ochrana heslom,
- ochrana HW zariadením,
- zálohovanie,
- šifrovanie dát,
- antivírové, antispyverové programy a pod.
- aktualizácia SW
- zabezpečená komunikácia na sieti.

Mechanizmy na zabezpečenie komunikácie na sieti.

- **Šifrovanie dát**
  - ⇨ Symetrické
  - ⇨ Asymetrické– **certifikačná autorita (verejné kľúče)**
- **Jednosmerné funkcie (kryptovacie hašovacie funkcie)**
  Prevod vstupného reťazca dát na krátky výstupný reťazec. Pre rovnaký vstupný reťazec sa vytvára vždy rovnaký výstupný reťazec – využitie pri ukladaní hesiel
- **Kontrolný súčet** je menšie množstvo dát, ktoré vznikne ako výsledok operácie **hašovacej funkcie** na väčšom dátovom celku. Kontrolný súčet sa používa na overenie pravosti súboru, či nejde o podvrh.
- **Elektronický podpis** - je náhrada za klasický podpis. Elektronické podpisy využívajú metódy asymetrického šifrovania a hašovacích funkcií na jednoznačné podpísanie textu. Zabezpečuje autenticitu a integritu dokumentu (obsah nebol po podpise zmenený).

Ochrana programového vybavenia.

- vytvorenie nepoužiteľnej kópie pri pokuse o kopírovanie
- špeciálny spôsob zápisu distribučného média, ktorý nie je možné bežnými prostriedkami kopírovať
- technická ochrana : **HARDLOCK** (zámok) –špeciálna prídavná karta
  HARDKEY – zasúva sa do sériového, paralelného portu resp. USB

Dôveryhodnosť web lokalít

Dôvera vo webovú lokalitu čiastočne závisí od toho, kto je jej vydavateľom, aké informácie lokalita požaduje a čo od nej očakávate. Ak neviete, či sa dá webovej lokalite dôverovať, odpovedzte na tieto otázky:

- *Navštevujete zabezpečenú lokalitu?*

- Ak navštevujete webovú lokalitu so zabezpečeným pripojením, používa protokol HTTPS a v paneli s adresou sa zobrazuje ikona zámku .

- *Patrí webová lokalita spoločnosti alebo organizácii, ktorú dobre poznáte?*
- *Požaduje webová lokalita osobné informácie?*

- Osobné informácie, napríklad číslo kreditnej karty alebo bankové údaje, poskytnite iba v prípade, že je to opodstatnené. Vstupný formulár pre registračné údaje musí byť zabezpečený. (nezadávajte dôverné informácie, ak sa na paneli s adresou nezobrazuje ikona zámku).

- *Umožňuje maloobchodná webová lokalita telefonický alebo e-mailový kontakt s nejakou osobou?*

Poskytuje telefónne číslo, na ktoré môžete zatelefonovať v prípade problémov, alebo ktoré môžete použiť na zadanie objednávky? Poskytuje webová lokalita zoznam svojich poštových adries? Má zverejnenú politiku vrátenia tovaru s prijateľnými podmienkami? Ak webová lokalita neposkytuje telefónne číslo ani fyzickú adresu, skúste sa e-mailom spojiť so spoločnosťou a požiadajte o tieto informácie.

- *Ak lokalitu nepoznáte, máte k dispozícii ďalšie informácie, ktoré pomôžu pri rozhodovaní?*

- info od priateľov, informácie o lokalite y iných zdrojov (napr. noviny) a pod.

Webová lokalita nemusí byť dôveryhodná, ak:

- na ňu používateľa odkazuje e-mailová správa od neznámej osoby,
- ponúka problematický obsah, napríklad pornografiu alebo nelegálne materiály,
- ponúka niečo podozrivo výhodné, čo poukazuje na možný podvod alebo predaj nelegálnych či pirátskych produktov,
- láka používateľov pomocou nepoctivých predajných praktík, pri ktorých produkt alebo služba nezodpovedá očakávaniu,
- vyžaduje kreditnú kartu na účely overenia totožnosti alebo osobné údaje, ktoré nie sú nevyhnutné,
- vyžaduje poskytnutie čísla kreditnej karty bez dôkazu o zabezpečení transakcie.

Zdroj: (úplný článok) **http://windows.microsoft.com/sk-sk/windows-vista/when-to-trust-a-website**

Počítačová kriminalita

Počítačové pirátstvo - Neoprávnené nakladanie s počítačovými programami takým spôsobom, ktorý patrí len autorovi, alebo inému nositeľovi autorského práva.

