UNIUNEA EUROPEANĂ
GUVERNUL ROMÂNIEI MINISTERUL MUNCII, FAMILIEI, PROTECȚIEI SOCIALE ȘI PERSOANELOR VÂRSTNICE AMPOSDRU
Fondul Social European POSDRU 2007-2013
Instrumente Structurale 2007-2013
MINISTERUL EDUCAȚIEI NAȚIONALE
OIPOSDRU
Universitatea POLITEHNICA din București

FONDUL SOCIAL EUROPEAN
Investeşte în oameni!
Programul Operaţional Sectorial pentru Dezvoltarea Resurselor Umane 2007 – 2013
Proiect POSDRU/107/1.5/S/76903 – ***Formarea viitorilor cercetatori-experti prin programe de burse doctorale (EXPERT)***

UNIVERSITATEA **POLITEHNICA** DIN BUCUREŞTI

Facultatea de Automatică şi Calculatoare
Departamentul Ingineria Sistemelor

Nr. Decizie Senat ..... din .....

TEZĂ DE DOCTORAT

Soluții eficiente de securitate informatică în sisteme de tip Enterprise

Effective IT security solutions in enterprise systems

Autor: Ing. Nicolae – Marius VLĂDESCU

Conducător de doctorat: Prof.dr.ing. Valentin SGÂRCIU

București 2014

CUPRINS

1. INTRODUCERE

1.1 Importanța securităţii datelor în companii mari şi foarte mari

Acţiunile zilnice din orice ţară în contextul actual sunt dependente în foarte mare măsură de mediul cibernetic, în special acele acţiuni care susţin mediul economic. Cu toate că mediul cibernetic ajută la dezvoltarea şi gestionarea resurselor, atacurile cibernetice şi ilegalităţile din spaţiul cibernetic au crescut simţitor în ultimii ani. În aceeași măsură, companiile mari trebuie să se asigure că sistemele de securitate informaționlă pot face față în permanenţă atacurilor şi ameninţărilor existente.

Companiile mari si foarte mari, indiferent de obiectul activității lor, sunt obligate să lucreze cu informație, din cauza volumului mare de acțiuni sau tranzacții pe care le desfășoară. Comunicarea între persoanele din interiorul companiilor este realizată în mare parte prin intermediul canalelor de comunicare tehnologice (telefon, email, internet, etc.). Este sigur sa afirmam că o mare parte a informațiilor din companiile mari si foarte mari sunt stocate si manipulate prin tehnologie. Această tehnologie poate fi exploatată de către persoane sau sisteme, în scopul de a profita de pe urma informațiilor extrase sau interceptate ilicit, sau în scopul de a aduce prejudiciu companiei țintă.

Din cauza riscurilor enorme pe care le implică securitatea informațională în companii mari şi foarte mari, acestea acorda o foarte mare importanţă problemelor de securitate a informaţiei. Cu toate acestea, companiile au costuri substanțiale anual, provocate de incidente legate de pierderea confidențialității, a integrității sau a disponibilității datelor sau din cauza nefuncționării sau funcționării defectuase a sistemelor informatice.

Una din problemele semnalate de managerii companiilor este reprezentată de problemele de securitate ridicate de noile tehnologii, teren netestat şi fără studii de benchmarking, pe care managerii se pot baza pentru a întreprinde acţiuni de premeditare şi securizare. Există îngrijorări majore legate de operarea în cloud, însă acestea provin din lipsă de înţelegere a cerinţelor de securitate, sau din achiziţionarea de servicii fără a verifica furnizorul în prealabil. Alegerea furnizorului de soluții integrate în cloud este un pas crucial în implementarea unor soluţii informatice bazate pe tehnologie cloud, pentru că toate

mijloacele informatice de securitate se găsesc la furnizor. Trebuie verificat de asemenea dacă furnizorul respecta normele şi procedurile în vigoare.

1.2 Riscuri şi ameninţări la adresa securității datelor în companii

Spaţiul cibernetic este format dintr-o reţea globală de computere şi fluxul de date prin acea reţea. Este o interconectare de reţele politice, economice, culturale şi personale. Spaţiul cibernetic nu este alcătuit doar din internet, computerele conectate la internet şi softurile care rulează pe computere, ci şi din sistemele electronice sau dispozitivele care pot fi conectate direct sau indirect la internet, sau din mecanismele care le conectează. Acestea pot include telefoane, sateliţi, cabluri, routere, servere, reţele sau floppy-disk-uri, cd-uri, dvd-uri, pentru că acestea fac posibilă conexiunea între două computere care nu sunt legate la internet. De aceea, acţiunile cibernetice ilegale sau atacurile cibernetice ridică un risc către toate componentele spaţiului cibernetic şi pot lua multe forme. Incidentele cibernetice sunt considerate acţiuni dăunătoare împotriva indivizilor privaţi, împotriva companiilor şi a bazelor lor de date, iar atacurile cibernetice sunt considerate acţiuni coordonate împotriva instituţiilor publice ale statului, asupra infrastructurii digitale, cât şi a infrastructurii sale critice prin spaţiul cibernetic [12][16].

2. ARHITECTURA SECURITĂȚII INFORMAȚIONALE

Asigurarea unui nivel acceptabil de securitate a informației se realizează plecând de la construirea unei arhitecturi care sa impună eficiența atributelor unui sistem de securitate informațională[23]:

- **Confidențialitatea** – asigurarea că datele pot fi accesate și vizualizate doar de către persoanele și sistemele autorizate. Acest atribut se obține prin controlarea dreptului de a citi informațiile. Divulgarea sau furtul informațiilor cu caracter sensibil pentru organizație, poate avea un efect devastator asupra companiei.
- **Integritatea** – asigurarea că datele nu sunt alterate sau modificate în niciun fel de către persoane sau entități neautorizate. Modificările pot fi făcute intenționat sau accidental.
- **Disponibilitatea datelor** – asigurarea că datele sunt disponibile persoanelor autorizate în orice moment prin disponibilitatea și funcționarea corectă a sistemelor de stocare a datelor, a controalelor de securitate folosite pentru protejarea lor și a canalelor de comunicație folosite pentru a primi și pentru a transmite date.

Aceste atribute sunt realizate prin implementarea anumitor reguli și politici de securitate, menite sa protejeze cele 3 segmente esențiale:

- **Resurse hardware** : servere de aplicații, UPS-uri, hard disk-uri, benzi magnetice, sisteme de ventilație si răcire, sisteme anti-incendiu
- **Resurse software:** aplicații, sisteme de operare
- **Canale de comunicație**

Pentru asigurarea securității celor 3 segmente, propun ca politicile și procedurile de securitate informațională sa fie propagate pe trei niveluri:

- **nivelul fizic** – definit de monitorizarea și controlul mediului în care sunt stocate echipamentele fizice ale infrastructurii hardware
- **nivelul logic** – definit de controale logice care folosesc software și date pentru a monitoriza și controla accesul la informație și sistemele informaționale.

- **nivelul administrativ** – definit de controale administrative care conțin politici, proceduri, standarde și indicații pentru a asigură eficiența atributelor de securitate informațională

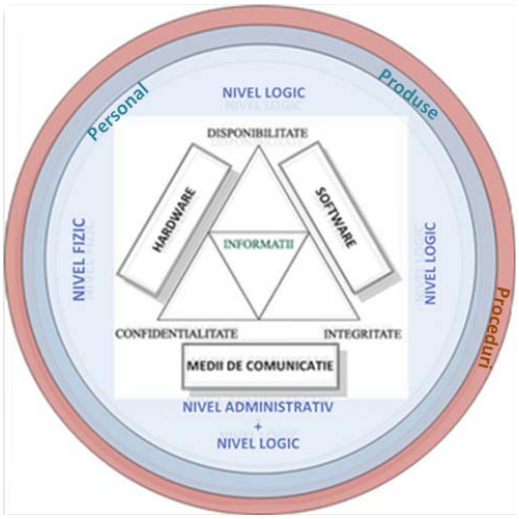

Fig. 2.1 Model de arhitectura de securitate informațională

Nivelul logic este cel mai pregnant nivel din arhitectura securității informaționale și are parte de cea mai mare atenție din partea arhitecților de securitate. Din cadrul elementelor de securitate de nivel logic, criptarea rezolva cele mai multe probleme, asigurând eficiența atributelor de integritate și de confidențialitate a datelor.

2.1 SECURITATEA INFORMATIONALA LA NIVEL FIZIC în data center.

Pentru a asigura baza de funcționare a activității, companiile investesc în masuri de securitate pentru protejarea echipamentelor fizice. Printre masurile de securitate la nivel fizic (a mediilor hardware) al companiilor mari și foarte mari se regăsesc [14]:

- Sistem de acces pe baza cardurilor de acces şi a biometriei
- Sistem de avertizare rapidă a detectării intruziunii
- Sistem de pază(umană) permanentă
- Sistem de supraveghere cu camere video cu circuit închis
- Sistem de monitorizare
- Puncte de control multiple în zonele controlate
- Conexiuni la internet redundante
- Rectificatori de tensiune
- Unităţi (CRAC) redundante pentru monitorizarea şi menţinerea temperaturii, pentru distribuirea aerului şi a umidităţii în data center sau în camera unităţii centrale a reţelei.
- Sisteme de alarmă a incendiului.
- Sisteme de alimentare fără întrerupere(UPS- Uninterruptable Power Supply) redundante

Securitatea reţelei este printre primele obiective ale administratorului de reţea. Gradul de securitate trebuie să fie direct proporţional cu ameninţările care ar putea apărea, şi trebuie făcută o analiză foarte amănunţită, care să ia în considerare dimensiunile organizaţiei, confidenţialitatea datelor şi resursele disponibile.

