5. CRESTEREA NIVELULUI DE SECURITATE

Exista urmatoarele modalitati prin care un administrator de retea poate imbunatati nivelul de securitate intr-o retea :

- Auditarea
- Calculatoare fara unitati de disc
- Criparea datelor

Auditarea

Prin operatia de auditare (inspectare, examinare) se inregistreaza intr-un jurnal de securitate al serverului anumite tipuri de evenimente. Aceste inregistrari indica utilizatorii care au incercat si eventual au reusit sa obtina acces la anumite resurse. In acest fel se pot identifica activitatile si persoanele neautorizate.

Auditarea permite inregistrarea unor evenimente cum ar fi :

- Incercari de deschidere si inchidere a unei sesiuni de lucru
- Conectarea si deconectarea la/de la resurse specificate
- Terminarea conectarii
- Dezactivarea conturilor
- Deschiderea, modificarea si inchiderea fisierelor
- Crearea sau stergerea de directoare
- Modificarea parolelor

Calculatoare fara unitati de disc

Calculatoarele fara unitati de disc (diskless computers) pot indeplini toate functiile unui calculator obisnuit, cu exceptia salvarii datelor pe o discheta sau pe un hard disc local. Aceste calculatoare sunt ideale pentru asigurarea securitatii unei retele, deoarece utilizatorii nu pot lua cu ei datele pe care le vizualizeaza. Aceste calculatoare comunica cu serverul si deschid o sesiune de lucru datorita unui cip ROM special, pentru initializare, instalat pe placa de retea a calculatorului. La pornirea calculatorului serverul prezinta utilizatorului un ecran de conectare. Dupa ce utilizatorul se autentifica, calculatorul este conectat in retea.

Criptarea datelor

Inainte de a fi transferate prin retea, datele sunt codate cu ajutorul unui utilitar de criptare. Atunci când datele ajung la calculatorul destinatar, codul receptionat este decriptat cu ajutorul unei chei, informatia redevine lizibila. Schemele de criptare avansata a datelor, automatizeaza atât procesul de criptare, cât si pe cel de decriptare. Cele mai bune sisteme de criptare sunt cele care folosesc componentele hardware, dar acestea sunt foarte scumpe.

DES (Data Encryption Standard) reprezinta standardul traditional folosit pentru criptare Atât expeditorul, cât si destinatarul trebuie sa aiba acces la cheie. Vulnerabilitatea sistemului DES consta in faptul ca singura modalitate prin care cheia ajunge de la un utilizator la altul este transmiterea ei, de cele mai multe ori printr-un canal nesigur.

CCEP este un standard mai nou, creat de NSA (National Security Agency), folosit de organizatiile guvernamentale. Producatorii sunt autorizati sa incorporeze algoritmi de criptare in sisteme de comunicatie, NSA sugerând ca ei insisi sa ofere utilizatorilor acestor sisteme cheile de criptare.