Introducere in Securitatea Sistemelor Informatice

Concepte generale, noțiuni elementare și fundamentale

Conf. Univ. Dr. Marius Iulian Mihăilescu

m.mihailescu.mi@spiruharet.ro

http://www.mariusmihailescu.com

Facultatea de Inginerie și Informatică
Universitatea Spiru Haret

23.02.2022

Overview

Concepte și definiții generale

Principiile de bază

Stabilirea cerințelor

Legislație

Eficiența sistemului de securitate

Standardul de securitate ISO/IEC 17799

Concepte și definiții generale

- Securitate cibernetică
  - Securitatea cibernetică se referă la setul de tehnologii, procese, și practici proiectate pentru protejarea rețelelor, dispozitivelor, programelor, și a datelor atunci când există atacuri, distrugeri, sau acces neautorizat.
- Securitatea Informației
  - *InfoSec* se referă la practicile de protejarea informației prin atenuarea riscurilor informaționale.
  - Parte componentă a managementului riscurilor.
  - Implică prevenirea sau cel puțin reducerea probabilității accesului neautorizat la date, ștergerea, coruperea, modificarea, inspectarea, inregistrarea sau devalorizarea informației.

Concepte și definiții generale (cont.)

- Securitatea rețelelor
  - Constă in politici, process și practici adoptate cu scopul prevenirii, detectării și monitorizării accesului neautorizat, abuzului, modificării, sau refuzul unui desktop/laptop/server dintr-o rețea și accesului la resursele rețelei.
- Criptologie
  - Știinta care se ocupă de comunicația datelor și stocarea acestora intr-o formă sigură și secretă. Cuprinde studiul criptografiei și al criptanalizei.
- Criptografie
  - Știință exactă, ramură a matematicii, cu rolul securizării informației, precum și cu autentificarea și restricționarea accesului intr-un sistem informatic.

Concepte și definiții generale (cont.)

- Criptanaliză
  - Reprezintă știința studiului metodelor folosite cu scopul obținerii accesului la înțelesul (claritatea) informațiilor criptate, fără a avea acces la informația secretă necesară in mod normal pentru aceasta.
- Steganografie
  - Știința sau arta de a scrie mesaje ascunse astfel incat existența acestora să fie cunoscută numai de destinatar și expeditor.
- Steganaliză
  - Studiul detectării mesajelor ascunse prin tehnici și algoritmi steganografici.

Principiile de bază

- Confidențialitate
  - Reprezintă proprietatea care asigură faptul că informația nu este făcută publică sau dezvăluită persoanelor neautorizate, entităților sau a altor procese (umane, informatice).
- Integritate
  - Integrtatea datelor reprezintă intreținerea și asigurarea acurateții și completitudinii datelor.
  - Datele nu pot fi modificate intr-o manieră neautorizată sau nedectată.
- Disponibilitate
  - Pentru orice sistem informatic, pentru a-și atinge scopul, informația trebuie să fie disponibilă atunci când este nevoie de ea.

Principiile de bază (cont.)

- Non-repudiere
  - Se aplică in aspecte și situații juridice.
  - Non-repudierea implică intenția unuia dintre participanți cu scopul de a duce la bun sfârșit obligațiile contractelor.
  - Pentru a dovedi că o persoană a spus o anumită propoziție, a scris o expresie specifică sau a efectuat o anumită acțiune. Pentru a repudia este de a pretinde că orice a fost spus, scris, comunicat sau efectuat nu a fost făcut de voi (sau de persoana in cauză).
  - Non-repudierea este o incercare activă de a crea artefacte care pot fi folosite impotriva unei persoane identificate care neagă că acestea sunt originea unei comunicări sau a unei acțiuni. Artefactele sunt identitatea, autentificarea identității și ceva care leagă o comunicare sau o acțiune față de identitate.

Stabilirea cerințelor

- Fiecare organizație trebuie să aibe posibilitate să-și identifice propriile cerințe de securitate.
- Trei surse principale:
  - Analiza riscurilor;
  - Legislația existentă;
  - Standardele și procedurile interne.

