SISTEME DE SECURITATE A REȚELELOR

Alexandru ZASTAVNEȚCHI*

Universitatea Tehnică a Moldovei, Facultatea Calculatoare, Informatică și Microelectronică, Departamentul Informatică și Ingineria Sistemelor, gr. IA-191, Chișinău, Republica Moldova

*Autorul corespondent: Alexandru Zastavnețchi, zastavnetchi.alexandru@iis.utm.md

Rezumat. *În acest articol se spune despre importanța aspectelor de securitate în rețelele de calculatoare. Se descriu diferite metode de atac a rețelelor și a mecanismelor de protecție a acestora. De asemena se spune despre formarea unei parole complexe, structurii și parametrilor acesteia. Într-același timp este abordată problema unui număr mare de parole care trebuie reținute și utilizate de personele cu o activitate sporită în rețea și modalitățile de soluționare a acesteia.*

Cuvinte-cheie: *securitatea informației, sistem informatic, sisteme de securitate, eficiența securității.*

Introducere

Securitatea informației se ocupă cu protejarea informației și sistemelor informatice, de încercări cu accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea sau distrugerea acestora. ISO/IEC27002/2013 descrie securitatea informațiilor prin trei criterii esențiale aprobate: confidențialitatea, integritatea și disponibilitatea.

Importanţa aspectelor

De securitate în reţelele de calculatoare a crescut odată cu extinderea prelucrărilor electronice de date şi a transmiterii acestora prin intermediul reţelelor. În cazul activării cu informaţii confidenţiale, este important ca avantajele de partajare şi comunicare aduse de reţelele de calculatoare să fie susţinute de facilităţi de securitate aprobate la nivel internațional. Acest aspect este de estență în condiţiile în care reţelele de calculatoare au ajuns să fie folosite inclusiv pentru realizarea unor operaţiuni bancare, cumpărături sau plați unor taxe. Persoanele care tind să aducă fraude securității reţelelor pot aparţine unor categorii diverse, comiţând fraude mai mult sau mai puţin grave: sunt cunoscute cazurile în care studenţii se amuză încercând să fure poşta electronică a celorlalţi, persoana sau "hacker"-ul care testează securitatea sistemelor sau urmăresc să obţină în mod neautorizat anumite informaţii, prin metodele de acces care în mod normal le-ar fi interzise, persoane care realizează fraude și furturi financiare (furtul numerelor de identificare, a cărţilor de credit, transferuri bancare ilegale etc.), persoanele care se ocupă cu spionaj industrial.

Problemele de asigurare a securităţii reţelelor

Acestea se grupează în următoarele domenii interdependente:

- confidenţialiatea face referință la asigurarea accesului la informaţie doar pentru utilizatorii autorizaţi şi blocarea sau nesatisfacerea accesului pentru persoanele neautorizate;
- integritatea se referă la asigurarea consistenţei informaţiilor (în cazul expedierii unui mesaj prin rețea, integritatea are grijă de protecţia împotriva unor tentative de modificare a mesajului în scopul unei persoane răufăcătoare);
- autentificarea asigură determinarea identităţii persoanei cu care se comunică (aspect de importanță sporită în cazul schimbului de informaţii confidenţiale sau unui număr orecare de mesaje în care identitatea transmiţătorului este esenţială);

Procedeele de autentificare

Sunt extrem de răspândite: recunoașterea fețelor, vocilor, amprentelor, a scrisului sau a semnăturilor unor persoane se încadrează în această categorie. Semnăturile și sigiliile sunt metode de autentificare folosite foarte frecvent [1].

Introducerea unor mecanisme de securitate în rețelele de calculatoare de arie largă, în particular – Internet-ul, asigură rezolvarea următoarelor aspecte:

- Bombardarea cu mesaje – mai cunoscut ca spam – expedierea de mesaje nedorite, de obicei cu un conținut comercial. Programele de e-mail pot implimenta facilitățile de blocare a mesajelor de tip "spam" prin descrierea de către utilizator a unor acțiuni corespunzătoare pentru aplicație asupra mesajelor, în funcție de cuvinte cheie sau de adresele (listele de adrese) de origine.
- Rularea unui cod (program) dăunător, de obicei, de tip virus - acesta poate fi un program Java sau ActiveX, respectiv un script JavaScript, VBScript etc. În mare parte programele de navigare permit utilizarea unor filtre specifice care permit să decidă dacă un anumit program va fi rulat sau nu, și numărul de restricții de securitate pentru rularea acestuia.
- Infectarea cu viruși specifici anumitor aplicații – poate fi prevenită prin instalarea unor programe de tip antivirus care sunt menite să detecteze viruși, devirusează fișierele infectate și introduc în ”zonă de carantin” fișierele care nu pot fi "dezinfectate".
- Accesarea prin rețea a unui calculator privat și "atacul" asupra acestuia. La nivelul protocoalelor de rețea, protejarea accesului la un calculator sau la o rețea de calculatoare este realizată prin sisteme de tip firewall, în baza unor comenzi specifice. Asemenea sisteme pot fi utilizate și invers securității, pentru blocarea accesului unui calculator sau a unei rețele de calculatoare la anumite adrese sau facilități din Internet.

Pentru asigurarea securității rețelei este importantă implementarea unor mecanisme specifice pornind de la nivelul fizic (protecția fizică a liniilor și dispozitivelor/ canalelor de transmisie), continuând cu proceduri de blocare a accesului la nivelul rețelei (firewall), până la aplicarea unor tehnici de codificare a datelor (criptare/ șifrare), metodă specifică pentru protecția comunicării între procesele de tip aplicație care rulează pe diverse calculatoare din rețea.

Împiedicarea interceptării fizice

Aceasta, este foarte costisitoare și dificilă, ea se poate realiza mai eficient pentru anumite tipuri de medii (de exemplu, detectarea interceptărilor pe fibre optice este mai simplă decât pentru cablurile cu fire de cupru). Astfel, se preferă implementarea unor mecanisme de asigurare a securității la nivel logic, prin tehnici de codificare/criptare a datelor transmise care urmăresc transformarea mesajelor astfel încât să fie înțelese numai de destinatar, tehnicile respective, devin mijlocul principal de protecție a rețelelor.

Autentificarea la un sistem informațional se face în general printr-un nume de utilizator și a unei parole. Parola este un cuvânt (șir de caractere) secret prin care utilizatorul dovedește identitatea sa. Deși parametrii stabilirii unei parole greu de presupus, mulți utilizatori oferă o mică importanță acesteia introducând unele date persoane, de obicei rău voitoare, să afle aceste parole.

Necesitatea reținerii unui număr mare de parole

O parolă complexă este un șir de caractere alcătuit din litere minuscule, majuscule, cifre și simboluri (@#&%*…). Siguranța și complexitatea parolei este dată și de numărul de caractere ce o compun, este considerată o parolă bună, cea care conține cel puțin 8 caractere. De reținut că timpul necesar pentru spargerea unei parole crește odată cu numărul de caractere din care este compusă.

Mulțumiri

Țin să mulțumesc pentru ajutorul acordat în realizarea acestui articol, dnei Daniela Istrati, lector universitar la Departamentul Informatcă și Ingineria Sistemelor.

Referințe Web:

1. *Dezvoltarea unei politici de securitate în rețea. Soluții de securitate hardware și software* [accesat 24.02.2020]. Disponibil: http://www.referatele.com/informatica/Dezvoltarea-unei-politici-de-s515.php