Analiza standardelor de securitate

Security Standards Analysis

Ioan-Cosmin MIHAI
"A.I. Cuza" Police Academy, Bucharest, Romania
cosmin.mihai@academiadepolitie.ro

Abstract

Cybersecurity standards help organizations to define and to practice security techniques to minimize the impact of informatics attacks. This paper analyzes the importance of security in the informatics domain and the series of standards ISO 27000.

Index terms: information security, security standards, ISO 27000

1. Importanța securității în domeniul informatic

Societatea îmbrățișează din ce în ce mai mult tehnologia informației. Informația, care până nu de mult avea la bază hârtia, îmbracă acum forma electronică. De aproximativ 15 ani, infrastructurile de comunicații s-au extins de la nivelul intern al organizațiilor (Intranet) către conectarea globală la nivelul Internet-ului, în special în cazul companiilor întinse pe arii geografice largi. Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil și un mijloc de comunicare atrage după sine riscuri specifice. Utilizarea Internet-ului în domenii vitale (sănătate sau militar) precum și în scopuri comerciale (sisteme bancare sau comerț electronic), a crescut acest potențial de risc.

Posibilitatea de accesare rapidă, în orice moment, a informației, precum și necesitatea de a asigura protecția acesteia împotriva furtului sau distrugerii au devenit cerințe care nu existau atunci când rețeaua și serviciile sale au fost create. Dependența puternică de informație și comunicații duce la urmări de o gravitate crescută a cazurilor de furt, modificare sau distrugere a informației, precum și deteriorare sau întrerupere a canalelor de comunicație. Sistemele informatice, indiferent de natura acestora, s-au dovedit de-a lungul timpului vulnerabile la atacuri, la accesări neautorizate ale informațiilor, la modificări ori distrugeri de informații, accidentale sau voite. Atenuarea și corectarea acestor vulnerabilități au devenit astăzi obligații ale oricărei organizații care deține calculatoare legate în rețea. Protejarea informației reprezintă așadar o activitate din ce în ce mai importantă, dat fiind faptul că ea poate circula printr-o rețea neprotejată cum este Internet-ul.

Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității și disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control.

Dezvoltarea tehnologică a fost acompaniată și de soluții de securitate, producătorii de echipamente și aplicații incluzând metode tehnice de protecție din ce în ce mai performante. Totuși, asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă

umană. De multe ori incidentele de securitate sunt generate de o gestiune și organizare necorespunzătoare și mai puțin din cauza unei deficiențe a mecanismelor de securitate.

Este important ca organizațiile ce utilizează Internetul să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect printr-o conștientizare în rândul angajaților a importanței securității informațiilor, înțelegerea tipologiei amenințărilor, riscurilor și vulnerabilităților specifice mediilor informatizate și aplicarea practicilor de control.

În urma implementării unor mecanisme de securitate într-o rețea de calculatoare, informațiile nu vor putea fi accesate sau interceptate de persoane neautorizate (curioase sau, eventual, chiar rău intenționate) și se va împiedica falsificarea informațiilor transmise sau utilizarea clandestină a anumitor servicii destinate unor categorii specifice de utilizatori ai rețelelor.

Informația este o valoare cu o importanță deosebită pentru o persoană fizică sau pentru o organizație și, în consecință, necesită o protecție adecvată. Securitatea informației protejează informația de o gamă largă de amenințări. În acest context, securitatea informației este caracterizată ca fiind cea care asigură și menține următoarele proprietăți:

- confidențialitate: proprietatea ca informația să nu fie disponibilă sau dezvăluită unor persoane, entități sau procese neautorizate;
- integritate: proprietatea de păstra acuratețea și completitudinea resurselor;
- disponibilitate: proprietatea de a fi accesibil și utilizabil la cerere de către o entitate autorizată.

Securitatea informației este obținută prin implementarea unui set adecvat de politici, practici, proceduri, structuri organizaționale și funcții software. Aceste elemente trebuie implementate în măsura în care se asigură atingerea obiectivelor specifice de securitate.