Formy počítačového/softvéroveho pirátstva

- Neoprávnené používanie počítačových programov – nelegálne kópie, alebo nedodržiavanie licencie
- Neoprávnené šírenie počítačových programov
- Zneužívanie web zdrojov – hudba, film a pod.
- Neoprávnené šírenie OEM verzií
- Plagiátorstvo

Počítačová kriminalita -Termínom počítačová kriminalita sa označujú trestné činy zamerané proti počítačom ako aj trestné činy páchané pomocou počítača. Ide o nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky, alebo ich zmenu.

Druhy počítačovej kriminality

- útok na počítač, program, údaje, komunikačné zariadenie:

fyzické útoky na zariadenie, vymazanie alebo pozmenenie dát, pôsobenie počítačových infiltrácií, nelegálna tvorba a rozširovanie kópií programov, získanie kópie hospodárskych dát, databáz zákazníkov, 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.

- zmena v programoch a údajoch**:**

zmena programov a údajov inými programami alebo priamymi zásahmi programátora, úprava v zapojení alebo inom atribúte technického vybavenia počítača.

- zneužívanie počítačových prostriedkov k páchaniu inej trestnej činnosti:

Manipulácia s údajmi ako napríklad zostavy v skladoch, tržby, nemocenské poistenie, stavy pracovníkov, stav účtov a podobne. Patria sem aj krádeže motorových vozidiel, falšovanie technickej dokumentácie, priekupníctvo, daňové podvody, falšovanie a pozmeňovanie cenín, úradných listín a dokladov, dokonca aj peňazí.

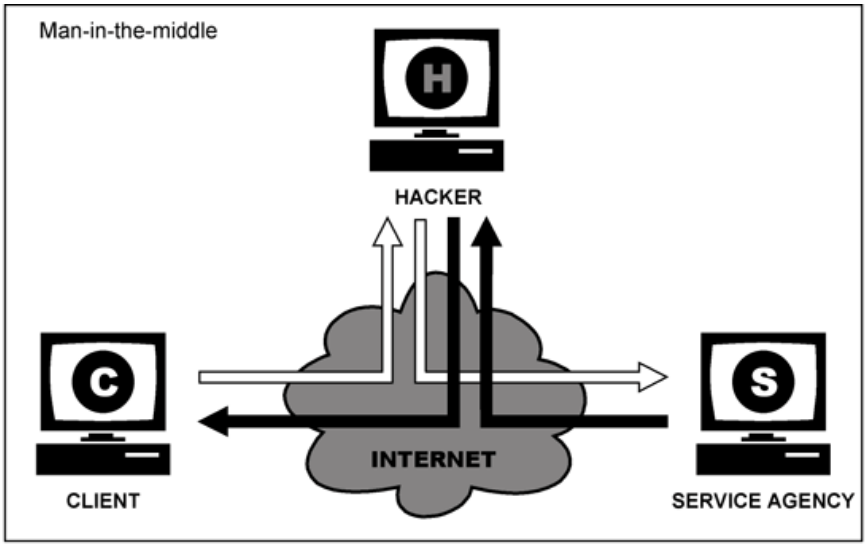
Sociálne inžinierstvo
Sociálne inžinierstvo je spôsob získavania dôverných informácií pomocou manipulácie. Využíva fakt, že človek je pravdepodobne najslabším článkom ochrany.
Metóda bežne používa telefóny alebo internet, pričom zneužíva dôverčivosť ľudí vydávaním sa za známe a existujúce spoločnosti či inštitúcie. Sociálne inžinierstvo môže prebiehať osobne, prostredníctvom komunikačného prostriedku (telefón, mail, ..) alebo prostredníctvom úpravy prostredia (napríklad zanechanie média na dostupnom mieste). Obrana voči všetkým formám sociálneho inžinierstva je takmer nemožná.

Ochrana
1. V prípade, že ste kontaktovaný prostredníctvom mailu, alebo telefónu so žiadosťou o poskytnutie informácií dôverného charakteru (heslá, žiadosť o poslanie dokumentov, ...) aj zo strany zdanlivo dôveryhodného a oprávneného zdroja, je potrebné si dôveryhodnosť tohto zdroja overiť iným komunikačným kanálom (napríklad zavolať na známe číslo tejto dôveryhodnej osoby, ...).
2. Organizácie by mali mať určené pravidlá, akým spôsobom sa môže žiadať o informácie z prostredia mimo organizácie a vytvoriť autentifikačné mechanizmy na overenie totožnosti.
3. Neposkytujte dôverné informácie osobe, ktorej identitu si neviete overiť.

