T8. Proiectarea și implementarea sistemului de securitate informațional în întreprindere (2 ore)

1) Standardele securității informaționale [1,2]

Datorită numeroaselor tipuri de atacuri existente în special în domeniul informatic, s-a simțit necesitatea de existență a unei politici de securitate a informației pentru toate organizațiile. În acest sens Organizația Internațională pentru Standardizare (ISO) împreună cu Comisia Internațională Electrotehnica (IEC) formează un sistem internațional specializat pentru standardizarea mondială. Organismele naționale care sunt membre ale ISO si 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 tari au statut de *Participanți* și alte 40 de țări au statut de Observatori.

Din seria ISO 27000 de standarde dedicate securității informației (serie actuală de standarde), fac parte următoarele standarde:

I. ISO/IEC 27000:2014 –Sisteme de management a securității informației, Prezentare generală și vocabular, 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.

II. ISO/IEC 27001:2013 –Specificații ale sistemelor de management al securității informației 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 întreprinderilor. Acest standard specifică cerințele pentru implementarea unor controale de securitate personalizate nevoilor întreprinderilor.

III. ISO/IEC 27002:2013 – Codul practică pentru managementul securității informației, stabilește principiile generale pentru inițierea, implementarea, menținerea și îmbunătățirea managementului securității informației într-o întreprindere.

IV. ISO/IEC 27003:2010 – Ghidul de implementare a sistemului de management al securității informației, este concentrat pe aspectele critice necesare pentru proiectarea și implementarea cu succes a unui sistem de management al securității informațiilor (ISMS), în conformitate cu ISO/IEC 27001:2013.

V. ISO/IEC 27004:2009 –Managementul securității informației, Evaluări:

- 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;
- oferă îndrumări în privința unor controale sau grupuri de controale așa cum se specifică în standardul ISO/IEC 27001;
- se aplică tuturor tipurilor de întreprinderi.

VI. ISO/IEC 27005:2011 –Managementul riscului securității informației:

- stabilește ghidul pentru managementul riscului securității informației;
- susține conceptele generale specificate în ISO/IEC 27001;
- este conceput pentru a asista la punerea cu succes în aplicare a securității informațiilor bazate pe o abordare de management al riscului;
- este aplicabil tuturor tipurilor de întreprinderilor care intenționează să gestioneze riscurile ce ar putea compromite securitatea informațiilor dintr-o întreprindere.

VII. ISO/IEC 27006:2011 –Cerințe pentru întreprinderile ce efectuează audit și certificare a sistemelor de management al securității informației:

- specifică cerințele și oferă îndrumări pentru întreprinderile ce efectuează audit și certificare a sistemului de management al securității informațiilor (ISMS);

- este destinat să sprijine acreditarea organismelor de certificare ce oferă certificare a sistemului de management a securității informațiilor.

VIII. ISO/IEC 27011:2016 –Ghidul managementului securității informației pentru întreprinderile din domeniul telecomunicațiilor bazat pe standardul ISO/IEC 27002.

Scopul acestui standard este de a defini îndrumări în sprijinul implementării managementului securității informațiilor în cadrul întreprinderilor de telecomunicații și le permite să întrunească cerințele de bază ale managementului securității informațiilor: confidențialitate, integritate și disponibilitate, precum și orice altă proprietate relevantă de securitate.

IX. ISO/IEC 27032:2012 – Ghid pentru securitatea cibernetică:

- oferă un cadru pentru partajarea informațiilor, coordonarea și tratarea incidentelor;
- oferă documentația necesară pregătirii sistemului informatic împotriva atacurilor, detectării și monitorizării acestora;
- utilizatorii vor putea răspunde în mod adecvat unor atacuri cum ar fi malware, spyware sau inginerie socială.

2) Principii de proiectare a sistemului de securitate informațională a întreprinderii [3]

Principiile de proiectare a securității pot fi organizate în grupuri logice după cum urmează:

I. Principii de proiectare structurală

Principiile de proiectare trebuie să fie analizate și revizuite în timpul dezvoltării, deoarece pot exista conflicte potențiale între interpretările lor specifice sistemului. Un principiu poate suprascrie sau altera un alt principiu. Aceste conflicte s-ar putea să nu fie satisfăcute simultan, dar, în funcție de obiectivele sistemului, un principiu poate fi accentuat într-o măsură mai mare decât celălalt.