Stabilirea cerințelor (cont.)

- Organizația își poate identifica propriile cerințe referitoare la securitate folosind o metodologie corespunzătoare pentru analiza riscurilor.
- Patru etape fundamentale:
  - Identificarea activelor care trebuie protejate;
  - Identificarea riscurilor/amenințărilor specifice fiecărui activ;
  - Ierarhizarea riscurilor;
  - Identificarea controalelor prin care vor fi eliminate/diminuate riscurile.
- Aspctele financiare nu se ignoră.
- **Un mecanism de control nu trebuie să coste organizația mai mult decât bunul ce trebuie protejat**.

Legislație

- *Legea nr. 161 din 19 aprilie 2003* privind unele masuri pentru asigurarea transparentei in exercitarea demnitarilor publice, a funcțiilor publice si in mediul de afaceri, prevenirea si sancționarea corupției.
- *Legea nr. 506 din 17 noiembrie 2004* privind prelucrarea datelor cu caracter personal si protecția vieții private in sectorul comunicațiilor electronice.
- *Legea nr. 677 din 21 noiembrie 2001* pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulație a acestor date.
- *Legea nr. 455 din 18 iulie 2001* privind semnătura electronica.
- *Legea nr. 544 din 12 octombrie 2001* privind liberul acces la informațiile de interes public.

Legislație (cont.)

- *Hotărârea nr. 1259 din 13 decembrie 2001* privind aprobarea Normelor tehnice si metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronica.
- Ordinul Avocatului Poporului nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
- Ordinul Avocatului Poporului nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulație a acestor date.
- Ordinul Avocatului Poporului nr. 54 din 18 aprilie 2002 privind stabilirea unor situații in care nu este necesara notificarea prelucrării unor date cu caracter personal care cad sub incidenta Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulație a acestor date.

Legislație (cont.)

- Hotărârea nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
- Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.
- Convențiile internaționale și reglmentările comunitare semnate de România sau in care România este parte.

Eficiența sistemului de securitate

- Eficiența sistemului de securitate depinde:
  - stabilirea unor obiective de securitate care să reflecte cerințele organizației;
  - sprijinului conducerii;
  - existența abilităților necesare realizării analizei riscurilor, a vulnerabilităților și a analizei de impact;
  - instruirea angajaților;
  - monitorizata controalelor implementate.

Standardul de securitate ISO/IEC 17799

- Secțiunea 1 - Politica de securitate
  - Obiectivul politicii de securitate constă in oferirea managementului instituției sprijinul necesar pentru asigurarea securității informațiilor din cadrul organizației.
  - Conducerea oricărei instituții trebuie să pună la dispoziție suportul necesar prin elaborarea unui document intitulat *Politica de Securitate*, document care trebuie adus la cunoștință tuturor angajaților.
  - Nu există documentul? Riscul ca rolurile și responsabilitățile relative la asigurarea securității informaționale să fie greșit înțelese.
  - instruirea angajaților;
  - monitorizata controalelor implementate.

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 2 - Organizarea securității
  - Obiectivul organizării securității constă in menținerea securității tuturor facilităților IT și activelor informaționale accesate de către terțe persoane, fiind recomandată stabilirea unui proces prin care accesul terților să fie controlat.
  - Scopul: asigurarea unei administrări unitare in cadrul organizației.
  - Fiecare utilizator al sistemului informațional este responsabil cu asigurarea securității datelor pe care le manipulează.
  - Rolul și atribuțiile persoanei care se află in poziția de responsabil cu securitatea informațiilor, sunt: *coordonarea și urmărirea respectării procedurilor și politicilor de securitate.*