Problema de securitate a informației trebuie să aibă în vedere de multe ori partajarea informațiilor sau interconectarea rețelelor private cu serviciile publice. Multe din sistemele existente pe piață au fost proiectate fără a avea ca principal obiectiv asigurarea unui anumit grad de securitate pentru că la momentul respectiv tehnologia nu era atât de dezvoltată și nici atât de accesibilă tuturor.

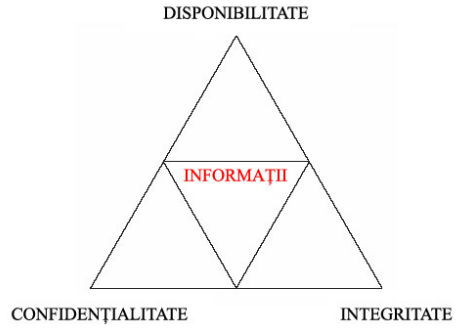

Fig. 1. Proprietățile securității informațiilor

Odată însă cu dezvoltarea Internet-ului ca și mijloc important al comunicării moderne, nevoia unor mecanisme de securitate a devenit o certitudine. În practică se apelează la soluții tehnice externe care să rezolve problemele de securitate fără a căuta să se identifice nevoile și cerințele specifice.

2. Analiza standardelor de securitate

Datorită numeroaselor tipuri de atacuri existente la ora actuală în domeniul informatic, s-a simțit nevoia de existența unei politici de securitate a informației pentru toate organizațiile. În acest sens Organizația Internațională pentru Standardizare (ISO) împreună cu Comisia Internațională Electrotehnică (IEC) formează un sistem internațional specializat pentru standardizarea mondială. Organismele naționale care sunt membre ale ISO și IEC participă la dezvoltarea standardelor internaționale prin intermediul comitetelor tehnice. Astfel, Statele Unite ale Americii, prin Institutul Național de Standardizare, ocupă poziția de Secretar, 24 de țări au statut de Participanți (Brazilia, Franța, Regatul Unit al Marii Britanii, Coreea, Cehia, Germania,

Danemarca, Belgia, Portugalia, Japonia, Olanda, Irlanda, Norvegia, Africa de Sud, Australia, Canada, Finlanda, Suedia, Slovenia, Elveția, Noua Zeelandă și Italia) și alte 40 de țări au statut de Observatori.

Primul standard privind managementul securității informației a fost standardul britanic BS 7799. Acesta a avut doua părți:

- BS 7799-1, care era un cod de practică, devenit in anul 2005 ISO/IEC 17799. În prezent, acestui standard i s-a schimbat numele în ISO/IEC 27002 pentru a face parte din seria ISO 27000 dedicată securității informației;

- BS 7799-2, acesta fiind primul standard după care se putea efectua certificarea unei organizații. Pe baza acestuia s-a elaborat primul standard oficial de certificare pentru un sistem de management al securității informației: ISO/IEC 27001.

În acest moment, din seria ISO 27000 de standarde dedicate securității informației fac parte următoarele standarde:

- **ISO/IEC 27000:2009** – Sisteme de management al securității informației – Prezentare generală și vocabular;

- **ISO/IEC 27001:2005** – Specificații ale sistemelor de management al securității informației;

- **ISO/**IEC **27002:2005** – Codul practică pentru managementul securității informației;

- **ISO/IEC 27003:2010** – Ghidul de implementare a sistemului de management al securității informației;

- **ISO/IEC 27004:2009** – Managementul securității informației – Evaluări;

- **ISO/IEC 27005:2008** – Managementul riscului securității informației;

- **ISO/IEC 27006:2007** – Cerințe pentru organizațiile ce efectuează audit și certificare a sistemelor de management al securității informației;

- **ISO/IEC 27011:2008** – Ghidul managementului securității informației pentru organizațiile din domeniul telecomunicațiilor bazat pe standardul ISO/IEC 27002.

- **ISO/IEC 27032:2012 –** Tehnici de securitate – Ghid pentru securitatea cibernetică.

