ADOPTAREA ŞI IMPLEMENTAREA STANDARDELOR EUROPENE DE SECURITATE A INFORMAŢIEI, CONDIŢIE ESENŢIALĂ PENTRU DEZVOLTAREA AFACERILOR ON-LINE ALE FIRMELOR DIN ROMÂNIA

drd.ing. Danilescu Laura
Reprezentant Regional zona sud-est
ECDL ROMANIA

Abstract:

E-business demands confidentiality and, integrity for transmitted information. The exponential growing of e-business, rises serious security problems about ensuring a secured business environment via Internet. Even a minority of users would create problems by steeling, erasing or damaging information, those risks are real and will ever be – and will expand with Internet growing.

Customers will agree those companies which offer the best security solution as well as ensure confidentiality, integrity and availability for their information. Now it's imperative that companies possess effective internal controls on what happens to their information. The solution is security standards implementation: BS 7799 / ISO17799.

Concepte cheie:

Societatea Informationala; Economia Internet; tehnnologiile de securitate a informatiei; confidentialitate, integritate si disponibilitate a informatiei.

Societatea Informationala

Lumea se transforma intr-un sat global, unde nu mai exista granite pentru afaceri, comunicatii sau comert.

Cateodata, o noua tehnologie altereaza profund peisajul si planteaza semintele unei schimbari radicale. Astazi este clar ca Internet este o asemenea tehnologie: In istoria comertului, au existat putine salturi majore privind capacitatea companiilor de a schimba informatii intre ele - o cerinta critica pentru conducerea afacerilor. Ultimul avans major a fost

inventia telefonului, in 1885. Astazi, facem un alt pas mare cu Internet. Asistam la o explozie a comertului electronic.

INTERNET, aceasta masiva infrastructira de retele schimba modul in care lumea abordeaza educatia, afacerile si alte activitati. Internet este deja propriul sau stat, cu propria sa economie si propria sa moneda (*digicash*); el modifica modul in care economia mondiala functioneaza.

Extrem de important pentru supravietuirea si succesul unei organizatii este managementul eficient al informatiei si al tehnologiilor informatiei (IT). In aceasta societate a informatiei globale – unde informatia circula prin cyberspatiu fara constrangeri de timp, distanta sau viteza – situatiile critice apar din:

- Dependenta marita de informatie si de sistemele care o furnizeaza
- Vulnerabilitatile crescande si un larg spectru de amenintari
- Costul investitiilor curente si viitoare in informatie si sistemele informationale

Importanta informatiei si a sistemelor de comunicatii pentru societate si economia globala se intensifica odata cu valoarea si cantitatea informatiei transmisa si stocata. Pentru multe organizatii, informatia si tehnologiile care o fac posibila reprezinta cele mai valoroase bunuri ale organizatiei.

In prezent, tot mai multa informatie este stocata si transmisa electronic

Ca societate, devenim din ce in ce mai dependenti de accesul si procesarea rapida a informatiei. Pe masura ce aceasta solicitarea creste, tot mai multa informatie este stocata si transmisa electronic, ceea ce cauzeaza schimbarea modului in care companiile abordeaza afacerile. Spre deosebire de informatia imprimata pe hartie, informatia in forma electronica poate fi potential furata de la distanta si este mult mai usor sa fie interceptat si modificata.

Afacerile electronice (*e-business*), solicita confidentialitate si integritatea pentru informatiile transmise. Cresterea exponentiala a afacerilor pe Internet ridica seriooase chestiuni de securitate in legatura cu asigurarea unui mediu de afaceri securizat via Internet. Deschiderea face Internet-ul vulnerabil la amenintari (spre exemplu, atrage crackerii). Chiar daca numai o minoritate a utilizatorilor va crea probleme organizatiilor prin furtul, stergerea sau alterarea informatiilor, aceste riscuri sunt reale si vor exista intotdeauna – iar pe masura ce Internet creste, aceste riscuri vor creste si ele.

