Hybrid Security Policies

Asist. Radu CONSTANTINESCU
Catedra de Informatică Economică, A.S.E. Bucureşti

Policy is defined as the rules and regulations set by the organization. They are laid down by management in compliance with industry regulations, law and internal decisions. Policies are mandatory. Security policies rules how the information is protected against security vulnerabilities and they are the basis for security awareness, training and vital for security audits. Policies are focused on desired results. The means of achieving the goals are defined on controls, standards and procedures.
Keywords: *security planning, hybrid policy, conflict of interest*

Introducere

O politică de securitate trebuie să răspundă fără echivoc la o serie de probleme şi anume: ce subiecţi pot avea acces, la ce resurse de sistem şi organizaţionale va fi permis accesul şi ce tip de acces va avea fiecare subiect pentru fiecare resursă. O politică de securitate trebuie să specifice în mod clar obiectivele organizaţiei privind securitatea: asigurarea protecţiei datelor împotriva scurgerilor de informaţii către entităţi externe, protejarea datelor faţă de calamităţile naturale, asigurarea integrităţii datelor sau asigurarea continuităţii afacerii. De asemenea trebuie precizat personalul răspunzător pentru asigurarea securităţii, care poate fi un grup restrâns de lucru, un grup de conducere sau chiar fiecare angajat. Este importantă implicarea organizaţiei în ansamblu la asigurarea securităţii care se poate concretiza în instruire în domeniul securităţii sau integrare a părţii de securitate în structura organizaţiei [Pfle03].

Modele de politici de securitate

Dintre cele mai cunoscute modele de politici de securitate sunt cele destinate asigurării confidenţialităţii şi integrităţii datelor. Politicile de confidenţialitate derivate din modele militare se mai numesc politici pentru fluxul de informaţie şi previn dezvăluirea neautorizată a informaţiilor. Modificarea neautorizată a informaţiilor este un obiectiv secundar. Dintre politicile de confidenţialitate este consacrat modelul Bell-LaPadula.

Politicile de integritate, aşa cum reiese şi din nume, se concentrează mai mult pe integritate decât pe confidenţialitate deoarece majoritatea companiilor din mediul economic sunt preocupate în principal de acurateţea datelor decât de relevarea acestora. De exemplu, un sistem de control al inventarului poate funcţiona corect dacă datele administrate devin publice dar nu şi în cazul în care acestea pot fi modificate în mod aleator. Dintre modelele consacrate de politici de integritate se pot aminti modelul Biba şi modelul Clark-Wilson.

Puţine organizaţii se rezumă să abordeze ca şi obiective de securitate doar problematica confidenţialităţii sau a integrităţii. Majoritatea îşi propun obiective mixte ce includ ambele subiecte într-o pondere definită în funcţie de context.

Modelul Zidului Chinezesc este un exemplu de politică mixtă care se adresează în aceeaşi măsură problemelor de integritate şi celor de confidenţialitate. Acesta descrie politici care presupun un conflict de interese asociat activităţii profesionale prestate. Un domeniu în care modelul are largă aplicativitate este cel al burselor de valori sau al societăţilor de investiţii. În acest caz, scopul este prevenirea unei situaţii în care un agent reprezintă doi clienţi ale căror interese sunt asemănătoare, iar agentul ar putea favoriza pe unul în detrimentul celuilalt.

Modelul Zidului Chinezesc: descrierea informală

Să considerăm o bază de date a unei firme de investiţii. Aceasta conţine înregistrările aferente unor companii cu privire la investiţii

sau alte date ce au fost solicitate. O serie de analişti folosesc aceste înregistrări pentru a putea direcţiona investiţiile. Să presupunem că *Agentul X* consiliază *Banca A* şi *Banca B* cu privire la investiţiile pe care acestea le fac. Acest lucru determină un potenţial conflict de interese ceea ce induce faptul că situaţia trebuie evitată. Următoarele definiţii subliniază acest lucru [Bish03]:

Definiţia 1: Obiectele dintr-o bază de date sunt constituite din informaţii referitoare la o anumită companie.

Definiţia 2: O mulţime de date (*CD*) va conţine obiecte asociate unei singure societăţi.

Definiţia 3: O clasă de conflicte de interese (CI) conţine mulţimile de date asociate unor companii aflate în poziţii de competiţie.