ISO/IEC 27000:2009 – Tehnologia informației – Tehnici de securitate – Sisteme de management al securității informației – Prezentare generală și vocabular

Acest standard oferă o imagine de ansamblu a sistemelor de management al securității informației ce fac obiectul familiei de standarde ISMS (Sisteme de Management a Securității Informației) și definește termenii din domeniu.

Un sistem de management al securității informației (ISMS) reprezintă o abordare sistematică a managementului informației astfel încât aceasta să îndeplinească cele 3 aspecte ale securității: confidențialitatea, integritatea și disponibilitatea. Sistemul de management al securității informației implică atât echipamentele hardware și procesele software, cât și întregul personal al unei organizații ce are acces la sistemul informațional.

Ca rezultat al implementării standardului ISO/IEC 27000:2009, toate tipurile de organizații (de exemplu societățile comerciale, agențiile guvernamentale sau organizațiile non-profit) pot obține:

- o imagine de ansamblu asupra familiei ISMS de standarde;

- o introducere în sistemele de management al securității informației (ISMS);

- o scurtă descriere a procesului PDCA – Plan-Do-Check-Act (Planifică-Implementează-Verifică-Acționează);

- o înțelegere a termenilor și definițiilor utilizate în întreaga familie ISMS de standarde.

Edward Humphreys, președinte al grupului de lucru care a dezvoltat acest standard, comentează:

“Tehnicile de securitate standardizate devin cerințe obligatorii pentru comerțul electronic, mediul sanitar, telecomunicații,

sectorul auto si multe alte domenii industriale, comerciale sau guvernamentale.

Standardul ISO/IEC 27000:2009 împreuna cu standardele din familia ISO/IEC 27000 are scopul de a ajuta organizațiile să obțină un nivel cât mai ridicat al securității informaționale".

Obiectivele standardului ISO/IEC 27000:2009 sunt de a oferi termeni, definiții și o introducere în familia ISMS de standarde care:

- definesc cerințele pentru sistemele de management a securității informației și pentru cele care certifică aceste sisteme;
- oferă suport, îndrumare detaliată și/sau interpretare a cerințelor și proceselor PDCA;
- oferă îndrumări pentru secțiunile specifice din familia ISMS de standarde;
- oferă evaluări pentru familia ISMS.

ISO/IEC 27001:2005 – Tehnologia informației – Tehnici de securitate – Specificații ale sistemelor de management al securității informației

Standardul ISO/IEC 27001:2005 (fostul BS 7799-2:2002) specifică cerințele pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui sistem de management al securității informației documentat în contextul riscurilor generale de afaceri ale organizațiilor. Acest standard specifică cerințele pentru implementarea unor controale de securitate personalizate nevoilor organizațiilor.

ISO/IEC 27001:2005 este menit să asigure selecție de controale de securitate adecvate ce protejează informațiile și oferă încredere părților interesate.

Este potrivit pentru diferite tipuri de utilizare, inclusiv pentru:

- formularea obiectivelor și cerințelor de securitate a organizațiilor;
- asigurarea că riscurile de securitate sunt gestionate în mod eficient din punct de vedere al costului;
- asigurarea unei conformități cu legislația și diverse reglementări;
- implementarea și gestionarea proceselor existente de management al securității informației;
- definirea de noi procese de management al securității informației;
- identificarea și clarificarea proceselor existente de management al securității informației;
- utilizarea lui de către conducerea organizațiilor pentru a determina starea activităților de management al securității informației;
- utilizarea de către auditorii interni și externi ai organizațiilor pentru a determina gradul de conformitate cu politicile, directivele și standardele adoptate de către organizație;
- furnizarea de informații relevante despre politicile de securitate a informației, directivele, standardele și procedurile către partenerii comerciali și alte organizații cu care organizația interacționează, din motive operaționale sau comerciale;
- punerea în aplicare a afacerii, activând securitatea informației;
- furnizarea de informații relevante despre securitatea informației clienților organizației.

ISO/IEC 27002:2005 – Tehnologia informației – Tehnici de securitate – Codul practică pentru managementul securității informației

Standardul ISO/IEC 27002:2005 este fostul standard ISO/IEC 17799:2005 căruia i s-a schimbat numele pentru a face parte din seria ISO 27000 dedicată securității informației. Stabilește principiile generale pentru inițierea, implementarea, menținerea și îmbunătățirea managementului securității informației într-o organizație.

