5. CONTROLUL ACCESULUI

Preliminarii

În această temă vom analiza metoda obligatorie care trebuie implementată în orice sistem informatic înainte de achiziționarea și configurarea altor tehnologii de securitate, și anume, controlul accesului. Controlul accesului este metoda prin care sistemele determină dacă și cum să admită un utilizator într-o zonă de încredere a organizației – adică sistemele informaționale, zonele restricționate precum sunt sălile de calculatoare etc.

Scopul:

- *studierea aspectelor importante ce țin de controlul accesului în organizații din perspectiva securității cibernetice, analiza tipurilor și modelelor de control al accesului fizic, logic și administrativ.*

Obiectivele educaționale:

- *discutarea importanței controlului accesului în sistemele informatice și înțelegerea conceptelor generale;*
- *studierea modelelor principale prin care are loc controlul accesului;*
- *studierea tipurilor de control al accesului.*

Finalitățile de referință:

- *înțelegerea importanței controlului accesului în sistemele informatice și rețelele de comunicații electronice ale companiei;*
- *capacitatea de a determina cel mai potrivit model de control al accesului pentru informații, într-un anumit context;*
- *dezvoltarea abilităților de implementare a tipurilor și modelelor diferite de control al accesului.*

Modalitățile de evaluare

Evaluarea masteranzilor se va efectua în baza testelor formative realizate pe parcursul semestrului de studiu, care vor conține întrebări de tip grilă, întrebări deschise și studii de caz. De asemenea, masteranzii vor îndeplini sarcini practice individuale sau de grup și vor prezenta oral o temă relevantă domeniului de securitate cibernetică. La finele semestrului masteranzii vor susține un examen care va acoperi toate temele din acest suport de curs

.

5.1. Concepte generale

Controalele tehnice nu pot asigura securitatea mediului tehnologic (IT), dar sunt aproape întotdeauna o parte esențială a programelor de securitate a informațiilor (InfoSec). Gestionarea, dezvoltarea și utilizarea controalelor tehnice privind tratarea riscurilor cu care se confruntă organizația necesită anumite cunoștințe și familiarizarea cu tehnologia care permite aceste controale.

Controlul accesului se realizează printr-o combinație de politici, programe și tehnologii [6]. Pentru a înțelege controalele de acces, trebuie mai întâi să se înțeleagă că acestea se concentrează pe permisiunile sau privilegiile pe care un subiect (utilizator sau sistem) le are asupra unui obiect (resurse), inclusiv dacă, când și de unde un subiect poate accesa un obiect și mai ales modul în care subiectul poate folosi acel obiect.

Controalele tehnice pot permite și/sau amplifica aplicarea politicilor acolo unde comportamentul uman este greu de reglat. O politică de parole care specifică puterea parolei (lungimea ei și tipurile de caractere pe care le folosește) reglementează cât de des parolele trebuie să se schimbe și interzice reutilizarea parolelor. Însă ar fi imposibil să se aplice o astfel

de politică dacă fiecare angajat va fi întrebat dacă s-a conformat sau intenționează să o facă. Această cerință este cel mai bine aplicată prin implementarea unei reguli automatizate în sistemul de operare. În figura 5.1 este ilustrat modul în care controalele tehnice pot fi implementate într-o infrastructură tehnică. Controalele tehnice care protejează amenințările din afara organizației sunt reprezentate în partea stângă a diagramei. Controalele care apără amenințările din interiorul organizației sunt afișate în partea dreaptă a diagramei. Indivizii din interiorul unei organizații au adesea acces direct la informații putând ocoli multe dintre cele mai puternice controale tehnice.