Elektronické bankové krádeže

Phishing je činnosť, pri ktorej sa podvodník snaží vylákať od používateľov rôzne heslá, napr. k bankovému účtu. Rozošle správy napr. o potrebnej zmene údajov. Používateľ klikne na odkaz v emaile, ktorý ho prepojí na webstránka, ktorá vyzerá ako presná kópia už existujúcej dôveryhodnej stránky, alebo ponúka nejaké výhody po prihlásení cez ich webstránku. Meno a heslo zadané do phishingovej stránky, sa odošlú podvodníkovi, ktorý ich môže zneužiť. Najlepšia ochrana proti phishingu je nedôverovať stránkam a e-mailom, ktoré chcú vylákať citlivé údaje, hlavne heslá. Zároveň sa odporúča použiť rôzne prihlasovacie údaje. Phishing je príkladom techniky sociálneho inžinierstva.

Man in the middle – MITM – jeho podstatou je snaha útočníka odpočúvať komunikáciu tak, že bude aktívnym prostredníkom. Útočník sa snaží získať súkromné kľúče komunikujúcich, vďaka ktorým dokáže správne podpisovať zmenené údaje. Ochranou je pravidelná výmena bezpečnostného certifikátu.



Pharming je spôsob, ktorým môže haker pripraviť o úspory klienta, ktorý využíva internet banking. Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu. Každej webadrese prislúcha IP adresa. Presmerovanie takejto adresy môže haker uskutočniť buď napadnutím servera DNS alebo zmenou súboru hosts priamo na počítači používateľa. Ak používateľ zadá mennú adresu do internetového prehliadača, miesto stránky banky sa zobrazí jej dokonalá napodobenina. Používateľ teda nezistí, že sa nachádza na inej stránke. Po zadaní údajov, ich získa neoprávnená osoba, ktorá takúto falošnú stránku vytvorila.

Doplnkové pojmy k téme:

Warez - je termín počítačového slangu označujúci autorské diela, s ktorými je nakladané v rozpore s autorským právom**.** Často je k dispozícií na voľné stiahnutie.
Cracking - odstraňovanie ochrany autorského diela. Výsledkom crackingu je – upravená aplikácia, **crack –** programček modifikujúci ochranný súbor po inštalácii, alebo **keygen -** software určený na generovanie licenčných čísel
Keylogger – program zaznamenáva stlačené klávesy – zisťovanie hesiel
Hacking –neoprávnené vnikanie do cudzích systémov. Využívajú sa:

- **spyware -** špeciálny software sledujúci činnosť v PC, môže odchytávať heslá prípadne sťahovať dáta z PC a pod.
- **využívanie chýb v systéme –** ochranou je pravidelné aktualizovanie
- **odpočúvanie sieťovej komunikácie –** predpokladom je fyzický prístup k médiu, najzraniteľnejšia je nekryptovaná wifi komunikácia.
- **útok hrubou silou resp. „**vylepšenie“ **slovníkový útok –** hľadanie hesla skúšaním všetkých možných kombinácií, resp. pri slovníkovom útoku skúšaním všetkých slov daného jazyka.
- **backdoor – zadné vrátka –** prostriedok najčastejšie program, ktorý dovolí vstup do systému bez mena a hesla (t.j čaká na danom porte)

Spam – nevyžiadaná e-mailová správa – reklamy a pod.
Hoax – nepravdivá poplašná správa (zoznam na hoax.cz)

Počítačové vírusy

Významná kapitola počítačovej kriminality.

Počítačový vírus je program, ktorý je schopný sám seba šíriť a môže mať deštrukčné účinky. O napadnutom súbore hovoríme ako o súbore **infikovanom,** uloženie súboru bez odstránenia vírusu nazývame **karanténa** a proces odstraňovania vírusu nazývame **liečenie.**

Najčastejšie sa vírus pripája k spustiteľnému súboru alebo infikujú bootovaciu (zavádzaciu) oblasť disku. Vírusy môžu byť **rezidentné** (trvalo spustené v operačnej pamäti), alebo **nerezidentné.**

Podľa činnosti vírusu v PC rozlišujeme vírusy:

