4. SECURITATEA INTRANETULUI

Intr-un intranet, problemele de securitate sunt urmatoarele :

- Securitatea Web serverului
- Securitatea serviciilor TCP / IP
- Securitatea Web browserelor clientilor pentru a limita ceea ce pot face ele.

O problema importanta in cadrul discutiilor pe marginea securitatii intranetului este cea referitoare la modalitatile de accesare : "daca exista sau nu posibilitatea de acces din exteriorul companiei, via Internet"

Acest lucru este de dorit in anumite cazuri, mai ales pentru persoanele din companie care calatoresc mult (departamentul marketing) si au nevoie de informatii stocate in cadrul intranetului companiei lor.

Pentru acele companii care se decid sa permita accesul din exterior (Internet) problemele se complica putin.

Securitatea Web serverului poate fi impartita in :

a) Autentificarea la nivel de utilizator / parola
b) Limitarea accesului prin intermediul adresei de retea
c) Criptarea tranzactiilor

Aceste trei tehnici se pot combina in moduri variate, creând mecanisme de securitate extrem de puternice si totodata flexibile.

a) Autentificarea prin nume utilizator / parola

Este nivelul de baza, asigurat de marea majoritate a serverelor de Web. Adica atunci când un utilizator doreste sa acceseze o anumita pagina Web, pe ecran apare o caseta de dialog care ii cere utilizatorului sa-si introduca numele si parola. Masurile de securitate se pot aplica la nivel de directoare, subdirectoare si /sau fisiere, folosind fisiere LACF (Local Acces Configuration File).

b)Autentificarea pe baza adresei de retea

Majoritatea serverelor de Web au si un alt mod de autentificare, folosind adresa IP (numerica) sau simbolica a statiilor client, ca criteriu de acces. Fiecare cerere de document a unui browser de Web contine adresa IP numerica a calculatorului care emite cererea. Serverul cauta numele de host al calculatorului care a facut cererea folosind aceasta adresa de IP si serviciul DNS (Domain Name Service). Se pot seta reguli de acces in fisierele de GACF (Global Access Configuration File) si apoi in fisierul LACF, bazându-se pe aceste adrese, astfel incât anumite calculatoare (cu anumite adrese) sa nu aiba acces la Web server.

c. Criptarea tranzactiilor

Securitatea Intranetului poate fi imbunatatita folosind tranzactii Web criptate. Exista mai multe solutii de criptare pentru Web.

Dintre multele propuneri, doar doua au ajuns la forma de standard :

- Secure HTTP (S - HTTP)
- Secure Socket Lazer (SSL)

Din pacate, cele doua protocoale nu sunt compatibile intre ele.

In acest caz se poate folosi doar un protocol, doar daca serverul de Web si browserele clientilor implementeaza acel protocol.

Valoarea Intranetului este de cele mai multe ori prea mare pentru a fi permis oricui din afara sa patrunda fara nici o restrictie. In acest caz, pe lânga masurile de securitate prevazute mai sus, se impune folosirea unui ***firewall***.

Firewall este un dispozitiv care sta intre Intranetul propriu si Internet si are scopul de a limita accesul spre sau dinspre intranet in exterior, bazându-se pe diferite politici de acces (Fig.8)

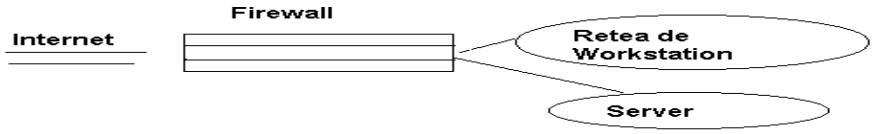

Fig. 8. Fire wall

Mai multe informatii despre firewall-uri se pot gasi la adresele :
http://www.greatcircle.com/firewalls/info/FAQ.html
http://www.greatcircle.com/firewalls/vendors.html