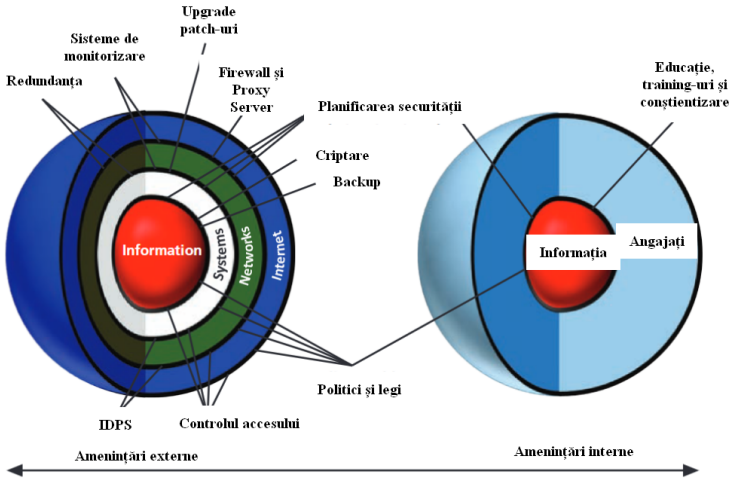

Fig. 5.1. Controale de securitate

Controlul accesului reprezintă regulamentul de utilizare al unui activ informațional, este modul în care organizațiile specifică cine poate folosi o anumită resursă și cum o poate folosi. Controlul accesului este o piatră de temelie a securității, fiind una dintre responsabilitățile predominante ale unui program de securitate cibernetică. Aceasta implică atât reglementări despre ce pot face utilizatorii cu activele, precum și restricționarea accesului la activele informaționale, protejează activele de accesul utilizatorilor neautorizați și se asigură că utilizatorii autorizați folosesc corect informațiile și permisiunile pe care le dețin.

Controlul accesului fizic constă din garduri, încuietori, uși, personal de securitate, capcane pentru a limita accesul la dispozitivele organizației. În mod similar, ***controlul tehnic al accesului constă în restricții tehnologice*** care limitează utilizatorii calculatoarelor în accesarea datelor organizației. Controlul accesului se referă la conceptul AAA – autentificare (cu parolă, PIN etc), autorizare (care îi sunt permisiunile) și audit (înregistrarea acțiunilor utilizatorului în sistem).

Un exemplu indicat care reflectă cum are loc controlul accesului în baza conceptului AAA este retragerea unei sume de bani de la un bancomat, după cum este reflectat în figura 5.2. Utilizatorul trebuie să dețină cardul pe care îl introduce în bancomat și codul PIN pentru a se autentifica. Când este autentificat, utilizatorul este autorizat să facă tranzacții bancare în dependență de resursele financiare pe care le deține, iar sistemul va înregistra, pentru audit, toate operațiunile bancare realizate de către utilizatorul respectiv.

