Implementarea unui sistem de management în securitatea informației

Ludmila Duca, Rodica Bulai
Universitatea Tehnică a Moldovei
ludmila.duca@ati.utm.md

Implementarea unui system de management al securității informației ne permite îmbunătățirea activității organizației şi creşterea încrederii de către client.

INTRODUCERE

Odată cu apariția Sistemelor Informaționale şi dezvoltarea rapidă a Tehnologiilor Informaționale în ultima perioadă este nevoie de a implementa Sisteme de Management în Securitatea Informației (SMSI).

I. NECESITATEA UNUI SMSI

Sistemele informatice şi rețelele de calculatoare din cadrul organizațiilor tot mai des sunt atacate şi securitatea este minima, ceea ce duce la mari probleme atât organizațiilor cât şi clienților acestor organizații.

În urma acestor atacuri informaționale datele confidențiale sunt deteriorate, modificate sau chiar șterse. Din această cauză mediul de afaceri are nevoie pentru a proteja resursele sale. Dar din păcate cele mai dese incidente de securitate a informației au loc în interiorul organizației, din cauza nerespectării măsurilor de securitate.

II. CERINȚELE FAȚĂ DE SMSI

La implemetarea unui SMSI este necesar de creat o structură organizatorică dependentă de managementul securității informației. Managerii responsabili de securitatea informației în organizație emit o politică de securitate a informației, care continuu este îmbunătățită.

În fişa postului a fiecărui angajat sunt descrise obligațiile şi responsabilitățile referitoare politicii de securitate. Personalul trebuie instruit în privința politicii de securitate şi are loc verificarea continua a respectării politicii de securitate. În cazul nerespectării politicii de securitate trebuie stabilite acțiuni disciplinare adecvate.

Este necesar de identificat sectoarele şi prioritățile la nivel de securitate a informației atât la nivel fizic cât şi la nivel de echipament. Trebuie elaborate instrucțiuni de securitate a informației cu descrieri detailate şi clare pentru angajați.

Identificarea şi clasificarea riscurilor informaționale este necesar pentru a minimiza sau chiar a evita apariția acestor riscuri. La calcularea riscurilor trebuie de ținut seama de infrastructura organizației şi la necesitate de propus o infrastructură nouă pentru minimizarea riscurilor informaționale. În baza analizei riscurilor este necesar de elaborat şi implementat planuri pentru situații de urgență. Planurile de urgență trebuie actualizate şi petrecute instruiri periodice a angajaților.

Pentru controlul alocării dreptului de acces este nevoie de elaborat o procedură şi accesul la procesele şi informația organizației să fie controlat în baza politicii de securitate şi autorizării accesului. Accesul la resursele organizației să fie limitat prin dispositive de securitate la nivel de sistem de operare. Dacă în cadrul organizației se utilizează calculatoare portabile şi lucrul la distanță este necesar de elaborate prevederi de securitate a informației.

Cerințele, politicile, prevederile legate de securitatea informației sunt definite, documentate şi aprobate de la bun început la implementarea unui SMSI.

Auditurile interne periodice ne ajută la monitorizarea securității informației. Auditurile au loc în baza politicilor referitoare de securitate din cadrul organizației şi sunt verificate sistemele informaționale şi platformele tehnice. Auditurile sunt planificate, efectuate şi urmărite de persoane instruite în domeniul securității informației care au o pregătire specială în domeniul dat.

III. FAMILIA ISO/IEC 27000

Familia standardelor ISO din domeniul securității informației sunt următoarele:

- ISO/IEC 27001 Tehnologia Informației. Tehnici de securitate. Cerințe pentru un system de management al securității informației [1];
- ISO/IEC 27002 Tehnologia informației. Tehnici de securitate. Cod de practice pentru managementul securității informației [2];
- ISO/IEC 27003 Tehnologia informației. Tehnici de securitate. Ghid de implementare [3];
- ISO/IEC 27004 Tehnologia informației. Tehnici de securitate. Măsuri;
- ISO/IEC 27005 Tehnologia informației. Tehnici de securitate. Managementul riscurilor securității informației;
- ISO/IEC 27006 Tehnologia informației. Tehnici de securitate. Cerințe pentru organisme care efectuează auditul şi certificarea sistemelor de management a securității informației.

Certificarea organizațiilor pe baza unui SMSI are loc în baza standardului ISO/IEC 27001. Standardul dat este aplicabil tuturor organizațiilor ce doresc îmbunătățirea şi respectarea securității informației atât din domeniul IT cât şi din alt domeniu.

Standardul ISO/IEC 27001 este un standard de management. El descrie cerințele pentru un SMSI, descrie ce trebuie de implementat în domeniul securității

informației.

La aplicarea SMSI este necesar ca sistemele de operare, soft-ul și aplicațiile utilizate în organizației să fie licentiate.

IV. CONCLUZII

Organizațiile devin tot mai dependente de domeniul IT și odată cu aceasta apare problema securității informației din cadrul organizației. Impementarea unui sistem de management a securității informației în organizație ne constată că eforturile și investițiile vor fi mai mici, iar beneficiile vor crește.

REFERINȚE

[1] http://www.iso.org/iso/catalogue_detail?csnumber=54534

[2] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533D. Knuth, The Art of Programming. Addison-Wesley, 1973

[3] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42105

[4] http://www.ghidmanagement.ro/resurse/PROIECTARE-SMSI+ISO+27001

[5] http://valygreavu.com/2010/02/08/iso27001-sistemul-de-management-al-securitatii-informationale-smsi/