IMPLEMENTAREA UNEI POLITICI DE SECURITATE EFICIENTE

Autor: Arina Lachi
Conducător ştiinţific: Pavel Nistiriuc

Universitatea Tehnică a Moldovei

Abstract: *Securitatea sistemelor informaţionale reprezintă un proces complex, dependent de o mulţime de factori interni sau externi de care este influenţată în mod direct. Iată de ce adoptarea unei politici de securitate ce va corespunde sistemului vizat este vitală. Păstrarea integrităţii, confidenţialităţii şi disponibilităţii informaţiilor revine ca sarcină importantă managementului sistemului informaţional, iar asta depinde de politica de securitate adoptată şi de modul în care este implementată. Politicile de securitate vor dicta cerinţele de bază şi obiectivele pe care trebuie să le îndeplinească o tehnologie şi va trebui să asigure: continuitatea afacerii şi protecţia informaţiilor confidenţiale.*

Cuvinte cheie: *Risc, securitate, sistem, cerinţe, politică de securitate, utilizator, audit, informaţie, şablon.*

Introducere

Securitatea electronică este definita astfel: "acele politici, recomandări şi acţiuni necesare minimizării riscului aferent efectuării tranzacţiilor electronice, risc ce se referă la breşe în sistem, intruziuni sau furt". Măsurile de securitate nu garantează eliminarea completă a oricărui risc, dar pot să-l reducă la un nivel acceptabil. Securitatea IT se concentrează pe crearea unei platforme de calcul unde persoanele sau programele să nu poată desfăşura acţiuni pentru care nu au drepturi alocate[1].

Cerinţe de securitate

Cerinţele de securitate pe care trebuie să le îndeplinească un sistem informatic sunt[1,2]:

a) Identificarea – reprezintă procesele şi procedurile necesare pentru stabilirea unei identităţi unice pentru un utilizator sau o entitate în cadrul unui sistem informatic. Identificarea permite contabilizarea tuturor operaţiunilor individuale şi previne accesul neautorizat.
b) Autentificarea - este procedura pentru verificarea identităţii entităţii care solicită acces la un sistem, procesul prin care sistemul validează informaţiile de conectare oferite de entitatea utilizatoare.
c) Controlul accesului – determină ce anume poate face o anumită entitate autentificată în sistem, având în vedere: controlul accesului la sistem, controlul accesului la reţea, clasificarea informaţiei, privilegiile.
d) Responsabilitatea – este strâns legată de măsurile de securitate impuse utilizatorilor sistemului, care vor fi răspunzători pentru acţiunile întreprinse după conectarea la sistem.
e) Auditul de securitate se ocupă cu analiza înregistrărilor activităţilor executate, pentru a determina dacă sistemul de protecţie este în concordanţă cu politicile şi procedurile de securitate stabilite. Scopul unui audit este de a identifica slăbiciunile legate de securitate, sau eşecurile care pot fi corectate sau controlate.
f) Integritatea sistemului – pentru a se menţine integritatea sistemului se iau următoarele măsuri:
   - separarea proceselor şi datelor utilizatorilor,
   - separarea proceselor şi datelor sistemului, protejarea software-ului, datelor si hardware-ului de modificări, fie că acestea sunt voite sau accidentale,
   - controlul acţiunilor şi operaţiilor de întreţinere.
g) Integritatea informaţiilor – presupune mecanisme de protecţie a datelor împotriva distrugerii sau accesului neautorizat şi mecanisme de înregistrare a modificărilor survenite.
h) Fiabilitatea serviciilor – se referă la cât de uşor şi sigur un utilizator autentificat poate accesa şi utiliza resursele unui sistem.
i) Documentarea privind securitatea – este vitală pentru menţinerea unui anumit sistem de securitate operaţional şi eficient[2,3].

Politicile de securitate formale vor dicta cerinţele de bază şi obiectivele pe care trebuie să le îndeplinească o tehnologie, pentru a asigura o administrare eficientă a sistemului informaţional de ansamblu.

Politica de securitate

Politica de securitate este o componentă a politicilor de dezvoltare a companiei prin care:

- se garantează continuitatea funcţională a proceselor de afacere,
- se asigură protecţia informaţiilor confidenţiale.

Pentru a realiza un sistem de protecţie eficient este necesar să se parcurgă următoarele cinci etape[1,3]:

- - evaluarea riscurilor,
- - definirea politicii de securitate,
- - implementarea,
- - administrarea,
- - auditul.

Politica de securitate la nivelul unei organizaţii joacă un rol esenţial fiind responsabilă chiar de managementul afacerilor. Pentru stabilirea politicii de securitate vor fi parcurse etapele:

- se analizează riscurile majore ale organizaţiei (pentru definirea procedurilor prin intermediul cărora vor fi prevenite riscurile ca urmare a apariţiei unor evenimente nedorite),
- se defineşte politica de securitate (pentru tratarea componentelor la care nu pot fi prevenite anumite acţiuni fără a impune măsuri de protecţie),
- stabilirea unui plan de urgenţă care se va aplica în cazul în care măsurile de protecţie sunt ineficiente, deoarece aceste probleme nu pot fi rezolvate numai prin definirea unei politici de securitate şi prin investirea de bani pentru anumite activităţi, în final se cere acordul şefului departamentului de management pentru acceptarea unor riscuri[4,5].

