COLEGIUL TEHNIC „VICTOR UNGUREANU”
CÂMPIA TURZII

PROIECT

PENTRU OBŢINEREA CERTIFICATULUI DE CALIFICARE
PROFESIONALĂ NIVEL 4

TEHNICIAN OPERATOR TEHNICĂ DE CALCUL

ABSOLVENT:
VINCZE-PETER S. AMALIA-STEFANIA

COORDONATOR:
prof. BOTA COSMIN

2019 – 2020

Securizarea reţelelor de calculatoare

CONŢINUT

ARGUMENT

Securitatea informaţiilor este acum o problemă majoră cu care se confruntă societatea electronică.

Indiferent de dimensiunea organizaţiei, odată cu creşterea explozivă a fluxului informaţional, o companie trebuie să găsească elementele care să asigure protecţia potrivită la nivel de reţea şi nivel de aplicaţie în faţa atacurilor din ce în ce mai sofisticate.

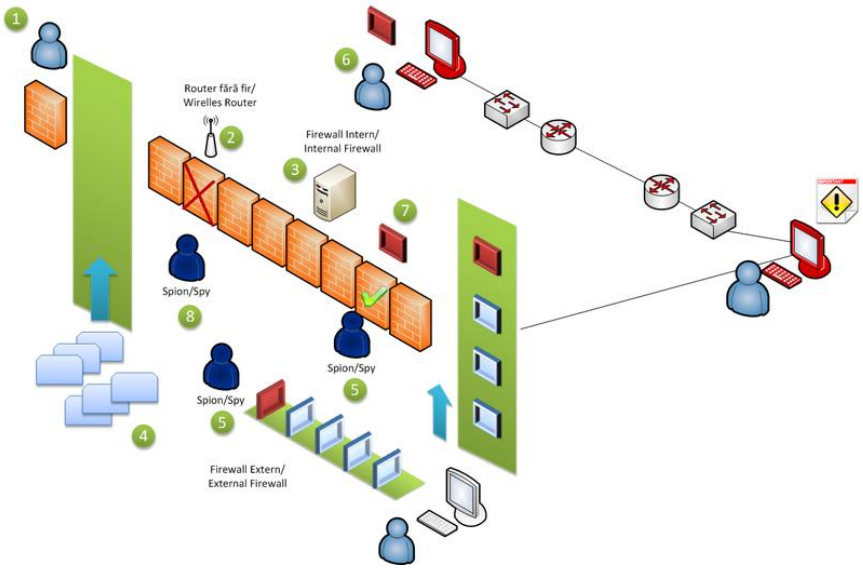
Securitatea este un concept despre care vorbeşte toată lumea. De la administratorii de reţea şi până la utilizatorii reţelelor "de bloc", toţi sunt interesaţi şi vor să îşi protejeze cât mai eficient reţeaua şi computerele. Fie că este computer personal sau integrat într-o reţea, că este o reţea privată cu sau fără conexiune la Internet, necesitatea securizării este certă.

Atacurile externe, viruşi, spam-uri, toate acestea au determinat pe posesorii de calculatoare şi pe administratorii de reţea să se ferească pe cât posibil, astfel încât sistemele, datele şi conexiunile lor să fie în siguranţă şi apărate de orice ar putea deteriora buna funcţionare a acestora.

Cele mai multe dintre aspectele tratate de securitatea pe Internet se bazează pe modalităţile de securizare a unei reţele şi pe crearea şi implementarea unei politici de securitate.

În condiţiile în care fiecare reţea în parte, oricât de mică, are la bază diferite forme de infrastructură, este mai greu să se definească o modalitate unică de securizare.

Astfel modul de securitate trebuie adaptată corespunzator fiecărei reţele, în funcţie de topologia ei şi de conexiunea la Internet.



INTRODUCERE

În primele decenii ale existenţei lor, reţelele de calculatoare au fost folosite de cercetătorii din universităţi pentru trimiterea poştei electronice şi de către funcţionarii corporaţiilor pentru a partaja imprimantele. In aceste condiţii, problema securităţii nu atragerea prea mult atenţia. Dar acum, când milioane de cetăţeni obişnuiţi folosesc reţelele pentru operaţiuni bancare, cumpărături şi plata taxelor, securitatea reţelei apare la orizont ca o mare problemă potenţială. In acest capitol, vom studia securitatea reţelei din mai multe unghiuri, evidenţiind numeroase pericole şi discutând mulţi algoritmi şi protocoale destinate a face reţele mai sigure.

Securitatea este un subiect vast şi acoperă o multitudine de imperfecţiuni. În forma sa cea mai simplă, ea asigură că persoane curioase nu pot citi sau, mai rău, modifica mesajele adresate altor destinatari. Ea se ocupă de cei care încearcă să apeleze servicii la distanţă, deşi nu sunt autorizaţi să le folosească. De asemenea, securitatea implică verificarea dacă un mesaj, ce pretinde că vine de la IRS şi spune: ’’Plăteşte până vineri’’, provine într-adevăr de la IRS şi nu de la mafia. Securitatea se ocupă de problemele legate de capturarea şi falsificarea mesajelor autorizate şi de cei ce încearcă să nege faptul ca au trimis anumite mesaje.