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 3 - Clasificarea și controlul activelor
  - Obiectivul clasificării este crearea premizelor necesare asigurării unei protecții corespunzătoare valorii activelor instituției.
  - Măsurile de protecție sunt proiectate in funcție de gradul de senzitivitate, și de semnificația economică a resurselor vizate.
  - Clasificarea informațiilor este necesară atât pentru a permite alocarea resurselor necesare protejării acestora, cât și pentru a determina pierderile potențiale care pot să apară ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 4 - Securitatea personalului
  - Număr foarte mare de incidente - Personalul din interiorul organizației, prin acțiuni rău intenționate sau chiar erori sau neglijență in utilizarea resurselor informaționale, genereaz.
  - ISO/IEC 17799 se concentrează pe riscurile de natură umană.
  - Etapa de selecție a angajaților reprezintă un aspect foarte important pentru securitatea informațiilor. Monitorizarea discretă a personalului angajat trebuie realizată in acord cu prevederile legale și să se desfășoare pe intreaga perioadă a contractului de muncă.
  - Evitarea neglijenței sau a greșelilor de operare se poate realiza printr-o informare corespunzătoare la amenințările la care sunt expuse informațiile.
  - Utilizatorii trebuie să primească instruirea corespunzătoare referitoare la procedurile de securitate și modul in care acestea trebuie respectate/urmate cu respect pentru politica organizației.

Standardul de securitate ISO/IEC 17799 (cont.)

- Obiectivul raportării incidentelor de securitate are ca obiectiv minimizarea efectelor negative sau a incorectei funcționări a echipamentelor.
- Implementarea politicilor și procedurile de securitate trebuie implementate astfel incât să asigure un răspuns consistent la astfel de incidente.

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 5 - Securitatea fizică
  - Obiectivul delimitării zonelor securizate constă in prevenirea accesului neautorizat sau afectarea facilităților oferite de sistemul informațional.
  - Secțiunea se ocupă de mecanismele prin care se asigură securitatea fizică a imobilului in care organizația își desfășoară activitatea.
  - Măsurile de control al accesului, ce sunt implementate la nivel de aplicație, baze de date sau rețea, pot deveni inutile cu condiția existenței unei protecții fizice corespunzătoare.

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 6 - Managementul comunicațiilor și al operării
  - Asigurarea integrității datelor și a aplicațiilor software necesită măsuri de protecție prin care să se prevină și să se detecteze introducerea unor aplicații ilegale in sistemul organizației
  - Trebuie dezvoltate proceduri și mecanisme de raportare care să identifice utilizarea necorespunzătoare a resurselor precum și perioadele de utilizare.
  - Măsurile de control al accesului, ce sunt implementate la nivel de aplicație, baze de date sau rețea, pot deveni inutile cu condiția existenței unei protecții fizice corespunzătoare.
  - Accesul programatorilor pe mediul de producție nu ar trebui permis, iar dacă anumite situații excepționale o cer, atunci ar trebui controlat indeaproape.
  - Aplicațiile tip antivirus trebuie instalate pe toate calculatoarele din sistem iar utilizatorii trebuie instruiți cu privire la folosirea acestora.

Standardul de securitate ISO/IEC 17799 (cont.)

- Alte componente care reprezintă obiectul managementului operării și comunicațiilor:
  - intreținerea sistemului, incluzând realizarea copiilor de siguranță, intreținerea jurnalelor de operare, menținerea inregistrărilor cu erori de operare și execuție.
  - adoptarea și implementarea unui management corespunzător asigurării rețelelor de calculatoare.
  - manipularea și securitatea mediilor de stocare - previne intreruperea activităților afacerii.
  - schimbul de aplicații și date intre organizații - previne pierderea, alterarea sau utilizarea necorespunzătoare a informației.

Standardul de securitate ISO/IEC 17799 (cont.)

- Protecția rețelelor implică tehnologii dedicate care se folosesc in implementarea măsurilor de securitate și asigurarea obiectivelor de control:
  - *filtru* - reprezentat de un set de reguli implementate la nivelul unui router sau firewall prin care acesta permite tranzitarea sau nu a traficului către și dinspre rețeaua unei companii;
  - *firewall* – dispozitiv prin care este controlat traficul dintre rețeaua companiei și rețelele externe acesteia;
  - *Sistem pentru Detectarea Intruziunilor (IDS – Intrusion Detection System)*, dispozitiv (hardware sau software) care se ocupă de inspectarea traficului unei rețele cu scopul identificării automate a activităților negative;

Standardul de securitate ISO/IEC 17799 (cont.)