Obiectivul său este să furnizeze indicații generale privind obiectivele general acceptate în managementul securității informațiilor. Standardul ISO/IEC 27002:2005 conține cele mai bune practici de control în următoarele domenii de management al securității informației:

- politica de securitate;

- organizarea securității informației;
- managementul activelor;
- securitatea resurselor umane;
- securitatea fizică și a mediului înconjurător;
- managementul comunicațiilor și al operațiilor;
- controlul accesului;
- achiziționarea sistemelor informaționale, dezvoltarea și mentenanța lor;
- managementul incidentelor de securitate a informațiilor;
- managementul afacerii continue.

Obiectivele de control în standardul ISO/IEC 27002:2005 sunt destinate să fie puse în aplicare pentru a îndeplini cerințele identificate printr-o evaluare a riscului. Standardul este conceput ca un ghid practic pentru dezvoltarea standardelor de securitate organizațională și practicele efective de management al securității și pentru a ajuta la construirea încrederii în activități inter-organizaționale.

ISO/IEC 27003:2010 – Tehnologia informației – Tehnici de securitate – Ghidul de implementare a sistemului de management al securității informației

Standardul ISO/IEC 27003:2010 se concentrează pe aspectele critice necesare pentru proiectarea și implementarea cu succes a unui sistem de management al securității informațiilor (ISMS), în conformitate cu ISO/IEC 27001:2005.

Acesta descrie procesul de design și specificații pentru un sistem de management a securității informațiilor de la inițiere și până la realizarea planurilor de implementare. Standardul ISO/IEC 27003:2010 descrie procesul de obținere a aprobării de implementare a unui ISMS, definește proiectul de implementare și oferă îndrumări cu privire la modul de concepere a unui proiect ISMS.

Președintele grupului de lucru ce a dezvoltat ISO/IEC 27003, prof. Edward Humphreys, a precizat:

"Prin utilizarea ISO / IEC 27003:2010, organizația va fi capabilă să dezvolte un proces pentru gestionarea informațiilor de securitate, oferind părților interesate asigurarea că riscurile legate de activele informaționale sunt menținute în permanență în parametrii optimi de siguranța, limite stabilite de însăși organizația implementatoare".

Standardul ISO/IEC 27003:2010 este destinat de a fi utilizat împreună cu standardele ISO/IEC 27001:2005 și ISO/IEC 27002:2005, fără a modifica sau elimina nicio prevedere stipulată de cele două standarde.

Acest standard oferă concepte legate de planificarea și proiectarea unui sistem de management al securității informației, rezultând într-un final un plan riguros de implementare a unui proiect ISMS.

ISO/IEC 27004:2009 – Tehnologia informației – Tehnici de securitate – Managementul securității informației – Evaluări

Standardul ISO/IEC 27004:2009 oferă îndrumări cu privire la dezvoltarea și utilizarea unor măsuri și măsurători în scopul de a evalua eficacitatea unui sistem de management al securității informației ISMS implementat. Acest standard oferă îndrumări în privința unor controale sau grupuri de controale așa cum se specifică în standardul ISO/IEC 27001. Standardul ISO/IEC 27004:2009 se aplică tuturor tipurilor de organizații.

ISO/IEC 27005:2008 – Tehnologia informației – Tehnici de securitate – Managementul riscului securității informației

Standardul ISO/IEC 27005:2008 stabilește ghidul pentru managementul riscului securității informației. Susține conceptele generale specificate în ISO/IEC 27001 și este conceput pentru a asista la punerea cu succes în aplicare a securității informațiilor bazate pe o abordare de management al riscului.

Cunoaşterea de concepte, modele, procese şi terminologia descrisă în ISO/IEC 27001 şi ISO/IEC 27002 este importantă pentru o înţelegere completă a ISO/IEC 27005:2008. Acest standard este aplicabil tuturor tipurilor de organizaţii (societăţi comerciale, agenţii guvernamentale sau organizaţii non-profit) care intenţionează să gestioneze riscurile care ar putea compromite securitatea informaţiilor dintr-o organizaţie.

