Lecția 6 Protejarea fișierelor

Arhivarea fișierelor

Arhivarea (*comprimarea* sau *împachetarea*) unui fișier/ folder este operația de reducere a dimensiunii astfel încât acesta să ocupe cât mai puțin spațiu pe mediul de stocare.

Arhivarea se recomandă pentru fișierele folosite mai rar sau a celor foarte voluminoase, precum și la transferurile de date prin Internet.

Obs: Majoritatea programelor si a documentațiilor disponibile pe Internet sunt arhivate pentru optimiza folosirea rețelei și timpul de descărcare a acestor informații.

Pentru ca un fișier arhivat să poată fi accesat trebuie mai întâi dezarhivat.

Pentru ca fișierele să poată fi arhivate/ dezarhivate trebuie să folosim *arhivatoare* (programe care comprimă/ decomprimă informațiile). Prin operația de arhivare se poate crea o arhivă. Arhiva este un fișier creat cu ajutorul programului de arhivare și poate conține unul sau mai multe fișiere și foldere, fără să fie afectat conținutul acestora.

Câteva avantaje ale utilizării arhivelor:

- se economisește spațiu pe dispozitivele de stocare;
- timpul de copiere al arhivelor este mai mic;
- transportul datelor se face mai ușor;
- fișierele din arhivă sunt protejate împotriva virușilor (de regulă virușii nu atacă arhive)
- se pot crea arhive executabile (nu mai necesită operația de dezarhivare, arhiva acționează ca un program executabil)
- posibilitatea de a proteja arhiva cu parolă

Ca un dezavantaj al utilizării arhivelor ar fi acela că înainte de utilizare, acestea trebuie dezarhivate.

Exemple de arhivatoare: Winrar, Winzip, Winace, PowerArchiver etc

În timp, în special pe platforma Windows s-au impus două mari formate de arhive: fișiere cu extensia .zip lansat in 1989 si fișiere cu extensia .rar lansat în 1993. Pe lângă aceste formate un utilizator poate întâlni și alte tipuri de arhive

Viruși informatici și antiviruși

Virusul informatic este un program creat de oameni, de dimensiuni mici, cu efecte distrugătoare (poate distruge programele sau echipamentele calculatorului). Sursele de proveniență a virușilor sunt diverse: citirea unui CD, DVD, memory stic sau dischete contaminate, folosirea softului pirat, Internetul.

Numărul actual al virușilor este foarte mare mai ales că zilnic apar alții noi. Fiecare program infectat poate la rândul lui să infecteze alte programe.

Virușii pot exista în calculator ca fișiere executabile sau atașate altor fișiere (paraziți). O dată intrat în calculator, virusul nu este activ imediat, el se activează când accesați fișierul cu care a fost adus.

Exista și viruși nedistructivi (din punct de vedere al datelor), care doar afișează un mesaj pe ecran, lansează o melodie sau doar se reproduc. Pagubele pe care le produc aceștia constau în timpul pierdut și banii utilizați pentru a-i îndepărta.

În funcție de ținta lor de distrugere virușii pot fi clasificați în:

- *viruși hardware* - afectează echipamentul fizic al calculatorului (se întâlnesc mai rar)
- *viruși software* - afectează software-ul calculatorului (inclusiv sistemul de operare)

Virușii software pot infesta:

a. programul aflat în sectorul de inițializare al hard-discului sau al memory stick (acești viruși sunt transmiși prin memory stick sau chiar CD/DVD și virusează calculatorul când acesta pornește cu dispozitivele).

b. fişierele executabile ale programelor (*.exe* şi *.com*)
c. fişierele de bibliotecă *.dll.* În momentul în care este rulat programul virusat, infestarea se extinde şi la alte programe.
d. anumite fişiere de date (*.doc*, *.dot*) - *viruşi macro.*

Când un virus intră într-un calculator al unei rețele el se răspândeşte rapid în toată rețeaua, provocând pagube uriaşe.

Simptomele care semnalează existența viruşilor:
- încetinirea funcționării calculatorului (a vitezei de lucru)
- accesarea greoaie a sau distrugerea fişierelor
- creşterea nejustificată a dimensiunii fişierelor
- pierderea irecuperabilă a informațiilor de pe hdd
- distrugerea tabelei de alocare a fişierelor (FAT)
- distrugerea sectorului de boot
- apar mesaje neobişnuite pe ecran (cursorul mouse-ului face mişcări ciudate, se deschid sau închid aplicații sau chiar computerul fără intervenția utilizatorului)

Principala măsură de protecție împotriva viruşilor este utilizarea unui *program antivirus*. (este esențial ca programul antivirus să fie instalat pe computer si să fie în stare de funcționare).

Programul antivirus are rolul de a:
- detecta viruşii şi a semnala prezența semnăturii unui virus
- dezinfecta sau şterge (de regulă, la cerere) fişierele virusate
- preveni contaminarea sistemului (dacă programul antivirus este actualizat regulat!)

Atenție!
Pentru a vă proteja calculatorul împotriva viruşilor:
- programul antivirus trebuie configurat corect
- scanați CD-urile, DVD-urile, stick-urile înainte de a le utiliza
- periodic, scanați întregul sistem
- realizați copii de siguranță ale informațiilor importante
- nu uitați în calculator memory stick sau orice sursă de stocare a informației neverificate! (ele pot conține *viruşi de boot* ce se declanşează la pornirea calculatorului)
- nu se recomandă existența în acelaşi timp a două programe antivirus instalate în calculatorul vostru! (dacă doriți instalarea unui alt program antivirus, asigurați-vă că l-ați dezinstalat pe cel care exista deja)
- scanarea *în timp real* trebuie să fie activată
- programul antivirus trebuie să efectueze o verificare planificată a harddiscului configurați programul antivirus astfel încât să scaneze implicit poşta electronică

Programul antivirus trebuie actualizat permanent; acesta are o bază de date în care sunt înglobate diferite tipuri de viruşi însă mereu apar alți viruşi.

Fişă de lucru
1. Identificați programul antivirus instalat în calculatorul vostru. Dacă nu aveți, descărcați unul gratuit de pe Internet şi instalați.
2. Scanați-vă sistemul!
3. Realizați o listă cu cei mai periculoşi viruşi. Care sunt efectele ce le provoacă?