2.2 SECURITATEA INFORMAȚIONALĂ LA NIVEL LOGIC

Securitatea în mediul virtual în companiile mari şi foarte mari trebuie sa fie instaurată în funcție de infrastructura software de care acestea dispun şi necesită o analiză preliminară amănunțită. Securitatea informațională la nivel logic este considerată a fi cea mai importantă latură a securității informatice, deoarece aduce cel mai mare prejudiciu companiilor şi este supusă unor riscuri mai mari decât securitatea la nivel fizic şi la nivel administrativ. Securitatea informațională la nivel logic în companii mari şi foarte mari are la baza următoarele metode:

- firewall-uri puternice, configurate pentru a proteja porturile, astfel încât să poată avea acces doar persoanele autorizate
- sisteme IDP redundante (Intrusion Detection & Prevention- sisteme de detectarea a intruziunii şi de prevenire)
- anti-viruși puternici actualizaţi în permanență
- rețele virtual private (VPN-uri), pentru informație sensibilă şi aplicaţii
- tunele criptate SSL
- folosirea de parole inteligente
- asigurarea că planurile şi procedurile de securitate dau randament
- evitarea creării de “single point of failure”- o parte din sistem care este esenţială pentru funcţionarea sistemului şi fără de care sistemul nu poate funcţiona. În cazul în care acea parte din sistem cedează, tot sistemul cedează, fără altă cale de repornire.
- folosirea criptării datelor în timpul transmisiei
- folosirea criptării datelor la scrierea pe disc
- folosirea infrastructurii cu chei publice
- folosirea criptării pentru toate transmisiile din internet

2.3 SECURITATEA INFORMAȚIONALĂ LA NIVEL ADMINISTRATIV

2.3.1 Calculatoare fără unităţi de disc

Companiile care au un grad mare de risc pentru datele manipulate de angajaţii lor, implementează în structura informaţională computere fără unităţi de disc, pe care angajaţii le pot folosi doar dacă se autentifica prin nume de utilizator şi parolă sau alte metode de autentificare: smartcarduri, amprentă, metode biometrice.

Un computer fără unitate de disc este un computer care este conectat la o reţea, iar fişierele stocate sau accesate de acesta se găsesc pe un server din reţea, el neavând o unitate de disc proprie. Singurul dezavantaj major este că dacă reţeaua nu funcţionează, computerul este inutil. Din perspectiva costurilor şi a metodelor de securitate care pot fi implementate pe aceste computere, acestea sunt net superioare calculatoarelor cu unitate de disc. Un astfel de computer conţine componentele obişnuite ale unui computer, cum ar fi procesor, memorie RAM, adaptor video, audio sau de reţea, însă foloseşte bootare în reţea pentru a încărca sistemul de operare.

Computerele fără unităţi de disc pot reduce costurile totale ale unei rețele locale, deoarece o capacitate de disc mai mare, care apoi să fie partajata de mai multe computere, este mult mai ieftină decât unităţile de capacitate mică. În plus, staţiile de lucru fără unităţi de disc simplifică procedurile de efectuare a copiilor de rezervă a datelor (backup) şi asigură o securitate mult mai mare datelor. Securitatea sporită pentru staţiile de lucru fără unitate de disc poate fi obţinută din următoarele motive:

- costurile de licenţiere pentru un sistem de securitate performant sunt mult mai mici pentru o singură staţie (serverul pe care sunt stocate toate informaţiile – cel care colectează toată informaţia de la staţiile de lucru)
- protocoalele de securitate sunt mult mai uşor de configurat pe un singur server
- logurile de erori sau de ameninţare sunt mult mai uşor de urmărit pe un singur server
- de obicei companiile care îşi permit implementează „data loss protection", concept care permite implementarea unor protocoale de securitate care urmăresc foarte atent datele sensibile care sunt manipulate de utilizatori. Sistemul poate avertiza administratorul său chiar direct utilizatorul, că acesta a încălcat un protocol de securitate şi ca datele pe care încearcă să le copieze, să le şteargă sau să le trimită prin reţea, sunt sensibile.
- Datele sunt mult mai protejate din punct de vedere fizic
- Serverele sunt conectate la unităţi de curent de rezervă
- Companiile investesc foarte mulţi bani în unităţi de disc criptate. Criptarea pe un singur disc poate fi configurată mult mai uşor, iar costurile mult mai mici decât pentru toate staţiile de lucru din companie.

2.3.2 Salvările pentru copii de rezervă ale datelor şi programelor(Backup-uri)

Administratorul de reţea trebuie să conceapă arhitectura operaţiunilor de salvare a datelor şi a programelor, pe suporţi magnetici, precum şi a păstrării acestora în condiții de deplină securitate, fără a exista situaţii în care acestea nu se pot executa din cauza arhitecturii de reţea sau a unor probleme tehnice cu reţeaua. De aceea, acesta trebuie să aibă în vedere crearea de cai redundante pentru salvarea datelor, să apeleze la mai mulţi furnizori de servicii de date (Internet), şi să creeze tunele securizate pentru salvarea datelor, cu acces limitat pe IP-uri, clase de IP-uri sau adrese MAC. De asemenea, acesta trebuie să construiască VPN-uri care să protejeze datele stocate ca şi copii de rezervă, astfel încât doar persoanele avizate sau programele de legătură să aibă acces la acestea. Administratorul trebuie să coordoneze cron-job-urile(activități programate care rulează cu regularitate) care efectuează copii de rezervă la anumite ore şi în anumite intervale, astfel încât acestea să nu intre în conflict unele cu celelalte, încercând să acceseze sau să folosească aceeași resursă simultan. Trebuie avut în vedere că aceste copii de siguranţă să fie stocate pe suporţi magnetici amplasaţi într-un mediu controlat şi monitorizat, în care să fie active toate protocoalele de securitate existente ca şi pentru datele din interiorul companiei. De obicei, companiile aleg rute(tunele) diferite şi locaţii diferite pentru salvarea copiilor de rezervă. De asemenea, administratorul trebuie să respecte reglementările în vigoare ale legilor de stocare, menţinere şi păstrare a copiilor de siguranţă în termenele de timp prevăzute de lege.

2.3.3 Data loss Prevention (DLP)

Data Loss Prevention (DLP) este definit de un set de tehnologii recent implementate pentru protecţia datelor şi a informaţiilor cu caracter sensibil. Soluţiile DLP monitorizează accesul la datele stocate în interiorul companiei pe de o parte, şi informaţiile transmise în exteriorul companiei pe de altă parte, oferind posibilitatea de a identifica tentativele de acces neautorizat la informaţie şi potenţialele scurgeri de informaţii neautorizate.

Accesul şi manipularea informaţiei se poate controla în trei puncte:

- La momentul accesării datelor din interiorul reţelei companiei, prin validarea accesului la aceste resurse de fiecare dată când acestea sunt utilizate
- La încercările de mutare/copiere a informaţiilor

- La fiecare accesare a datelor, chiar dacă se află într-un mediu necontrolat – date confidenţiale copiate de persoane autorizate la un moment dat pot fi transformate în date inutilizabile, chiar dacă acestea au fost scoase în prealabil din companie.

O soluţie Data Loss Prevention are următoarele funcţii:

- Descoperirea şi clasificarea datelor: acest obiectiv este îndeplinit prin căutare, inventariere şi clasificare a informaţiei aflată pe mediile de stocare ale sistemelor companiei
- Monitorizarea şi protejarea informaţiilor: în funcţie de modul de configurare, sistemul monitorizează şi poate bloca manipularea datelor într-un mod neconform politicilor de securitate instaurate de către companie. Datele pot fi securizate proactiv pentru a preveni scurgerile de informaţii confidenţiale
- Administrare şi raportare: sistemul alertează automat persoanele responsabile cu verificarea securităţii cu privire la potenţialele activităţi incorecte. În special sunt raportate modurile în care sunt manipulate informaţiile clasificate şi principalele ameninţări ridicate de către utilizatorii interni la adresa integrităţii şi securităţii datelor confidențiale.

  Sistemele DLP funcționează în conjuncție cu mecanisme de securitate informațională cum ar fi soluții anti-virus, pe care companiile le instalează atât la nivel de server cât si la nivel de client(cum ar fi laptopuri si tablete). Soluțiile DLP vizează protecția datelor pe toate stările în care se găsesc datele:

  - **Date în repaus** (Data at rest) – date stocate în perimetrul rețelei pe medii mari de stocare, cum ar fi baze de date, servere de fișiere din rețea si magazii de date (data warehouses)
  - **Date în mișcare** (Data in motion) – datele transmise prin internet prin protocoale diferite: HTTP, HTML, FTP, către locații din afara domeniului companiei
  - **Date în folosire** (Data in use) – date stocate si folosite pe dispozitive media mobile, cum ar fi laptopuri si tablete

3. Managementul riscului pentru compromiterea datelor si a sistemelor tehnologice

Riscul reprezintă probabilitatea de apariție a unui eveniment, care, prin alterarea stării sau atributelor unui sistem sau ale unor informații, poate aduce prejudicii companiei care le deține. Pericolele la care este supusa o companie care un sistem de management al riscurilor foarte bine pus la punct includ: pierderi financiare, afectarea reputației, afectarea reputației terților, pierderea oportunităților de afaceri, reducerea performantei sistemelor tehnologice si a organizației, incapacitatea sistemelor sau a personalului sat si exercite activitatea, din cauza sistemelor nefuncționale sau a funcționarii deficitare, etc. [28]. Pentru determinarea probabilității de apariție a unui eveniment cu factor de risc, se analizează amenințările sistemelor informatice si impactul pe care acestea le pot avea.

3.1 Puncte cheie în managementul riscului în tehnologia informației

Procesul de management al riscului din punct de vedere al securităţii datelor şi sistemelor presupune următoarele etape:

3.1.a. **Identificarea vulnerabilităţilor** – prin vulnerabilitate înțelegându-se orice caracteristica a sistemului care îl poate expune la amenințări. Acea caracteristica

este definita de puncte slabe în sistemul informatic, care poate fi exploatat de către sisteme sau persoane rău intenționate si care poate afecta un sistem informatic, sarcinile pe care le executa acesta, sau informațiile stocate la nivel de sistem.