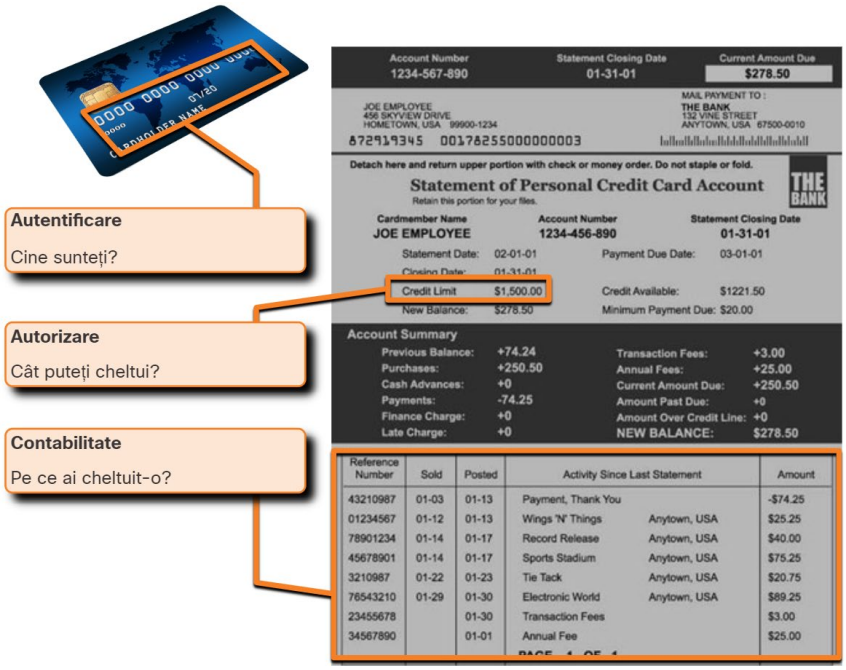

Fig. 5.2. Conceptul AAA [3]

La fel ca și situația descrisă mai sus, utilizatorul unui calculator trece prin aceleași etape descrise în tabelul 5.1.

Tabelul 5.1. Principiul AAA în sistemele informatice

Acțiune	***Descriere***	***Scenariu***	***Proces***
Identificare	Introducerea credențialelor	Accesul la oficiu și accesarea contului de lucru	Utilizatorul introduce numele de utilizator în sistem
Autentificare	Validarea credențialelor	Sistemul verifică validitatea datelor introduse	Utilizatorul introduce parola de acces
Autorizare	Utilizatorul obține acces la sistemul informatic	Accesul la sistemul informatic	Sistemul autorizează utilizatorul cu anumite drepturi de acces asupra resursele
Audit	Înregistrarea acțiunilor utilizatorului	În timpul zilei de lucru utilizatorul accesează mai multe resurse la care are autorizat accesul	Sistemul informatic înregistrează acțiunile utilizatorului când acesta a fost autentificat în sistem

De asemenea, e necesar a clarifica și terminologia utilizată pentru accesul utilizatorului la informații în cadrul organizației, și anume:

- ***obiectul*** – reprezintă o resursă specifică, așa ca un fișier sau dispozitiv la care are acces utilizatorul autorizat;
- ***subiectul*** – este utilizatorul sau procesul care accesează obiectul;
- ***operațiunea*** – reprezintă acțiunea propriu-zisă realizată de către un subiect asupra unui obiect.

Există anumite principii fundamentale care trebuie să fie urmate pentru atribuirea și utilizarea controalelor de acces:

- ***Principiul limitării*** accesului utilizatorilor numai la informațiile solicitate pentru a-și îndeplini sarcinile atribuite. Dacă utilizatorul face parte din Departamentul Marketing, probabil că nu va avea nevoie de acces la informațiile cu care gestionează alte departamente. Mai mult ca atât, este posibil să nu aibă nevoie de acces nici măcar la

toate informațiile departamentului de marketing. Ar trebui să aibă acces doar la informațiile de care are nevoie pentru a-și îndeplini sarcinile de lucru.

- ***Cel mai mic privilegiu*** – persoanele autorizate ar trebui să aibă numai drepturile minime de acces la date și la utilizarea acestora. Accesul la date și drepturile de utilizare descriu ce pot și nu pot face utilizatorii cu acele date. Aceasta este denumită în mod obișnuit CRUD, autorizația de a crea, citi, actualiza și șterge datele. Utilizatorii ar trebui să aibă alocat numai cel mai mic privilegiu necesar pentru a-și îndeplini atribuțiile. Dacă tot ce trebuie să facă este să citească un fișier, nu ar trebui să li se permită să-l modifice sau să îl șteargă.