Fie *CI(O)* clasa *CI* care conţine obiectul *O* şi fie *CD(O)* mulţimea de date care conţine obiectul *O*. Modelul presupune că fiecare obiect aparţine unei singure clase *CI*.

Agentul X are acces la obiectele *CD* aferente *Băncii A*. Deoarece datele *CD* ale *Băncii A* sunt în aceeaşi clasă *CI* ca şi cele ale *Băncii B*, rezultă că *Agentul X* nu poate avea acces la obiectele din mulţimea de date *CD* asociate *Băncii B*.

Problema implică şi coordonate temporale. Să presupunem că *Agentul X* a lucrat iniţial pentru portofoliul *Băncii B* şi apoi a fost transferat să lucreze cu portofoliul *Băncii A*. Cu toate că momentan utilizează o singură mulţime de date *CD* din clasa *CI* aferentă băncilor, o mare parte din informaţiile însuşite în activitatea anterioară este valabilă în continuare. Prin urmare se ajunge din nou la un conflict de interese. Vom considera următoarea regulă, unde *PR(S)* reprezintă mulţimea de obiecte pe care *S* o poate citi.

Condiţia de securitate simplă, versiunea preliminară: Subiectul *S* poate să citească obiectul *O* dacă şi numai dacă una din următoarele condiţii este adevărată.

1. Există un obiect *O'* accesat de *S* şi *CD(O')=CD(O)*.
2. Pentru toate obiectele *O'*, $O' \in PR(S) \Rightarrow CI(O') \neq CI(O)$

Iniţial, $PR(S)=\varnothing$ şi prima solicitare de citire este în mod sigur garantată. În cazul situaţiei descrise anterior, clasa *CI* asociată *Băncii A* este aceeaşi cu cea asociată *Băncii B*, astfel că se aplică punctul 2 din condiţia de securitate simplă şi rezultă că *Agentul X* nu poate accesa un obiect ce aparţine *Băncii B*.

Ca urmare a acestei reguli, apar o serie de consecinţe. Odată ce un subiect citeşte orice obiect dintr-o clasă *CI*, singurele obiecte din clasa respectivă ce vor putea fi accesate sunt din aceeaşi mulţime de date ca şi obiectul citit. Astfel dacă *Agentul Y* accesează date din mulţimea asociată *Băncii B*, acesta nu va mai avea acces la datele din mulţimea asociată *Băncii A*.

În al doilea rând, numărul minim de subiecţi necesari pentru a putea accesa fiecare obiect dintr-o clasă *CI* este acelaşi cu numărul mulţimilor de date *CD* din clasa respectivă. Astfel o firmă va trebui să aibă un număr de agenţi echivalent cu numărul de elemente distincte din clasa respectivă.

În practică, companiile dispun de informaţii ce pot fi făcute publice, cum ar fi bilanţul sau alte rapoarte ce trebuie furnizate statului. Modelul nu trebuie să restricţioneze aceste informaţii, care trebuie să fie disponibile tuturor. Prin urmare, modelul va distinge datele publice de cele private. Datele private vor intra sub incidenţa condiţiei de securitate simplă, iar cele publice nu. Condiţia poate fi reformulată astfel:

Condiţia de securitate simplă: Subiectul *S* poate să citească obiectul *O* dacă şi numai dacă una din următoarele condiţii este adevărată.

1. Există un obiect *O'* accesat de *S* şi *CD(O')=CD(O)*;
2. Pentru toate obiectele *O'*, $O' \in PR(S) \Rightarrow CI(O') \neq CI(O)$;
3. *O* este un obiect privat.

Să presupunem că *Agentul X* şi *Agentul Y* lucrează în aceeaşi companie, iar *Agentul X* poate să citească obiecte ce conţin informaţii cu privire la *Banca A* iar *Agentul Y* poate să citească informaţii aferente *Băncii B*. Să presupunem că amândoi pot să citească obiecte aferente mulţimii de date *CD* asociată *Societăţii de Asigurări C*. În cazul în care *Agentul A* poate scrie obiecte din mulţimea *CD* a *Societăţii de Asigurări C*, este posibilă situaţia

ca acesta să citească informaţii din mulţimea asociată *Băncii A* şi să le scrie în cea asociată *Societăţii C*. *Agentul Y* va putea astfel să le citească, determinând un conflict de interese. Condiţia de securitate simplă va trebui să fie completată astfel:

*Proprietatea *:* Un subiect *S* poate să scrie un obiect *O*, dacă şi numai dacă sunt respectate următoarele două condiţii:

1. Condiţia de securitate simplă permite ca *S* să citească *O*;
2. Pentru toate obiectele private *O'*, *S* poate să citească *O'* $\Rightarrow$ *CD(O')=CD(O)*.