ISO/IEC 27006:2007 – Tehnologia informaţiei – Tehnici de securitate – Cerinţe pentru organizaţiile ce efectuează audit şi certificare a sistemelor de management al securităţii informaţiei

Standardul ISO/IEC 27006:2007 specifică cerinţele şi oferă îndrumări pentru organizaţiile ce efectuează audit şi certificare a sistemului de management al securităţii informaţiilor (ISMS). Standardul este în esenţă destinat să sprijine acreditarea organismelor de certificare ce oferă certificare a sistemului de management a securităţii informaţiilor.

Cerinţele cuprinse în ISO/IEC 27006:2007 trebuie să fie demonstrate în termeni de competenţă şi fiabilitate de către orice organizaţie de certificare ISMS şi orientările cuprinse în ISO/IEC 27006:2007 oferă servicii de interpretare adiţionale a acestor cerinţe pentru orice organizaţie de certificare ISMS.

ISO/IEC 27011:2008 – Tehnologia informaţiei – Tehnici de securitate – Ghidul managementului securităţii informaţiei pentru organizaţiile din domeniul telecomunicaţiilor bazat pe standardul ISO/IEC 27002

Scopul acestui standard este de a defini îndrumări în sprijinul implementării managementului securităţii informaţiilor în cadrul organizaţiilor de telecomunicaţii.

Adoptarea prezentului standard va permite companiilor de telecomunicaţii să întrunească cerinţele de bază ale managementului securităţii informaţiilor: confidenţialitate, integritate şi disponibilitate, precum şi orice altă proprietate relevantă de securitate.

ISO/IEC 27032:2012 – Tehnologia informaţiei – Tehnici de securitate – Ghid pentru securitatea cibernetică

Acest standard oferă un cadru pentru partajarea informaţiilor, coordonare şi tratarea incidentelor. Standardul oferă documentaţia necesară pregătirii sistemului informatic împotriva atacurilor, detectării şi monitorizării acestora. Utilizatorii vor putea răspunde în mod adecvat unor atacuri cum ar fi malware, spyware sau inginerie socială.

Potrivit organizatorului grupului de lucru responsabil de elaborarea acestui standard, Johann Amsenga, faptul că reţelele care alcătuiesc spaţiul virtual le aparţin mai multor proprietari stă la baza mai multor probleme de securitate, deoarece aceştia nu comunică între ei şi au o percepţie diferită asupra securităţii din cauza diferenţelor dintre activităţile pe care le desfăşoară şi dintre reglementările pe care le aplică. În acest context, standardul ISO 27032 reprezintă o soluţie globală care va ajuta la atenuarea riscurilor care ameninţă securitatea cibernetică.

3. Concluzii

Standardele de securitate definesc şi facilitează asigurarea securităţii datelor şi a sistemelor informatice împotriva atacurilor existente la ora actuală pe Internet

Identificarea elementelor care să asigure un grad corespunzător de securitate presupune o planificare riguroasă şi identificarea exactă a obiectivelor. Gradul de expunere a sistemelor informaţionale variază în funcţie de domeniul în care activează fiecare organizaţie. Cu cât acest risc este mai mare, atenţia care trebuie acordată securităţii datelor ar trebui să fie mai mare. Instituţiile financiare, industria apărării, aerospaţială, industria tehnologiei informaţiei sau industria electronică sunt sectoarele cu cel mai mare grad de risc în ceea ce priveşte securitatea informaţiilor.

Este important ca fiecare organizație să poată să-și identifice propriile cerințe de securitate. Pentru aceasta trebuie să se definească o politică de management al securității informațiilor care să includă un cadru de lucru pentru stabilirea obiectivelor, să țină cont de cerințele de securitate ale afacerii, de legislația existentă și să stabilească criteriile de estimare a riscului.

În abordarea utilizată de o organizație pentru evaluarea riscului se identifică o metodă de evaluare a riscului conform cerințelor de securitate, legale și reglementate ale afacerii, se concep criteriile de acceptare a riscurilor și se identifică nivelurile de risc acceptabile pentru afacere.