Majoritatea problemelor de securitate sunt cauzate intenţionat de persoane răuvoitoare care încearcă să obţină anumite beneficii, să atragă atenţia, sau să provoace rău cuiva. Câţiva dintre cei care comit în mod obişnuit astfel de fapte sunt menţionaţi în fig.8-1. Din această listă trebuie să rezulte clar că realizarea unei reţele sigure implica ceva mai mult decât păstrarea ei fără erori de programare. Aceasta implică surclasarea unor adversari adeseori inteligenţi, dedicaţi şi uneori bine dotaţi material. Trebuie de asemenea să fie clar că măsurile care pot contracara inamici accidentali vor avea un impact redus asupra unor adversari serioşi. Arhivele poliţiei arată că cele mai multe atacuri nu au fost săvârşite de străini prin ascultarea unor linii telefonice, ci de către angajaţi ranchiunoşi. În consecinţă, sistemele de securitate ar trebui proiectate ţinând seama de acest fapt.

I. PLANIFICAREA SECURITĂŢII REŢELEI

Intr-o reţea de calculatoare, trebuie sa existe garanţia ca datele secrete sunt protejate, astfel încât doar utilizatorii autorizaţi sa aibă acces la ele.

Vulnerabilitatea reţelelor de calculatoare se manifestă în două moduri:

- Modificarea sau distrugerea informaţiei (atac la integritatea fizică)
- Posibilitatea folosirii neautorizate a informaţiilor

Asigurarea „securităţii datelor" stocate în cadrul unei reţele de calculatoare, presupune proceduri de manipulare a datelor care să nu poată duce la distribuirea accidentală a lor şi/sau măsuri de duplicare a datelor importante, pentru a putea fi refăcute în caz de nevoie.

A avea o reţea de calculatoare cu acces sigur la date, presupune o procedură de autentificare a utilizatorilor şi/sau de autorizare diferenţiată pentru anumite resurse.

Orice reţea trebuie asigurată împotriva unor daune intenţionate sau accidentale. Există patru ameninţări majore la securitatea unei reţele de calculatoare :

- Accesul neautorizat

  Un firewall de rețea protejează o rețea de calculatoare împotriva accesului neautorizat. Acesta ar putea lua forma unui dispozitiv hardware, a unui program software sau a unei combinații între cele două. Firewall-urile de rețea protejează o rețea internă de calculatoare împotriva accesului rău intenționat din exterior, cum ar fi site-urile infestate cu malware sau porturile de rețea deschise și vulnerabile. Puteți găsi firewall-uri de rețea în case, școli, companii și intraneturi.

- Alterarea electronică a datelor

  O schemă de semnătură digitală este formată de obicei din 3 algoritmi:

  → Un algoritm de generare a cheilor care alege o cheie privata uniform aleatoare dintr-un set de chei private posibile. Algoritmul produce la ieșire cheia privată împreună cu o cheie publica corespunzătoare.

  → Un algoritm de *semnare* care, când i se prezintă un mesaj și o cheie privată, produce o semnătură.

→ Un algoritm verificare a semnaturii care, primind mesajul, cheia publică și semnătura, poate accepta sau respinge mesajul în raport cu autenticitatea sa.

- Furtul de date

  Amenințările asupra datelor dvs. pot veni dintrun mediu intern sau extern. Hackerii pot accesa rețelele care nu sunt asigurate întrun mod corect, hoții pot sparge biroul dumneavoastră și fura echipamente iar personalul ar putea extrage date pe medii externe portabile.
- Daunele intenţionate sau accidentale

  Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la rețelele de comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de "blocare a serviciului", precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.

Cade în sarcina administratorului de reţea să asigure o reţea sigură, fiabilă şi pregătită să facă faţă pericolelor de mai sus.

Vom considera că o reţea de calculatoare este sigură dacă toate operaţiile sale sunt întotdeauna executate conform unor reguli strict definite, ceea ce are ca efect o protecţie completă a entităţilor, resurselor şi operaţiilor. Lista de ameninţări constituie baza definirii cerinţelor de securitate. O dată acestea fiind cunoscute, trebuie elaborate regulile conform cărora să se controleze ansamblul operaţiilor reţelei.

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

Pentru a defini o *reţea sigură de calculatoare* trebuie elaborate următoarele :

- Lista cerinţelor de securitate
- Regulile de protecţie şi securitate
- Mecanismele de securitate

II. DEFINIREA POLITICILOR DE SECURITATE

Asigurarea securităţii reţelei presupune adoptarea unui set de norme, reguli si politici, care să nu lase nimic la voia întâmplării. Intr-o reţea de calculatoare modelul de securitate presupune:

1. Securitatea fizică reprezintă nivelul exterior al modelului de securitate si constă, în general, în încuierea echipamentelor informatice într-un birou sau într-o altă incintă. Securitatea fizică merită o consideraţie specială. Problema cea mai mare o constituie salvările pentru copii de rezervă ale datelor si programelor si siguranţa păstrării suporţilor de salvare. În aceste situaţii, reţelele locale sunt de mare ajutor: dacă toate fisierele schimbate frecvent rezidă pe un *server,* aceleasi persoane (sigure si de încredere), care lansează salvările pentru *mainframe*-uri, pot face aceleasi lucruri si la *server*. Calculatorul, ca orice piesă costisitoare, ar trebui să fie protejat si de pericolul furtului. Păstrarea în afara zonelor publice este una dintre cele mai bune forme de protecţie. Simpla închidere a echipamentelor va preveni mutările ascunse, precum şi furtul. Într-un sistem în care prelucrarea este distribuită, prima măsură de securitate fizică care trebuie avută în vedere este prevenirea accesului la echipamente. Pentru a învinge orice alte măsuri de securitate, trebuie să se dispună de acces fizic la echipamente. Acest lucru este comun tuturor sistemelor de calcul, distribuite sau nu.

