FISA DE DOCUMENTARE NR. 5

SECURITATEA RETELELOR DE CALCULATOARE

Fundamentele şi principiile securităţii sistemelor de calcul şi 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*. 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.

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

c) 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.

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).

Majoritatea companiilor care se ocupă de securitatea sistemelor informatice sunt de acord cu privire la următoarele nivele minime care trebuiesc satisfăcute pentru a fi protejaţi la un nivel acceptabil:

a) necesitatea instalării unei aplicaţii de tip anti-virus: aceasta aplicaţie este vitală să fie instalată şi mai mult, să aibă toate actualizările la zi în ceea ce priveşte definiţiile de viruşi;
b) aplicaţie de tip firewall – această aplicaţie a devenit o cel puţin la fel de importantă componentă ca cea anterioară;
c) aplicaţie de tip anti-spyware care să fie la fel, actualizată cât mai des;
d) criptarea informaţiilor cu statut personal, privat;
e) este foarte important şi ca utilizatorul să folosească parole cât mai „bune" şi aici ne referim la lungimea lor (la ora actuală o parolă de 4 caractere se poate sparge într-un timp foarte scurt de ordinul zecilor de minute, la o parola de 8 caractere acest lucru ajungând la ordinul zilelor, mai ales dacă conţin simboluri, cifre şi litere atât mici cât şi mari);
f) nu în ultimul rând este foarte important ca utilizatorul să aibă o conduită precaută, să nu descarce orice programe găsite pe net, să citească orice mesaj de atenţionare venit din partea aplicaţiilor de tip antivirus, firewall, anti-spyware;
g) realizarea periodică de backup-uri ale datelor pentru a putea fi protejat în cazul unor atacuri reuşite sau incidente de genul incendiilor, inundaţiilor sau altor forme asemănătoare.

Ca metode de identificare a viruşilor deosebim:

a) identificarea bazată pe semnătură (signature based) este cea mai comună variantă. Pentru identificarea viruşilor cunoscuţi fiecare fişier este scanat ca şi conţinut (întreg şi pe bucăţi) în căutarea informaţiilor păstrate într-un aşa-numit dicţionar de semnături;

b) identificarea bazată pe comportament (malicious activity), în acest caz aplicaţia antivirus monitorizează întregul sistem pentru depistarea de programe suspecte în comportament. Dacă este detectată o comportare suspectă, programul respectiv este investigat suplimentar, folosindu-se de alte metode (semnături, heuristic, analiză de fişier, etc.). Este de menţionat că aceasta metodă poate detecta viruşi noi;

c) metoda heuristică (heurisitc-based) este folosită pentru detectarea viruşilor noi şi poate fi efectuată folosind două variante(independent sau cumulat): analiza de fişier şi emulare de fişier. Astfel analiză bazată pe analiza fişierului implică căutarea în cadrul acelui fişier de instrucţiuni „uzuale" folosite de viruşi. Cea de-a doua metodă este cea de emulare în care se rulează fişierul respectiv într-un mediu virtual şi jurnalizarea acţiunilor pe care le face.

d) un mod relativ nou se bazează pe conceptul de semnături generice – ceea ce s-ar traduce în posibilitatea de a neutraliza un virus folosindu-se de o semnătură comună. Majoritatea viruşilor din ziua de astăzi sunt aşa-numiţii – viruşi de mutaţie – ceea ce înseamnă că în decursul răspândirii sale el îşi schimbă acea semnătură de mai multe ori. Aceste semnături generice conţin informaţiile obţinute de la un virus şi în unele locuri se introduc aşa-numitele wildcard-uri – caractere speciale care pot lipsi sau pot fi distincte – aplicaţia software căutând în acest caz informaţii non-continue.

Conceptul de securitate hardware se referă la posibilităţile de a preveni furtul, vandalismul şi pierderea datelor. Se identifică patru mari concepte:

a) securizarea accesului – posibilitatea de a restricţiona şi urmări accesul la reţea (posibilităţile de a îngrădi clădirile şi de a securiza punctele de acces în cadrul unităţii)

b) securizarea infrastructurii – protejarea caburilor, echipamentelor de telecomunicaţii şi dispozitivelor de reţea – gruparea pe cât posibil în locaţii puternic securizate a tuturor echipamentelor de comunicaţie, camere de supravegheat – cu conectare wireless pentru zone greu accesibile – firewall-uri la nivel hardware, posibilitatea de a monitoriza modificarea cablării şi a echipamentelor intermediare de comunicaţie – ex. monitorizarea switch-urilor, routerelor etc.;

