

### 3. CE REPREZINTA MASURILE DE SECURITATE IN INTERNET ?

In primul rând trebuie definit la ce anume se face referire când se vorbește despre securitatea datelor sau securitatea accesului la date ?

Diferența ne e chiar așa subtilă.

*A asigura unei rețele de calculatoare securitatea datelor stocate în cadrul ei, presupune proceduri de manipulare a datelor care nu pot duce la distrugerea accidentală a lor și/sau măsuri de duplicare a datelor importante, pentru a putea fi refăcute în caz de nevoie.*

*A avea o rețea de calculatoare cu acces sigur la date presupune o procedură de autentificare a utilizatorilor și/sau de autorizare diferențiată pentru anumite resurse.*

Când se discută despre securitatea Intranetului se are în vedere mai ales ultimul aspect, cel referitor la securitatea accesului.

Subiectul securității datelor în general, nu are nimic special pentru intranet – există o serie de principii care au fost și rămân valabile și după apariția Intranetului.

O problemă importantă în cadrul discuțiilor pe marginea securității Intranetului este cea referitoare la modalitățile de accesare: „dacă există sau nu posibilitatea de acces din exteriorul companiei, via Internet”.

Acest lucru este de dorit în anumite cazuri, mai ales pentru persoanele din companie care călătoresc mult (departamentul marketing) și au nevoie de informații stocate în cadrul intranetului companiei lor.

Pentru acele companii care se decid să permită accesul din exterior (Internet) problemele se complică puțin.

Este nevoie de două lucruri :

Ø *O modalitate de autentificare a utilizatorilor.*

Partea de autentificare a utilizatorilor este implementată de obicei prin instalarea unor softuri specializate, așa numite fire-wall-uri (zid de foc – protective).

În principiu există două modalități de autentificare a accesului : *selectie pe baza numarului IP al clientului, sau pe baza validarii unei perechi nume-parola.*

Ø *O modalitate de tranzitare sigură a datelor în cadrul rețelei publice (Internetul).*

Această problemă a stat mult timp (și continuă să o facă) pe agenda de lucru a unor companii, în special cu specific bancar, care doresc să-și extindă activitatea pe Internet. Ca urmare au apărut mai multe soluții, putine ajungând însă la stadiul de standard (cum este SSL – Secure Sockets Layer). Problema nu are o rezolvare garantată la momentul actual, dar sunt de așteptat progrese însemnate în viitorul apropiat.

În momentul actual guvernul Statelor Unite impune restricții la exportul tehnologiilor care includ o fază de criptare. Coroborând acest fapt cu acela că 75% din softul mondial provine din USA, se obține o situație care nu încurajează dezvoltarea tehnologiilor sub acest aspect.