2. Securitatea logică constă din acele metode care asigură controlul accesului la resursele si serviciile sistemului. Ea are, la rândul ei, mai multe niveluri, împărţite în două grupe mari: **niveluri de securitate a accesului** *(SA)* si **niveluri de securitate a serviciilor** *(SS).*

- **Securitatea accesului** *(SA)* cuprinde:
  - → **accesul la sistem** *(AS)*, care este răspunzător de a determina dacă si când reţeaua este accesibilă utilizatorilor. El poate fi, de asemenea, răspunzător pentru decuplarea unei staţii, ca si de gestiunea evidenţei accesului. *AS* execută, de asemenea, deconectarea forţată, dictată de supervizor. *AS* poate, de exemplu, să prevină conectarea în afara orelor de serviciu si să întrerupă toate sesiunile, după un anumit timp;

→ **accesul la cont** *(AC)*, care verifică dacă utilizatorul care se conectează cu un anumit nume si o parolă există si are un profil de utilizator valid;

→ **drepturile de acces** *(DA)*, care determină ce privilegii de conectare are utilizatorul (de exemplu, el poate avea sesiuni care totalizează 4 ore pe zi sau poate utiliza doar staţia 20).

- **Securitatea serviciilor** *(SS)*, care se află sub *SA*, controlează accesul la serviciile sistemului, cum ar fi fire de asteptare, *I/O* la disc si gestiunea **server**-ului. Din acest nivel fac parte:

  → **controlul serviciilor** *(CS)*, care este responsabil cu funcţiile de avertizare si de raportare a stării serviciilor; de asemenea, el activează si dezactivează diferitele servicii;

  → **drepturile la servicii** *(DS)*, care determină exact cum foloseste un anumit cont un serviciu dat; de exemplu, un cont poate avea numai dreptul de a adăuga fisiere pentru o anumita imprimanta, dar are drepturi depline de a adăuga şi a sterge fisiere pentru o altă imprimantă.

  → **Servicii de înalt nivel specifice software-lui** *(SIS)* **si servicii la nivel scăzut specifice hardware-lui** *(SSH)*. *SIS* sunt operaţiuni care nu sunt limitate *hardware* – de exemplu cererea de a deschide un fisier după nume. Ele sunt de fapt construite prin *SSH* si pot necesita mai multe funcţii de nivel scăzut pentru a se executa. *SSH* sunt dependente de ***hardware*.** Aceste servicii sunt "cărămizile" fundamentale de construcţie ale sistemului si acoperă nivelurile de *I/O* la sectoarele de disc si de alocare/eliberare a blocurilor de memorie.

O dată stabilită conexiunea, *SA* validează si defineste contul. Operaţiile ce trebuie executate sunt controlate de *SS*, care împiedică cererile ce nu sunt specificate în profilul utilizatorului. Accesul într-un sistem de securitate perfect trebuie să se facă prin aceste niveluri de securitate, de sus (*AS*) în jos (*SSH*). Dar când **serverele** folosesc doar *SA* pentru a controla accesul la sistem, pentru ca apoi să permită execuţia apelurilor directe la *SSH*, nivelurile *SS* sunt usor de evitat, iar operaţiunile neautorizate pot fi executate fără a fi detectate. Aceasta se întâmplă când toate celelalte niveluri ale *SS* sunt implementate si executate în ***server***-ul client. Orice sistem care permite evitarea unuia sau mai multor niveluri ale modelului de securitate implică riscul de a fi nesigur.

Politicile de securitate stabilesc orientarea generală şi oferă linii directoare pentru administratorii şi utilizatorii de reţea, în cazul unor situaţii neprevăzute. Cele mai importante politici de securitate sunt:

- Prevenirea
- Autentificarea
- Instruirea

Prevenirea este cea mai bună politică de protejare a datelor. Prin prevenirea accesului neautorizat în reţea, datele vor fi în siguranţă.

Autentificarea este politica prin care se asigură o prima linie de apărare împotriva utilizatorilor neautorizaţi. Aceasta înseamnă, că accesul într-o reţea necesită un **nume de utilizator** valid şi **o parolă**.

Instruirea este o politică pe care administratorul de reţea trebuie să o promoveze permanent în rândul utilizatorilor. Pentru aceasta, administratorul trebuie să elaboreze un ghid, clar, concis cu noţiunile pe care utilizatorii trebuie sa le cunoască cu privire la procedurile de operare şi de asigurare a securităţii.

III. SECURITATEA FIZICĂ A ECHIPAMENTELOR

Primul lucru care trebuie luat în considerare pentru protejarea datelor îi reprezintă securitatea fizică a echipamentelor hardware ale reţelei.

Gradul de securitate depinde de :

- Dimensiunile organizaţiei
- Confidenţialitatea datelor
- Resursele disponibile

Asigurarea securităţii serverelor

Intr-o reţea de dimensiuni mari în care majoritatea datelor sunt confidenţiale, serverele trebuie să fie la adăpost de eventualele distrugeri intenţionate sau accidentale. Cea mai simplă soluţie este de a închide serverele într-o încăpere în care accesul este limitat.

