Sistemul de management al securității informaționale ISO/IEC 27001:2013. Algoritmul de implementare.

Cojocaru Igor, Guzun Mihail
Institutul de Dezvoltare a Societății Informaționale.
idsi@asm.md
Ionescu Răzvan
Organismul de Certificare RINA SIMTEX, România.
office@simtex.ro

***Abstract* — Lucrarea reflectă studii referitoare la contextul actual al lumii informatice, care impune necesitatea implementării unor măsuri de securitate eficiente, ce ar zădărnici încercările de corupere sau furt de informații cu consecințe grave pentru organizații. Este prezentată istoria abordării sistemice în domeniul securității informației. Sunt descrise compartimentele ediției actuale a standardului de management al securității informației - ISO/IEC 27001:2013, metodologia de implementare şi documentele de sistem în baza cărora urmează să se realizeze implementarea, menținerea şi îmbunătățirea continuă a sistemului.**

***Cuvente cheie* — ISO/IEC 27001, active informaționale, securitate, informație, management.**

1. INTRODUCERE

Instaurarea erei informatice constituie în prezent una dintre cele mai mari realizări tehnico-ştiințifice, având un impact pozitiv asupra tuturor laturilor vieții societății contemporane. La etapa actuală, activitatea celor mai multe organizații depinde în proporție de peste 65 % de propriul lor sistem informatic [1]. Dezvoltarea şi ampla implementare a tehnologiilor informaționale a generat însă, un şir de probleme legate de asigurarea integrității, confidențialității şi a disponibilității informației aflate pe suport electronic. Problema securității informației se acutizează pe măsură ce sunt inventate şi puse în aplicare metode tot mai sofisticate de atac asupra informației. Datele din Tabelul 1 sunt o dovadă elocventă a daunelor pricinuite de incidentele legate de breşele de securitate din cadrul organizației. Cauzele acestor incidente cu consecințe atât de grave sunt cele mai diverse - vulnerabilitățile tehnice ale sistemelor informaționale, livrarea neintenționată a datelor, breşe în sistemul de gestionare a resurselor umane etc. Aplicând, însă metoda identificării cauzei de rădăcină pentru fiecare caz concret utilizând metoda ”De 5 ori ”De ce?”[3], putem constata, că în toate cazurile descrise, incidentele s-au produs în urma lipsei unei abordări sistemice pentru protejarea informației. O asemenea abordare oferă standardele internaționale de management al securității informaționale din familia ISO 27000 care, fiind bazate pe cele mai bune practici acumulate până în prezent, oferă companiilor îndrumări privind protejarea activelor informaționale.

TABELUL 1. ZECE DIN CELE MAI DEVASTATOARE BREŞE DE SECURITATE DIN ISTORIA RECENTĂ [2]

Organizația	Descriere a incidentului
Department of Veterans' Affairs, Anglia	Anul 2006. Pierderea unei baze de date. Daune de 20 mln USD
Target	Anul 2013. Furt de informații despre cardurile de credit şi datele personale a peste 40 mln de clienți
TJ Maxx and Marshalls	Anul 2007. Furt de informații despre carduri de debit şi credit.
Epsilon	Furt de date despre clienți. Pierderi de peste 270 mln USD.
Sony PlayStation	Anul 2011. Furt de date despre cardurile bancare a peste 100 mln de clienți.
CardSystems Solutions	Anul 2005. Sustragerea a peste 40 mln de conturi.
Heartland Payment Systems	Anul 2009. Compromiterea a 130 mln carduri în rezultatul infectării PC. Pierderi – 140 mln USA.
HM Revenue & Customs	Anii 2011-2012. peste 1000 incidente de securitate. Pierderea discurilor cu informațiile a 25 mln persoane care beneficiau de ajutor social.
AOL	Anul 2007. Divulgare neintenționată a datelor cu caracter personal. Pierderi – 500 mln USD.
Certegy Check Services	Sustragerea de către unul din angajați a informației despre 8,5 mln clienți şi transmiterea către brokerii de date. Pierderi – 850 mii USD.

2.STANDRDUL ISO/IEC 27001:2013[4]. OBIECTIVE. ISTORIC. STRUCTURĂ.

