

Tema nr.1 Concepte generale privind Securitatea Informației

1. Concepte generale privind SI.
2. Scurtă istorie a securității informaționale.
3. Nivelele de structurare a conceptului de SI

Lector univ. R.Bulai

Concepte generale privind SI

- Informatia reprezinta cea mai mare valoare in orice organizatie, alaturi de resursele financiare si cele umane
- Indiferent de forma pe care o îmbracă, mijloacele prin care este memorată, transmisă sau distribuită, informația trebuie protejată.

Concepte generale privind SI

Securitatea informației este procesul de protejare a datelor prelucrate, stocate și transmise contra accesării, modificări și/sau distrugerii, de asemenea, protejarea resurselor informaționale contra încercărilor de limitare a procesului de funcționare a acestora.

Concepte generale privind SI

SI are ca scop oferirea celor mai importante tehnologii, solutii si servicii profesionale aferente ariilor de securitate, networking, infrastructura de acces, storage si virtualizare, precum si suport activ pentru generarea acestora.

SI poate fi definită ca un sistem global menit să asigure un nivel adecvat de protecție a informațiilor și a activelor aferente, în scopul de a garanta Disponibilitatea, Integritatea si Confidențialitatea.

Principii

- **DISPONIBILITATEA** proprietatea accesării și utilizării informației doar de către o entitate autorizată
- **INTEGRITATEA** proprietatea de a proteja corectitudinea și caracterul complet al informațiilor
- **CONFIDENTIALITATEA** proprietatea prin care informațiile nu sunt divulgate sau puse la dispoziția unor persoane neautorizate, entități sau procese

Scurtă istorie a securității informaționale

Se pot puncta câteva generații, pe planul evoluției
TI cu impact asupra Sistemelor de securitate:

- G.I – sec. sist. bazate pe calculatoare mari
- G.II – sec. sist. distribuite
- G.III – sec. microcalc., inclusiv a rețelelor locale
- G.IV – sec. Internetului
- G.V – sec. comerțului și afacerilor electronice
- G.VI – sec. afacerilor mobile
- G.VII – sec. globală a lumii virtuale, a întregului spațiu cibernetic

Scurtă istorie a securității informaționale

- La nivel international, in 1960 a fost constituita Federatia Intern. pentru Prelucrarea Informatiilor (IFIP) sub auspiciile Unesco care reuneste peste 58 de tari si depaseste 35000 de membri specialisti.
- Activitatea federatiei este coordonata de 13 comisii tehnice, fiecare cu un numar diferit de grupuri de lucru (101 gr.).
- Comisia TC11 (1984) – *Protectia si securitatea in sistemele de prelucrare a informatiilor*, avind 11 grupuri de lucru: ex. WG11.1(1992) – Managementul SI, WG11.2 (1985) – Securitatea sist. mici, WG11.3(1987) – Sec. datelor si aplicatiilor, WG11.4 – Sec.retelelor etc., WG11.9(2004) – Criminalistica in mediul digital...

Scurtă istorie a securității informaționale

- In 1974 s-a infiintat Institutul pentru Sec. Calculatoarelor (CSI – www.gocsi.com) pentru formarea specialistilor in sec. informatiilor, calculatoarelor si retelelor.
- In 1990 Comitetul pentru Informatii, Calculatoare si Politici de Comunicatie ale OECD (Organizatia pentru Cooperare si Dezvoltare Economica) a constituit un grup de experti care au realizat si semnat in 1992 *Ghidul pentru securitatea sistemelor informationale*.

Istorie

- La începutul anilor '90 BSI (British Standard Institution) a dezvoltat o serie de standarde ca răspuns la cererile industriei, guvernului și mediului de afaceri de a crea o structură comună pentru SI.
- În 1995 autoritatea de reglementare din Marea Britanie a adoptat în mod oficial BS7799.
- În 2000 ISO a preluat primele 4 părți ale BS și le-a publicat sub numele "ISO 17799 – Code of Practice".
- În 2002 a fost revizuită partea a doua a standardului BS7799 pentru a reflecta și prevederile ISO 9001, ISO 14001.
- În 2005 este publicat sub denumirea ISO 27001, totodată, ISO 17799 devine ISO 27002.