În exemplul anterior, *Agentul X* poate să citească obiecte atât din mulţimea de date asociată *Băncii A* cât şi din cea asociată *Societăţii C*. Prin urmare condiţia 1 este îndeplinită. Presupunând că mulţimea de date a *Băncii A* conţine şi date private, ceea ce este foarte probabil, din cauză că *Agentul X* poate să citească aceste obiecte, *condiţia 2* este falsă. Prin urmare *Agentul X* nu va putea scrie obiecte din mulţimea de date asociată *Societăţii C*.

Modelul Zidului Chinezesc: formalizare matematică

Fie o mulţime de subiecţi *S*, *O* o mulţime de obiecte şi $L=C\times D$ o mulţime de etichete. Vom defini funcţiile de proiecţie $l_1:O\rightarrow C$ şi $l_2:O\rightarrow D$. Mulţimea *C* corespunde unui set de clase *CI* iar mulţimea *D* corespunde unui set de obiecte *CD*. Valoarea asociată lui $s\in S$ şi $o\in O$ din matricea de acces este *H(s,o)* şi poate lua valorile adevărat şi fals. Valoarea adevărat apare în cazul în care *s* are sau a avut acces de citire la obiectul respectiv iar valoarea fals în cazul invers. O relaţie de tipul *R(s,o)* reprezintă cererea lui *s* pentru a citi obiectul *o* [Bish03].

Prima prezumţie a modelului este că o mulţime de date *CD* nu poate fi cuprinsă în două clase *CI*. Prin urmare, dacă două obiecte se regăsesc în aceeaşi mulţime *CD* acestea vor trebui să se regăsească şi în aceeaşi clasă *CI*.

Axioma 1: Pentru toate elementele $o, o'\in O$, dacă $l_2(o)=l_2(o')$, atunci $l_1(o)=l_1(o')$.

Vom specifica şi abordarea pentru cazul contrar:

Lema 1: Pentru toate elementele $o, o'\in O$, dacă $l_1(o)\neq l_1(o')$, atunci $l_2(o)\neq l_2(o')$.

Prin urmare două obiecte situate în clase *CI* diferite se vor regăsi în seturi de date *CD* diferite.

Axioma 2: Un subiect *s* poate să citească un obiect *o* dacă şi numai dacă pentru toţi $o'\in O$, iar *H(s,o')=A (adevărat)*, atunci fie $l_1(o')\neq l_1(o)$ fie $l_2(o')=l_2(o)$.

Axioma este reprezentarea formală a condiţiei de securitate simplă. Un subiect poate să citească un obiect dacă şi numai dacă nu a citit deja obiecte din alte seturi de date din cadrul aceleiaşi clase *CI* sau dacă a citit deja obiecte din mulţimea de date *CD* asociată obiectului respectiv. Această regulă trebuie aplicată din primul moment pentru a putea fi valabilă pentru toate stările prin care trece sistemul. Starea cea mai simplă în care acest lucru este valabil este cea în care nu s-a înregistrat încă nici un acces la obiecte. În această stare orice cerere de acces la obiecte va fi satisfăcută. Vom formaliza aceste lucruri în axiomele următoare:

Axioma 3: H(s,o)=F (*fals*) pentru toţi $s\in S$ iar $o\in O$ este o stare iniţială sigură.

Axioma 4: Dacă pentru $s\in S$ şi pentru toţi $o\in O$, *H(s,o)* este falsă atunci orice cerere *R(s,o)* este garantată.

Următoarea teoremă sintetizează faptul că un subiect nu poate să citească obiecte din cadrul unei clase *CI* decât dintr-un singur set de date.

Teorema 1: Să presupunem că un subiect $s\in S$ a citit un obiect $o\in O$. Dacă *s* poate să citească $o'\in O$, $o'\neq o$, atunci $l_1(o') \neq l_1(o)$ sau $l_2(o') = l_2(o)$.