Protejarea cablului

Cablul de cupru, cum ar fi cel coaxial, se comportă asemeni echipamentelor radio, emiţând semnale electrice. Cu un echipament de ascultare adecvat, această informaţie poate fi monitorizată. De asemenea, pe cablul de cupru se poate intercala un dispozitiv de interceptare, astfel încât informaţiile sa fie furate direct. In acest context, în faza de proiectare, traseele cablurilor trebuie să fie stabilite în aşa fel, încât să nu permită accesul persoanelor neautorizate. Cablurile de cupru pot fi dispuse în structura clădirii, prin tavan, perete, sau podea. Un cablu Ethernet este una dintre cele mai comune forme de cablu de rețea utilizat pentru rețelele cu fir. Cablurile Ethernet conectează dispozitivele dintr-o rețea locală, cum ar fi PC-urile, routerele și switch-urile. Având în vedere că acestea sunt cabluri fizice, ele au limitările lor, atât la

distanța pe care o pot acoperi și încă să transporte un semnal corespunzător, cât și durabilitatea lor. Aceste limite sunt un motiv pentru care există diferite tipuri de cabluri Ethernet optimizate pentru a efectua anumite sarcini în anumite situații.

Salvările pentru copii de rezervă ale datelor şi programelor

Siguranţa efectuării operaţiunilor de salvare a datelor şi programelor, pe suporţi magnetici, precum şi a păstrării acestora în condiţii de deplină securitate, este o mare problemă.

Administratorul de reţea trebuie să prevadă reguli şi norme stricte pentru efectuarea operaţiunilor de salvare, cât şi pentru condiţiile de păstrare în siguranţă a suporţilor magnetici respectivi.

1. Deschideți baza de date pe care doriți să o copie de rezervă.
2. Selectați Fișier > Salvare ca.
3. Sub Tipuri de fișiere, selectați Salvare bază de date ca.
4. Sub Complex, selectați Backup bază de date, apoi selectați Salvare ca.
5. Dacă doriți, modificați numele de fișier copie de rezervă.
6. Selectați tipul de fișier pentru baza de date copie de rezervă, apoi selectați Salvare.

IV.SECURITATEA PRIN FIREWALL

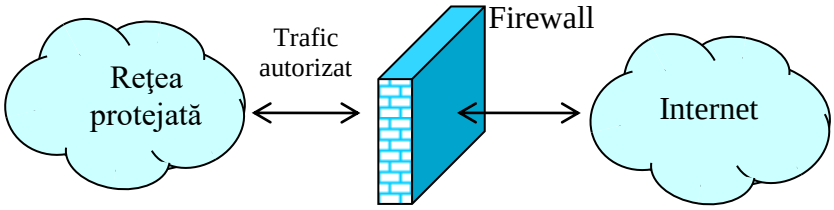
În reţelele de calculatoare, un **firewall** este un dispozitiv sau o serie de dispozitive configurate în aşa fel încât să filtreze, să cripteze sau să intermedieze traficul între diferite domenii de securitate pe baza unor reguli predefinite.

Un **firewal** (zid de protecţie, perete antifoc) este un sistem de protecţie plasat înter două reţele care are următoarele proprietăţi:

- obligă tot traficul dintre cele două reţele să treacă prin el şi numai prin el, pentru ambele sensuri de transmisie;
- filtrează traficul şi permite trecerea doar a celui autorizat prin politica de securitate;

- este el însuşi rezistent la încercările de penetrare, ocolire, spagere exercitate de diverşi.

Un firewall nu este un simplu ruter sau calculator care asigură securitatea unei reţele. El impune o politică de securitate, de control a accesului, de autentificare a clienţilor, de configurare a reţelei. El protejează o reţea sigură din punct de vedere al securităţii de o reţea nesigură, în care nu putem avea încredere.



Dispunerea unui firewall

Fiind dispus la intersecţia a două reţele, un firewall poate fi folosit şi pentru alte scopuri dcât controlul accesului:

- pentru monitorizarea comunicaţiilor dintre reţeaua internă şi cea externă (servicii folosite, volum de trafic, frecvenţa accesării, distribuţia în timp de etc.);
- pentru interceptarea şi înregistrarea tuturor comunicaţiilor dintre cele două reţele;
- pentru criptare în reţele virtuale.

IV.1. Funcţionarea firewal-ului

Un firewall, lucrează îndeaproape cu un program de routare, examinează fiecare pachet de date din reţea (fie cea locală sau cea exterioară) ce va trece prin serverul gateway pentru a determina dacă va fi trimis mai departe spre destinaţie. Un firewall include de asemenea sau lucrează împreună cu un ***server proxy*** care face cereri de pachete în numele staţiilor de lucru ale utilizatorilor. În cele mai întâlnite cazuri aceste programe de protecţie sunt instalate pe calculatoare ce îndeplinesc numai această funcţie şi sunt instalate în faţa routerelor

Soluţiile firewall se împart în două mari categorii:

- prima este reprezentată de soluţiile profesionale hardware sau software dedicate protecţiei întregului trafic dintre reţeaua unei întreprinderi (instituţii -> ex.: Universitatea "Dunărea de Jos" Galaţi) şi Internet;
- cea de a doua categorie este reprezentată de firewall-urile personale dedicate monitorizării traficului pe calculatorul personal. Utilizând o aplicaţie din ce-a de a doua categorie veţi putea preîntâmpina atacurile colegilor lipsiţi de fair-play care încearcă să acceseze prin mijloace mai

mult sau mai puţin plăcute resurse de pe PC-ul dumneavoastră. În situaţia în care dispuneţi pe calculatorul de acasă de o conexiune la Internet, un firewall personal vă va oferi un plus de siguranţă transmisiilor de date.

