BS7799-2/ISO17799 şi auditul Planului de Securitate

Lect.dr. Adrian MUNTEANU
Catedra de Informatică Economică, Universitatea „Al. I. Cuza" Iaşi

Deşi standardele şi auditul amintite în titlu abia au început să-şi facă simțită prezența pe piața autohtonă, unii din partizanii BS au început să se *inflameze* lansând prematur o modă care nu a prins în totalitate nici la casele mai mari. Sau în cel mai fericit caz să-şi promoveze ori de câte ori au ocazia *produsul* pe motiv că cine are BS are în mod automat şi securitate informatică. Dincolo de marketing-ul necesar oricărui produs nou care apare pe piață, realitatea e puțin mai complicată decât pare la prima vedere.

Mitul BS

Înainte de a intra în alte detalii mi-am propus să clarific mitul care a luat naştere pe piața românească IT&C începând cu 2003-2004, odată cu apariția OMF1077/2003 respectiv OMCTI 218/2004.

British Standard Institution (BSI) a dezvoltat la începutul anilor '90 o serie de standarde ca răspuns la cererea industriei, guvernului şi mediului de afaceri de a crea o structură comună pentru securitatea informațiilor. În 1995, autoritatea de reglementare din Marea Britanie a adoptat în mod oficial **BS7799.** Cu toate acestea, de atunci şi până astăzi, standardul nu a fost şi nici nu este mandatar nici măcar pentru companiile din țara mamă.

Pe piața autohtonă s-a lansat ideea că, dacă o companie este certificată/evaluată (conformă) în baza BS7799 şi are un sistem informațional în conformitate cu acest standard, în mod automat sistemul informațional este *sigur!* Mi se pare cam forțată această afirmație.

În primul rând nu poate afirma nimeni, despre nici un sistem, că ar fi 100% sigur. Fiind o colecție a celor mai bune practici din domeniul *managementului securității informaționale*, BS7799 oferă de fapt sprijin organizațiilor în adoptarea unor controale interne mai eficiente. Sunt destule voci care critică acest standard pentru că nu are cum să acopere toate spețele legate de securitatea informațională, evoluția tehnologică fiind mult mai rapidă. Mai mult, la sfârşitul acestui an se aşteaptă să fie lansată Partea a 3 a acestui standard care să integreze auditul şi managementul securității informaționale cu alte sisteme de management.

BS7799 nu trebuie văzut ca un certificat de *bună purtare*! Este un standard public şi a reprezentat baza pentru standardul internațional ISO 17799. Acest lucru nu poate fi contestat. Sunt avantaje reale care rezultă ca urmare a conformării cerințelor acestui standard. Dar în acelaşi timp, pe piața românească BS a fost adoptat de o mulțime de firme care oferă consultanță în domeniu, pe post de panaceu al securității informaționale şi, nu în ultimul rând, o sursă bună de venituri (a se vedea www-ul): cursuri, instruire, certificare etc.

Înainte de a prezenta realitatea mai trebuie să amintesc că în decembrie 2000 ISO a preluat primele 4 părți ale BS şi le-a publicat sub numele „ISO 17799". Pe la sfârşitul anului 2002 partea a doua a BS 7799 a fost revizuită pentru a reflecta şi prevederile ISO 9001: 2000, ISO 14001: 1996 şi principiile OECD.

Realitatea BS

BS 7799 este alcătuit din două părți. BS7799 Part 1: 2000 se numeşte „Code of Practice" şi enumără un set de practici de care *se poate ține cont* şi care *pot fi implementate* în diverse situații.

Acest cod a fost adoptat şi de către ISO devenind, după cum spuneam, ISO 17799. La această oră nu există nici o schemă de certificare disponibilă pentru ISO 17799 deoarece nici acesta nu este un standard mandatar.

BS7799 Part 2: 2000 se intitulează „Specification for Information Security Management Systems" şi a fost dezvoltat pentru companiile din Marea Britanie care doreau să se pregătească pentru certificare în conformi-

tate cu BS7799. În concluzie, atunci când se vorbeşte pe piaţă despre certificare/conformitate BS, se are în vedere Partea a 2 a Standardului şi nu ISO 17799. Certificatul este eliberat de BSI sau de către un evaluator calificat şi acreditat BS7799. La fiecare 3 ani organizaţia trebuie recertificată.

BS7799: 2000 este organizat în 10 secţiuni care acoperă următoarele domenii:

1. *Politica de Securitate*: orice organizaţie *trebuie* să aibă un document care să definească şi să explice securitatea informaţională.
2. *Securitatea organizaţională*: defineşte principiile care stau la baza managementului securităţii în orice organizaţie.
3. *Securitatea personalului*: descrie cerinţele legate de recrutarea şi instruirea angajaţilor, managementul incidentelor din sistem.
4. *Securitatea fizică şi a mediului de lucru*: sunt avute în vedere controalele generale implementate în cadrul organizaţiei.
5. *Managementul operaţional şi al comunicaţiilor*: acoperă procedurile documentate cu privire la operarea la calculator şi comunicarea informaţiilor.
6. *Controlul accesului*: principiile care guvernează accesul securizat la informaţii.
7. *Dezvoltarea şi întreţinerea sistemelor*: cerinţele legate de securitate trebuie avute în vedere în fiecare etapă a ciclului de viaţă al unui sistem.
8. *Planificarea continuităţii afacerii*: analiza de impact, proceduri de refacere, testare
9. *Conformitatea***:** securitatea informaţională trebuie să fie conformă cu orice prevedere legală aplicabilă. Pentru a fi în conformitate cu BS7799 Part 2, o organizaţie trebuie să aibă implementat şi documentat propriul sistem de management al securităţii informaţionale în conformitate cu obiectivele de control stipulate în Clauza 4 a standardului BS.
10. *Certificarea BS* este cea care oferă probe şi asigurări că o organizaţie a atins obiectivele controlului stipulate în standard. Aceasta presupune realizarea unui audit de către un evaluator independent care va verifica implementarea controalelor stipulate în Standard. Procesul prin care se poate obţine conformitatea cu acest standard este similar cu obţinerea certificării ISO 9000.