A. Economia și eleganța

- *Cel mai mic mecanism comun*
- *Abstractizare clară (Clear Abstractions)*
- *Dependențe parțial*
- *Acces eficient prin mediere*
- *Partajarea*
- *Complexitate redusă*

B. Evoluția sistemelor securizate

Principiul evoluției sistemelor securizate precizează că trebuie construit un sistem pentru a facilita menținerea proprietăților sale de securitate în fața modificărilor aduse interfeței, structurii funcționale sau configurației. Aceste modificări pot include actualizări ale sistemului, activități de întreținere, reconfigurare etc. Beneficiile acestui principiu includ costuri reduse ale ciclului de viață pentru vânzător, costuri reduse de proprietate pentru utilizator, precum și o securitate îmbunătățită a sistemului.

C. Încredere

- *Componentele de încredere*
- *Ierarhia de încredere pentru componente*
- *Valoare inversă de modificare (The Modification Threshold*
- *Protecție ierarhică (Hierarchical Protection)*
- *Elemente de securitate minimizate (Minimized Security Elements)*
- *Cel mai mic privilegiu (Least Privilege)*
- *Adevărata încredere în sine (Self-reliant Trustworthiness)*

D. Compoziție

- *Securitatea componentei distribuite (Secure Distributed Composition)*
- *Canale de comunicare de încredere (Trusted Communication Channels)*

II. Logică și funcție

Principiile asociate cu logica și funcția sunt aplicabile atât la nivelul sistemului, cât și la nivelul componentelor.

- *Securitate implicită (Secure defaults)*
- *Incident (defect) securizat (Secure Failure)*
- *Auto-analiză (Self Analysis)*
- *Responsabilitate și trasabilitate (Accountability and Traceability)*
- *Protecția continuă a informațiilor (Continuous Protection of Information)*
- *Securitatea economică (Economic Security)*
- *Securitatea Performanței (Performance Security)*
- *Siguranță ergonomică (Ergonomic Security)*
- *Siguranță acceptabilă (Acceptable Security*)

III. Ciclul de viață al sistemului

Câteva principii ghidează ciclul de viață al sistemului pentru a contribui la securitatea inițială și continuă a sistemului.

- *Utilizați proceduri repetitive și documentate*
- *Rigurozitate procedurală (Procedural Rigor)*
- *Modificării sigure sistemului (Secure System Modification)*
- *Documentație suficientă pentru utilizatori (Sufficient User Documentation)*.

3) Asigurarea integrității, confidențialității și accesibilității informației în întreprindere

Obiectivele fundamentale de securitate, care se regăsesc printre cerințele unui mediu de afacere sunt:

- ***Confidențialitatea*** **-** susține principiul "celui mai mic privilegiu" prin faptul că numai persoanele, procesele sau sistemele autorizate ar trebui să aibă acces la informații pe baza necesității de a cunoaște. Nivelul de acces pe care trebuie să-l aibă persoanele autorizate este la nivelul necesar pentru a-și face treaba. În ultimii ani, o atenție sporită este dedicată confidențialității informațiilor și necesității de a le proteja de persoanele care ar putea fi capabile să comită crime prin accesul neautorizat la informații. Furtul de identitate este actul de asumare a identității prin cunoașterea informațiilor confidențiale obținute din diverse surse.

O măsură importantă pe care arhitectul de securitate ar trebui să o utilizeze pentru a asigura confidențialitatea informațiilor este clasificarea datelor. Acest lucru ajută la determinarea persoanelor care ar trebui să aibă acces la informații (publice, numai pentru uz intern sau confidențiale). Identificarea, autentificarea și autorizarea prin intermediul controalelor de acces sunt practici care susțin păstrarea confidențialității informațiilor. Un exemplu de control pentru protejarea confidențialității este criptarea informațiilor. Criptarea informațiilor limitează gradul de utilizare a informațiilor în cazul în care acestea sunt accesate de o persoană neautorizată.

- ***Integritatea*** **-** principiul conform căruia informațiile ar trebui protejate împotriva schimbărilor intenționate, neautorizate sau accidentale. Informațiile stocate în fișiere, baze de date, sisteme și rețele trebuie să se bazeze pe procesarea corectă a tranzacțiilor și furnizarea de informații exacte pentru luarea deciziilor în afaceri.

Sunt puse în aplicare controale pentru a se asigura că informațiile sunt modificate prin practici acceptate. Exemple de controale includ controale de conducere, cum ar fi segregarea (separarea)

sarcinilor și implementarea practicilor de testare care ajută la asigurarea integrității informației. Operațiunile bine formate și securitatea programelor de actualizare oferă metode consistente de aplicare a modificărilor aduse sistemelor. Limitarea capacității de modificare pentru persoanele autorizate (cu necesitate documentată de acces) limitează expunerea la modificări intenționate și neintenționate.

- ***Disponibilitatea*** - principiul care asigură că informațiile sunt disponibile și accesibile utilizatorilor atunci când este necesar.