Standardele internaționale de securitate

Familia ISO/IEC 2700k

- **ISO/IEC 27001:2005 “Sistemul de Management al Securității Informației”**
- **ISO/IEC 27002:2005/ Cor 1:2007 (sau ISO 17799:2005) “Codul de practică pentru Managementul Securității Informației”**
- ISO 27003: “Direcțiile implementării SMSI”
- ISO 27004: “Măsuri”
- **ISO 27005: “Gestiunea riscurilor în securitatea informațională”**
- ISO 27006: “Cerințe pentru organizațiile care efectuează auditul și certificarea SMSI”
- ISO 27007: “Linii directoare pentru auditul SMSI”

ENISA (European Network and Information Security Agency) - **Agentia Europeana pentru Securitatea Retelelor si a Informatiei**

- Formal, ENISA a luat fiinta in urma adoptarii Regulamentului comun (EC) No.460/2004 al Parlamentului European si al Consiliului Uniunii Europene din data de 10 martie 2004.
- A fost conceputa pentru a intensifica posibilitatile Uniunii Europene, a Statelor Membre ale Uniunii Europene si ale comunitatii de afaceri de a preveni, de a gestiona si de a rezolva problemele de securitate a retelelor si a informatiei, conform Rezolutiei Consiliului: “eAction Plan: Information and Network Security”, adoptata in data de 31 mai 2001 la Waxholm.
- Aceasta noua agentie a Uniunii Europene a devenit operationala in luna septembrie 2005, dupa redislocarea efectuata din Bruxelles in Creta, cat si dupa intrarea in functiune a Staff-ului care a fost recrutat prin concurs tip EU25 dintre candidati provenind din intreaga Europa, constituind o structura creata cu misiunea si scopul de a supraveghea un domeniu foarte specific si important, deopotriva tehnic, stiintific si managerial, Curtea Europeana de Justitie consfintind legalitatea crearii ENISA in data de 2 mai 2006.

Nivelele de structurare a conceptului de SI

Securitatea fizică

Conceptul de securitate poate fi structurat pe trei niveluri, după cum urmează:

1. **Securitate fizică:** este nivelul „exterior” al securității și constă în prevenirea, detectarea și limitarea accesului direct asupra bunurilor, valorilor și informațiilor; de exemplu, într-un sistem distribuit, prima măsură de securitate care trebuie avută în vedere este cea de securitate fizică, prin prevenirea accesului fizic la echipamente: un anumit infractor care dorește să sustragă informații din sistem, trebuie, mai întâi, să intre în contact fizic cu echipamentul.

În afara aspectelor prezentate, securitatea fizică implică luarea măsurilor de protecție împotriva incendiilor, inundațiilor, scăpărilor de gaze și a calamităților naturale, toate aceste măsuri fiind legate de protecția, în ansamblu, a clădirilor împotriva pericolelor potențiale.

Nivelele de structurare a conceptului de SI

Securitatea logică

2. **Securitate logică:** reprezintă totalitatea metodelor ce asigură controlul accesului la resursele și serviciile sistemului; securitatea logică poate fi împărțită în două mari niveluri:
- *niveluri de securitate a accesului;*
 - *niveluri de securitate a serviciilor.*

Principalele *niveluri de securitate a accesului* sunt:

- c. nivelul de acces la sistem: acest nivel este răspunzător de gradul de accesibilitate al utilizatorilor în sistem, de decuplarea sau de cuplare a unor stații;
- d. nivelul de acces la cont: acest nivel verifică dacă utilizatorul are un profil valid pentru sistem;
- e. nivelul drepturilor de acces: după ce un utilizator trece prin cele două niveluri anterioare, el va primi de la sistem anumite drepturi de conectare.

Principalele *niveluri de securitate a serviciilor* sunt:

- f. nivelul de control al serviciilor: acest nivel este răspunzător de funcțiile de raportare a stării serviciilor și, respectiv, de avertizare;
- g. nivelul de drepturi la serviciu: determină modul de utilizare a unui anumit cont de servicii.

Nivelele de structurare a conceptului de SI

Securitatea juridică

3. **Securitate juridică:** este nivelul alcătuit dintr-o colecție de legi naționale care reglementează actul de violare a nivelurilor de securitate fizică și logică și stabilește sancțiuni penale ale acestor acte; aici este important de subliniat că sistemul de securitate fizică trebuie astfel conceput, încât să permită în orice situații analiză posteveniment care să fie utilizată ca „martor” în procesul de realizare a obiectivului de securitate juridică.