Cum astăzi majoritatea utilizatorilor tind să schimbe clasica conexiune dial-up cu modalităţi de conectare mai eficiente (cablu, ISDN, xDSL sau telefon mobil), pericolul unor atacuri reuşite asupra sistemului dumneavoastră creşte. Astfel, mărirea lărgimii de bandă a conexiunii la Internet facilitează posibilitatea de "strecurare" a intruşilor nedoriţi.

Astfel, un firewall este folosit pentru două scopuri:

- pentru a păstra utilizatorii locali (angajaţii, clienţii) *în reţea*
- pentru a păstra *în afara reţelei* utilizatorii rău intenţionati (viruşi, viermi cybernetici, hackeri, crackeri)

IV.2. Politica firewall-ului

Înainte de a construi un firewall trebuie hotărâtă politica sa, pentru a şti care va fi funcţia sa şi în ce fel se va implementa această funcţie

Politica firewall-ului se poate alege urmând câţiva paşi simpli:

- alege ce servicii va deservi firewall-ul
- desemnează grupuri de utilizatori care vor fi protejaţi
- defineşte ce fel de protecţie are nevoie fiecare grup de utilizatori
- pentru serviciul fiecărui grup descrie cum acesta va fi protejat
- scrie o declaraţie prin care oricare alte forme de access sunt o ilegalitate

Politica va deveni tot mai complicată cu timpul, dar deocamdată este bine să fie simplă şi la obiect

IV.3. Ce "poate" şi ce "nu poate" să facă un firewall

Un firewall poate să:

- monitorizeze căile de pătrundere în reţeaua privată, permiţând în felul acesta o mai bună monitorizare a traficului şi deci o mai uşoară detectare a încercărilor de infiltrare;
- blocheze la un moment dat traficul în şi dinspre Internet;
- selecteze accesul în spaţiul privat pe baza informaţiilor conţinute în pachete;
- permită sau interzică accesul la reţeaua publică, de pe anumite staţii specificate;
- şi nu în cele din urmă, poate izola spaţiul privat de cel public şi realiza interfaţa între cele două.

De asemeni, **o aplicaţie firewall nu poate**:

- interzice importul/exportul de informaţii dăunătoare vehiculate ca urmare a acţiunii răutăcioase a unor utilizatori aparţinând spaţiului privat (ex: căsuţa poştală şi ataşamentele);
- interzice scurgerea de informaţii de pe alte căi care ocolesc firewall-ul (acces prin dial-up ce nu trece prin router);
- apăra reţeaua privată de utilizatorii ce folosesc sisteme fizice mobile de introducere a datelor în reţea (USB Stick, dischetă, CD, etc.);
- preveni manifestarea erorilor de proiectare ale aplicaţiilor ce realizează diverse servicii, precum şi punctele slabe ce decurg din exploatarea acestor greşeli.

IV.4. Importanţa utilizării unui firewall (paravan de protecţie Internet)

Firewall-ul poate împiedica persoanele străine să intre pe computerul personal prin Internet. Dacă utilizaţi Microsoft Windows XP, activaţi firewall-ul predefinit - Internet Connection Firewall. Paşii sunt:

1. Trebuie să vă asiguraţi că sistemul de operare este Windows XP. Pentru aceasta faceţi clic pe Start, apoi pe Executare. În caseta de dialog Executare, tastaţi winver. Faceţi clic pe OK. Vi se va arăta ce versiune de Windows utilizaţi.

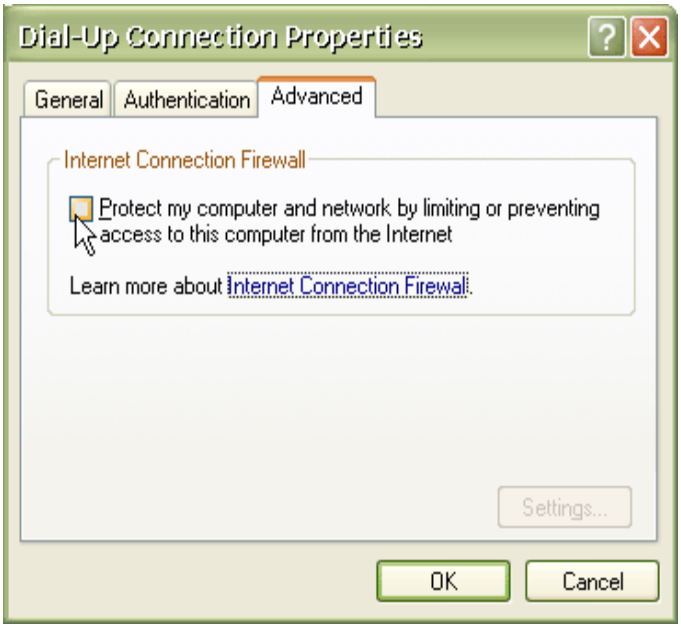
2. Faceţi clic pe Start, apoi pe Panou de control

3. Faceţi clic pe Conexiuni de reţea şi Internet, apoi pe Conexiuni în reţea. **Sfat**: Dacă nu este vizibilă categoria Conexiuni de reţea şi Internet, faceţi clic pe Comutare la Vizualizare pe categorii, în partea din stânga sus a ecranului.

4. Sub categoria Linie comutată sau LAN sau Internet de mare viteză, faceţi clic pe pictogramă pentru a selecta conexiunea pentru care doriţi o mai bună protecţie

5. Dacă bara de activitate este la stânga, sub Activităţi în reţea, faceţi clic pe Schimbarea setărilor acestei conexiuni (sau faceţi clic cu butonul drept pe conexiunea pentru care doriţi o mai bună protecţie, apoi faceţi clic pe Proprietăţi).

