Securitate rețele

3.4. Controlul accesului la date

3.4.1. înţelegerea scopului unui cont de utilizator în cadrul unei reţele şi accesarea lui cu ajutorul unui nume de utilizator şi a unei parole

- O reţea neprotejată permite conectarea oricărui utilizator neautorizat, care poate avea acces la date confidenţiale şi care poate compromite integritatea acestora.
- Din acest motiv, orice reţea trebuie să fie protejată cu ajutorul unui nume de utilizator şi a unei parole. Astfel, doar utilizatorii cu drepturi de acces se pot conecta la reţea, facilitând în acest fel şi procesul de evidenţiere a persoanelor conectate.

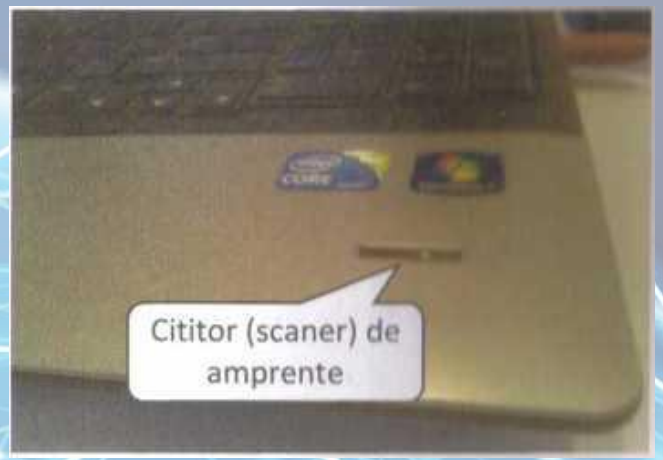
3.4.2. Recunoaşterea regulilor legate de politicile de parolare

- Pentru mulţi utilizatori alegerea unei parolei corecte este un lucru dificil, din moment ce există atât de multe lucruri care necesită parole în aceste zile. Memorarea lot constituie o problemă reală.
- Probabil din cauza aceasta o mulţime de oameni aleg parolele lor foarte prost. Simplele sfaturi de mai jos sunt menite să vă ajute în alegerea unei parole bune:
  - folosiţi cel puţin opt caractere în cadrul parolei. Cu cât parola conţine mai multe caractere, cu atât este mai sigură.
  - Folosiţi un amestec aleatoriu de caractere, litere mari și litere mici, cifre, semne de punctuaţie, spaţii şi simboluri.
  - Nu folosiți un cuvânt găsit într-un dicţionar.
  - Nu folosiți aceeaşi parolă de două ori

- Nu folosiţi parole bazate pe informaţii personale, cum ar fi: nume, prenume ziua de naştere, numele soţiei, numele animalului de companie etc.
- Nu folosiţi parole bazate pe lucruri situate în apropiere de dvs. Parolele de genul *monitor, tastatură, telefon, imprimantă* etc. sunt inutile.
- Nu fiţi tentaţi să folosiţi una dintre acele parole atât de comune care sunt uşor de reţinut, dar nu oferă nicio garanţie de securitate (de **exemplu** *parolă, password).*
- Nu folosiţi niciodată o parolă bazată pe numele dvs. de utilizator, numele contului, numele computerului sau adresa de e-mail.
- Nu divulgaţi nimănui parolele dumneavoastră.
- Schimbaţi periodic parolele.

3.4.3. Identificarea tehnicilor de bază de securitate biometrică, utilizate în controlul accesului, precum: scanare de amprente, scanare oculară

- Un scaner (cititor) de amprente reprezintă un dispozitiv de securitate care utilizează o imagine a amprentei, pentru a autentifica un utilizator.
- Cu ajutorul aplicaţiilor software de securitate, se poate utiliza amprenta digitală pentru logare în aplicaţii si site-uri web securizate, ca alternativă la clasicele nume de utilizator şi parolă asociată.
- Scanerele retiniene sunt, de obicei, utilizate pentru identificare şi autentificare. Scanarea retinei a fost utilizată de către mai multe agenţii guvernamentale, inclusiv FBI, CIA şi NASA. Cu toate acestea, în ultimii ani, scanarea retinei a devenit mai populară comercial.



- Avantajele scanării oculare:
  - Apariţia redusă de alarme false.
  - Extrem de fiabile, deoarece nu există doi oameni cu acelaşi model al retinei.
  - Identificarea persoanei se realizează foarte rapid.
- Dezavantaje:
  - Precizia de măsurare poate fi afectată de o boală, cum ar fi cataracta.
  - Precizia de măsurare poate fi, de asemenea, afectată de astigmatism sever.
  - Procedura de scanare este percepută de unele persoane ca fiind invazivă.
  - Nu este foarte uşor de utilizat.
  - Subiectul scanat trebuie să fie aproape de camera optică.
  - Costul echipamentului este foarte mare.