3.1.b. Stabilirea măsurilor de limitare a riscului – în urma studierii infrastructurii hardware si software a companiei, a riscurilor expuse prin vulnerabilități si amenințări, se decid metodele de limitare a riscului. Pentru aceasta se optează pentru următoarele abordări:

- Nu se implementează activitatea generatoare de risc (aceasta situație este foarte puțin probabila având în vedere ca se lucrează cu informație la nivel global) – este valabila doar pe un cerc restrâns de companii
- Transferul riscului prin externalizare, mutând responsabilitatea riscului către o companie specializata care se ocupa de limitarea riscului în companii. Aceasta este una dintre cele mai productive alegeri, din doua motive:
    1. Compania specializata în limitarea riscului cunoaște cele mai bune metode de protecție împotriva amenințărilor si vulnerabilităților, fiind aria sa de expertiza
    2. Daunele provocate de apariția unui incident sunt acoperite intr-o măsura parțiala sau totala de către compania care deține responsabilitatea
- Limitarea riscurilor prin implementarea de politici, masuri si tehnici de securitate foarte puternice; este foarte important ca aceste masuri sa fie de actualitate si sa tina cont de ultimele tehnici folosite de persoane, sisteme sau programe rău intenționate.

Scopul general în adoptarea acestor masuri este acela de a reduce riscurile la care este supusa tehnologia si informația dintr-o companie la nivel acceptat. Nu exista nivel de risc 0, de accesa se evaluează situații si scenarii pe care sa aplice reguli si politici de securitate, astfel incit sa minimizeze cat mai mult dauna produsa de un incident.

3.2 Activități specifice managementului riscului

Riscurile implicate în securitatea informaționala din cadrul unei companii se împart în riscuri care provin si rămân în mediul tehnologic (hardware, software la nivel de sistem de operare, software la nivel de aplicații, date) si riscuri adiacente mediului tehnologic(dezastre naturale, furt de date si aplicații, erori umane, management deficitar).

Activitățile specifice managementului riscului urmăresc o descriere circulara, fiind o activitate continua, deoarece metodele de atac se schimba cu o rata alerta. Acestea sunt următoarele:

- Identificare – procesul de identificare a riscului în cadrul unei companii care are implementat un sistem de corelare de evenimente cu factor de risc are loc la nivel de incident.
- Analiza – procesul de investigare a unui risc pentru a determina natura, impactul pe care îl generează si tipul acestuia.
- Evaluarea impactului – procesul de determinare a nivelului de propagare a riscului către alte sisteme sau funcționalitatea ale acestora si a nivelului de cost provocat companiei

- Evaluarea vulnerabilităţilor – procesul de analiza a sistemelor implementate si a punctelor slabe ale acestora si a gradului de exploatare a acestor vulnerabilități de către persoane sau sisteme râu intenționate
- Monitorizare – procesul de urmărire continua a activităţilor sistemelor din cadrul companiei, în scopul identificării unor situații sau posibile situații de risc pentru sistemele tehnologice din companie
- Măsuri de limitare – procesul de instaurare a unor politici de securitate sau a unor reguli de corelare intre evenimentele cu factor de risc, care au menirea de a proteja sistemele, aplicațiile si datele companiei de riscurile care pot apărea sau sunt inevitabile.

3.3 Evaluarea riscurilor

Evaluarea riscurilor este un factor important în determinarea impactului pe care acestea le-ar putea genera asupra companiei. Securitatea sistemului este raportată la gradul de identificare a vulnerabilităţilor și depinde direct de arhitectura sistemului IT. Politicile de securitate instaurate pot indica probabilitatea de apariție a riscurilor, în funcție de cât de puternice și de pregătite sunt să facă față amenințărilor viitoare.

Evaluarea riscurilor are la baza următoarele acțiuni:

1. **Caracterizarea sistemului** – procesul în care sunt adunate informații privind componentele sistemului informational
2. **Identificarea amenințărilor**
3. **Identificarea vulnerabilităților**
4. **Analiza masurilor de prevenire** asupra situațiilor de risc si a celor de contracarare a apariției acestora.
5. **Determinarea probabilității de apariție** a situației de risc – această probabilitate depinde de gradul de motivare al atacatorului și de gradul de eficiență al sistemelor de securitate implementate în companie.
6. **Determinarea impactului** pe care îl generează riscul – impactul generat de către o situație de risc este indicat de gradul de pierdere pe care îl poate aduce companiei.
7. **Determinarea riscului** – acest procedeu se realizează prin ponderarea probabilității de apariție a situației de risc cu impactul pe care aceasta îl are asupra companiei.[28]

   Nivelul de risc generat prin procedeul de determinare a riscului implică luarea unor decizii cu referire la acțiunile care trebuie luate pentru a pregăti compania pentru o astfel de situație.
8. **Recomandări privind instaurarea masurilor de securitate** – în cazul în care se decide instaurarea unor masuri suplimentare de securitate sau îmbunătățirea celor existente în vederea reducerii nivelului de risc al sistemelor tehnologice, trebuie sa se țină cont de legislația si reglementările în vigoare, de politica organizațională companiei, de impactul operațional si de eficacitatea masurilor instaurate.
9. **Documentarea rezultatelor** – acest proces este foarte important și constă în elaborarea unui raport de evaluare a riscurilor, care ajuta managerii actuali si viitori în luarea deciziilor privind sistemul operațional, bugetul, procedurile implementate, politica si schimbările pe care le adopta în companie.

4. Creșterea securității informaționale folosind corelatoare de evenimente pentru interpretarea elementelor cu factor de risc

Companiile mari au în general un departament de tehnologie cu o ramura în securitate. De obicei, exista mai mulți administratori responsabili cu păstrarea securității sistemelor și datelor la un nivel cat mai ridicat. Distribuția acestora se face pe roluri și este asigurată 24 de ore pe zi. Volumul mare de date care trebuie analizate zilnic face imposibila urmărirea completa a evenimentelor din sisteme. Odată cu creșterea exponențială a datelor, amenințările la adresa companiilor cresc de asemenea. Atacatorii din zilele noastre sunt profesioniști care învață în permanență noi metode de atac și care se specializează prin încercări repetate de exploatare a vulnerabilitățile noi ale sistemelor.

Din cauza numărului mare de sisteme de securitate implementate în companii si a numărului foarte mare de evenimente care trebuie monitorizate, echipele de securitate folosesc în zilele noastre sisteme de management al evenimentelor si de securitate a informației [15]. Acestea au rolul de a agrega toate logurile provenitele de la sistemele cu factor de risc din companie intr-un singur sistem centralizat, care poate facilita raportarea si investigarea incidentelor în timp util.

4.1 Corelatoare de evenimente

Corelatoarele de evenimente reprezintă instrumente importante de management al rețelelor din companii. Acestea preiau activități individuale și alarme semnalate la nivel de rețea și le analizează centralizat, pentru a determina cauza problemelor apărute în rețea. Corelarea este definită ca fiind stabilirea și găsirea de relații între entități. Aceasta este o tehnica cunoscută de securitate pentru a îmbunătății eficiența în identificarea amenințărilor și în analiza proceselor, prin combinarea informațiilor din diferite surse. Pentru a asigura un sistem cat mai sigur de securitate informațională, se instalează o serie cat mai ampla de sisteme de monitorizare în infrastructurile software și hardware ale companiei. Analiza logurilor de eroare și de alarma generate de aceste sisteme a ajuns o provocare chiar și pentru cei mai experimentați analiști de securitate, din cauza numărului foarte mare de notificări. De aceea, primul pas al corelatoarelor de evenimente în micșorarea timpului de analiză pentru evenimente cu potențial de risc, este să centralizeze toate logurile într-o locație comună. Ulterior, acesta este capabil să efectueze legături între aceste loguri, pe baza unor reguli bine definite, pentru a aduce în atenție cele mai importante amenințări. O contribuție foarte relevantă adusă de corelator este eliminarea cazurilor de fals pozitiv și fals negativ [4].

Sistemele de Management al Evenimentelor și de securitate a Informației (SIEM) combină consolidarea evenimentelor cu corelarea amenințărilor, managementul incidentelor și raportarea într-o singură soluție [4]. Un scop principal este sa se folosească o tehnica de corelare automată a evenimentelor pentru a crește eficiența în cazul incidentelor în derulare. Automatizarea analizei unei cantități mari de informație și reducerea numărului de evenimente care trebuie analizate, permite un nivel de acționare asupra amenințărilor mai sporit [13]. De exemplu, un singur atac poate genera loguri care indică o scanare a porturilor în firewall, recunoașterea unei semnături de atac în IDS –Sistem de detectare a intruziunilor, și o serie suspicioasă în logările la serverul web. La fiecare etapă, corelatorul de evenimente interconectează aceste incidente și le categorisește ca elemente ale aceleiași alerte, sporind gradul de severitate treptat. Scopul acestei corelări este să genereze o alarmă către persoanele atribuite genului și gradului de amenințare și să ia acțiuni bazate pe reguli predefinite de către administrator. Acuratețea detecției incidentelor este diminuată dacă aceste incidente nu sunt raportate în timp real cu acurateță mare.

În figura de mai jos este descris modul în care corelatorul interacționează cu sistemele integrate pe care le monitorizează. Spre exemplu, sistemul de securitate 1 poate fi reprezentat de un firewall al companiei, sistemul de securitate 2, un sistem IDPS, iar sistemul 3 poate fi

un server web. Toate aceste sisteme, individual, generează o cantitate enorma de loguri zilnic. Un singur firewall poate genera peste un gigabyte de date care conțin loguri intr-o singura zi, iar un IDS poate genera peste 500,000 de mesaje pe zi. Cel mai mare dezavantaj al alertelor produse de către aceste sisteme este acela ca majoritatea alertelor sunt dominate de fals pozitiv, adică indica posibile breșe de securitate sau incidente, cu toate ca nu are loc niciun astfel de incident. Corelatorul poate investiga mai multe loguri provenite de la același sistem de securitate, sau poate combina logurile tuturor sistemelor, pentru a furniza alerte ale incidentelor reale [5].

