1.2. Noțiuni de securitate a reţelelor de calculatoare



Pentru a se putea înţelege ceea ce doreşte a se „apăra” în cadrul reţelei, se vor prezenta mai întâi natura atacurilor ce pândesc o reţea de calculatoare. Acestea se identifică în trei mari categorii: ***confidenţialitate***, ***disponibilitate*** şi ***integritate***. Între acestea există o interdependenţă foarte strânsă, evidenţiindu-se faptul că disponibilitatea şi confidenţialitatea sunt efectiv legate de integritate.

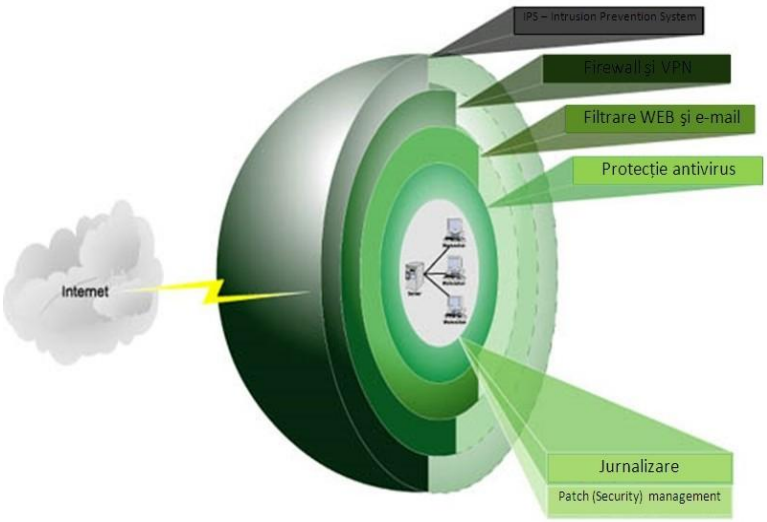


Fig. 1.2.1 Nivele distincte pentru creşterea securităţii unei reţele



Pentru a înţelege ceea ce se ascund în spatele acestor trei noţiuni, să detaliem:

a) Atacuri care se referă la ***integritatea*** reţelei ca sumă de echipamente interconectate şi a legăturilor dintre acestea şi/sau la integritatea datelor ce circulă în cadrul ei. Această categorie generează politici diferite prin prisma celor două forme de integritate: fizică – a echipamentelor şi legăturilor dintre acestea şi informaţională – relativ la date şi folosirea lor. Ca definiţii acceptate pentru integritate deosebim: *integritatea datelor* – se referă la calitatea, autenticitatea, corectitudinea şi acurateţea informaţiilor stocate într-un sistem informatic şi *integritatea sistemelor* – drept posibilitatea operării corecte şi cu succes a resurselor informatice.

b) Atacuri care atentează la ***confidenţialitatea*** sistemului. Prin aceasta înţelegem informaţia care este disponibilă doar în cazurile în care politicile de securitate sunt îndeplinite. De multe ori această proprietate este atât de importantă încât este cerută de lege sau prin contract.

c) Atacuri care atentează la ***disponibilitate*** se referă la acele forme de atac care încearcă sau chiar reuşesc să facă inutilizabil sistemul prin privarea posibilităţii de a-şi oferi disponibilitatea (răspunsul şi tratarea cererilor existente) utilizatorilor înregistraţi sau pur şi simplu prin punerea sistemului în forma de „negare a serviciilor”.


Reţelele şi resursele ataşate de acestea sunt expuse diferitor tipuri de atacuri potenţiale, cum ar fi: atacuri la integritate (atacuri la autentificare, furtul sesiunilor, atacuri de protocol, tehnici de manipulare – „social engineering”, tehnici de manipulare neglijente, abuz de privilegii explorarea uşilor din spate – „backdoors”), atacuri la confidenţialitate (divulgarea neglijentă, interceptarea informaţiei, acumularea informaţiilor) şi atacuri la disponibilitate (interferenţe, supresii, furnizarea de informaţii neaşteptate) forme de atac detaliate în cele ce urmează.


Atacurile de autentificare – situaţia în care o persoană sau un program reuşeşte să se identifice ca o altă persoană/aplicaţie şi astfel să obţină diferite avantaje nelegitime (spoofing). Include furtul direct de parole (shoulder-surfing) sau prin ghicirea sau dezvăluirea acestora. Această formă de atac se poate contracara de cele mai multe ori prin educarea utilizatorilor.


Furtul sesiunilor – o formă prin care un utilizator care a fost autentificat este „înlocuit” de atacator folosindu-se de toate privilegiile acestuia pentru accesul la informaţii sensibile. În cazul prevenţiei, este obligatorie crearea de politici privind aplicaţiile pe care utilizatorii le folosesc sau modul în care sunt folosite precum şi prin utilizarea de aplicaţii antivirus.