6. În fila Complex, sub Paravan de protecţie a conexiunii la Internet, selectaţi caseta din dreptul Protejare computer şi reţea prin limitarea sau prevenirea accesului la acest computer din Internet.



Dacă aveţi mai multe conexiuni la Internet, cum ar fi o conexiune pe bandă largă şi o linie comutată, repetaţi paşii de la 4 la 6 pentru fiecare conexiune.

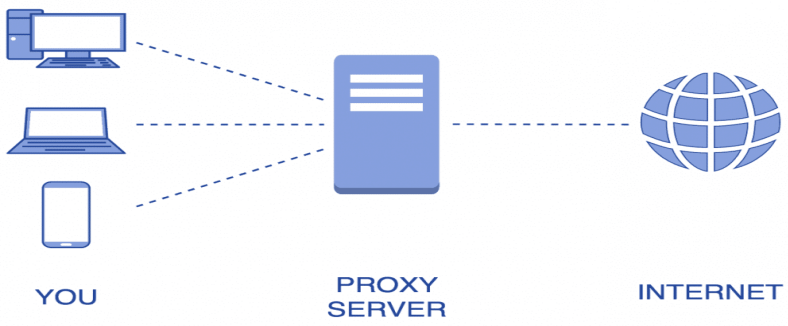
V.SERVER PROXY

Serveşte la izolarea unuia sau mai multor calculatoare pentru a putea fi protejate. Două reţele pot fi conectate printr-un server proxy, acesta asigurând legătura între reţele şi calculatoarele de protejat.

Pentru aplcaţiile din cele două reţele adresa IP a clientului va fi cea a serverului proxy. Cât timp există o conexiune la un server HTTP, browser-ul se va conecta la serverul proxy şi va cere să se afişeze URL-ul solicitat. Serverul proxy este cel care va gestiona cererea şi care va returna rezultatul browser-ului.

De asemenea, serverul proxy va obliga toate cererile să treacă prin el, reducând numărul de porturi care nu-i corespund.

Un server proxy are avantaje suplimentare în materie de performanţe. Dacă doi utilizatori cer în acelaşi timp aceeaşi pagină, aceasta va fi memorată în serverul proxy şi va fi încadrată mult mai rapid la o cerere ulterioară. Serverul proxy poate filtra cererile în funcţie de regulile impuse.



VI.SECURITATEA ACTIVE DIRECTORY

Active Directory reprezintă inima reţelelor bazate pe sisteme de operare Windows. Principalele avantaje oferite de implementarea Active Directory în reţea sunt descrise în continuare.

- **Autentificarea utilizatorilor** – permite identificarea fără echivoc a fiecărui utilizator al reţelei pe bază de utilizator şi parolă unică
- **Autorizarea accesului la resurse** – pentru fiecare resursă din reţea pot fi configurate liste de acces care specifică explicit permisiunile pe care le au utilizatorii sau grupurile asupra resursei respective.
- **Administrarea centralizată** a tuturor serverelor şi staţiilor de lucru din reţea.
- **Aplicarea consistentă a unor politici** de securitate în cadrul reţelei. Acesta din urmă este în particular un avantaj foarte important în procesul de securizare al reţelei.

VI.1. Proiectare. Aplicare

La proiectarea Active Directory trebuie respectate câteva principii de design pentru a putea aplica uşor măsuri de securitate:

- Minimizarea numărului de domenii. Acestea fiind arii de securitate distincte, un număr cât mai mic de domenii, preferabil unul singur, permite aplicarea uşoară a politicilor de securitate;

- Aplicarea politicilor generice de securitate la nivelul întregului domeniu şi completarea acestora cu măsuri specifice la nivele inferioare.

Pentru aplicarea politicilor de securitate se foloseşte **Group Policy**. Deoarece politicile se aplică la mai multe nivele (domeniu, site, *organization unit*, local) şi pot fi blocate sau suprascrise, trebuie realizat un plan detaliat privind utilizarea Group Policy. De un real ajutor este *Group Policy Management Console* care permite evaluarea rezultatului aplicării de politici multiple.

Câteva politici tipice care pot fi aplicate în cadrul unui domeniu:

- dezactivarea stocării parolei ca LMHash
- configurarea nivelului de compatibilitate *LanManager* pentru autentificare
- blocarea conturilor la introducerea greşită a parolei combinată cu impunerea de parole cu complexitate sporită
- interzicerea posibilităţii de enumerare a obiectelor din Active Directory pentru clienţii anonimi

Pentru o listă completă de setări de securitate care pot fi aplicate cu Group Policy, consultaţi *Windows Server 2003 Security Guide*.

Active Directory este o condiţie necesară pentru a putea aplica în mod sistematic politici de securitate în cadrul reţelei şi pentru a putea reduce complexitatea administrării. Pornim de la principiul simplu că o reţea sigură este una bine proiectată, configurată şi administrată. Active Directory ne oferă aici un avantaj important.