Internet deschide noi modalitati pentru consumatori, firme si guverne. Comenzile si platile electronice pot fi administrate eficient si facil; posta electronica si paginile web au devenit resurse institutionale. Cu toate acestea, pana cand protectia si securitatea informatiilor nu vor fi asigurate, beneficiile comunicatiilor si afacerilor electronice nu vor fi depline.

Economia Internet

Sistemele de informatii legate in retele sunt rapid adoptate de organizatii in intreaga lume pentru a imbunatatii comunicatiile, eficienta, controlul oeprational si – in final - competitivitatea. Realizarea afacerilor pe Internet este rapida si la costuri relativ reduse - motive suficiente, irezistibile pentru ca firmele sa considere afacerile electronice ca alternative viabile.

Economia Internet a crescut mai rapid decat se intrevedea acum cativa ani. Ceea ce a pornit ca un canal alternativa pentru marketing s-a transformat rapid intr-un sistem economic complet constand din:

- comunicatii atot-cuprinzatoare, retele de comunicatii la preturi scazute, care folosesc tehnologiile si standardele Internet,
- aplicatii si capital uman care permite conducerea afacerilor prin acesta infrastructira de retele,
- piete electronice interconectate care opereaza folosind infrastuctura de retele si aplicatii existenta,
- producatori si intermediari care furnizeaza o mare varietate de produse si servicii pentru a facilita eficienta si lichiditatea,
- un cadru legal, inca in formare, pentru conducerea afacerilor electronice.

Folosirea Internet-ului si a altor mijloace de comunicare aduce numeroase beneficii si permite obtinerea de avantaje concurentiale. Internet permite firmelor sa isi largeasca afacerile in moduri care nu ar fi fost posibile inainte. Este o noua lume a afacerilor, una plina de posibilitati, facuta posibila de emergenta mediilor de calcul distribuite, unde firmele pot beneficia de comunicatii rapide, metode avansate de colectare a datelor, lanturi de furnizori electronice si alte avantaje ale acestei noi ere a procesarii informatiei. Aceste solutii au marit – si vor mari in continuare – eficienta cu care firmele opereaza si rezultatele lor financiare – dar ele au marit si riscul de securitate informatica.

Aceste conectari sunt nediscriminatorii; ele traverseaza frontiere si conecteaza firme, scoli, camine si guverne. Cu aceasta explozie in conexiunii vine accesul. Intocmai cum un

telefon poate accesa orice alt telefon pe glob, orice calculator poate, potential, accesa si schimba informatii cu alte calculatoare interconectate. Nu exista nici un control al accesului in retele precum Internet. Fiecare calculator individual trebuie sa solicite autentificare si autorizare a accesului.

Proliferarea calculatoarelor la preturi din ce in ce mai mici si dramatica expansiune a interconectivitatii au exacerbat problemele de acces neautorizat si alterarea a informatiilor. Dezvoltarile tehnologice au marit mult securitatea sistemelor informatice, dar, in acelasi timp, au dat potentialilor atacatori sansa unor penetrari mult mai rapide in sistemele informatice (fie ele personale, guvernamentale sau ale firmelor), aceasta cu efecte, in unele cazuri, foarte serioase. Conectivitatea permite acces la o multime de resurse, rapid si eficient, dar ea permite si o cale de acces [Power, 1995] in care atacatorii pot surpasa sistemele de autentificare desemnate sa protejeze sistemele.

Frecventa atacurilor care dauneaza financiar sau in alte moduri organizatiile este in crestere. Organizatile sunt atacate atat din interior cat si din exteriorul perimetrului lor electronic,
iar protejarea impotriva unor asemenea atacuri solicita mai mult decat simpla folosire a tehnologiilor de securitate informatica.

Securitatea informatica furnizeaza procesele manageriale, tehnologia si asigurarea ca se poate avea incredere in tranzactiile de afaceri; asigura ca serviciile informatice sunt utilizabile si pot rezista adecvat unor probleme cauzate de erori, atacuri deliberate sau dezastre; asigura ca accesul la informatie este permis numai celor care trebuie sa aiba acces”

Tehnologiile de securitate a informatiei bine folosite inseamana pentru companii pastrarea reputatiei, a potentialului si evitarea unor pierderi financiare. Consecintele incidentelor de securitate informatica pot fi dezastruoase – dar ele pot fi evitate. Vechile metode de securitate informatica raman importante, dar pe masura ce firmele dobandesc o noua identitate virtuala, acestea nu mai sunt suficiente.