Controlul accesului se clasifică astfel:

- ***Controlul accesului fizic***: garduri, detectoare de mișcare, încuietoare de laptop, uși încuiate etc.
- ***Controlul accesului logic***: criptarea datelor, cartelele inteligente, parolele, biometria, listele de control al accesului (ACL) care definesc tipul de trafic permis într-o rețea, protocoalele care reprezintă un set de reguli ce guvernează schimbul de date, firewall-urile ce împiedică traficul de rețea nedorit, sistemele IDPS care detectează și previn atacurile în rețea.
- ***Controlul accesului administrativ*:** politicile, procedurile, controalele, clasificarea datelor, instruirea angajaților. Politicile sunt declarații de intenție. Procedurile sunt etapele detaliate necesare pentru efectuarea unei activități; procedurile de angajare implică pașii pe care organizația îi parcurge pentru a găsi angajați calificați; controalele de fond sunt o analiză a ocupării forței de muncă care include informații despre verificarea trecutului privind ocuparea forței de muncă, istoricul creditelor și al criminalității; clasificarea datelor în baza sensibilității acestora; instruirea în domeniul securității are ca scop educarea angajaților cu privire la politicile de securitate într-o organizație.

Strategiile de control al accesului se clasifică în ***discreționare*** (implementate de către utilizator) și ***non-discreționare*** (implementate de către organizație).

5.2. Tipuri de control al accesului

Tipurile de control al accesului securizat sunt [3]:

- *Controalele preventive*. Comenzile de acces preventive opresc activitatea nedorită sau neautorizată. Pentru un utilizator autorizat, un control preventiv de acces înseamnă restricții. Atribuirea privilegiilor specifice unui utilizator pe un sistem este un exemplu de control preventiv. Un alt exemplu ar fi o politică de utilizare adecvată care interzice utilizarea bunurilor companiei în scopuri personale.
- *Controalele de atenuare* care includ: criptarea datelor, paznicii, auditul, camerele web sau un firewall. Un exemplu ar fi un semn care indică monitorizarea video, descurajând potențiale acțiuni.
- *Controalele detective* – detectează sau identifică un incident sau amenințare când are loc, de exemplu, software-ul anti-malware.
- *Controalele corective* – remediază o circumstanță sau atenuează daunele produse în timpul unui incident, de exemplu, modificările realizate la configurațiile unui firewall va bloca reapariția unui atac diagnosticat.
- *Controalele de recuperare* – permit a restabili funcționalitatea sistemului, de exemplu backup-urile și alt software de recuperare.
- *Controalele compensatorii* – evită anumite pierderi prin actualizarea diferitor politici, ca de exemplu politica parolelor.

5.3. Modele de control al accesului

Controlul accesului discreționar (DAC Discretionary Access Control) este cel mai puțin restrictiv, utilizatorul putând alege tipul de acces la propria resursă.