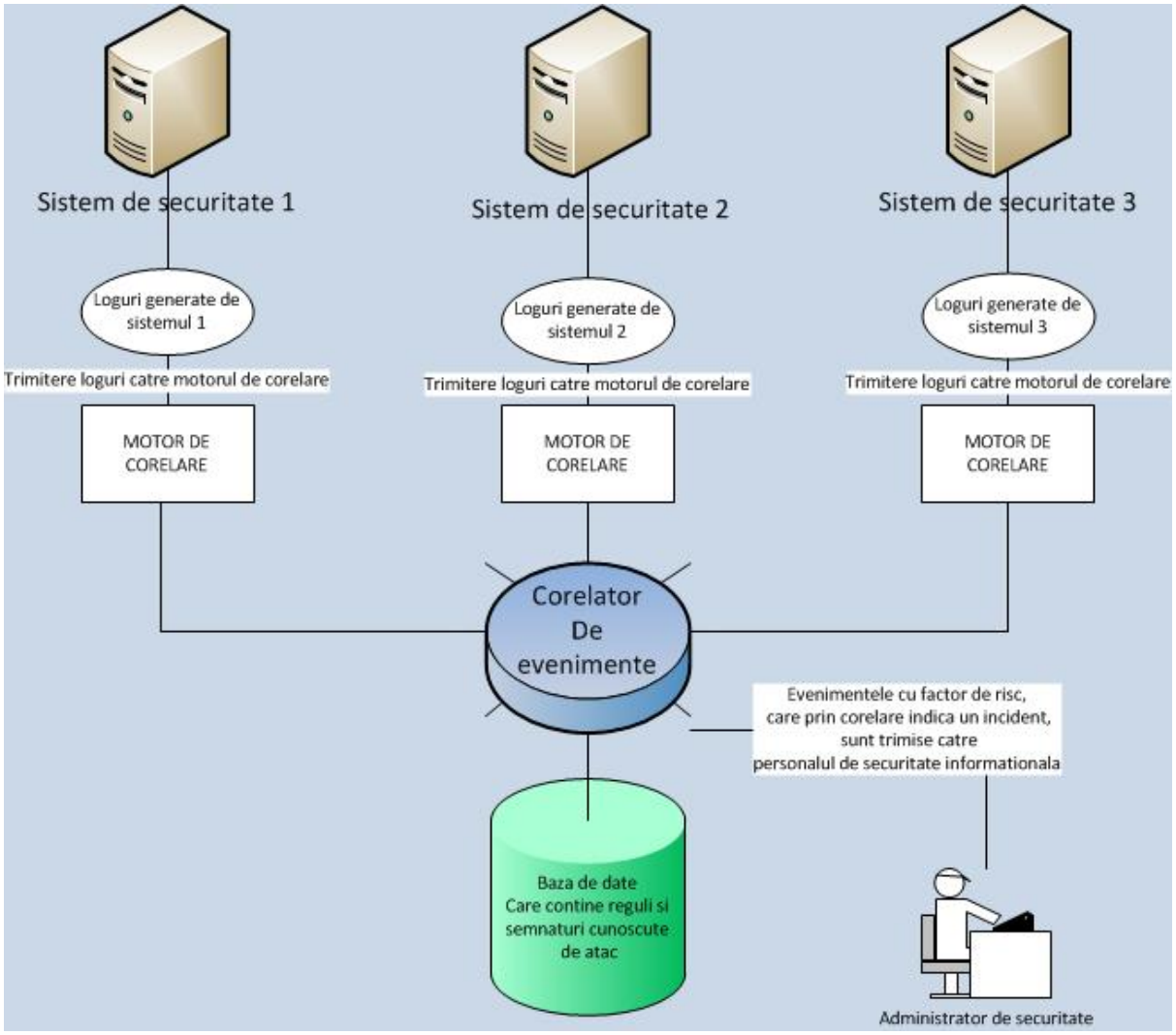

Fig. 4.1: Model arhitectural pentru un corelator de evenimente cu factor de risc

4.1.1 Rolul corelatoarelor de evenimente în securitatea informațională

Rolul corelatoarelor de securitate este acela de a ajuta administratorii de securitate să răspundă în timp real eficient amenințărilor de securitate. Având capabilități de analiză în timp real a evenimentelor provenite de la mai multe surse de alertă cu privire la amenințările de securitate, acestea pot efectua sarcini care pentru un om ar fi imposibil de efectuat, din cauza timpului foarte scurt de analiza si a volumului foarte mare de date care trebuie analizate. Avantajul pe care omul îl deține în fața corelatoarelor de evenimente este acela ca omul poate corela si evenimente legate de incident, care nu apar în regulile de corelare care declanșează alarma de securitate.

Prin inter-corelarea evenimentelor generate de surse independente de alertă, corelatoarele de evenimente ajută la:

- **Identificarea situațiilor cu risc real**. Există foarte multe situații în care logurile de eroare generate de către sistemele monitorizate nu prezintă factor de risc, cum ar fi autentificări eșuate pentru acces la platforme interne generate de către angajați. În acest caz, un exemplu de atac semnalat de către corelator ar fi „20 de încercări eșuate de autentificare pentru contul de utilizator *username*, de la stația cu IP xxx.xxx.xxx.xxx".
- **Identificarea cauzei unei probleme de securitate**. În cazul în care exista semnalmente ale unui atac, însă acesta nu a fost depistat în timp real, corelatorul poate acorda un ajutor semnificativ analistului de securitate informațională din companie, pentru a determina care au fost toate acțiunile corelate cu acel posibil atac.
- **Efectuarea de predicții** în legătură cu posibile amenințări viitoare sau tendințe ale acțiunilor provenite din mediul intern sau extern.

4.1.2 Fals pozitiv și fals negativ

Un fals pozitiv este definit de un eveniment sau o alarmă care indică o situație cu risc real, chiar dacă acel eveniment nu prezintă factor de risc. Exemple de fals pozitiv pot fi:

- Declanșarea unei alarme ca un sistem sau serviciu nu este operațional, cu toate că este.
- Un sistem IDPS identifică o activitate ca fiind rău intenționată, cu toate că nu este.
- Un email este clasificat ca spam, cu toate că nu este.

Un fals negativ este definit de un eveniment care indică faptul ca o situație este normală, cu toate că aceasta este una care prezintă factor de risc. Exemple de fals pozitiv pot fi:

- Raportarea unui serviciu ca fiind operațional, cu toate că nu este.
- Eșecul unui IDPS de a identifica o activitate malware.
- Un email este clasificat ca fiind ham(non-spam), cu toate ca este spam.

4.1.3 Tipuri de corelatoare de evenimente

Exista o varietate de tipuri de corelatoare de evenimente, însă cele mai utilizate sunt corelatoarele de evenimente care rulează pe baza unor reguli bine stabilite și cele care rulează pe baza statisticilor și modelelor învățate în timp.

4.1.3.1 Corelatoare de evenimente bazate pe reguli predefinite

Corelatoarele de evenimente care rulează pe baza regulilor impuse de către administratori, trebuie să recunoască metode de atac și puncte vulnerabile din sisteme. Pe baza acestor metode, corelatoarele sunt configurate prin aplicarea de reguli de recunoaștere. Astfel de reguli sunt în general construite de către furnizorii de soluții de corelare de evenimente, pe baza unor statistici și tendințe observate în rețelele și infrastructurile reale. De exemplu, un administrator poate defini o regula pentru a monitoriza scanările de porturi pe componentele infrastructurii interne. Daca se detectează ca aceste scanări de porturi încearcă să identifice porturi de telnet deschise, regula ar putea monitoriza încercările de conectare prin telnet pentru o perioadă determinata de timp, după detectarea scanărilor de porturi. Dacă o conexiune telnet este identificată și a plecat de la o anumită adresă IP, corelatorul de evenimente trimite o alerta administratorului.

4.1.3.2 Corelatoare de evenimente bazate pe statistici

Corelatoarele de evenimente care folosesc această tehnică nu dețin informații despre regulile de atac cunoscute, ci se bazează pe studierea comportamentului și a activității normale a sistemelor. Evenimentele în desfășurare sunt analizate de un algoritm și pot fi comparate cu tiparele de activitate acumulate, pentru a deosebi activitățile normale de cele

suspecte. Aceasta tehnica se bazează pe analiza indicatorilor de timp și valoare. Companiile trebuie sa seteze valoarea sistemelor pe care le dețin (servere și dispozitive de rețea) și potențialul de pierdere pe care ar putea sa îl genereze, dacă aceste sisteme sunt compromise. Cele mai multe corelatoare de evenimente care folosesc aceasta tehnică folosesc următoarea formulă pentru determinarea riscului generat de un atac pentru un anumit sistem:

Risc = Server(valoare) * Vulnerabilitate(severitate) * Amenințare(criticalitate)

În cazul exemplului prezentat de atac IIS Unicode, daca serverul WEB este compromis și serverul a fost categorisit ca fiind un sistem critic pentru companie, atunci factorul de risc este critic. Cu cât criticalitate, severitatea sau valoarea setată pentru un anumit server este mai mare, cu atât factorul de risc este mai ridicat.

4.1.4 Etape premergătoare corelării

Corelatorul de evenimente trebuie sa culeagă informații de la sistemele cu care este integrat. Fiecare dintre aceste sisteme generează loguri de alertă sau de eroare în formatul său propriu stabilit de furnizor. Înainte de instalarea regulilor de corelare a evenimentelor cu factor de risc, trebuie efectuate următoarele etape premergătoare:

4.1.4.a Agregarea logurilor

Etapa de transmitere a logurilor generate de fiecare sistem individual de securitate către un sistem central de consolidare a logurilor este una crucială și prezintă factor de risc, deoarece este posibil ca logurile să fie interceptate și alterate sau există riscul ca acestea sa nu fie trimise în timp util sau în număr complet. De aceea, transmisia datelor trebuie securizată prin criptare.