- criptare comunicațiilor – procesul prin care datele sunt aduse intr-o formă neinteligibilă persoanelor neautorizate;
- Rețea Virtuală Privată (VPN – Virtual Private Network) - o rețea care permite comunicarea intre două dispozitive prin intermediul unei infrastructuri publice (nesigure)
- zona demilitarizată (DMZ) - reprezintă o parte a rețelei care permite accesul controlat din rețeaua Internet. Mașinile dependente de accesul direct la rețeaua Internet, cum ar fi serverele de email și cele de web sunt adesea plasate in astfel de zone, izolate de rețeaua internă a organizației.

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 7 - Controlul accesului
  - Confidențialitatea reprezint și se ocupă de protejarea informațiilor impotriva oricărui acces neautorizat.
  - Controlul accesului incepe cu stabilirea cerințelor de acordare a drepturilor de utilizare a informațiilor.
  - Trebuie să existe proceduri formale prin care să se controleze alocarea drepturilor de acces la serviciile și resursele IT.
  - Utilizatorii autorizați trebuie să parcurgă o instruire cu privire la maniera in care trebuie raportate activitățile sau acțiunile considerate suspecte.

Standardul de securitate ISO/IEC 17799 (cont.)

- Standardul prevede măsuri de control pentru fiecare nivel al sistemului informațional:
  - controlul accesului la serviciile rețelei - conexiunile la serviciile rețelei trebuie controlate iar pentru obținerea accesului la astfel de servicii este recomandată implementarea unei proceduri formale.
  - controlul accesului la nivelul sistemului de operare – sistemul de operare trebuie să prevadă măsuri de restricționare a accesului la date existente pe calculatore.
  - controlul accesului la aplicații - prevenirea accesului neautorizat la informațiile gestionate de aplicațiile software.

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 8 - Dezvoltarea și intreținerea sistemului
  - Obiectivele de control prevăzute in cadrul acestei secțiuni a standardului au ca scop să se asigure că noile sisteme dezvoltate au prevăzute mecanisme de securitate, prin:
    - dezvoltarea cerințelor și analiza specificațiilor de securitate;
    - validarea datelor de intrare
    - controlul procesării interne
    - autentificarea mesajelor transmise electronic
    - validarea datelor de ieșire
    - utilizarea tehnicilor de criptare
    - utilizarea mecanismelor de semnare electronică
    - protejarea codului aplicațiilor și a fișierelor sistemului de operare

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 9 - Planificarea continuității afacerii
  - Un plan de continuitate a afacerii reprezintă o serie de măsuri pentru reacție in caz de urgență, de operare alternativă și de restaurare a situației in caz de dezastru.
  - Scopul unui plan de continuitate este de a asista organizațiile in a continua să funcționeze atunci când activitatea normală este intreruptă.
  - Asigurarea continuității afacerii presupune parcurgerea etapelor de documentare, testare și implementare a planului de continuitate a afacerii.

Standardul de securitate ISO/IEC 17799 (cont.)

- Secțiunea 10 - Conformitatea
  - Proiectarea, operarea sau gestiunea sistemelor informaționale pot face obiectul unor reglementari, legi sau angajamente contractuale in ceea ce privește securitatea.
  - Pentru evitarea incălcării dispozițiilor legale, standardul include o serie de măsuri, precum:
    - identificarea legislației aplicabile
    - utilizarea adecvată a licențelor software sau a materialelor protejate de drepturi de autor
    - protejarea inregistrărilor organizației (inregistrări contabile, chei de criptare, jurnale de activitate, medii de stocare, proceduri de lucru)

Bibliografie

Recomandări bibliografice pentru aprofundare:

- Popa Sorin Eugen - *Securitatea Sistemelor Informatice*, Capitolul 1 - paginile 5-15, http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf.
- Suportul pentru CISSP și CISM. Capitolele 1 și 2.