ISO/IEC 27001 include specificațiile referitoare la Sistemul de Management al Securității Informației (SMSI) și stabilește un set de reguli referitoare la managementul riscurilor de securitate a informației. Standardul poate fi aplicat de părțile interne (ex.: angajații) și externe (ex.: clienți, furnizori, organisme de certificare, organele puterii de stat ș.a.) pentru evaluarea capacității organizației de a îndeplini cerințele specificate referitoare la securitatea informației. SMSI, organizat în conformitate cu acest standard internațional, reprezintă un cadru global de management prin intermediul căruia organizația identifică, analizează și ține sub control riscurile de securitate a informației. SMSI permite să asigure ca aranjamentele de securitate sunt bine puse la punct pentru ca organizația să facă față la amenințările de securitate indiferent de originea, caracterul și țintele lor. Cerințele expuse în acest standard sunt aplicabile organizațiilor de orice tip (societăți comerciale, structuri guvernamentale, organizații non-profit), dimensiune (de la organizațiile micului business până la companiile transnaționale) și domeniu de activitate (comercial, bancar, militar, sănătate, producție, învățământ, guvernare etc.).

Bazele implementării unui SMSI care să se adreseze explicit organizațiilor conform unei metodologii recunoscute pe scară largă, au fost puse în 1990 prin publicarea unor linii directoare pentru asigurarea securității informației în cadrul sistemelor și rețelelor, de catre Organizația pentru Dezvoltare și Cooperare Economică (OECD). Aceste linii directoare au stat la baza elaborării unui cod de bună practică în securitatea informației, elaborat de catre Departamentul Industriei și Comerțului al Guvernului Britanic. Acest departament a pus ulterior către Institutul de Standardizare din Marea Britanie (BSI) sarcina să promoveze acest cod. În 1995 BSI a publicat standardul BS 7799-1 ca un set de cerințe pentru implementarea voluntară a unui SMSI în cadrul organizațiilor. Mai târziu a apărut și partea a doua, BS 7799-2 „Information Security Management Systems - Specification with Guidance For Use". Acesta era un set de indrumări specifice și mai detaliate pentru implementarea unui SMSI eficient. Ulterior s-a pus problema transformării acestui standard britanic, recunoscut inițial doar de către UKAS ca standard național, într-un standard internațional. În anul 2002 în BS 7799 a fost incorporată abordarea bazată pe procese PDCA (”Plan-Do-Ceck-Act”, Edward Deming) ca ulterior, în a. 2005 să se transforme în standardul internațional ISO/IEC 27001:2005.

ISO/IEC 27001 a fost totalmente revizuit în septembrie 2013. Actuala ediție a standardului este structurată astfel, încât să poată fi ușor integrată cu alte sisteme de management reglementate de ISO, cum ar fi sistemul de management al calității, mediului, sănătății și securității ocupaționale etc. În acest caz procedurile de control al neconformităților, documentelor și înregistrărilor, procedurile de audit intern, analiză a sistemului de management vor fi comune pentru toate sistemele de management implementate în organizație.

Pentru a facilita implementarea standardului ISO/IEC 27001 au fost elaborate în set de standarde complementare, după cum urmează:

ISO/IEC 27000:2014 – prezintă o caracteristică generală a standardelor familiei ISO 27000 și vocabularul aplicat în standarde.

ISO/IEC 27002:2013 – este un cod de bune practici în domeniul securității informației care include obiectivele de control în domeniul SMSI și măsurile de securitate pentru atingerea acestor obiective.

ISO/IEC 27003:2010 – este un ghid pentru implementarea standardului ISO/IEC 27001.

ISO/IEC 27004:2009 – oferă indicații privind aplicarea metricilor de securitate.

ISO/IEC 27005:2011 – stabilește abordări referitoare la evaluarea, analiza și tratarea riscurilor de securitate.

ISO/IEC 27006:2011 – stabilește cerințe pentru organismele de certificare a sistemelor de management ale securității informației.

ISO/IEC 27007:2011 – stabilește regulile de auditare a SMSI.

Aceste standarde prezintă un suport important pentru implementarea, menținerea și îmbunătățirea continuă a SMSI din cadrul organizației.

În Tabelul 2 sunt prezentate compartimentele standardului ISO/IEC 27001:2013 și fazele ciclului PDCA la care se referă aceste compartimente.

TABELUL 2. COMPARTIMENTELE STANDARDULUI ISO/IEC 27001:2013

01.Generalități.	Principii generale
02.Compatibilitatea cu alte sisteme de management.	
1. Domeniu de aplicare.	**P. Planificare**
2. Referințe normative.	Principii generale
3.Termeni și definiții.	
4. Contextul organizației.	**P. Planificare**
5.Responsabilitatea managementului.	
6. Planificare.	
7. Menținere.	
8. Implementarea SMSI.	**D. Executare**
9. Evaluarea eficacității.	**C. Verificare**
10. Îmbunătățire.	**A. Acțiuni de îmbunătățire**
Anexa A (normativă). Obiective de control și măsuri pentru atingerea obiectivelor.	