c) securizarea accesului la calculatoare – folosind lacăte pentru cabluri – mai ales pentru laptopuri – carcase ce se pot închide, eventual cutii securizate ce conţin unităţile centrale ale desktop-urilor;

d) securizarea datelor – în special pentru prevenirea accesului la sursele de date – ca de ex. Hard disk-urile externe vor trebui ţinute în carcase prevăzute cu lacăte, precum şi dispozitive de siguranţă pentru stick-uri USB. O atenţie foarte mare trebuie oferită soluţiilor de back-up folosite, suporturile acestor date trebuiesc să fie stocate şi transportate în locaţii şi în condiţii foarte sigure(stricte).

Implementarea unei soluţii de securitate foarte puternice este o procedură foarte dificilă ce implică de multe ori costuri foarte mari, cât şi personal calificat şi foarte disciplinat.

De multe ori aceste echipamente conţin un întreg ansamblu de soluţii – firewall, antivirus, criptări, IDS (Intrusion Detection System), VPN (virtial private network), trafic snaping. Aceste soluţii se bazează pe cipuri ASIC (Application-Specific Integrated Circuit) care sunt circuite integrate personalizate să efectueze o anumită sarcină (se elimină cazurile generale, implementându-se algoritmi speciali, specializaţi şi optimizaţi). Versiuni similare sunt aşa numitele SoC (System on a Cip) care conţin şi alte blocuri funcţionale (procesare pe 32 de biţi, memorie ROM, RAM, EEPROM, Flash). Aceste echipamente totuşi au preţuri foarte mari, prohibitive pentru companiile mici şi mijlocii, ele folosindu-se în special în cadrul marilor companii multi-naţionale.

Menirea unei soluţii de securitate software este de a înlocui şi eventual de a îmbunătăţi soluţia de tip hardware(decizie luată în special din cauza preţului dispozitivelor hardware specializate).

Si soluţiile software se pot organiza într-un mod asemănător cu cel prezentat în fişa 2.2, cu precizările următoare:

a. la nivelul „accesului” se pot folosi sistemele de monitorizare folosindu-se de coduri de acces, camere de supraveghere cu detecţia mişcării
b. la nivel de „infrastructură” firewall-uri software, sisteme de monitorizare ale reţelei în vederea detectării de modificări la nivel de cablări, schimbări de configurare, declanşări de alarme, etc.;
c. la nivel de „date” – posibilităţi de backup automate, păstrate în diferite locaţii, programe de criptare, etc;
d. la nivelul „calculatoarelor” - IDS (Intrusion Detection Systems) – care pot monitoriza modificările din cadrul codului programelor şi sesizează activitatea „neobişnuită” a reţelei, folosirea de aplicaţii de detectare a elementelor de tip malaware (viruşi, spyware, adware, grayware);

Din alt punct de vedere este foarte important de evidenţiat faptul că aceste soluţii de securitate se mai clasifică şi în funcţie de importanţa lor, astfel, deosebim:

a. aplicaţii de tip firewall – pentru filtrarea datelor din cadrul unei reţele;
b. aplicaţii pentru detectarea codurilor dăunătoare: aplicaţii antivirus, aplicaţii anti-spamware, anti-adware, anti-grayware la nivel de reţea;
c. obligativitatea actualizării de patch-uri pentru sistemele de operare şi aplicaţii instalate pentru a minimiza posibilităţile de infectare folosind breşele de securitate nou apărute.

Conform unui studiu al companiei Blue Coat care prezintă primele 5 cele mai bune practici de securitate pentru conectarea la internet, se disting direcţiile de urmat în următoarea perioadă (luni, ani) şi anume:

1. Alăturarea la o comunitate de supraveghere (community watch). Din ce în ce mai mulţi utilizatori, se unesc în comunităţi de supraveghere păstrate în aşa numitele „cloud services” – reţele între care există relaţii bine-stabilite, de încredere şi dependenţă, bazându-se pe concepte de procesare în reţea(folosindu-se astfel de puterea de procesare oferită de fiecare calculator din cadrul ei) – pentru a se proteja unii pe alţii. Când o persoană detectează o ameninţare, aceasta este percepută de fiecare utilizator din cadrul norului (cloud) astfel ajungând să se apere fiecare utilizator. Aceste comunităţi sunt un pas foarte important în asigurarea securităţii deoarece conferă avantaje foarte puternice comparativ cu alte soluţii singulare, deoarece are la dispoziţie mai multe resurse şi soluţii defensive.