4.1.4.b Normalizarea logurilor

După ce sunt aduse într-un singur punct comun, logurile trebuie reformatate, din formatul lor, intr-un format unic, comun, interpretabil de către corelator. Ulterior, logurile sunt inserate în baza de date a corelatorului. Este foarte important ca în procesul de formatare să nu existe pierderi sau alterări ale datelor. De aceea, aceasta este o etapă foarte atent testată și verificată în procesul de integrare.

4.1.4.c Reducerea dimensiunii logurilor

După inserarea în baza de date, setul de date trebuie redus, pentru a putea fi corelat mai ușor. Acest lucru se poate materializa prin eliminarea duplicatelor, compresia de date, filtrarea logurilor și combinarea celor similare intr-un singur eveniment. Metoda de combinare a evenimentelor nu este recomandata de foarte mulți integratori, pentru că prin aceasta se pot pierde date importante care ajuta la investigarea incidentelor, după ce acestea au avut loc.

După ce logurile sunt agregate, normalizate și redimensionate, corelatorul de evenimente poate începe sa le analizeze.

4.1.4.d Prioritizarea logurilor

Prioritizarea informațiilor relevante pentru securitatea informationala se realizează prin corelarea evenimentelor care conțin meta-date cum ar fi servicii, vulnerabilități, mașini sursă si destinație, etc.

In procesul de prioritizarea, atributele critice sunt:

- Codul incidentului identificat
- Descrierea incidentului
- Versiunea si tipul sistemului de operare al mașinii pe care a apărut incidentul
- Porturile, serviciile si aplicațiile pe mașina pe care a apărut incidentul

- Referințe

Scorul de relevanță al incidentului este calculat pentru fiecare alertă, bazându-se pe probabilitatea de apariție a incidentului. Pentru fiecare alertă, corelatorul caută în baza de date a incidentelor pentru incidente dependințe intre incidente.

Prioritizarea incidentelor este realizată prin corelarea evenimentelor cu meta-date cum ar fi servicii, hardware si vulnerabilități. Componenta pentru prioritizarea datelor este localizată în două arii ale lanțului de detecție. Fiecare log este analizat, iar meta-datele sale sunt identificate intr-o baza de date care specifică daca meta datele aparțin unei alerte de nivel inferior sau de nivel superior.

5. Implementare corelator de evenimente

5.1 Răspunsul corelatorului de evenimente la amenințări interne.

Amenințările interne sunt privite ca violări de securitate venite din partea persoanelor din interiorul companiei. Aceste amenințări sunt mult mai des întâlnite decât amenințările externe, din cauza faptului ca persoanele din companie au acces mai ușor și cunosc mult mai bine infrastructurile hardware și software ale companiei. Cele mai periculoase amenințări sunt reprezentate de administratori, consultanți sau parteneri ai companiei, care au drepturi aproape depline asupra sistemelor.

Cele mai importante surse de evenimente cu grad mare de risc din mediul intern provin din:

- **Sistemul Data Loss Prevention**
- **Controlerul de domeniu Active Directory**
- **Dispozitive VPN**
- **Sistem de operare**

Corelatorul de evenimente poate identifica evenimentul care a generat acordarea de drepturi suplimentare sau drepturi de administrator, unei persoane care nu are un rol de administrare a sistemelor în companie, sau i s-au acordat drepturi de VPN fără o aprobare preliminara de la superiorul sau direct. Acesta este un caz în care drepturile sunt retrase și contul este blocat temporar, până la repunerea în drepturi de către un administrator cu drepturi depline.

5.1.1 Răspuns la furt de proprietate intelectuală sau date sensibile.

Furtul de proprietate intelectuala este foarte des întâlnit în companii și este de obicei greu de identificat. Acest fenomen apare cu preponderență în situațiile în care angajatul se afla în perioada de preaviz, în condițiile în care acesta si-a depus demisia sau a fost concediat. De cele mai multe ori, angajatul copiază pe un dispozitiv de memorie externa informații confidențiale sau sensibile, cum ar fi proceduri de lucru, baze de date ale clienților companiei, software. etc. În acest caz, corelatorul de evenimente trebuie sa preia informații de la sistemul Active Directory și de la sistemul Data Loss Prevention. Procedura de lucru instaurată în companie ar trebui sa urmeze o regulă de setare a atributelor *angajat_in_preaviz* și *timp rămas permis în companie* a angajatului respectiv. Corelatorul de evenimente trebuie să înceapă să „asculte” tot traficul pe care acel angajat îl generează atât intern cât și extern și să identifice dacă acesta încearcă sa copieze o cantitate mare de informație pe o unitate de stocare externa, sau dacă încearcă să trimită în internet informație cu caracter sensibil, chiar daca avea implicit dreptul de a o face. În cazul în care angajatul se află într-o stare cu statut special, angajatul intră intr-un modul de tratare special, în care drepturile îi sunt restricționate automat în conformitate cu anumite reguli impuse.

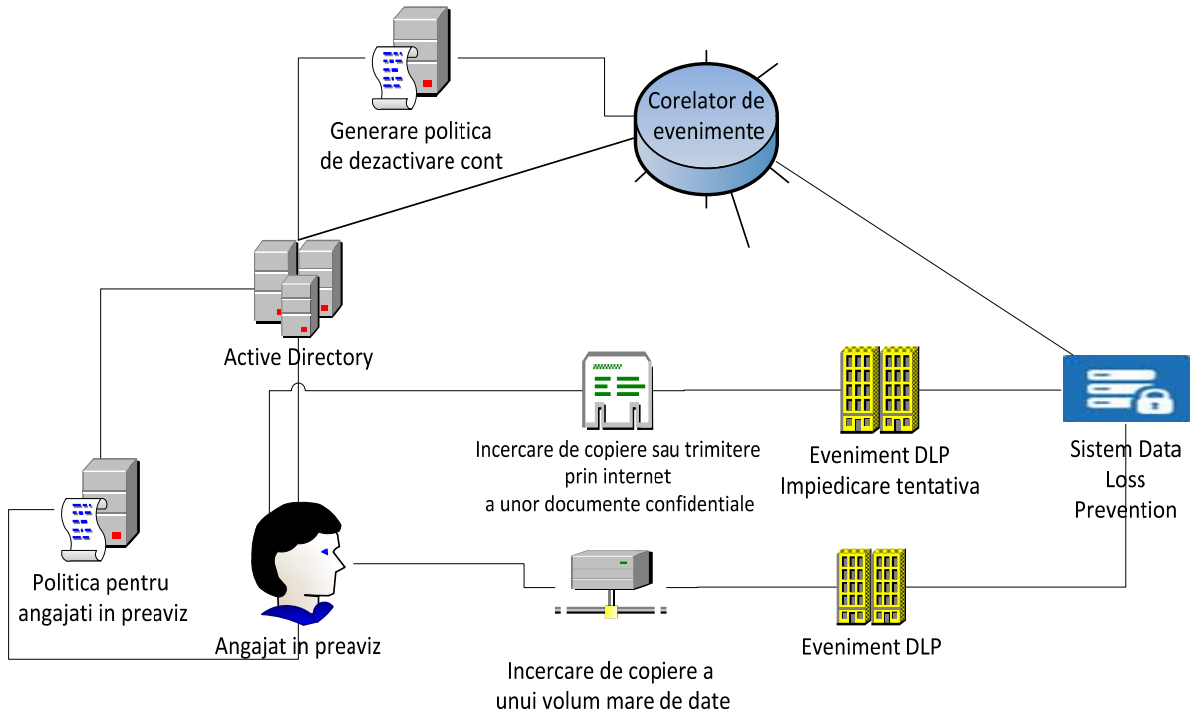

Fig. 5.1: Acțiunile corelatorului de evenimente la tentativele de furt intelectual sau de date confidențiale

În exemplul prezentat, este descrisă o regulă care corelează logurile provenite de la Active Directory și de la sistemul Data Loss Prevention. Sistemul Data Loss Prevention indică faptul că un angajat încearcă o posibila tentativă de fraudă, iar sistemul Active Directory indică faptul ca acel angajat este un angajat cu statut special. Ca urmare, pentru evenimentul rezultat din corelarea celor doua evenimente (unul provenit de la DLP, iar celalalt de la AD) factorul de risc a crescut. Ca atare, acest eveniment este împins intr-o zona de risc cu nivel crescut. Pe baza regulii setate în corelator pentru acest eveniment, se generează o alarma care trimite notificare către administratori și activează o politică de dezactivare sau suspendare de cont pentru acel angajat. În consecință, contul angajatului cu statut special, care a încălcat o politica de securitate, va fi suspendat în Active Directory. Fiind controler de domeniu, toata activitatea informațională din interiorul companiei este suspendată forțat pentru acest angajat. În urma acestui incident, un administrator de securitate este obligat sa investigheze cazul și sa îl raporteze unui superior al acelui angajat. În urma unui flux de acțiuni (workflow), contul angajatului poate fi reactivat din ADUC (Active Directory Users and Computers).