Anexa A (normativă) reprezintă un set de instrumente pentru implementarea ISO/IEC 27001:2013 (14 clauze, 35 obiective principale de control și 114 măsuri de control). Aceste instrumente urmează să fie utilizate la identificarea riscurilor și a oportunităților de securitate a informației și la elaborarea planurilor de îmbunătățire prin reducerea nivelului de risc și prin valorificarea oportunităților de securitate.

Clauzele Anexei A ISO/IEC 27001:2013:

A 5. Politici de securitate.
A 6. Organizarea securității informației.
A 7. Securitatea resurselor umane.
A 8. Managementul resurselor.
A 9. Controlul accesului.
A 10. Metode criptografice.
A 11. Securitatea fizică și a mediului de lucru.
A 12. Securitatea operațiunilor.
A 13 Securitatea comunicațiilor.

A 14. Achiziționarea, dezvoltarea şi mentenanța sistemelor.
A 15. Relații cu furnizorii.
A 16. Managementul incidentelor.
A 17.Aspecte de securitate informațională în managementul continuității afacerii.
A 18. Conformitate cu cerințele legale şi alte cerințe.

3. METODOLOGIA IMPLEMENTĂRII SMSI

Implementarea SMSI este o decizie strategică a organizației. Prin implementarea unui SMSI o organizație îşi poate identifica nivelul necesar de securitate, îşi poate dezvolta planuri, strategii, îşi poate distribui bunurile (activele) către anumiți deținători de resurse în baza propriei analize de risc şi poate lua măsuri tehnice şi non-tehnice de securizare a acestora. Conceptul cheie al implementării unui SMSI într-o organizație este axat pe îmbunătățirea celor trei atribute ale informației: *confidențialitate, integritate şi disponibilitate.*
Procesul de implementare urmează să fie organizat respectându-se principiul PDCA. Următorii paşi pot fi parcurşi pentru implementarea unui SMSI eficace şi eficient în cadrul organizației:

PLANIFICAREA SMSI.

Pasul 1. Obținerea acordului şi a angajamentului Directorului general.
Acest angajament este de importanță majoră pentru succesul unui proiect de implementare SMSI. Angajamentul trebuie să fie declarat în cadrul unei adunări cu participarea reprezentanților tuturor nivelurilor ierarhice ale organizației.

Pasul 2. Stabilirea structurii de conducere a SMSI.
Directorul general stabileşte prin decizie instituirea unui Comitet de Securitate a Informației şi a conducătorului Comitetului, care urmează să coordoneze toate activitățile de implementare, menținere şi îmbunătățire a SMSI.

Pasul 3. Evaluarea inițială a sistemului de securitate a informației al organizației. Definirea domeniului de aplicare.
Orice organizație, chiar dacă nu are un SMSI documentat şi certificat, întreprinde anumite măsuri de securitate în baza unor cerințe legale, a experienței manageriale a conducătorilor şi a altor factori. Obiectivul acestui pas este de a evalua gradul de corespundere a sistemului de management existent cu prevederile standardului de referință. În cadrul acestei evaluări se stabileşte contextul organizatiei dpdv al securității informației, interesele părților externe şi interne privind SMSI. Tot la această fază se stabileşte domeniul de aplicare al sistemului (procese, locații, activități, măsuri de control aplicabile/neaplicabile din Anexa A ISO/IEC 27001:2013. Evaluarea urmează să fie finalizată cu un raport, în care să fie reflectată starea curentă a SMSI în comparație cu cerințele referențialului.

Pasul 4. Elaborarea declarației de Politică în domeniul SMSI.
Proiectul politicii urmează să fie elaborat de Comitetul de securitate, ținându-se cont de prevederile p. 5.2 al referențialului. Acesta este examinat şi aprobat de Directorul general şi adus la cunostința tuturor angajaților şi a altor părți interesate prin instruiri, includerea lui în regulamentul de ordine internă, publicarea pe pagina web, afişarea pe panoul informativ al organizației.
În baza politicii sunt stabilite obiectivele privind securitatea informației în organizație.