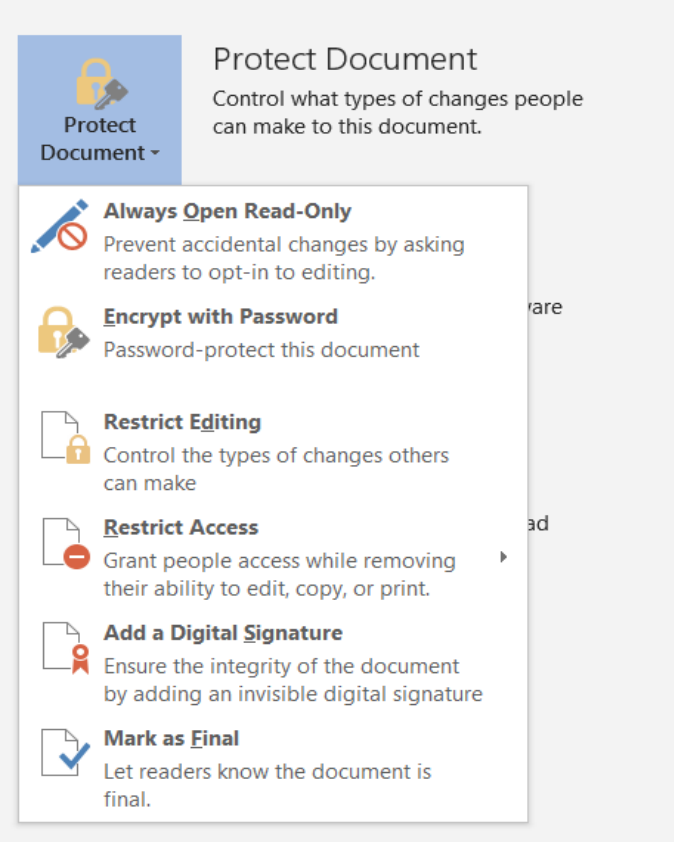

Fig. 5.3. Controlul accesului discreționar

Proprietarul unui obiect determină dacă permite accesul la un obiect în cazul controlului accesului discreționar (DAC). DAC acordă sau restricționează accesul la obiecte în funcție de dorința proprietarului obiectului. După cum sugerează și numele, controalele sunt discreționare, deoarece proprietarul unui obiect cu anumite permisiuni de acces poate transmite acele permisiuni unui alt subiect.

În sistemele care utilizează controale discreționare de acces, proprietarul unui obiect poate decide care subiecți pot accesa acel obiect și ce tip de acces specific pot avea utilizatorii. O metodă comună pentru a realiza acest lucru sunt permisiunile, după cum se arată în figura 5.3. Proprietarul unui fișier poate specifica permisiunile altor utilizatori. Listele de control al accesului sunt un alt mecanism comun utilizat pentru implementarea controlului accesului discreționar. O listă de control al accesului utilizează reguli pentru a determina ce tip de trafic de date poate intra sau ieși dintr-o rețea.

Controalele non-discreționare se clasifică astfel: *controlul obligatoriu al accesului (MAC), controlul accesului bazat pe roluri, controlul accesului bazat pe reguli, controlul accesului bazat pe atribute (ABAC) și controlul accesului bazat pe timp (TAC).*

Controlul obligatoriu al accesului (MAC)

Controlul obligatoriu al accesului (MAC) restricționează acțiunile pe care un subiect le poate efectua cu un obiect. Un subiect poate fi un utilizator sau un proces. Un obiect poate fi un fișier, un port sau un dispozitiv de intrare / ieșire. O regulă de autorizare impune dacă un subiect poate accesa sau nu un obiect. Exemple indicate sunt clasificarea datelor și claritatea măsurilor de securitate implementate. Organizațiile folosesc MAC unde există niveluri diferite de clasificări de securitate. Fiecare obiect are o etichetă și fiecare subiect este autorizat să

acceseze obiectul în baza autorizației avute. Un sistem MAC restricționează un subiect bazat pe clasificarea de securitate a obiectului și pe eticheta atașată utilizatorului. Un exemplu relevant în domeniul militar sunt clasificările Secret și Top Secret (figura 5.4). Dacă un fișier (un obiect) este considerat secret, acesta este clasificat (etichetat) Top Secret. Singurele persoane (subiecți) care ar putea vizualiza fișierul (obiectul) sunt cele cu o autorizație de tip Top Secret. Aceasta depinde de mecanismul de control al accesului pentru a se asigura că o persoană (subiect) care are doar o autorizație secretă nu obține niciodată acces la un dosar etichetat ca secret de top. În mod similar, un utilizator (subiect) eliminat pentru accesul Secret Top nu poate schimba clasificarea unui fișier (obiect) etichetat Top Secret. În plus, un utilizator Top Secret nu poate să trimită un fișier Top Secret unui utilizator care a fost eliminat doar pentru a vedea informații secrete.

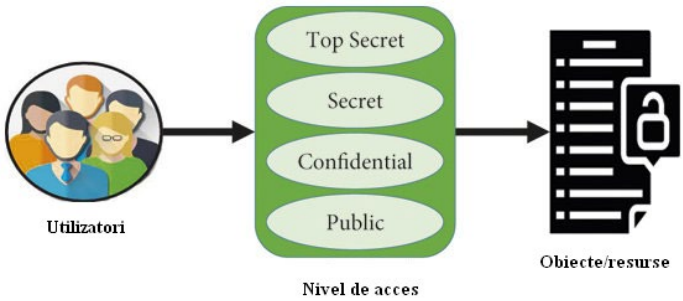

Fig. 5.4. Controlul obligatoriu al accesului MAC

Controlul accesului bazat pe roluri (RBAC)