Atacurile protocoalelor – de multe ori această formă de atac se bazează pe slăbiciunile sistemelor criptografice. Este o formă „elevată”, de multe ori problemele bazându-se pe posibilitatea aflării unor erori matematice sau a unor „slabiciuni” care permit ca o cheie criptografică să fie derivată algebric(sau geometric prin extrapolare). Datorită formei atât de complexe şi elevate, această formă de atac nu poate fi evitată decât printr-o analiză a protocoalelor criptografice de către experţi în domeniu.


Tehnici de manipulare – este o formă de atac care ia amploare prin prisma „încrederii” şi oferirii unor informaţii private, sensibile unor persoane neautorizate. Ca formă preventivă se indică instruirea utilizatorilor suplimentată de o minimalizare a privilegiilor utilizatorilor pentru a reduce efectele unei tehnici de manipulare reuşite.


Metode de acces neglijente – discutăm aici în special de aplicaţia de tip firewall. Mulţi utilizatori din cauza neinformării sau necunoaşterii modului de folosire sau doar din dorinţa de a nu fi „sâcâit” dezactivează această aplicaţie. O formă binecunoscută de prevenţie este segmentarea resurselor între care nu există relaţii pentru a preveni atacuri din alte zone ale reţelei.


O formă specială de atac este cea a *abuzului de privilegii*. Este specială şi din cauza faptului că se referă, la atacurile venite din interior (peste 80%), marea majoritate venind

din partea unor angajaţi sau fost angajaţi nemulţumiţi sau în căutarea unor informaţii ce le pot aduce beneficii personale(de ordin material sau nu). Atacurile prin abuzul de privilegii poate fi relativ uşor de contracarat folosindu-se de minimizarea privilegiilor oferite fiecărui utilizator, precum şi prin distribuirea responsabilităţilor mari printre mai mulţi angajaţi.

*Folosirea de Backdoors* – este o metodă ce se referă la unele „erori” de cele mai multe ori introduse intenţionate în cadrul aplicaţiilor, „erori” ce pot oferi acces la sistemul pe care rulează. O formă gravă a acestei metode este faptul că este foarte greu de depistat şi remediat.

După cum s-a observat exista în formele de atac asupra integrităţii datelor o foarte mare diversitate de metode, aceasta şi din cauza importanţei acesteia (odată „îngenunchiată” aceasta, accesul la celelalte două – confidenţialitatea şi disponibilitatea – este mult mai simplu) în securitatea unei reţele de calculatoare.

*Divulgarea neglijentă* are lor în momentul în care informaţia devine accesibilă în accidental atacatorului. Ca metodă de protecţie se desprinde iarăşi educarea utilizatorilor şi folosirea unor politici de confidenţialitate în concordanţă.

*Intercepţia informaţiei* – este metoda prin care informaţia este interceptată la momentul trecerii printr-un mediu nesigur, nesupravegheat corespunzător. Ca metodă profilactică se desprinde folosirea de protocoale de criptare precum şi folosirea reţelelor private virtuale (VPN) pentru transferul informaţiilor dintr-o locaţie într-alta.

*Metoda acumulării de informaţii* se foloseşte de culegerea de informaţii din diferite surse pentru a deduce unele informaţii private. Întrucât este o metodă destul de complexă, protecţia împotriva ei nu este bine definită, fiind legată de totalitatea politicilor de securitate definite şi folosite.

*Interferenţele* sau *bruiajele* reprezintă una dintre cele mai răspândite forme de atac la disponibilitatea sistemului. O formă foarte răspândită este cea a atacurilor prin inundare, care face ca numărul de procese deschise să fie mai mare decât un sistem a fost proiectat să le efectueze efectiv (ping flood). Succesul unor astfel de forme de atac poate fi limitat sau chiar îndepărtat dacă se introduc unele filtre de admisie şi detecţie sau prin adăugarea de capacitate adiţională.

*Supresia jurnalizării* este un tip special de interferenţă şi este folosit adesea împreună cu alte tipuri de atacuri. Se folosesc metode prin care efectiv se limitează mesajele jurnalizabile sau prin generarea unui trafic atât de mare încât aflarea propriu-zisă a informaţiei utile să fie foarte dificilă. Metodele de prevenţie se bazează pe analiza

statistică a jurnalelor şi implementarea de canale de administrare private.

Furnizarea de informaţii neaşteptate se referă la generarea unui anumit comportament care forţează sistemul să intre în incapacitatea de a-şi continua lucrul. Ca forme de prevenţie se recomandă utilizarea de update-uri şi fix-uri care să trateze corespunzător situaţiile particulare ce pot genera blocarea sistemului respectiv.