Demonstraţie: Vom face demonstraţia prin presupunere prin absurd. Deoarece *s* poate să citească *o* rezultă că *H(s,o)=A*. Să presupunem că *s* poate să citească şi obiectul *o'*, atunci *H(s,o')=A*. Din ipoteză avem că $l_1(o') = l_1(o)$ şi $l_2(o') \neq l_2(o)$. Sintetizând rezultă că:

$$H(s,o)=A \wedge H(s,o')=A \wedge l_1(o') = l_1(o) \wedge l_2(o') \neq l_2(o) \quad (*)$$

Fără a pierde din generalitate vom presupune mai întâi că *s* poate să citească *o*. Prin urmare *H(s,o)=A* şi din *Axioma 2* rezultă că *s* poate să citească *o'* atunci când fie $l_1(o')\neq l_1(o)$, fie

$l_2(o')=l_2(o)$. De aici obţinem pentru expresia (*) următoarea formă:
$(l_1(o')\neq l_1(o) \vee l_2(o')=l_2(o)) \wedge (l_1(o') = l_1(o) \wedge l_2(o') \neq l_2(o))$,
ceea ce este echivalent cu:
$(l_1(o')\neq l_1(o) \wedge l_1(o') = l_1(o) \wedge l_2(o') \neq l_2(o)) \vee (l_2(o')=l_2(o) \wedge l_1(o') = l_1(o) \wedge l_2(o') \neq l_2(o)$,
însă:
$l_1(o')\neq l_1(o) \wedge l_1(o') = l_1(o) = F$ (**) şi
$l_2(o')=l_2(o) \wedge l_2(o') \neq l_2(o) = F$ (***).
Din (**) şi (***) rezultă că expresia (*) este falsă, ceea ce contrazice ipoteza.

Lema 2: Presupunând că un subiect $s \in S$ poate să citească un obiect $o \in O$, atunci s nu poate să citească obiectul o' pentru care $l_1(o') = l_1(o)$ şi $l_2(o') \neq l_2(o)$. Lema este o consecinţă imediată a *Teoremei 1*.

Teorema 2: Fie $c \in C$ şi $d \in D$. Presupunând că există n obiecte $o_i \in O$, $1 \leq i \leq n$, pentru care $l_1(o_i)=c$ şi $l_2(o_i)\neq l_2(o_j)$, $1 \leq j \leq n$ şi $i \neq j$ atunci pentru toate aceste obiecte o există un $s \in S$ care poate să le citească dacă şi numai dacă $n \leq |S|$.

Demonstraţie: Din *Axioma 2* rezultă că în cazul în care un subiect s poate să citească un obiect $o \in O$, atunci el nu poate să citească nici un alt obiect $o' \in O$. Deoarece există n astfel de obiecte rezultă că trebuie să fie cel puţin n subiecţi pentru a se respecta condiţiile teoremei.

În continuare vom aborda problematica datelor publice. Fie $v(o)$ versiunea ce conţine numai date publice ale obiectului o. În cazul în care $v(o)=o$ înseamnă că obiectul conţine numai date publice. Toate versiunile de acest tip ale obiectelor existente sunt ţinute într-un set de date special care face parte dintr-o clasă *CI* ce nu mai conţine nici un alt set de date.

Axioma 5: $l_1(o)= l_1(v(o)) \Leftrightarrow l_2(o)= l_2(v(o))$
Scrierea este permisă doar dacă informaţia nu se poate transmite indirect între doi subiecţi, de exemplu obiectul nu poate fi folosit ca un fel de cutie poştală. Următoarea axiomă surprinde acest lucru.

Axioma 6: Un subiect $s \in S$ poate scrie un obiect $o \in O$ dacă şi numai dacă următoarele condiţii sunt respectate simultan:

1. $H(s,o)=A$;
2. Nu există $o' \in O$ şi $H(s,o')=A$ astfel încât $H(s,o')=A$, $l_2(o')\neq l_2(o)$, $l_2(v(o))$ şi $l_2(o')\neq l_2(v(o'))$.

Următoarea definiţie surprinde noţiunea de flux informaţional statuând faptul că informaţiile pot trece de la un obiect la altul în cazul în care subiectul le poate accesa pe amândouă.