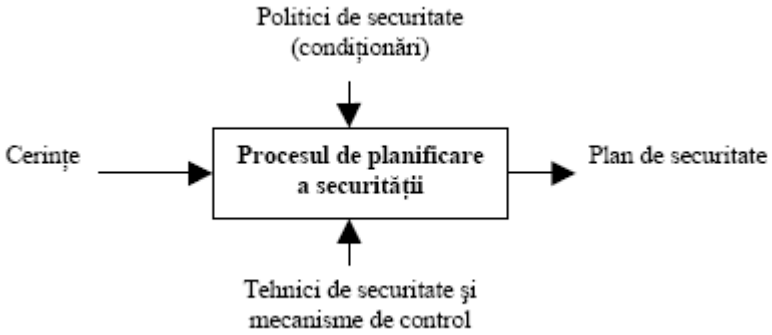

Fig.1 Etapele de creare a planului de securitate

Există mai multe motive pentru care trebuie să fie concepută politică de securitate pentru sisteme şi reţeaua din care ele fac parte:

- O politică solidă ne permite să conturăm securitatea ca un "sistem" ca fiind un set de diferite caracteristici. Spre exemplu, fără o politică, un administrator poate decide să închidă accesul telnet, pentru că transmite parole necriptate, dar să lase deschis accesul ftp, ce deţine aceeaşi slăbiciune. O politică bună de securitate permite identificarea măsurile ce merită aplicate şi cele care nu[2].
- Pentru a diagnostica problemele, conduce audituri sau depista intruşii, este posibil să trebuiască să se intercepteze traficul prin reţea, să se inspecteze istoricul autentificărilor şi comenzilor utilizatorilor şi să se analizeze directoarele home. Utilizatorii trebuie înştiinţaţi de aceste acţiuni, pentru că altfel ele pot deveni ilegale.
- Conturile de utilizator compromise reprezintă unele din cele mai comune ameninţări ale securităţii unui sistem. Trebuie să se explice utilizatorilor importanţa securităţii şi cum să practice o securitate solidă.

Politica efectivă, este un document, sau mai multe documente, ce evidenţiază caracteristicile reţelei şi ale sistemului (cum ar fi serviciile oferite), utilizarea acceptabilă şi utilizarea interzisă, "practici solide" de securitate. Toţi utilizatorii ar trebui înştiinţaţi de politica de securitate, dar şi de modificările aduse acesteia în vederea actualizării[3].

O politică de securitate ar trebui să conţină, cel puţin, următoarele subiecte:

- Utilizare acceptabilă:
  - Aplicaţii Screen saver,

- Manipularea parolei,
- Descărcarea şi instalarea aplicaţiilor,
- Informaţii ce menţionează că utilizatorii sunt monitorizaţi,
- Utilizarea de aplicaţii anti-virus.

➢ Manipularea informaţiei sensibile (în orice formă scrisă, hârtie sau format digital) :

- o Curăţarea biroului şi încuierea informaţiilor confidenţiale,
- o Oprirea sistemului PC înainte de a părăsi spaţiul,
- o Utilizarea encripţiei,
- o Manipularea cheilor colegilor de încredere,
- o Manipularea materialului confidenţial în călătorii[4].

Utilizatori diferiţi pot necesita nivele sau tipuri diferite de acces, deci politica poate varia pentru a acoperi toate situaţiile. Politica de securitate poate deveni foarte mare în conţinut, iar informaţiile vitale pot fi uşor uitate. Politica pentru personalul IT poate conţine informaţii ce sunt confidenţiale pentru utilizatorul obişnuit, fiind vitală împărţirea acesteia în mai multe politici mai mici; spre ex. Politica de Utilizare Acceptabilă, Politica pentru parole, Politica pentru Mesageria Electronică şi Politica pentru Accesul la Distanţă.

Abordarea cea mai bună privind politicile de securitate aplicate în cadrul unei reţele este de a aplica un set de politici de bază la nivelul întregului domeniu, politici care să se aplice tuturor maşinilor (servere şi staţii de lucru) şi tuturor utilizatorilor. Aceste politici vor fi completate diferenţiat cu alte politici suplimentare, aplicabile anumitor roluri funcţionale pe care le au serverele şi staţiile din reţea. Această abordare simplifică modul de gestionare al politicilor şi asigură că este implementat un nivel de securitate de bază (baseline) pentru întreaga reţea.

Două lucruri sunt foarte importante atunci când e necesară asigurarea unui nivel de securitate de bază pentru toate sistemele din reţea:

- sistemele trebuie să fie menţinute la zi din punct de vedere al patch-urilor şi fix-urilor de securitate,
- trebuie să fie aplicat un set de configurări de securitate de bază pe toate sistemele din reţea, adică să se efectueze întărirea securităţii sistemelor(hardening).