Controlul accesului bazat pe roluri (RBAC) depinde de rolul subiectului, exemplu reflectat în figura 5.5. Rolurile sunt funcții de serviciu în cadrul unei organizații. Rolurile specifice necesită permisiuni pentru a efectua anumite operații. RBAC poate funcționa în combinație cu DAC sau MAC prin aplicarea politicilor fiecăruia. RBAC ajută la implementarea administrării de securitate în organizații mari cu sute de utilizatori și mii de posibile permisiuni. Organizațiile acceptă pe scară largă utilizarea RBAC pentru a gestiona permisiunile calculatorului într-un sistem sau aplicație ca o bună practică.

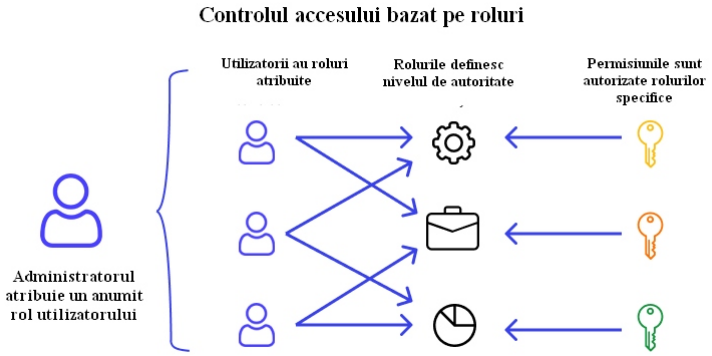

Fig. 5.5. RBAC

Controlul accesului bazat pe reguli

Controlul accesului bazat pe reguli (figura 5.6) utilizează liste de control al accesului (ACL) pentru a putea determina dacă se poate acorda acces. Un exemplu al unei astfel de reguli este acela că nu există niciun angajat care să aibă acces la fișierul de salarizare după orele de lucru. Ca și în cazul MAC, utilizatorii nu pot schimba regulile de acces. Organizațiile pot combina controlul accesului bazat pe reguli cu alte strategii pentru implementarea restricțiilor

de acces. De exemplu, metodele MAC pot utiliza o abordare bazată pe reguli pentru implementare.

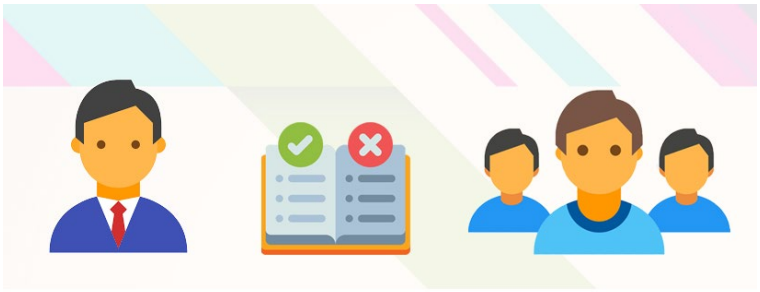

Fig.5.6. Controlul accesului bazat pe reguli

Controlul accesului bazat pe atribute (ABAC)

Controlul accesului bazat pe atribute (ABAC) – permite sau respinge solicitările utilizatorilor bazate pe atributele utilizatorului și atributele obiectului, precum și pe elemente ale mediului care pot fi definite la nivel global și pot fi mai relevante pentru politicile aplicate (figura 5.7).