Etapele obţinerii acestei certificări pot fi sintetizate astfel:

- Organizaţia decide să implementeze prevederile BS7799.
- Odată luată această decizie, conducerea trebuie să desemneze o echipă care să elaboreze Politica de Securitate a organizaţiei.
- Acest document trebuie revizuit, aprobat şi adus la cunoştinţa tuturor angajaţilor.
- Organizaţia trebuie să decidă apoi care componentă organizaţională va fi supusă certificării BS (Scopul certificării).
- Acest scop trebuie documentat, rezultând *ISMS Scope Document* (Scopul Sistemului de Management al Securităţii Informaţionale).
- În cadrul acestui Scop trebuie identificate activele organizaţiei (şi valoarea asociată acestora) care trebuie protejate (Inventarul activelor).
- Pentru acest inventar se va realiza Analiza de Risc: ameninţările, vulnerabilităţile şi impactul asupra activelor ce trebuiesc protejate.
- În baza rezultatului acestei analize se identifică riscul acceptabil.
- Se documentează controalele care vor fi implementate pentru a menţine riscurile în limite acceptabile. Acestea vor fi preluate din *BS7799* sau din *alte documente* recunoscute ca fiind „cele mai bune practici" ale domeniului.
- Fiecare control considerat relevant trebuie să se adreseze unui risc.
- După completarea acestor etape se trece la implementarea controalelor.
- După implementarea controalelor se realizează Analiza breşelor pentru a identifica controalele care nu au fost implementate în totalitate sau pentru care utilizatorii necesită instruire.
- Se implementează acţiunile corective prin care se remediază situaţiile identificate anterior.
- Toată documentaţia se pune la dispoziţia unei firme/evaluator care este acreditată să ofere certificare în baza BS7799.
- Auditorii firmei vor efectua o verificare formală prin care certifică existenţa fizică a controalelor documentate.

- Dacă situaţia faptică este conformă cu documentaţia se eliberează certificatul de conformitate.

Auditul

De la jumătatea anului 2003 auditul sistemelor informaţionale şi profesiunea de auditor (CISA – Computer Information System Auditor) au devenit realitate şi în România. Companiile care doresc să emită facturi într-un singur exemplar pe suport clasic sau băncile care apelează la soluţii de tip mobile banking au nevoie de serviciile CISA.

„A fost întocmit un raport de audit asupra planului de securitate, efectuat de o echipă formată din personal independent, specializat şi atestat. Prin atestare se înţelege certificarea personalului ca auditor de sisteme informatice, oferită de Asociaţia de Audit şi Control al Sistemelor Informatice (ISACA) - Information Systems Audit and Control Association. (OMFP1077/2003, art.1, lit. g)"

„Opinia de audit menţionată la art. 5 lit. f[1]) va fi întocmită de către o persoană certificată ca auditor de sisteme informatice (CISA). În procesul de auditare, auditorul poate solicita concursul unor experţi (OMCTI 218/2004, art. 6 al. 1)

Acestea sunt extrase din singurele (din nefericire) acte normative care fac referire la *auditul sistemelor informaţionale*, mai precis la *auditul planului de securitate* al unei organizaţii. Actele normative menţionate nu fac referire la nici un standard. Legiuitorul român doreşte din partea unui CISA exprimarea unei opinii cu privire la *planul de securitate* al organizaţiei şi nu asupra *sistemului de management al securităţii*. Altfel spus, se doreşte o opinie independentă cu privire la planul de securitate al unei organizaţii.

Aşa stând lucrurile, CISA va face apel la standardele ISACA (Information System Audit and Control Association) şi la CobIT (Control Objectives for Information Technology) şi va efectua un *audit de conformitate* cu prevederile respectivelor acte normative şi nu cu BS7799. Aceasta deoarece cele două Ordine prezintă şi conţinutul Planului de securitate ce trebuie realizat de organizaţii şi auditat de către CISA!

Concluzie

BS7799-2 este un standard managerial pentru protejarea activelor informaţionale ale organizaţiilor. Având în vedere că atât conformitatea cât şi certificarea sunt procese continue şi costisitoare, organizaţiile trebuie să-şi analizeze foarte bine beneficiile rezultate în urma unui astfel de proces. Nu certificarea realizată de către evaluator este cea consumatoare de resurse financiare ci implementarea controalelor care să conducă la conformitatea cu prevederile standardului.

Odată certificată o organizaţie nu se poate considera sigură. Poate însă dovedi în faţa terţilor că are implementate controalele necesare să-i diminueze riscurile legate de utilizarea IT&C în afacere. Pentru un auditor, conformitatea sau certificarea BS pe care o deţine o organizaţie reprezintă un punct de plecare în planificarea misiunii sale. Dar nu şi o garanţie a securităţii sistemului.

Scopul oricărui audit, deci şi cel al planului de securitate, îl reprezintă identificarea riscurilor componentei auditate şi asigurarea că riscul rezidual este *acceptabil* pentru cel care a cerut să fie auditat.

Bibliografie

www.mcti.ro
www.bsi-global.com
www.itsecurity.com
www.isaca.org

[1] Asupra planului de securitate