- bez deštrukčnej činnosti
- vírusy napádajúce súbory – prepisujú zdrojové súbory (stačí preinštalovať)
- ničiace dáta
- modifikujúce dáta
- odosielajúce dáta
- ničiace HW – resp. ničiace BIOS matičnej dosky

Vírusy sa vo všeobecnosti snažia maskovať pred antivírovým programom. Ak je totiž vírus nemaskovaný – tj. jeho zdrojový kód aj infikované kópie sa nemenia – sú relatívne ľahko identifikovateľné pre antivírový program. Vírusy, ktoré pri kopírovaní menia svoj zdrojový kód nazývame **polymorfné. Neviditeľné resp. Stealth vírusy –**maskujú svoju činnosť, väčšinou rezidentné, pri kontrole sám deinfikuje súbor. Po použití súbor znova infikuje a až potom ukladá.

Malware

Je vo všeobecnosti označenie softwaru so škodlivým účinkom. Sú to vírusy + škodlivé programy, nepotrebujú hostiteľa. Patria sem:

- **trójske kone –** nemusia sa šíriť, veľmi často sa ukrývajú za užitočnú činnosť – môžu pracovať ako **logické** alebo **časové bomby** (spúšťačom je čas resp. splnenie podmienky), **backdoor, spyware** alebo **dropper** (v stanovených časových intervaloch „vpúšťa“ so systému ďalší malware,
- **worms - červy** - obsahuje škodlivý kód, môže byť realizovaný ako emailový alebo sieťový červ,
- **spamery** – napadnutý PC sa stáva šíriteľom spamu
- **dialery –** pracujú na PC s vytáčaným pripojením, presmerovávajú volania na platené stránky

Prejavy prítomnosti ⇒ škody spôsobené počítačovými vírusmi.

- veľký a náhly počet výskytu chybných sektorov
- problémy sa spúšťaním aplikácií
- problémy s obrazovkou
- náhla strata pamäťového priestoru
- prudké spomalenie systému
- častý výskyt chýb kontrol integrity súborov

Spôsoby šírenia počítačových vírusov

- infikované médiá
- infikované súbory stiahnuté z internetu
- elektronická pošta
- sieť

Ochrana pred infikovaním – preventívne opatrenia

- Inštalácia vhodného antivírového programu a jeho aktualizácia.
- Aktualizovaný OS
- Zálohovanie dôležitých údajov.
- Preverovať cudzie zdroje
- Preverovať pôvod správ v elektronickej pošte s prílohou – nespúšťať žiadny spustiteľný súbor pokiaľ si nie sme úplne istý dôveryhodnosťou odosielateľa

Používanie antivírových programov

Antivírové programy využívajú viacero metód na vyhľadávanie vírusov, ale nie je možné tvrdiť že existuje zaručene účinný antivírový program s dokonalou detekciou vírusov. Každý z týchto programov má svoju účinnosť detekcie, ktorá je podmienená použitým vyhľadávacím algoritmom, ale aj časom vzniku daného antivírového programu vzhľadom k tomu, že každý deň vznikajú nové druhy vírusov.

Typy antivírových programov (podľa použitej metódy)

- Programy sledujúce zmeny v súboroch - odhaľujú vírus ak je v súboroch vykonaná neoprávnená zmena v obsahu súboru. Tieto antivírové programy nie sú vhodné na detekciu neviditeľných vírusov.
- Rezidentné antivírové programy - sledujú činnosť systému a upozornia na podozrivé správanie programu. Tieto programy majú vysokú účinnosť detekcie, ale značne spomaľujú činnosť systému.
- Kontrola programových kódov, kde sa vyhľadávajú vírusové identifikátory ,čo sú vo väčšine prípadov hexadecimálne reťazce znakov - dĺžka asi 10 -16 B.
- Programy , ktoré porovnávajú súbor s dostupnou databázou vírusov . Ich účinnosť je podmienená kvalitou obsahu databázy a jej aktualizácie.
- heuristická analýza – analýza neznámych kódov, dá sa určiť pravdepodobnosť, či je daná aktivita vyvolaná kódom typická pre vírusy.

4.Využívanie IKT v spoločnosti

Využitie počítačov

V súčasnej dobe hovoríme o rozvoji informačnej spoločnosti. S prenosom a spracovaním informácií sa stretávame skoro všade napr.