Dezactivarea contului de utilizator din Active Directory se realizează prin efectuarea următorilor pași:

- Declanșarea regulii de dezactivare emisă de corelatorul de evenimente cu factor de risc (operațiune efectuata la nivel de DLP)
- Construirea scriptului de dezactivare a contului de Active Directory a angajatului care a generat incidentul (efectuată la nivel de DLP)
- Rularea scriptului (operațiune efectuată la nivel de AD)

La nivel de proces, acțiunile se translatează in:

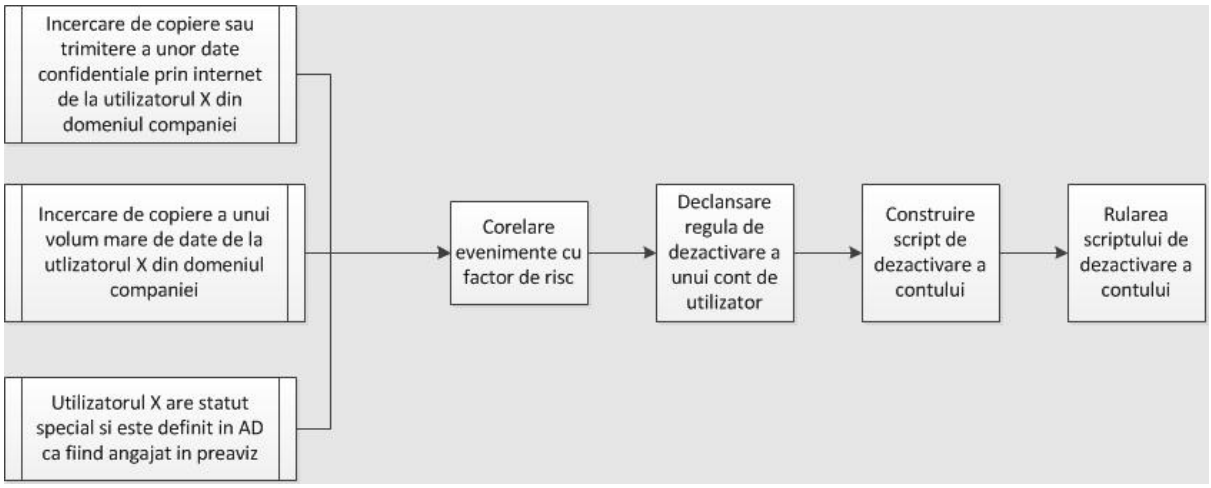

Fig. 5.2: Dezactivarea contului de utilizator din Active Directory pentru un angajat cu statut special care a declanșat o regula de securitate

Construirea scriptului de dezactivare a contului de Active Directory a angajatului care a generat incidentul se efectuează ținând cont de anumiți parametrii. Comanda de dezactivare este „dsmod" și are următoarea sintaxa:

dsmod user <UserDN> -disabled {yes|no}

Parametru	**Descriere**
<UserDN>	Specifică numele obiectului utilizatorului
-disabled	Setează valoarea UF_ACCTDISABLED în userAccountControl
{yes|no}	Specifică dacă acel cont este dezactivat (**yes**) sau activat (**no**)

Numele obiectului utilizatorului este definit în general de 3 atribute:

- CN - Common Name : numele efectiv al utilizatorului stocat în Active Directory
- OU – Organizational Unit: structura care grupează obiectele din domeniu
- DC – Domain Controller: sistem de autentificare și de autorizare pentru toți utilizatorii și toate computerele din domeniul Windows dintr-o rețea. Acesta permite definirea și impunerea politicilor de securitate pentru toate computerele și utilizatorii și poate instala sau actualiza programe.

Figura de mai jos prezintă o consola Command Prompt care conține linia de comandă care dezactivează un cont de utilizator în Active Directory.

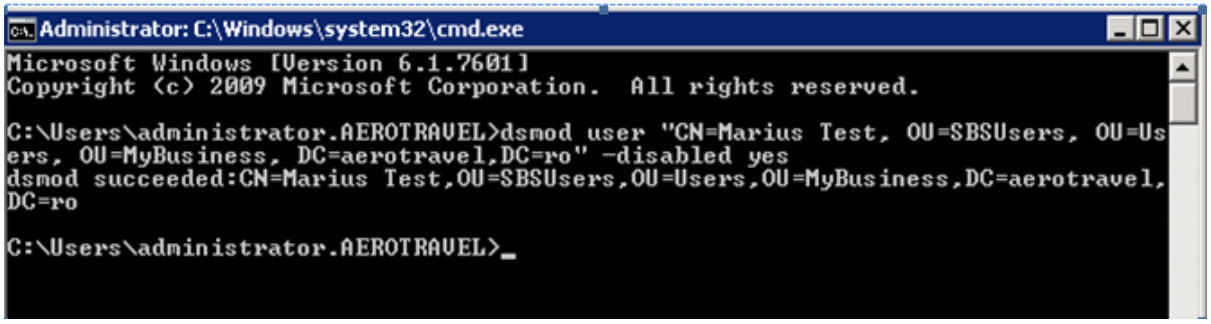

Fig. 5.3 Linie de comanda pentru dezactivarea contului unui utilizator din Active Directory

Linia de comandă care dezactivează contul pentru un utilizator este integrată într-un script „**.bat**” care rulează la nivel de AD. Scriptul .bat este rulat în urma declanșării regulii de securitate pentru incident și amenințare din partea angajatului cu statut special.

5.1.2 Reguli de corelare a evenimentelor cu factor de risc pentru securitatea internă

Pentru descrierea regulilor de corelare care pot avea un impact major în păstrarea securității informatice interne la un nivel ridicat, vom prezenta scenarii de caz pentru fiecare situație care ar declanșa o regula de corelare de evenimente cu factor de risc.

Regulile de corelare a evenimentelor cu factor de risc pentru securitatea internă au în componență 2 elemente de referință:

- **Nivelul de confidențialitate a datelor procesate**. Acest nivel este setat prin intermediul sistemului de Data Loss Prevention, care are în componență modulul de setare a datelor de natura confidențială. Prin intermediul acestui modul, se triază datele cu caracter sensibil și se atribuie grade de sensibilitate pentru acestea. Spre exemplu, se poate seta ca formatul unui contract confidențial sa primească eticheta de date confidențiale. Pe baza unor tehnici de recunoaștere, toate documentele care conțin acest format, vor fi etichetate ca fiind confidențiale.
- **Statutul și poziția angajatului în companie**. Aceste atribute pot fi setate în cadrul sistemului Active Directory Users and Computers. Acesta permite managementul utilizatorilor, al grupurilor, al unităților organizaționale și a altor obiecte din AD. Obiectele din Active Directory se împart în resurse(ex: imprimante, servere), servicii(ex: poșta electronică) și resurse umane(ex: utilizatori, grupuri de utilizatori). Structura de baza a obiectului e definită de o schemă, care definește tipul obiectelor care pot fi stocate ca sub-obiecte în obiect. O schema este compusa din două meta-date sau două tipuri de obiecte: clase și atribute. Acestea permit schemei sa fie extinsă sau modificată. Datorită faptului ca meta-datele schemei fac parte din obiectul pe care îl descriu, în momentul în care o chema este modificata, efectele impuse de aceasta modificare se propaga pe toate obiectele din Active Directory la care a fost aplicata schema inițială.

Utilizatorii setați în Active Directory și în sistemul Data Loss Prevention pot avea trei statuturi:

- Utilizator normal (cu drepturi restrânse)
- Administrator (utilizator cu drepturi depline)
- Utilizator cu statut special:
  - ***Angajat în preaviz***
  - ***Angajat în concediu***
  - ***Angajat în practică***
  - ***Angajat venit de la concurență***

Fiecare utilizator din domeniu este integrat intr-un grup din AD. Acestui grup i se pot seta reguli și politici diferite. Utilizatorilor cu statut special li se setează reguli stricte și valoare de risc mare. Orice acțiune suspectă care vine din partea unui utilizator cu statut special este transformată în incident și este corelata cu alte acțiuni, chiar daca acestea nu prezintă factor de risc.

Pentru angajații cu statut special, cel mai important aspect este monitorizarea tipului și volumului de date pe care acesta încearcă să le manipuleze. Pentru angajații care sunt în preaviz, în momentul în care se primește notificare de la departamentul de resurse umane că

un angajat începe perioada de preaviz și se acorda timp de acces inga 30 de zile, acest termen se setează în Active Directory de către un administrator de domeniu.

Similar se poate seta și perioada de expirare pentru un angajat în practică.

5.1.2.a Regula de corelare 1. Angajat cu statut special încearcă sa trimită date sensibile prin intermediul poștei electronice, aflându-se în perioada de preaviz.