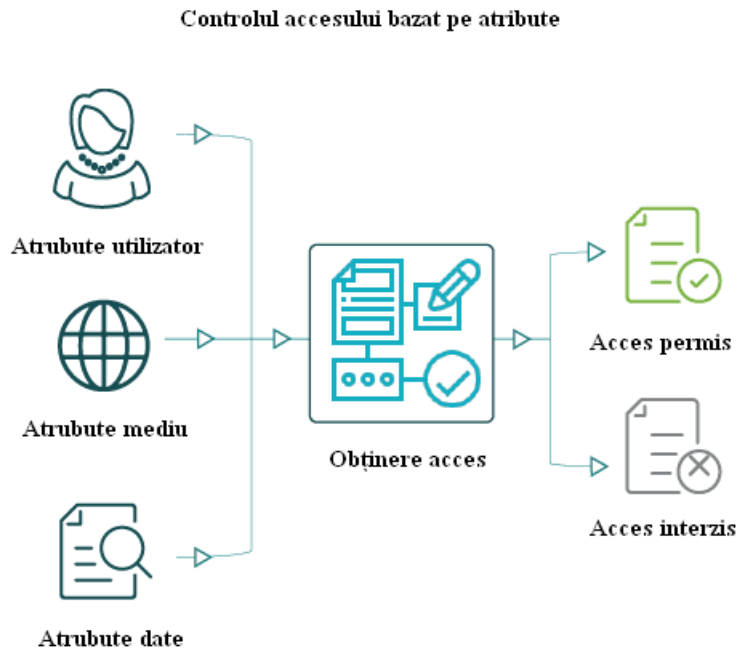

Fig. 5.7 ABAC

Controlul accesului bazat pe timp (TBAC)

Controlul accesului bazat pe timp este o metodă de securitate cibernetică care reglementează accesul la resursele informatice în funcție de intervalele de timp specifice (figura 5.8). Această abordare este utilizată pentru a spori securitatea sistemelor informatice, limitând accesul la resurse doar în anumite perioade prestabilite.

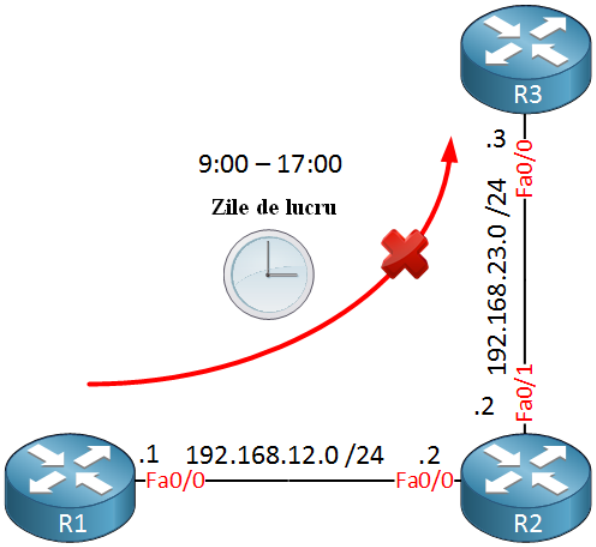

Fig. 5.8. Controlul accesului bazat pe timp, TBAC

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. Analizați și descrieți importanța controlului accesului la sistemele informatice ale unei organizații la alegere.
2. Analizați și descrieți importanța controlului accesului la rețelele de comunicații electronice ale unei organizații la alegere.
3. Care din tipurile de control al accesului este mai puțin restrictiv?
4. Care este contextul de care depinde tipul de control al accesului implementat?
5. Prezentați câte un exemplu relevant pentru fiecare tip de control al accesului.
6. Identificați câte un exemplu relevant pentru modelele de control al accesului: MAC, DAC, RBAC, RBAC, ABAC, TBAC.
7. Care este relația tipică dintre rețeaua publică, firewall și rețeaua de încredere?
8. Ce reprezintă din perspectiva controlului accesului un proces care facilitează accesul utilizatorului la un fișier?
9. Enumerați principiile pe care se bazează conceptul AAA și dați un exemplu din viața reală unde sunt implicate aceste principii.
10. Descrieți, în baza unei organizații la libera alegere, modelele de control al accesului care pot fi utilizate. Argumentați răspunsul.