Počítače a zamestnanie
a) *odborné počítačové miesta*, ktoré by bez počítačov neexistovali (správca siete, programátor)

Softwarová firma – novodobý fenomén z hľadiska zamestnanosti. Zaoberá sa vývojom, predajom a servisom IKT. Vznikli nové typy zamestnaní:

- *servisný technik* – stará sa o HW a SW firmy
- *správca siete* – zabezpečuje chod PC siete – veľmi často sa spája s funkciou správca siete
- *programátor* – pomocou programovacích jazykov vytvára aplikácie
- *analytik* – pripravuje zadanie pre programátora, zaoberá sa zadaným projektom v prvých fázach, navrhuje spôsob, programové štruktúry a pod. Funkcia existuje v dvoch úrovniach
    - *programátor- analytik* – pri malých projektoch, navrhuje aj programuje jeden
    - *softvérový inžinier* – vyššia úroveň analytika, pri veľkých projektoch pripravuje podklady pre programátorský tímy pracujúce na jednotlivých častiach projektu
- *tester* – testovanie funkčnosti projektu

- *dizajnér(webdizajnér)* – vzhľadový návrh

b) *miesta kde sa PC používajú ako nástroj* – novinár, spisovateľ, účtovník ⇒ vyniká pojem elektronickej kancelárie –vybavenie: PC, fax, tlačiareň, skener, kamera, pripojenie na internet. Vzniká možnosť komunikovať s inými kanceláriami (obchodný partner, klient, zamestnanec pracujúci doma a pod.) po sieti.
GROUPWARE – skupina programov podporujúcich vzájomnú spoluprácu kancelárií. Ďalej je možné rozvíjať vzájomnú komunikáciu pomocou *videokonferencií*

Počítače a rodina
- nástroj na vzdelávanie a získavanie informácie (multimediálne CD, encyklopédie)
- nástroj na zábavu

Hendikepovaní a počítače
Rozvoj moderných technológií umožnil aj postihnutým, aby sa zapojili do života spoločnosti. Pričom hendikepom nemyslíme len zdravotné postihnutie, ale aj diskrimináciu na základe predsudkov voči príslušníkom nejakej etnickej či náboženskej skupiny. Počítače umožňujú komunikáciu medzi ľuďmi bez ohľadu na tieto predsudky. Pre ľudí, ktorí vďaka vážnemu telesnému postihnutiu nemôžu využívať štandardné vstupné a výstupné zariadenia existujú ich špeciálne prispôsobené ekvivalenty napr.: vstupy, ktoré sa dajú ovládať jedným prstom, zariadenia pre slabozrakých a nevidiacich (napr. hmatový výstup, tlačiareň v braillovom písme, hlasový výstup ....)

Obchod, financie a priemysel
- obchod – vyhodnocovanie čiarového kódu
- financie
  - ♦ bezhotovostné platby
  - ♦ PIN kód – identifikačný kód
  - ♦ digitálna forma peňazí – napr. telefónne karty
  - ♦ internet banking
- priemysel
  - ♦ CAD – aplikačné programy na návrh výrobkov
  - ♦ CIM – návrh výrobku, príprava výrobku ale aj riadenie výroby
  - ♦ roboty – neodmysliteľná súčasť automatizácie
    - nahradzujú ľudí v nebezpečnom alebo zdraviu škodlivom prostredí resp. pri veľmi presných prácach alebo monotónnych činnostiach

Doprava
- využitie CAD,CIM systémov pri riadení výroby áut
- počítačové simulácie
- trenažéry
- riadenie dopravnej činnosti

Zdravotníctvo
- ♦ CT – počítačová tomografia – pomocou gama žiarenia sa vytvorí veľa snímkov pacienta z rôznych pohľadov. Z digitalizovaných výsledkov sa potom pomocou počítača vytvorí ostrý obraz prierezu pacientovým telom.
- ♦ EKG
- ♦ ultrazvuk
- ♦ mikrooperácie
- ♦ databázy –evidencia liekov aj pacientov

Počítače v živote spoločnosti

- informačné systémy – systém určený na zber, udržiavanie a spracovávanie údajov.

- *administratívne a logistické systémy pre komerčnú sféru* – účtovníctvo, skladové hospodárstvo, objednávkové systémy
- *elektronické obchody*
- *geografické informačné systémy*- modelovanie povrchu, mapy, katastrálne členenie, majitelia pozemkov a pod.

Vedieť diskutovať na témy:

- Vplyv informatizácie spoločnosti (IKT) na jednotlivca.
- Výhody a nevýhody elektronizácie štátnej a miestnej správy.
- Potreba informačných technológií v rozvoji vedy, ekonomiky a vzdelávaní.