VII.SECURIZAREA STAŢIILOR WINDOWS

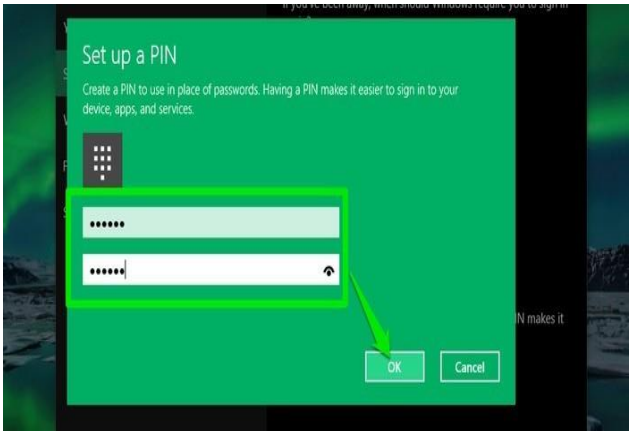
Abordarea ce mai bună privind politicile de securitate aplicate în cadrul reţelei este de a aplica un set de politici de bază la nivelul întregului domeniu, politici care să se aplice tuturor maşinilor (servere şi staţii de lucru) şi tuturor utilizatorilor. Aceste politici vor fi completate diferenţiat cu alte politici suplimentare, aplicabile anumitor roluri funcţionale pe care le au serverele şi staţiile din reţea.

Această abordare simplifică modul de gestionare al politicilor şi ne asigură că avem un nivel de securitate de bază **(baseline)** pentru întreaga reţea.

Două lucruri sunt foarte importante atunci când dorim să asigurăm un nivel de securitate de bază pentru toate sistemele din reţea:

- Sistemele trebuie să fie menţinute la zi din punct de vedere al patch-urilor şi fix-urilor de securitate. Despre acest lucru vom discuta mai tîrziu în cadrul acestui articol.

- Trebuie să aplicăm un set de configurări de securitate de bază pe toate sistemele din reţea, adică să facem întărirea securităţii sistemelor (*hardening*). Despre acest lucru discutăm aici
-



VII.1. Politici pentru toate calculatoarele

Iată câteva setări de securitate care merită luate în considerare pentru securizarea de bază a sistemelor şi pot fi aplicate cu un *Group Policy Template* la nivelul întregului domeniu Active Directory:

a) Politici de audit

- Account logon & Management
- Directory Service Access
- Object Access
- System Events

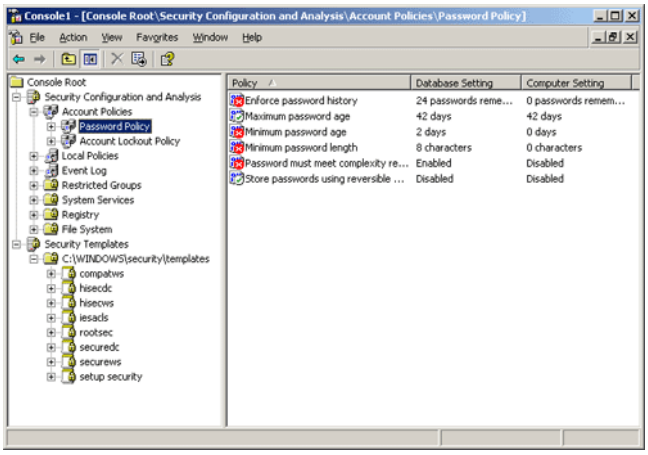
b) Privilegiile utilizatorilor

- Allow log-on locally
- Logon cu Terminal Services
- Deny log-on as a batch job
- Deny force shutdown from Remote system

VII.2. Aplicare cu Active Directory

Cel mai simplu este să pornim de la un *template* cu măsuri de securitate, pe care să-l adaptăm la cerinţele noastre şi să-l aplicăm în întreaga reţea. Putem face acest lucru cu ajutorul lui *Security Configuration Manager*. Acesta conţine: template-uri care definesc setările ce trebuie aplicate pentru

câteva configuraţii tipice, *snap-in*-ul *MMC Security Configuration & Analysis*, utilitarul linie de comandă ***secedit*** cu ajutorul căruia se poate automatiza procesul de aplicare al politicilor.



Consola MMC a Security Configuration & Analysis şi template-urile predefinite penrtu politicile privitoare la parole

Template-urile de securitate sunt fişiere text cu extensia **.inf** ce conţin un set predefinit de setări de securitate. Aceste setări pot fi adaptate şi aplicate asupra sistemelor din reţea. Setările de securitate disponibile includ: aplicarea de ACL-uri pe chei de Registry şi fişiere, aplicarea de politici de conturi şi parole, parametri de start la servicii, setarea de valori ale unor chei de Registry.

Template-urile sunt aditive, adică se pot aplica succesiv mai multe template-uri. Ordinea de aplicare este importantă: setările din ultimul template aplicat vor suprascrie setările anterioare. Template-urile pot fi aplicate global, cu ajutorul Group Policy, sau individual, cu ajutorul **Security Configuration & Analysis.**

Template-urile pot fi obţinute din mai multe surse: Windows Server 2003 vine cu un set predefinit de template-uri, în **Windows Server 2003 Security Guide** puteţi găsi template-uri adiţionale, CIAC, SANS, NSA publică propriile recomandări şi template-uri pentru sistemele de operare Microsoft.

Security Configuration & Analysis este un snap-in MMC cu ajutorul căruia putem crea o bază de date cu setări de securitate, putem importa template-uri şi putem aplica setări suplimentare, iar apoi putem compara setările sistemului cu template-ul creat în baza de date. Comparaţia este non-distructivă, adică sunt raportate doar diferenţele între starea actuală a sistemului şi template-ul ales. De asemenea, putem aplica setările respective asupra sistemului curent.

SECEDIT este un utilitar linie de comandă cu ajutorul căruia putem automatiza operaţiile de aplicare ale template-urilor folosind script-uri. Parametrii programului permit analiza, configurarea, importul, exportul, validarea sau **rollback**-ul setărilor de securitate aplicate sistemelor.

