Universitatea Titu Maiorescu
Facultatea de Stiinta si Tehnologie a Informatiei

Aspecte de baza ale securitatii informatiei

Introducere

Ce este informatia ? Informatia este conceptul care sta la baza acestei ere. Informatia, daca nu este deja,cu siguranta va fi obiectul principal de lucru in anii ce vor urma. Cand spunem informatie, ne gandim in principal la informatia digitala. Odata cu dezvoltarea tehnologiei, spatiile virtuale care mai demult existau doar in imaginatie au inceput sa prinda viata. Astfel a luat nastere WWW-ul (world wide web). Acest acronim este unul dintre cele mai cunoscute deoarece toata lumea stie ca “pe www poti gasi orice”; orice informatie cu caracter public bineinteles. Printre alte inventii digitale care ne faciliteaza accesul la informatie se numara FTP (file transfer protocol) si bineinteles motoarele de cautare.

Search engines …. cine nu a auzit de Google sau Altavista ? Motoarele de cautare reprezinta unele dintre cele mai puternice ustensile pentru accesul la informatia digitala. Acestea stocheaza in baza lor de date informatii despre content-ul serverelor.

Revenind la ideea de la care am plecat si anume aceea ca informatia sta la baza multor activitati pe care le desfasuram ne punem problema: “Ce facem cu informatiile sensibile?”.Pe cat de simplu pare, pe atat de complicat este raspunsul: “le protejam”.

Nevoia de securitate la nivel informational este din ce in ce mai stringenta.
Pe zi ce trece numarul companiilor care au nevoie de canale securizate creste; numarul persoanelor care doresc confidentialitatea informatiilor creste; si lista continua.

Din aceste dorinte de confidentialitate, existente dealtfel de mult timp dar sub alte forme, s-au nascut ideile, teoriile, programele si cercetarile legate de securitatea informatiei.

Ceva mai concret

Securitatea informatiei….este o denumire prea generala. In primul rand trebuie sa intelegem nevoile de securitate ale unei persoane sau companii etc.

La nivelul unui utilizator obisnuit nevoia de securitate se refera in general la:

- Protejarea datelor impotriva coruperii (pastrarea integritatii OS-ului)
- Protejarea datelor impotriva furtului
- Protejarea sistemului impotriva atacurilor

La nivelul unei firme, nevoia de securitate consta in:

- Protejarea datelor confidentiale de accesul persoanelor neautorizate
- Recuperarea datelor in cazul unui dezastru
- Comunicari securizate cu alte filiale sau alte companii

La nivelul unei retele, nevoia de securitate consta in:

- Protejarea de atacuri de tip DoS/DDoS
- Protejarea serverelor de accesul neautorizat (compromitere)
- Protejarea impotriva interceptarii traficului

Aceste exemple pentru home-user, company & network sunt doar cateva din intreaga lista pe care o putem completa la fiecere.

De asemenea, pe langa home-user, company & network exista multe alte obiecte/domenii care necesita securizare, cele mentionate fiind printre cele mai importante.

Plecand de la proverbul “roata mica rastoarna carul mare” am tendinta sa afirm ca exemplele mentionate, desi par cunoscute de toata lumea, ele sunt cele care iti dau de furca cel mai mult datorita simplitatii lor; de aceea am sa incerc sa evidentiez cateva concepte/tehnici esentiale pentru a incerca rezolvarea acestor “mici probleme”.

Pareri legate de home-useri

Desi exista foarte multe alternative, Microsoft inca detine un procent important pe planul sistemelor de operare folosite de utilizatorii obisnuiti. Datorita acestui fapt ma voi axa in continuare pe incercarea de imbunatatire a securitatii a unui sistem Windows XP foarte des intalnit. Este “safe” sa presupunem ca utilizatorii care folosesc altceva au “macar o idee” despre ceea ce fac.

Protectia impotriva bug-urilor software ale sistemului de operare. Pentru aceasta etapa rezolvarea este cat se poate de simpla: setarea update-urilor automate sau updatarea manuala a sistemului cat mai des. In acest fel vom fi protejati de programele care ataca gaurile de securitate existente, deoarece sistemul fiind la zi nu va mai contine vulnerabilitati (cel putin teoretic).

Protectia impotriva virusilor. Evident; folosirea unui antivirus. In conditii normale, un antivirus ar trebui ales in functie de caracteristicile sale (viteza de reactie, metoda de update, pozitia sa intr-un top de specialitate, avantaje/dezavantaje fata de alte produse) si bineinteles de cost.

Protectia impotriva atacurilor. Daca sunt atacuri de tip exploit, update-urile la zi ar trebui sa rezolve problema, daca nu firewall-ul sau antivirusul ar trebui sa le opreasca.
Daca sunt atacuri de tip flood, fiind tinta finala nu avem cum sa le oprim decat comunicand isp-ului problema.

Morala acestei scurte pareri este: folositi produse comerciale licentiate deoarece au un suport tehnic mai bun cat si un grad de securitate mai mare si intotdeauna faceti update la programe.