2. Schimbarea mentalităţii defensive „one against the Web” (singur împotriva Internetului). Soluţiile personale de protejare împotriva atacurilor criminale care vizează furtul de date, de orice natură, devin foarte repede „învechite” întrucât aceste atacuri devin din ce în ce mai complexe şi mai sofisticate tehnologic. Sistemele de protecţie bazate pe semnături actualizate zilnic sunt forme de protecţie depăşite. Nu se compară aceste soluţii cu ceea ce se poate oferi prin soluţiile cu design hibrid folosite de comunităţile de supraveghere, care se bazează pe servicii de protecţie ce se actualizează odată la 5 minute, beneficiind de serviciile defensive a peste 50 de milioane de utilizatori.

3. Schimbarea politicilor bazate pe „producţie” în politici bazate pe „protecţie”. Dacă soluţia existentă la momentul actual este mai veche de 1 an, atunci această soluţie este bazată pe „producţie” – adică la momentul instalării s-a luat în calcul mărirea productivităţii utilizatorilor prin blocarea de site-uri cu conţinut obscen şi neproductiv(ex. jocuri online). Cum s-a ajuns ca peste 90% din conţinutul malaware să vină de la site-uri populare şi „de încredere”, Internetul-ca un tot unitar - a ajuns să fie principalul „furnizor” de acest conţinut. Pentru protejare de atacuri venite din Internet este necesar să se blocheze toate formele de download venite din partea unor site-uri necunoscute sau cu reputaţii ştirbe, blocând astfel o întreagă cale de acces al ameninţărilor de tip malaware în reţeaua locală.

4. Folosirea de servicii Web real-time (în timp real) de evaluare. Conţinutul Web cuprinde o multitudine de metode de filtrare de adrese URL care actualizează zilnic listele URL statice conţinute de fiecare site. Serviciile Web care oferă posibilitatea de a evalua site-urile devin unelte foarte puternice şi necesare pentru a suplimenta valoare de protecţie oferită de soluţiile de filtrare de URL. Dealtfel aceste servicii oferă un real ajutor şi utilizatorilor finali, oferind informaţii în timp real cu privire la conţinutul paginilor vizitate, utilizatorii bucurându-se de navigări relativ sigure folosind politici de securitate acceptabile.

5. Protejarea utilizatorilor ce se conectează de la distanţă. Posibilitatea de a lucra la distanţă a devenit o foarte importantă unealtă de lucru pentru majoritatea utilizatorilor. Adăugarea unui agent de tip client, legat la o comunitate de supraveghere poate proteja mai bine utilizatorii la distanţă. Centralizarea politicilor de management poate oferi protecţia necesară oferită de filtrarea de conţinut şi blocarea de malware de pe site-urile detectate de o întreaga reţea defensivă a unei comunităţi de supraveghere.

Producătorii de hardware au venit cu soluţia simplă de a oferi un nivel de securitate crescut folosind funcţii bazate pe parole (maxim 8 caractere) pentru accesul la resursele unui calculator, această formă de acces fiind o formă des întâlnită, şi la îndemâna oricui. Este aşa-numita „parolare din BIOS”. Sunt câteva aspecte care conferă acestei forme de securizare anumite avantaje şi dezavantaje:

- este la îndemâna oricui (se regăseşte în orice laptop sau desktop);
- oferă un grad suplimentar de securitate sistemului, reţelei, etc.;
- se poate securiza doar setările BIOS sau şi partea de bootare (prin parolarea doar a BIOS-ului se pot dezactiva de ex. alte surse pentru bootare);
- are un număr de 3 încercări pentru a introduce parola validă (privit dintr-un anumit punct de vedere este un avantaj, dar poate fi şi un dezavantaj);
- nu se pot securiza datele de pe HDD (cu excepţia unor cazuri speciale – ex. seria IBM ThinkPad), acestea fiind accesibile prin montarea în altă unitate;
- odată blocat sistemul (s-a depăşit nr de încercări pentru introducerea parolei) sistemul este blocat şi este necesară intervenţia specializată (posibile soluţii pentru utilizatorul obişnuit: resetarea BIOS-ului prin acţionarea unui buton, setarea unui jumper sau scoaterea bateriei CMOS);
- pentru anumite tipuri de BIOS sunt deja cunoscute unele parole „backdoor” care pot oferi acces pe sistem, făcând această formă de securizare inutilă;