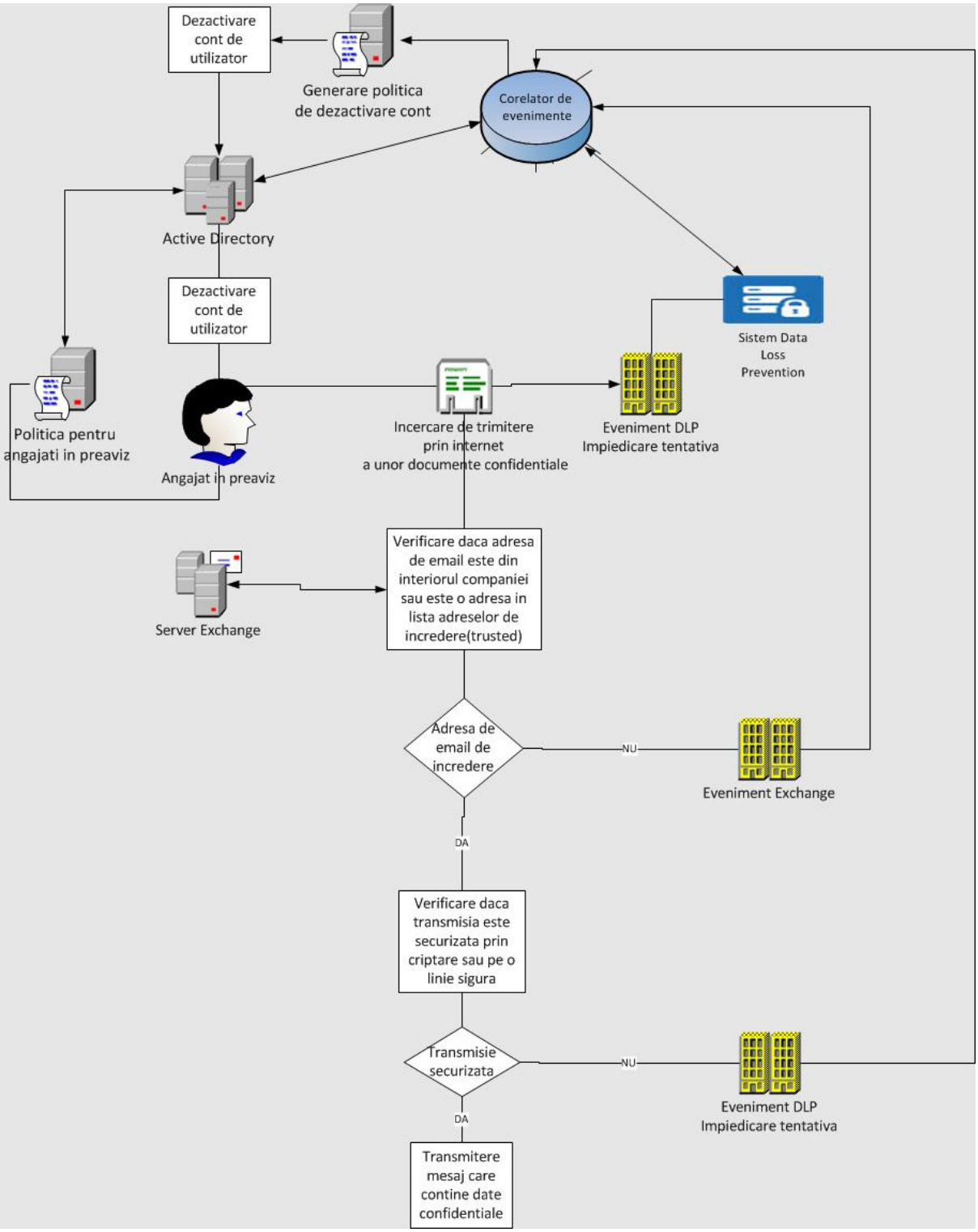

Fig. 5.4: Corelare de evenimente pentru încercarea de transmitere a datelor sensibile de către un utilizator din interiorul companiei.

În scenariul de mai sus un utilizator cu statut special(angajat în preaviz), încearcă să trimită prin internet un email care conține date catalogate a fi confidențiale. Deoarece acesta este supus unor reguli speciale de securitate în Active Directory, emailul este reținut și se efectuează un set de verificări. În primul rând se verifică dacă adresa la care se dorește trimiterea se afla în lista de adrese de încredere (trusted) din companie. În cazul în care aceasta adresă este recunoscută, se verifică dacă transmisia este securizată. În cazul în care oricare din aceste doua verificări generează răspuns negativ, se creează eveniment care este transmis către corelatorul de evenimente. Prin corelare, oricare din aceste evenimente crește gradul de risc pentru incidentul creat. Ca efecte pentru acest incident, contul de AD al utilizatorului este dezactivat, iar administratorii de securitate sunt alertați pentru a investiga evenimentele. Administratorii și superiorul angajatului decid dacă angajatului i se va reactiva sau nu contul. În cazul în care contul acestuia este reactivat, se decide dacă utilizatorul își păstrează drepturile pe care le deținea, sau i se restrâng.

5.1.2.b Regula de corelare 2. Un angajat care figurează ca ieșit din companie în sistemul electronic de pontaj se autentifică pe un computer din interiorul companiei

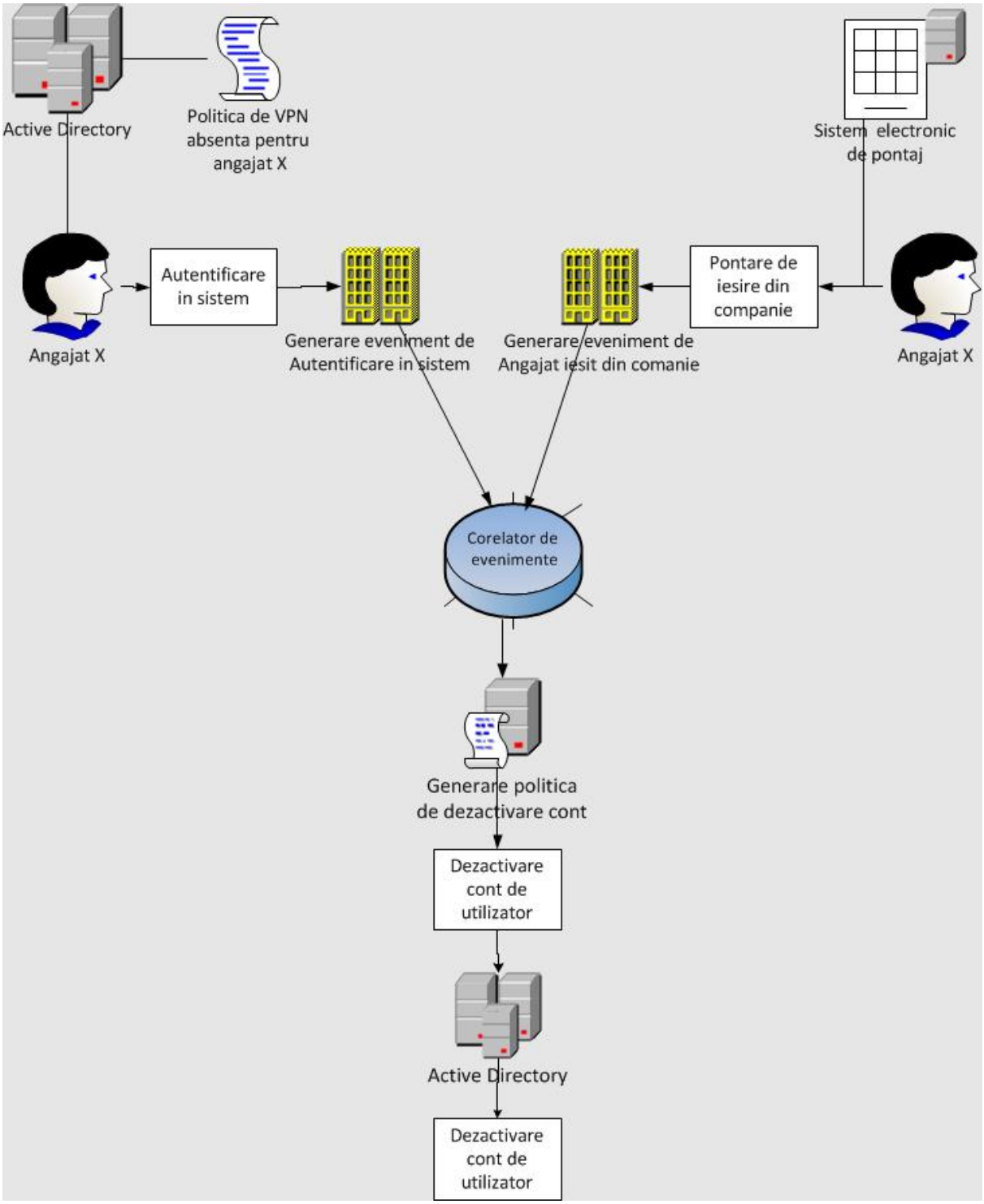

Fig. 5.5 Corelare între sistemul de pontaj și autentificarea utilizatorilor în sistem

În situația prezentată în figura 3.7, un angajat a pontat pentru ieșire folosind cardul electronic de acces în companie, dar până la schimbarea stării de pontare pentru intrare, se autentifica în sistem folosind credențialele de Active Directory. Conectarea în Active Directory din afara companiei este permis doar pentru utilizatorii cu drepturi extinse, care dețin o politica de acces la VPN (Virtual Private Network), prin care pot accesa resursele companiei remote(de la distanță). Aceștia folosesc un tunel securizat prin care se face transferul de pachete tranzitate. Corelatorul de evenimente generează un incident prin corelarea evenimentului de autentificare în sistem al unui utilizator care nu deține politica de

VPN și starea de angajat care nu se afla fizic în companie. Cele trei evenimente generate: faptul că angajatul nu se află fizic în companie, nu are dreptul de a se conecta de la distantă și totuși este logat în sistem, demonstrează prin corelare faptul că a apărut o situație cu factor de risc. În urma generării logului de incident, se poate bloca contul utilizatorului sau se poate genera o alertă.

Sistemele DLP sunt de regulă configurate să blocheze tentativele de încălcare a politicilor de securitate și sa avertizeze utilizatorul despre motivul blocării. Prin astfel de evenimente, utilizatorul poate învăța metodele și regulile sistemelor de securitate DLP, astfel încât să le poată ocoli. Una din cele mai încercate tentative de ocolire a sistemului DLP, este de a face captura de ecran datelor confidențiale, după care să salveze acea captură ca și imagine. În acest fel, sistemul DLP nu poate recunoaște semnătura de informație confidențială. Din fericire, sistemele DLP tratează acest caz printr-o altă regulă, care împiedică utilizatorul sa efectueze captura de ecran, în cazul în care această captură vizează informații confidențiale.

Un caz netratat de către sistemele DLP este acela în care utilizatorul poate transmite informații sensibile în internet ar fi cazul în care utilizatorul trimite emailul unei persoane care se găsește în lista de încredere, dar trimite aceeași informație unei adrese care nu se afla în lista de încredere folosind funcția BCC (Blind Carbon Copy), care îi permite expeditorului să ascundă persoane cărora să le trimită conținutul emailului. Corelatorul de evenimente poate trata un astfel de caz, prin urmărirea logurilor provenite de la serverul de Exchange.