Pasul 5. Completarea inventarului activelor informaționale. Clasificarea activelor.
Prin termenul ”active” trebuie să se subînțeleagă toate bunurile din cadrul organizației, care trebuie să fie protejate. Acestea includ, dar nu se limitează la:

- Elemente de infrastructură.
- Informații şi date.
- Documente pe hârtie.
- Echipamente fizice.
- Oamenii şi cunoştințele lor.
- Imaginea, valorile, obiectivele, strategia de piață, politica de prețuri şi reputația etc.

În urma definitivării inventarului bunurilor informaționale şi non-informaționale aceste resurse se clasifică în funcție de importanța lor pentru organizație. Aici se vor lua în considerație recomandările oferite de standardul ISO/IEC 27002:2013 privind criteriile de clasificare:

- Cerințele legale.
- Valoarea.
- Criticitatea.
- Sensibilitatea la dezvăluire sau modificare.

La această fază trebuie să fie stabiliți proprietarii activelor, în responsabilitatea cărora va intra actualizarea clasificării, elaborarea măsurilor de protecție şi asigurarea respectării acestor măsuri.

Pasul 6. Abordarea privind analiza şi managementul riscului.
La această etapă se defineşte metodologia identificării şi gestionării riscurilor de securitate a informației. La elaborarea metodologiei urmează să se respecte recomandările standardului ISO/IEC 27005:2011, care se bazează pe identificarea activelor şi a amenințărilor ce pot exploata vulnerabilitățile acestor active informaționale. Se ia în vedere impactul pierderii confidențialității, integrității şi disponibilității informației, dar şi probabilitatea că o amenințare să exploateze o vulnerabilitate existentă. Documentul final al etapei este planul de tratare a riscurilor, care va include şi responsabilii de gestionare a riscurilor şi de acceptare a riscurilor reziduale după tratarea lor.

Pasul 7. Declarația de aplicabilitate.
În urma evaluării inițiale a SMSI, analizei de risc şi a clasificării activelor se propun încă din etapa de planificare a implementării sistemului anumite măsuri de securitate. Astfel se redactează documentul numit Declarația de aplicabilitate, ce conține măsurile de securitate propuse în Anexa A a standardului ISO/CEI 27001:2013, care au fost selectate pentru a reduce riscurile calculate la pasul anterior la un nivel acceptabil. Întrucât nu toate cele 114 măsuri din anexă sunt aplicabile organizației, unele dintre acestea pot fi declarate neaplicabile (excluderi). În spiritul standardului, orice excludere este justificată în Declarația de Aplicabilitate.
Odată cu finalizarea Declarației de aplicabilitate se poate considera că partea de planificare a SMSI este încheiată, ceea ce permite trecerea la etapa următoare a ciclului Deming şi anume:

IMPLEMENTAREA SMSI.

Pasul 8. Realizarea Planului de tratare a riscului.
În această etapă se aplică efectiv măsurile de securitate propuse în faza de Planificare a SMSI.

Aplicarea efectivă presupune determinarea acţiunilor corespunzatoare ale managementului, alocarea de resurse şi definirea responsabililor ce trebuie să ducă la îndeplinire aplicarea corectă şi completă a măsurilor de securitate.

Pasul 9. Elaborarea documentelor necesare SMSI.

Informaţiile documentate care, conform cerinţelor standardului, trebuie să fie elaborate în cadrul SMSI, sunt:

- Declaraţia de aplicabilitate (clauza 4.3 a standardului).
- Declaraţia de Politică a securităţii informaţiei (5.2).
- Procedura de evaluare a riscurilor (6.1.2).
- Procedura de tratare a riscurilor (6.1.3).
- Obiectivele în domeniul securităţii informaţiei (6.2).
- Înregistrări referitoare la competenţa personalului care activează în domeniul SMSI (7.2).
- Documente de planificare şi control operaţional (8.1).
- Rezultatele evaluării riscurilor (8.2).
- Deciziile de tratare a riscurilor (8.3).
- Înregistrări referitoare la monitorizări şi măsurări în cadrul SMSI (9.1).
- Programul de audit intern al SMSI şi rezultatele auditurilor (9.2).
- Înregistrările referitoare la Analiza SMSI efectuată de management. (9.3).
- Înregistrările referitoare la neconformităţi şi acţiunile corective întreprinse (10.1).
- Alte documente SMSI identificate de organizaţie ca necesare pentru funcţionarea SMSI (7.5.1b), cum ar fi cele care ar putea facilita aplicarea controalelor de securitate stabilite în anexa A a standardului, fişele de post, regulamentele interne şi altele.

