Controlul accesului in sistemele informatice

Conf. Univ. Dr. Marius Iulian Mihăilescu

m.mihailescu.mi@spiruharet.ro

Facultatea de Inginerie și Informatică
Universitatea Spiru Haret

09.03.2022

Overview

Scopul

Scop și motivație

Controlul accesului in sistemele informatice se implementează cu scopul reducerii riscului la care sistemele informatice sunt expuse și pentru reducerea pierderilor care pot apărea in caz de dezastre.

Tipuri de control

- *Control preventiv* - previne apariția unor incidente in sistem.
- *Control detectiv* - descoperirea unor apariții ciudate fără a avea o epxplicație logică.
- *Control corectiv* - readucerea la normalitate a sistemului după anumite incidente la care un sistem este expus.
- *Control administrativ* - utilizează proceduri și politici, care ajută la instruirea și conștientizarea asupra pericolelor, verificarea generală, monitorizarea la locul de muncă, verificarea activității și identificarea pericolelor informatice pe perioada concediilor.
- *Control logic sau tehnic* - cuprinde restricții privind accesarea sistemului și a măsurilor prin care protecția informațiilor este asigurată.
- *Control fizic* - reprezintă gărzile de pază și protecție.

Metode pentru controlul accesului

- Controlul impus și ogligatoriu al accesului
- Controlul discret al accesului
- Controlul nediscret al accesului

Combinarea formelor diferite de control

- se pot obține următoarele combinații:
  - preventiv - administrativ
  - preventiv - tehnic
  - preventiv - fizic
    - detectiv - administrativ
    - detectiv - tehnic
  - detectiv - fizic

Control preventiv - administrativ

- se concentrează pe mecanismele software;
- mecanismele software sunt menite și contribuie la atingerea obiectului controlului;
- mecanismele cuprind politicile si procedurile organizaționale;

Control preventiv - tehnic

- vizează utilizarea tehnologiilor pentru consolidarea politicilor de control al accesului;
- se poate realiza prin sistemele de operare, prin aplicații sau printr-o componentăsuplimentară hard/soft;
- mecanismele cuprind politicile si procedurile organizaționale;
- controale: protocoalele, criptarea, cardurile de acces inteligente, biometria, pachetele software pentru realizarea controlului local sau de la distanță, parolele, meniurile , softul de scanare a virușilor etc.
  - protocoalele, criptarea și cardurile inteligente sunt mecanisme tehnice de protejare a informațiilor și parolelor impotriva eventualelor deconspirări.
  - Biometria apelează la tehnologii precum amprenta digitală, a retinei, irisului pentru autentificarea solicitanților de accesare a resurselor sistemului.
  - Pachetele software ce realizează controlul accesului gestionează accesul la resursele ce dețin informații aflate pe plan local sau la distanță.

Control detectiv - fizic

- identificarea violărilor politicilor de securitate folosind diferite mijloace tehnice.
- detectarea intrușilor;
- generarea de rapoarte care cuprind coruperea securității.

Identificare și autentificare

- pentru identificarea unei persoane se folosesc patru moduri:
  - ceea ce se află in posesia unei persoane;
  - ceea ce individualizează persoana;
  - ceva ce persoana știe;
  - locația geografică.

Principiile de bază ale controlului accesului

- *"simpla posesie a unui element de control al accesului nu trebuie să constituie și proba accesului privilegiat la informațiile importante ale firmei, intrucât el poate fi dobândit și pe căi ilegale dau poate fi contrafăcut"* [1]
- *"atunci când valorile patrimoniale sunt deosebit de importante și mecanismul de protecție trebuie să fie pe măsură"* [1]
- *"nici unei persoane nu trebuie să i se garanteze accesul permanent, gestiunea sau cunoașterea informațiilor secrete numai pe motivul poziției ierarhice pe care o deține"* [1].

Controlul accesului prin obiecte

- cartele de plastic/electronice/RFID
- dispozitive biometrice [2]
- carduri inteligente (criptare/decriptare)

Bibliografie

Recomandări bibliografice pentru aprofundare:

- Popa Sorin Eugen - *Securitatea Sistemelor Informatice*, Capitolul 2 - paginile 16-24, http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf.
- Mihailescu Marius Iulian and Nita Stefania Loredana. Security of Biometrics Authentication Protocols Practical and Theory Applications. 2015. Open WorldCat, https://nbn-resolving.org/urn:nbn:de:101:1-20151006955.
- Suportul pentru CISSP și CISM.