Iată câteva setări de securitate care merită luate în considerare pentru securizarea de bază a sistemelor şi pot fi aplicate cu un Group Policy Template la nivelul întregului domeniu Active Directory:

Politici de audit[2,4]:

- Account logon & Management,
- Directory Service Access,
- Object Access,
- System Events.

Privilegiile utilizatorilor:

- Allow log-on locally,
- Logon cu Terminal Services,
- Deny log-on as a batch job,
- Deny force shutdown from Remote system.

Cel mai simplu este să se pornească de la un şablon cu măsuri de securitate, care să fie adaptat la cerinţele sistemului şi să fie aplicat în întreaga reţea. Acest lucru este posibil de făcut cu ajutorul Security Configuration Manager. Acesta conţine: şabloane care definesc setările ce trebuie aplicate pentru câteva configuraţii tipice, snap-in-ul MMC Security Configuration & Analysis, utilitarul linie de comandă secedit cu ajutorul căruia se poate automatiza procesul de aplicare al politicilor.

Şabloanele de securitate sunt fişiere text cu extensia .inf ce conţin un set predefinit de setări de securitate. Aceste setări pot fi adaptate şi aplicate asupra sistemelor din reţea. Setările de securitate disponibile includ: aplicarea de ACL-uri pe chei de Registry şi fişiere, aplicarea de politici de conturi şi parole, parametri de start la servicii, setarea de valori ale unor chei de Registry. Şabloanele sunt aditive, adică se pot aplica succesiv mai multe şabloane. Ordinea de aplicare este importantă: setările din ultimul şablon aplicat vor suprascrie setările anterioare. Template-urile pot fi aplicate global, cu ajutorul Group Policy, sau individual, cu ajutorul Security Configuration & Analysis.

Şabloanele pot fi obţinute din mai multe surse: produsele software ale companiei Microsoft vin cu un set predefinit de template-uri,iar în ghidul de securitate a sistemului de operare Windows (Security Guide) pot fi găsite şabloane adiţionale, CIAC, SANS, NSA publică propriile recomandări şi şabloane pentru sistemele de operare Microsoft.

Security Configuration & Analysis este un snap-in MMC cu ajutorul căruia e posibil de a crea o bază de date cu setări de securitate, pot fi importate şabloane şi se pot aplica setări suplimentare, iar apoi se pot compara setările sistemului cu şablonul creat în baza de date[4]. Comparaţia este non-distructivă, adică sunt raportate doar diferenţele între starea actuală a sistemului şi şablonul ales. De asemenea, pot fi aplicate setările respective asupra sistemului curent.

SECEDIT este un utilitar linie de comandă cu ajutorul căruia se pot automatiza operaţiile de aplicare ale template-urilor folosind script-uri. Parametrii programului permit analiza, configurarea, importul, exportul, validarea sau rollback-ul setărilor de securitate aplicate sistemelor.

Aplicând şabloane de securitate asupra sistemelor se poate obţine un nivel de securitate de bază care în timp poate fi îmbunătăţit suplimentar.

Concluzii

Atunci cînd are loc crearea şi implementarea politicii de securitate se porneşte de la vîrful piramidei manageriale, unde se află top managerii. Deoarece ţine de competenţa acestui nivel să fie fixate declaraţia din care reiese: importanţa resurselor informaţionale necesare pentru atingerea obiectivelor strategiilor propuse, dar şi formularea clară a sprijinului acordat tehnologiilor informaţionale precum şi coordonarea activităţilor de definire a procedurilor şi normelor de securitate pe nivelele inferioare. O politică de securitate eficientă ar trebui să înglobeze ca o primă parte prevederile generale, obligatorii impuse de legislaţia în vigoare, iar pe de altă parte ar trebui să conţină un set de reguli interne orientate pe diferite domenii, cum ar fi: securitatea fizică este şi cea mai importantă parte în menţinerea securităţii, dar des este ignorată de administratori, securitatea reţelei din care face parte sistemul, protocoalele şi serviciile implementate şi utilizate iar atît timp cît calculatoarele sunt făcute să proceseze, ele vor utiliza o mulţime de aplicaţii ce prezintă vulnerabilităţi, securitatea personalului şi factorul uman, securitatea stocării datelor, politica de parole şi desigur planul de dezastru pentru continuitatea afacerii deoarece în momentul în care apare o situaţie critică, acest plan va ajuta la restaurarea rapidă şi temporară a unui nivel acceptabil de desfăşurare a activităţii.

Bibliografia

1. King, C.M., Dalton, C.E., Osmanaglu, T.E. – Security Arhitecture: Design, Deployment& Operations,Osborne/McGraw-Hill, New York, 2001.
2. Andress, M. – Surviving Security: How to Integrate People, Process and Technology, SAMS, Indianapolis, 2002.
3. Karnyanszky T.M. – "Reţele de calculatoare si comunicatii de date", Editura Augusta Timisoara, 2001.
4. www.securizare.ro.
5. Held G., Hundley K. – "CISCO - arhitecturi de securitate", Editura Teora, 2000