Aplicând template-uri de securitate asupra sistemelor obţinem un nivel de securitate de bază peste care putem clădi suplimentar.

VIII. SECURIZAREA SUITEI MICROSOFT OFFICE

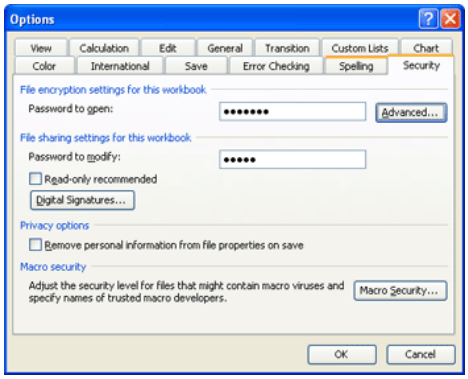
Microsoft Office a fost în mod tradiţional ţinta atacurilor cu viruşi, viermi, cai troieni datorită setului bogat de funcţionalităţi ale suitei care puteau fi exploatate: folosirea de cod macro, automatizarea transmiterii de e-mail-uri, rularea de componente ActiveX etc. În versiunile noi ale suitei, Office XP şi Office 2003, au fost introduse un set de măsuri de securitate care practic înlătură aceste probleme.

Mai există însă o componentă care nu poate fi neglijată şi anume utilizatorii. În ultima perioadă autorii de viruşi se bazează mai mult pe *social engineering* pentru a convinge utilizatorii să ruleze executabilele ataşate la e-mail-uri.

Iată câteva dintre setările disponibile:

Securitatea codului macro:

- Opţiunea implicită este High, care nu permite decât rularea codului macro semnat care a fost declarat în lista de surse de încredere. Setarea Medium permite utilizatorului să aleagă dacă va rula codul macro. Low nu este recomandată. Office 2003 introduce o setare suplimentară: Very High Security.



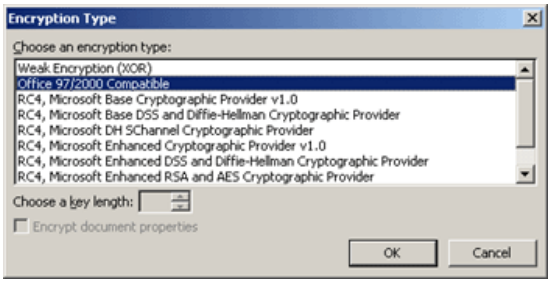
Semnături digitale

- Pentru verificarea autenticităţii şi integrităţii documentelor, acestea pot fi semnate digital folosind certificate X.509 v3. Semnăturile sunt stocate în document, aşa că orice recipient poate verifica autenticitatea şi integritatea acestuia. Implicit la Office 2003 este activă şi setarea de verificare a revocării certificatului.

A) Protecţia documentelor cu parolă şi semnături digitale

Surse de încredere

- listă de certificate ale unor producători consideraţi de încredere. Lista poate fi controlată centralizat cu Group Policy



Controale ActiveX

- Opţiuni pentru configurarea execuţiei controalelor

Protecţia cu parole şi criptarea documentelor

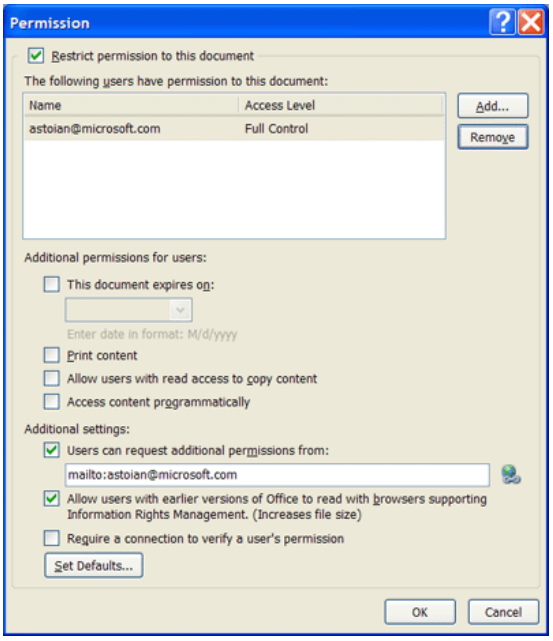
- Documentele pot fi protejate la deschidere folosind parole şi criptate folosind diverşi algoritmi

B) Protecţia cu parole şi criptarea documentelor tipuri de criptare disponibile

Opţiuni de confidenţialitate

- Office permite eliminarea informaţiilor personale la salvarea documentului pentru a nu permite identificarea autorului.

Information Rights Management (IRM)



- Este un ccide nou introdus în Office 2003 ce permite protecţia la partajarea ccidental de informaţii prin limitarea acţiunilor pe care recipienţii le pot face asupra documentului. Se pot configura permisiuni care restricţionează accesul la citire, tipărire, copierea conţinutului sau se poate configura expirarea documentului după o anumită perioadă. Pentru a putea folosi acest sistem este necesar ca serviciile IRM să fie instalate pe un Windows Server 2003 din reţea.

BIBLIOGRAFIE

1. Tom Thomas**, Securitatea Retelelelor,**titlul original **Network Security first-step,** Corint, 2005
2. Radu Lucian Lupşa, **Reţele de calculatoare,** Casa cărţii de ştiinţă, 2008
3. **http://facultate.regielive.ro**
4. **http://ro.wikipedia.org/wiki/Securitatea_re%C8%9Belelor_de_calculatoare**