Despre importanta tehnologiilor de securitatea a informatiei

Informatia, produsele informatiei, precum si costurile si beneficiile rezultate din informatie devin din ce in ce mai mult transnationale. Informatia este “putere”, ea are o valoare, iar capacitatea de a stoca si procesa anumite informatii poate furniza un important avantaj asupra competitorilor.

Informatia este utila doar atat timp cat ramane valida, nealterata. Unul dintre modurile cele mai insidioase pentru un competitor de a obtine avataje consta in sabotarea bazelor de date ale rivalilor in moduri subtile; impactul unor asemenea actiuni poate fi devastator.

Informatia este un bun foarte important, in consecinta trebuie protejat adecvat pentru a asigura continuitate, a minimiza posibile daune si a maximiza beneficiile si oportunitatile de afaceri.

Cu toate ca intruziunile informatice pot avea costuri foarte ridicate, multe firme nu au alocat resurse suficiente pentru a se proteja. Situatia este in schimbare, iar ceea ce odata a fost vazut doar ca o durere de cap, capata o importanta din ce in ce mai mare – aceasta nu reprezinta o surpriza deoarece tehnologiile de securitate a informatiei sunt considerate astazi un important factor, de care depinde succesul unei organizatii.

In mediul de afaceri electronice din zilele noastre, tehnologiile de securitate a informatiei pot servi la obtinerea de profituri si noi oportunitati de afaceri, nu numai sa reduce riscurile. Tehnologiile de securitate a informatiei nu vizeaza doar prevenirea dezastrelor, ci ele reprezinta mijloace de realizare a obiectivelor de afaceri. Tehnologiile de securitate a informatiei sunt absolut necesare pentru asigurarea succesului, prin urmare ele trebuiesc incluse in procesul de gandire strategica a firmelor. Securitatea informatica trebuie vazuta ca un proces care este esential in indeplinirea nevoilor legitime ale partenerilor si clientilor si nu ca ceva care “poate fi adaugat”. Pe de alta parte, companiile trebuie sa trebuie sa se asigure ca departamentele lor de marketing si relatii cu publicul sunt versate in principiile tehnologiilor de securitate a informatiei pentru a putea comunica efectiv publicului masurile care sunt luate pentru a proteja banii si intimitatea clientilor. In afara de ratiuni comerciale, firmele au obligatii legale sa asigure protectia datelor personale ale clientilor lor.

Tehnologiile de securitate a informatiei au mai multe componente si atribute care trebuiesc considerate cand se analizeaza riscul potential. In linii mari, acestea pot fi clasificate in trei mari categorii:

Confidentialitatea - protectia informatiilor in sistem astfel incat persoane neautorizate nu le pot accesa. Este vorba despre controlarea dreptului de a citi informatiile. Aproape fiecare organizatie are informatii care, daca sunt divulgate sau furate, ar putea avea un impact semnificativ asupra avantajului competitional, valorii de piata sau a veniturilor. Aditional, o firma poate fi facuta responsabila pentru divulgarea de informatii private. Aspecte cruciale ale confidentialitatii sunt indentificare si autentificarea utilizatorilor.

Integritatea - protectia informatiilor impotriva modificarilor intentionate sau accidentale neautorizate. Este vorba despre nevoia de a se asigura ca informatia si programele sunt modificate numi in maniera specificata si autorizata si ca datele prezente sunt originale, nealterate sau sterse in tranzit. Ca si in cazul confidentialitatii, identificarea si autentificarea utilizatorilor sunt elemente cheie ale unei politici de integritatea a informatiilor.

Disponibilitatea – se refera la asigurarea ca sistemele de calcul sunt accesibile utilizatorilor autorizati cand si unde acestia au nevoie si in forma necesara (conditia ca informatia stocata electronic este unde trebuie sa fie, cand trebuie sa fie acolo si in forma necesara).