Pasul 10. Modificarea fişelor de post ale angajaţilor din domeniul SMSI.

La această etapă se revizuiesc toate fişele de post ale angajaţilor implicaţi în domeniul SMSI prin includerea unor clauze noi care reies din documentele SMSI deja elaborate, cum ar fi activele (bunurile informaţionale) de care răspunde angajatul, riscurile pe care trebuie să le gestioneze, clauzele de confidenţialitate şi clauzele specifice locului de muncă. În fişa postului se stabilesc şi tipurile de documente/informaţii la care fiecare angajat implicat are acces. Tot în fi□ele de post sunt specificate şi competenţele funcţiilor cu responsabilităţi în domeniul SMSI.

Pasul 11. Instruirea angajaţilor.

Instruirile sunt de importanţă critică, deoarece un sistem de management poate fi realizat cu succes doar în cazul participării competente şi conştiente a tuturor angajaţilor cu reponsabilităţi de control asupra proceselor organizaţiei. Instruirile trebuie să se desfăşoare la toate etapele realizării proiectului şi să realizeze obiectivele de cunoaştere a prevederilor standardului internaţional, a procedurilor interne de management şi a documentelor externe aferente activităţii organizaţiei.

Pasul 12. Aplicarea efectivă a procedurilor necesare SMSI.

Punerea în practică a documentelor dezvoltate anterior se face la această etapă de către fiecare responsabil de proces.

Aplicarea documentelor este în stransă legatură cu implementarea măsurilor de securitate descrise în Planul de tratare a riscului.

VERIFICARE

Pasul 13. Revizuirea şi actualizarea periodică a documentelor SMSI.

Unul din obiectivele monitorizării implementării SMSI este de a corecta documentele elaborate în scopul adaptării acestora cât mai bine la situaţia concretă din organizaţie. Etapa include revizii de documente, retragerea celor vechi şi distribuirea celor corectate.

Pasul 14. Auditul intern

Practica comună pentru monitorizarea sistemului este cea a auditului intern. Astfel se poate vedea nivelul de implementare al măsurilor de securitate. Auditul intern trebuie efectuat în toate compartimentele implicate în SMSI şi se desfă□oară prin interviuri ale angajaţilor, observaţie directă, testarea sistemelor. O componentă necesară în verificarea implementării măsurilor tehnice este auditul tehnic, care se desfăşoară cu instrumente speciale operate de personal calificat în domeniu. Auditurile interne se concretizează cu nişte concluzii, care sunt incluse în Rapoartele de audit intern (RAI). Constatările sunt comunicate parţilor implicate pentru a fi rezolvate.

Pasul 15. Analiza efectuată de management.

Analiza efectuată de management (AEM) este o etapă importantă întrucât, după parcurgerea unui ciclu PDCA complet, lansează premise pentru desfăşurarea unui nou ciclu de dezvoltare a sistemului. În cadrul Analizei urmează să fie colectate şi analizate datele de intrare, enumerate în p. 9.3 al standardului de referinţă. Este necesar să se menţină dovezi ale efectuării acestei analize. În urma AEM trebuie să se propună măsuri de îmbunătăţire a SMSI, alocare de resurse dacă este cazul, să se actualizeze analiza de risc şi implicit, planul de tratare a riscului.

ACŢIUNI DE ÎMBUNĂTĂŢIRE A SISTEMULUI

Pasul 16. Implementarea rezultatelor AEM

În urma AEM datele de ieşire trebuie implementate în scopul îmbunătăţirii SMSI. Rezultatele AEM trebuie şi ele comunicate şi înţelese de către părţile interesate. Datele de ieşire pot include atât acţiuni corective cât şi preventive.

Algoritmul descris mai sus se realizează în cadrul Institutului de Dezvoltare a Societăţii Informaţionale, pentru a adapta SMSI existent, certificat de RINA SIMTEX OC, România, la versiunea actuală a standardului ISO/IEC 27001.

REFERINŢE

[1] http://ro.scribd.com/doc/99927620/Securitatea Informationala

[2] Silviu Marian Banila, ANALIZA: Cele mai importante brese de securitate din istoria recentă. https://ro.stiri.yahoo.com/analiza-cele-mai-importante-brese-securitate-din-istoria-091834763.html

[3] Mike Sondalini, Understanding How to Use The 5 Whys for Root Cause Analysis. http://www.lifetime-reliability.com/tutorials/lean-management-methods/How_to_Use_the_5-Whys_for_Root_Cause_Analysis.pdf

[4] ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements