SECURITATEA REȚELELOR DE CALCULATOARE

1. **Planificarea securitatii retelei**

Intr-o retea de calculatoare, trebuie sa existe garantia ca datele secrete sunt protejate, astfel incât doar utilizatorii autorizati sa aiba acces la ele.

Vulnerabilitatea retelelor de calculatoare se manifesta in doua moduri :

- Modificarea sau distrugerea informatiei (atac la integritatea fizica)
- Posibilitatea folosirii neautorizate a informatiilor

Asigurarea „securitatii datelor" stocate in cadrul unei retele de calculatoare, presupune proceduri de manipulare a datelor care sa nu poata duce la distribuirea accidentala a lor si/sau masuri de duplicare a datelor importante, pentru a putea fi refacute in caz de nevoie.

A avea o retea de calculatoare cu acces sigur la date, presupune o procedura de autentificare a utilizatorilor si/sau de autorizare diferentiata pentru anumite resurse.

Orice retea trebuie asigurata impotriva unor daune intentionate sau accidentale. Exista patru amenintari majore la securitatea unei retele de calculatoare :

- Accesul neautorizat
- Alterarea electronica a datelor
- Furtul de date
- Daunele intentionate sau accidentale

Cade in sarcina administratorului de retea sa asigure o retea sigura, fiabila si pregatita sa faca fata pericolelor de mai sus.

Vom considera ca o retea de calculatoare este sigura daca toate operatiile sale sunt intotdeauna executate conform unor reguli strict definite, ceea ce are ca efect o protectie completa a entitatilor, resurselor si operatiilor. Lista de amenintari constituie baza definirii cerintelor de securitate. O data acestea fiind cunoscute, trebuie elaborate regulile conform carora sa se controleze ansamblul operatiilor retelei.

Aceste reguli operationale se numesc "***servicii de securitate***", iar implementarea serviciilor se face prin protocoale de securitate.

Pentru a defini o ***retea sigura de calculatoare*** trebuie elaborate urmatoarele :

- Lista cerintelor de securitate
- Regulile de protectie si securitate
- Mecanismele de securitate