Următorul pas este de a identifica riscurile cu care se confruntă organizația:

- identificarea resurselor ce trebuie protejate;
- identificarea amenințărilor specifice fiecărei resurse;
- identificarea vulnerabilităților ce pot fi exploatate;
- identificarea impactului în cazul unui atac informatic reușit.

Odată ce riscurile au fost identificate, ele trebuie să fie analizate și evaluate. Astfel, organizația trebuie:

- să evalueze impactul asupra afacerilor organizației care ar putea rezulta în urma unei căderi a sistemului de securitate, ținând cont de consecințele pierderii confidențialității, integrității și disponibilității resurselor;
- să evalueze în mod realist probabilitatea ca această cădere a sistemului de securitate să apară în cazul amenințărilor și vulnerabilităților preponderente, cât și impactul asociat acestor resurse și a măsurilor de securitate implementate în mod curent;
- să estimeze nivelurile riscului;
- să determine dacă riscul este acceptabil sau necesită tratare, folosind criteriile stabilite anterior.

Se evaluează apoi opțiunile pentru reducerea riscurilor. Aceste acțiuni includ aplicarea măsurilor de securitate corespunzătoare, evitarea riscurilor posibile și transferarea anumitor riscuri către alte părți: asiguratori sau furnizori de servicii.

Pentru a-și defini sistemul de management al securității informațiilor, o organizație trebuie să decidă:

- care amenințări trebuie eliminate și care se pot tolera;
- care resurse trebuie protejate și la ce nivel;
- cu ce mijloace poate fi implementată securitatea;
- care este prețul (financiar, uman, social etc.) măsurilor de securitate care poate fi acceptat.

Un aspect important în stabilirea mecanismelor de securitate îl constituie partea financiară. Un mecanism de control nu trebuie să depășească valoarea bunului ce trebuie protejat.

Odată stabilit sistemul de management al securității informațiilor, următoare etapă constă în selecția serviciilor de securitate - funcțiile individuale care sporesc securitatea. Fiecare serviciu poate fi implementat prin metode variate pentru implementarea cărora este nevoie de așa-numitele funcții de gestiune a securității. Gestiunea securității constă în controlul și distribuția informațiilor către toate sistemele în scopul utilizării serviciilor și mecanismelor de securitate și al raportării evenimentelor de securitate ce pot apărea către administratorii de rețea.

Sistemul de management a securității informațiilor trebuie în permanență monitorizat, organizația având sarcina de a analiza procedurile, incidentele de securitate apărute și posibilele erori din rezultatele procesării pentru a îmbunătăți eficacitatea acestuia.

Bibliografie

[1]. ISO 27001: Sistemul de management al securității informațiilor - Cerințe, 2005.

[2]. ISO 27002: Codul de practică al managementului securității informațiilor, 2005.

[3]. C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*, New York: Addison Wesley, 2003.

[4]. Julia H. Allen *et al.*, *Improving the Security of Networked Systems*, CrossTalk, 2000.

[5]. C. Pețа, "Securitatea cibernetică - latură actuală a securității naționale (I)," *Studii de securitate publică*, vol. 2, no. 3(7), 2013.

[6]. S. Bellovin and W. Cheswich, *Firewalls and Internet Security*, MA: Addison-Wesley Publishing Co., 2007.

[7]. K. Borders and A. Prakash, "Web Tap: Detecting Covert Web Traffic," in *Proc. 11th ACM Conf. Computer and Communications Security*, New York, NY, USA, 2004, pp. 110-120.

[8]. R. Lupu, E. Borcoci, M. Stanciu and A. Pinto, "The Architecture Design for Content-Aware Network Security Services," *UPB Scientific Bulletin*, series C, vol. 73, no. 3, 2011.

[9]. D. G. Firesmith, "Security Use Cases," *J. Object Technology*, vol. 3, 2003, pp. 53-64.

[10]. D. Oprea, *Protecția și securitatea informațiilor. Ed. II*, București: Ed. Polirom, 2007.