Întrucât nu există o autoritate centralizată care să asigure managementul reţelelor este necesar instalarea de diferite nivele de securitate pentru siguranţa traficului. Dintre aceste nivele menţionăm: firewalls, routers, Intrusion Detection Systems şi alte componente: VPN, criptari etc.

Obiectivele principale ale securităţii reţelelor de calculatoare sunt de a proteja reţeaua, echipamentele şi mesajele din cadrul ei contra accesului neautorizat şi în general de accesul din afara ei. Se pot diferenţia un număr de 3 mari obiective:

1. Să ofere controlul în toate punctele din cadrul perimetrului reţelei pentru a bloca traficul care este maliţios, neautorizat sau prezintă riscuri pentru siguranţa reţelei.
2. Să detecteze şi să răspundă la încercările de pătrundere în reţea.
3. Să prevină mesajele din cadrul ei să fie interceptate sau modificate.

Este de precizat că setările de securitate nu pot elimina complet riscurile. Scopul este de a minimiza efectele pe cât posibil şi să elimine riscurile excesive sau nenecesare (mitigation şi contingency).

Trebuie avut de-asemenea în vedere şi faptul că scopul securităţii reţelei este să ofere conectivitatea la un preţ şi o rată risc/cost acceptabilă.

Principiile securităţii reţelelor de calculatoare se pot sintetiza şi astfel:

a) „Least privilege” – să se dea acces doar dacă este necesar şi doar pentru ceea ce este obligatoriu;

b) Folosirea de nivele de securitate distincte, care să se întrepătrundă (defense in depth) – vezi fişa 1.1

c) Controlul perimetral – plasarea de controale stricte la fiecare capăt de reţea;

d) Refuzarea oricăror drepturi care nu sunt specificate prin exemplificare.

În acelaşi timp totuşi principiile enumerate mai sus trebuiesc să se întrepătrundă cu următoarele:

a) „keep it simple” – trebuie să înţelegi pentru a putea să protejezi;

b) Să ascunzi pe cât posibil informaţiile cu privire la reţea;

c) Tehnologizarea nu este suficientă – o securizare bună constă în mult mai multe decât cele mai recente tehnologii sau „state-of-the-art” software şi hardware;

d) Politici de securitate – absolut necesare pentru a defini nivele de risc şi direcţii generale pentru generarea de practici şi proceduri de securitate şi implementare.



Nu în ultimul rând trebuie menţionat şi rolul utilizatorului final în cadrul întregului concept de securitate, astfel este necesar ca fiecare administrator sau utilizator să încerce să urmeze următoarele sfaturi:

a) jurnalizarea şi monitorizarea – absolut necesară pentru detectarea din timp şi răspunsul prompt la problemele principale;

b) criptarea informaţiilor cruciale care sunt transmise folosind reţele nesigure – informaţiile senzitive care sunt trimise în text simplu pot fi foarte uşor interceptate;

c) nu realizaţi relaţii de încredere bazate pe adrese IP – adresele IP pot fi „spoofed" – „clonate" cu ajutorul unor unelte şi aplicaţii;

d) „weakest link" – un sistem este atât de sigur pe cât este cea mai slabă componentă;

e) Minimizaţi riscul nenecesar – întrucât nu se poate elimina riscul complet, asiguraţi-vă contra riscurilor excesive sau nenecesare (prin realizarea de back-up-uri)

Activitatea de învăţare 1.2.1 Tipuri de atacuri asupra reţelelor

Obiectivul/obiective vizate:

- La sfârşitul activităţii vei fi capabil să identifici diferitele tipuri de atacuri asupra unei reţele.

Durata: 30 min



Tipul activităţii: Potrivire

Sugestii : activitatea se poate desfăşura frontal şi individual

Sarcina de lucru:

Completaţi următorul tabel cu datele de mai jos

Atacuri contra		
confidenţialităţii	**disponibilităţii**	**integrităţii**

Completaţi tabelul de mai sus cu literele din dreptul textelor din lista de mai jos, asa cum se potrivesc in cele 3 coloane

a) supresii,
b) atacuri la autentificare,
c) furtul sesiunilor,
d) tehnici de manipulare neglijente,
e) furnizarea de informaţii neaşteptate
f) abuz de privilegii,
g) explorarea uşilor din spate – „backdoors”
h) divulgarea neglijentă,
i) tehnici de manipulare – „social engineering”,
j) interceptarea informaţiei,
k) atacuri de protocol,
l) acumularea informaţiilor
m) interferenţe,

Pentru rezolvarea sarcinii de lucru consultaţi *Fişa de documentare 1.2* precum şi sursele de pe Internet.