Definiţia 4: Informaţiile pot trece de la obiectul $o \in O$ la $o' \in O$ dacă există un subiect $s \in S$ astfel încât $H(s,o)=A$ şi $H(s,o')=A$. Acest lucru poate fi scris astfel: (o,o').

Informaţiile pot circula şi în cazul în care accesul este de tip *read-only*, deoarece s poate manipula informaţiile conţinute de ambele obiecte, acesta funcţionând pe modelul unei entităţi terţe. Următoarea teoremă specifică faptul că informaţiile private sunt reţinute în setul de date propriu iar cele publice pot circula în mod liber în sistem.

Teorema 3: Pentru un sistem dat, mulţimea informaţiilor care pot circula este:
$\{(o,o') \mid o \in O \wedge o' \in O \wedge l_2(o) = l_2(o') \vee l_2(o) = l_2(v(o))\}$

Demonstraţie: $F=\{(o,o') \mid o \in O \wedge o' \in O \wedge (\exists) s \in S$ *a.î.* $(H(s,o)=A \wedge H(s,o')=A)\}$ este mulţimea tuturor fluxurilor de informaţii din sistem, conform *Definiţiei 4*. Fie mulţimea F^* închiderea tranzitivă a mulţimii F, care reprezintă toate fluxurile de informaţii ce pot să survină în momentul în care sistemul schimbă starea. Regulile ce interzic accesul de scriere vor condiţiona care dintre fluxuri vor fi permise. *Axioma 6* exclude elementele din mulţimea:
$X=\{(o,o') \mid o \in O \wedge o' \in O \wedge l_2(o) \neq l_2(o') \wedge l_2(o) \neq l_2(v(o))\}$.
Fluxurile posibile rămase se regăsesc în diferenţa dintre mulţimea F^* şi X:
$F^*-X=\{(o,o') \mid o \in O \wedge o' \in O \wedge \neg(l_2(o) \neq l_2(o') \wedge l_2(o) \neq l_2(v(o)))\}$, ceea ce este echivalent cu forma:
$F^*-X=\{(o,o') \mid o \in O \wedge o' \in O \wedge (l_2(o) = l_2(o') \vee l_2(o) = l_2(v(o)))\}$, ceea ce trebuia demonstrat.

Concluzii

Orice plan de securitate trebuie să specifice politica de securitate a unei companii sau entități. O politică de securitate conține precizarea scopurilor şi a intențiilor. La o primă vedere toate politicile de securitate sunt similare având ca obiectiv prevenirea breşelor de securitate. În realitatea elaborarea unei politici de securitate este un proces dificil care presupune adaptarea la specificul organizației.

Spre deosebire de politicile de confidențialitate, modelul Zidului Chinezesc nu asociază etichete de securitate subiecților. De asemenea este fundamental menținerea istoricului accesărilor anterioare, ceea ce pentru un model de tipul Bell-LaPadula este un amănunt nerelevant. Un alt aspect este faptul că în momentul inițial un subiect poate accesa orice set de date, ceea ce este inadmisibil pentru o politică de confidențialitate. Modelul Zidului Chinezesc inhibă creşterea odată ce subiecții accesează mai multe obiecte, în schimb modelul Bell-LaPadula constrânge din primul moment setul de obiecte ce poate fi accesat de un subiect. Acesta nu poate fi schimbat decât prin intervenția unui responsabil autorizat care poate modifica acceptabilitatea unui subiect sau clasificarea unui obiect.

Modelele de integritate, cum ar fi modelul Clark-Wilson abordează aspecte cum ar fi validarea sau verificarea precum şi controlul accesului. Deoarece modelul Zidului Chinezesc are ca obiectiv asigurarea exclusiv a controlului accesului, acesta nu poate emula integral un model de integritate.

Bibliografie

[Bish03] Bishop, M. – "*Computer Security Art and Science"*, Ed. Addison-Wesley, 2003

[PaBi01] Patriciu, V., Bica - "*Securitatea comertului electronic*", Ed. All, 2001

[PaVa99] Patriciu V., Vasiu I, Patriciu S. – "*Internetul şi dreptul*", Bucureşti, Ed. AllBeck,1999

[Pfle03] Pfleeger, C. – "*Security in Computing",* Ed. Prentice Hall, 2003

[Tane01] Tanenbaum, A. – "*Modern Operating Systems*", Ed. Prentice Hall, 2001.