  Cele două domenii principale care afectează disponibilitatea sistemelor sunt:

  1. Atacurile de negare a serviciilor (Denial-of-Service attacks);
  2. Pierderea (anularea) serviciului prestat (Loss of service) din cauza unui dezastru, care ar putea fi provocat de *om* (de exemplu, incapacitatea planificării corecte a unui accident de sistem, hardware învechit și testarea slabă rezultă în prăbușirea sistemului după upgrade) sau *naturale* (de exemplu, cutremur, tornadă, uragan, incendiu și inundații).

  În ambele cazuri, utilizatorul final nu are acces la informațiile necesare pentru desfășurarea afacerii. Importanța acestuia pentru supraviețuirea organizației vor determina cât de semnificativ va fi impactul perioadei de nefuncționare. Lipsa unor controale de securitate adecvate poate crește riscul de viruși, distrugerea datelor, penetrarea externă sau atacurile DOS (Denial-of-Service). Astfel de evenimente pot împiedica utilizarea sistemului de către utilizatorii normali.

Instrumentele de control includ un sistem de detectare antiviruși și malware actualizat și activ, planuri de gestionare a incidentelor și planificarea recuperării dezastrelor sau planificarea continuității afacerii, care asigură funcționarea departamentului folosind procese alternative atunci când apare o întrerupere a sistemului informatic pentru o perioadă definită. Repararea în caz de catastrofe presupune recuperarea tuturor sau a unor părți ale sistemelor de procesare a tehnologiei informației. Recuperarea în caz de catastrofe și continuitatea activității întreprinderii implică minimizarea impactul efectelor critice asupra întreprinderii.

4) Certificarea securității sistemului informațional al întreprinderii

Fiecare întreprindere, indiferent dacă este mare sau mică, locală sau internațională trebuie să urmeze principiul calității în special având în vedere perspectiva concurenței și a globalizării.

Procesul de certificare a întreprinderii presupune câteva etape:

1. ***Înregistrarea***, întreprinderea face apel la serviciile firmei de certificare;

2. ***Procesul de ofertă***, întreprinderea primește o ofertă de la firma de certificare (preț, termeni, servicii);

3. ***Semnarea contractului.*** Este completat un formular de profil al întreprinderii care presupune un chestionar despre întreprindere și o cerere de evaluare, înregistrare sau transferul de înregistrare. Întreprinderea primește un contract în ceea ce privește certificarea.

4. ***Pre evaluarea***. Un auditor este atribuit întreprinderii care va descrie etapele de audit iar unul sau doi auditori fac o analiză sumară a întreprinderii pentru sesiza dacă sunt neconformități evidente la standard (deobicei se cere o taxă suplimentară pentru acest serviciu) iar ca rezultat se prezintă un scurt raport scris asupra a ceea ce auditorii au găsit.

5. ***Auditul de certificare / înregistrare.*** Este înaintat un program de audit pentru înregistrare pentru evaluarea conformității cu standardul de înregistrare. Auditul începe cu o ședință de deschidere. În timpul auditului auditorii colectează probe de conformitate prin intervievarea persoanelor, verifică documente și vizitează procesele în acțiune. La sfârșitul auditului, în cadrul unei reuniuni de închidere, auditorul principal prezintă rezultatele și rezum dacă sunt în conformitate sau nu, urmat de un raport scris cu privire la constatări. În cazul în care întreprinderea

nu este pe deplin în conformitate, auditorul va lucra cu managementul pentru a dezvolta un program de măsuri corective.

6. ***Aprobarea certificatului.*** Fiind aprobat, certificatul de evaluare este emis și începe un ciclul de supraveghere (3 ani). În cazul în care la un moment dat întreprinderea se află in neconformitate atunci va fi pusă într-un ciclu de acțiuni corective. Pe parcursul auditurilor de supraveghere, standardele cer să efectuarea auditurilor interne de sistem de calitate în mod regulat. Îmbunătățirea continuă a sistemului este necesară în majoritatea sistemelor de management. Cei mai mulți certificatori recomanda o urmărire constantă ca interes major. După trei ani, organismul de certificare va prezenta noi contracte pentru re-evaluare și supraveghere.

Bibliografia:

1. http://www.euroqual.pub.ro/ijisc-international-journal-of-information-security-and-cybercrime-2017/
2. http://www.securitatea-informatiilor.ro/standarde-de-securitate/standarde-de-securitate/
3. T. V. Benzel, C. E. Irvine, T. E. Levin, G. Bhaskara, T. D. Nguyen, P. C. Clark, *Design Principles for Security*, Monterey, California.