Universitatea Titu Maiorescu
Facultatea de Stiinta si Tehnologie a Informatiei

Caz real : Windows XP Proffesional (cu licienta) + SP2 + update la zi + Panda Titanium (cu licienta) +LavaSoft Ad-Ware = 1 an + crestere de functionare perfecta.

Pareri legate de companii si retelele acestora

In cadrul unei firme situatia se complica. Securitatea deja trebuie sa existe pe mai multe nivele: cel de retea, cel de acces exterior, cel de acces interior si cel de acces fizic.

- Legat de accesul fizic: daca exista informatii sensibile, acestea trebuie stocate pe servere dedicate care sa fie tinute intr-o locatie sigura. Prin locatie sigura intelegem camera de stocare cu acces limitat pe baza de cheie/cartela eletronica; camera care este supravegheata video non-stop.De asemenea accesul persoanelor autorizate in aceasta camera trebuie sa fie consemnat intr-un jurnal.
- Pentru protectia si backup-ul datelor se recomanda folosirea unui sistem mirror la distanta, aflat intr-un datacenter dedicat sau, daca informatiile sunt prea sensibile, aflat intr-o incinta separata. Spun incinta separata deoarece in cazul unui dezastru natural datele nu trebuie sa se piarda. De asemenea, la o cantitate mare de date importante se poate crea un SAN propriu.
- Accesul angajatilor la resursele informationale cu nivelul de confidentialitate mediu sau mai mare trebuie sa se faca pe baza de logare/autentificare. Acesta autentificare se face fie prin metoda clasica cu user si parola fie prin metode mai moderne cum ar fi amprentele biometrice.
- Metoda de autentificare este de preferat sa fie una centralizata (Ex. Ms. ActiveDirectory) care permite controlul accesului unui utilizator spre fiecare resursa disponibila. Folosind aceasta metoda se obtine un management si un audit mai bun al operatiilor de verificare zilnice.
- De multe ori “compromiterea” vine din interior. In mod voluntar sau involuntar un angajat poate compromite integritatea sistemelor.Din aceasta cauza trebuie sa punem accentul pe securitatea interna a companiei; acest nivel trebuie sa fie cat mai transparent posibil pentru a facilita buna functionare atat a relatiilor sociale cat si a celor informationale din cadrul companiei.
- Legat de securitatea la nivel de access extern. De preferat este o politica cat mai dura de genul “drop all , selective permit”. Serverele interne care nu au nevoie de access la internet sa fie separate logic de restul serverelor; cele de content/mail sa fie puse intr-o structura de firewall DMZ. Daca nu se poate creata o structura DMZ se recomanda a nu li se aloca ip-uri “publice” ci a folosi tehnologii de tip NAT/PAT pentru a controla mai bine accesul IN/OUT al informatiei spre/dinspre servere.
- Canale securizate. O companie cu mai multe puncte de lucru trebuie sa asigure o legatura intre aceste puncte; pentru siguranta, legatura trebuie sa fie si securizata.
  Cel mai des intalnit mod de a interconecta mai multe locatii pe un canal privat de date il reprezinta retelele virtuale private(VPN). Dupa cum spune si numele, conceptul de distanta intre angajati dispare – la nivel electronic cel putin -. Angajatii companiei se vor conecta de acasa, de pe drum sau de la birou la reteaua companiei. Astfel vor avea acces la toate resursele la care intr-un mod clasic ar fi avut doar de la punctul de lucru.

Cea mai des folosita metoda este aceea in care se foloseste un server central pentru autentificare si “poarta de acces la retea”, server care trebuie sa aiba destula latime de banda cat sa suporte cel putin 75% din angajati conectati la retea simultan. In functie de metoda de autentificare aleasa, de metoda de criptare a datelor si de metodele de compresie configuratia hardware a serverului variaza.

Creearea unui VPN se poate face folosind ca transportator o retea publica (internet-ul). Drept urmare, datele circula printr-un mediu public dar intr-o forma criptata; datorita acestui fapt avem acel procent fie mic fie mai mare de nesiguranta legata de confidentialitatea datelor.

Pentru o siguranta sporita exista anumite solutii care ofera o interconectare privata la un nivel mai jos (la nivel layer <3 pe OSI). Dintre acestea amintim : dark fiber (fibra dedicata punct la punct pentru unire a doua locatii), MPLS (Multi Protocol Label Switching).

Concluzie

Securitatea informationala este un domeniu mult prea vast si cu prea multe domenii conexe pentru a fi detaliat complet undeva. Lumea este in continua miscare, cerintele de securitate si confidentialitate cresc pe zi ce trece, amentintarile tin pasul.

Acest scurt articol a avut rolul unei introduceri generale ale principalelor aspecte din securitatea electronica din ziua de azi.

Dumitru Laurentiu
Universitatea Titu Maiorescu
Facultatea de Stiinta si Tehnologie a Informatiei
Anul II