Importanta pe care fiecare dintre aceste cerinte o joaca in cadrul operatiilor unei firme (si de aici nivelul de perturbare potential) depinde de la industrie la industrie si de la firma la firma. Obiectivul tehnologiilor de securitate a informatiei consta in protejarea intereselor celor care se bazeaza pe informatii impotriva daunelor care pot rezulta din incapacitatea de a se asigura disponibilitatea, confidentialitatea si integritatea informatiilor.

PERSPECTIVE

In viitorul apropiat nu se intrevede o scadere a numarului de inovatii si a complexitatii aplicatiilor si echipamentelor. Internetul va continua sa creasca atragând un numar record de utilizatori, echipamente, conexiuni si aplicatii in timp ce arhitectura de baza va ramâne intr-o stare de fluctuatie continua. Altfel spus, incarcarea va creste continuu chiar daca elementele infrastructurii nu au timp suficient sa se stabilizeze si sa fie complet testate. Utilizatorii si infrastructura vor continua sa fie sub o presiune constanta din partea hackerilor si rauvoitorilor care vor avea acces la unelte de atac din ce in ce mai puternice. Retelele publice si private vor fi si mai interconectate. Astfel, securitatea unei retele va depinde si mai mult de securitatea altor retele cu care are contact direct sau indirect. Fara granite fizice si cu o multitudine de legi neuniforme (in cazul in care exista) in statele unde se afla retele, in viitorul apropriat va ramâne inca dificil sa depistam si sa condamnam criminalii informatici.

Cumparatorii se vor indrepta spre producatorii care ofera pe lânga produsele lor si cea mai buna solutie pentru un anumit segment de securitate, in pofida celor care ofera solutii de tipul toate intr-una, care s-au dovedit neadaptate realitatii.

Ca urmare a noilor reglementari in domeniul securitatii TI (cum ar fi semnatura electronica), se vor accelera cererile de solutii de securitate. De asemenea, vor continua seria de fuziuni si preluari de companii din domeniul securitatii TI.

Experiente care nu trebuie ignorate

- Conform Datamonitor, pierderile globale produse de actiunile hackerilor, virusilor si a altor brese de securitate in domeniul informatiilor depasesc 15 mld.$ anual.
- 7% din veniturile anuale se pierd datorita lipsurilor in securitatea sistemelor informatice ale firmelor (conform Omni Consulting, pe baza unui studiu efectuat asupra a 3.000 de companii).
- Virusul "I Love You" a produs companiilor pierderi directe de 960 mil.$ si de productivitate de 7,7 mld.$. Paguba in primele 5 zile a fost de 6,7 mld.$ (conform Computer Economics).
- Europenii au pierdut 267,5 mil.$ in 2000 datorita fraudelor asupra cartilor de credit folosit on-line ca urmare a slabei securitati a siturilor web si a breselor de securitate (conform Uniunii Europene).
- Pierderea medie per victima fraudata prin Internet a fost de 665$ (conform Internet Fraud Complaint Center).
- Industria din intreaga lume a pierdut aproximativ 1,2 mld.$ datorita atacurilor DoS asupra comertului electronic (conform estimarii Yankee Group).
- Vânzatorii de aplicatii software au pierdut aproximativ 12,2 mld.$ in 1999 datorita pirateriei software (conform estimarii International Planning and Research).
- Din totalul de companii care efectueaza afaceri on-line, 99% se tem de fraudele on-line, dar 60% dintre ele cheltuiesc mai putin de 1% din veniturile lor pentru prevenirea lor (conform Worlwide E-Commerce Fraud Prevention Network).

Se observa ca solutiile tehnologice, echipamentele si produsele deja existente nu sunt suficiente pentru a asigura un management eficace al securitatii informationle. Devine acum o necesitate imperativa pentru companii instalarea unui sistem de securitate efectiv. Solutia: implementarea standardelor de securitate BS 7799/ ISO 17799.