5.2 Răspunsul corelatorului de evenimente la amenințări externe

Cele mai importante surse de evenimente cu grad mare de risc din mediul extern provin din:

* **Sistemul IPS –IDS :** aici sunt identificate semnăturile de atac și evenimentele cu factor de risc pentru securitatea informației
* **Firewall:** aici sunt identificate scanări succesive a porturilor sau încercări de accesare a porturilor de la IP-uri, care nu sunt autorizate, sau sunt în lista neagră a firewall-ului
  Server WEB: aceste atacuri sunt cele mai frecvente, pentru că atacatorul are acces la interfața web și poate încerca diferite metode de a exploata serverul web prin intermediul acestei interfețe.

Un exemplu de acțiune în caz de atac extern este expus în figura de mai jos. Sistemul Firewall detectează o scanare de porturi de la un IP, caz în care generează un log de eveniment, pe care îl trimite corelatorului de evenimente. Intr-un interval de timp scurt, sistemele de detectare și prevenire a intruziunii detectează o semnătură de atac, caz în care este generat un log pe care îl trimite corelatorului de evenimente. Gradul de risc a crescut, iar corelatorul de evenimente transpune succesiunea de evenimente intr-un un log de eveniment cu grad mare de risc(potențial atac). În acest caz, oprește cererile venite de la acel IP și contactează persoanele care tratează aceste cazuri. Dacă se identifică și o serie suspicioasă de logări la serverul WEB, gradul de risc crește, iar cazul este escalat către o echipa specializată. Corelatorul de evenimente escalează treptat cazurile de amenințări, în funcție de gradul de risc al acestora.

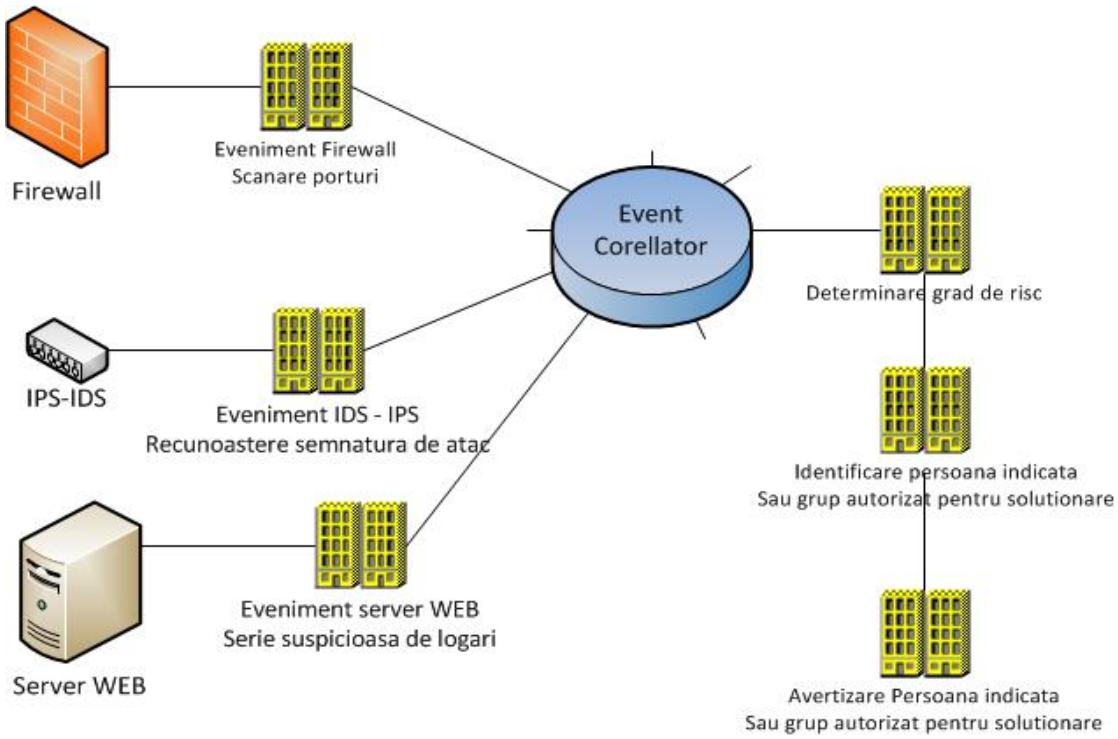

Fig. 5.6 Răspunsul corelatorului de evenimente la potențiale atacuri externe

Răspunsul corelatorului de evenimente trebuie să avertizeze persoana indicată pentru tratarea cazurilor de amenințări externe, dar poate să și ia masuri pentru a înlătura amenințarea: trimite log de avertizare către Firewall pentru a nu permite cereri de la IP-ul respectiv și comanda sistemelor de prevenire a intruziunii să blocheze orice pachet și cerere de la acel IP.

5.2.1 Scenariu de atac extern analizat de corelatorul de evenimente

Să presupunem că atacatorul lansează o serie de probe care caută scripturi CGI exploatabile. CGI – Common Gateway Interface este o metodă standard pentru generarea de content dinamic pe paginile web și aplicații web. Acesta creează o interfață între serverele web și programele care generează contentul web. Aceste programe sunt cunoscute ca și scripturi CGI .

Vom folosi 3 vulnerabilități cunoscute:

- CVE-1999-0067: CGI phf permite execuția de comenzi la distanță, folosind metacaractere;
- CVE-1999-0172: CGI FormMail permite execuția de comenzi la distanță;
- CVE-1999-0936: BNBSurvey survey.cgi permite execuția de comenzi la distanță prin metacaractere shell;

In prima fază vom analiza independent logurile generate de fiecare sistem de securitate instalat în rețea, pentru cele 3 probe lansate de atacator. Ulterior, vom analiza corelarea acestora, pentru a obține o imagine mult mai bună asupra atacului.

Routerul CISCO va emite în urma atacului următoarele loguri:

May 31 09:27:44 router.company.com 1410875: May 31 09:27:43: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 152.63.146.6(1459) -> 192.168.100.1(80), 1 packet

May 31 09:27:50 router.company.com 1410880: May 31 09:27:50: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 152.63.146.6(1673) -> 192.168.100.2(80), 1 packet

May 31 09:27:54 router.company.com 1410883: May 31 09:27:53: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 152.63.146.6(1750) -> 192.168.100.3 (80), 1 packet

May 31 09:27:57 router.company.com 1410885: May 31 09:27:56: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 152.63.146.6(1722) -> 192.168.100.5(80), 1 packet

May 31 09:27:58 router.company.com 1410886: May 31 09:27:57: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 152.63.146.6(1930) -> 192.168.100.6(80), 1 packet

May 31 09:28:01 router.company.com 1410888: May 31 09:28:00: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 152.63.146.6(1976) -> 192.168.100.7(80), 1 packet

May 31 09:28:05 router.company.com 1410891: May 31 09:28:04: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 152.63.146.6(2167) -> 192.168.100.8(80), 1 packet
.
. <data pruned>
.

Din logurile generate de către routerul CISCO, observăm ca în data de 31 mai la ora 09:27, a avut loc o serie de încercări de conectare directa în rețeaua 192.168.100.0/24, de la IP-ul sursa 152.63.146.6. Putem sa deducem ca are loc o încercare de scanare a serverelor web ale companiei, după încercările de conectare la portul TCP 80. Observăm ca nu a fost emis un log de respingere a cererii de conectare pentru IP-ul intern 192.168.100.4, deoarece acesta este un server web al companiei. ACL-ul routerului nostru a fost configurat sa accepte traficul pe portul TCP 80 cu porturi sursa efemere pentru 192.168.100.4, deoarece acesta este serverul web al companiei. Uitându-ne la logurile routerului, deducem ca IP-ul 152.63.146.6 a scanat întreaga clasa C, în căutare de servere WEB. Observat independent de alte surse, routerul nu oferă alte informații despre intențiile atacatorului.

Informații oferite de router:

Cine	152.63,146.6
Ce	Scanare generală a rețelei 192.168.100.0/24 în căutare de servere WEB
Când	31 mai în intervalul 09:27-09:28
Unde	În rețeaua companiei DMZ (zona demilitarizată)
De ce	Probabil căutare servere web vulnerabile

Firewall-ul Gauntlet va emite următoarele loguri:

Jun 1 06:08:50 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http cmd=get dest=192.168.100.4 path=/cgi-bin/phf ID=29142174970

Jun 1 06:08:54 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http cmd=get dest=192.168.100.4 path=/cgi-bin/formmail ID=29142174971

Jun 1 06:08:58 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http cmd=get dest=192.168.100.4 path=/cgi-bin/survey.cgi ID=29142174972

Din logurile generate de firewall, se observă că în data de 1 iunie, a avut loc o serie de conectări http la serverul web al companiei, de la IP-ul 152.63.146.6. se observă în căile URL faptul că au existat încercări de acces la 3 scripturi: phf, formmail și survey.cgi.

Informații oferite de Firewall:

Cine	152.63,146.6
Ce	3 conectări http la rețeaua 192.168.100.0/24 cu încercări de acces la scripturi CGI: phf, formmail și survey.cgi. Nu se cunoaște dacă scripturile au fost accesate. Nu există alte conexiuni http de la acest IP, deci pare că este o activitate de atac.
Când	1 iunie la ora 06:08:50
Unde	În rețeaua companiei DMZ (zona demilitarizată)
De ce	Scripturile phf, formmail și survey.cgi sunt scripturi exploatabile, care permit acțiuni cu control la distanta

IDS-ul (Sistemul de detecție a intruziunilor) Snort va emite următoarele loguri:

[**] [1:886:3] WEB-CGI phf access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:50.764332 152.63.146.6:3308 -> 192.168.100.4:80
TCP TTL:52 TOS:0x0 ID:61884 IpLen:20 DgmLen:280 DF
*****AP*** Seq: 0x591AF831 Ack: 0x92D23FAF Win: 0x16D0 TcpLen: 32**
TCP Options (3) => NOP NOP TS: 59902357 300726
[Xref => http://www.securityfocus.com/bid/629]
[Xref => http://www.whitehats.com/info/IDS128]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0067]

[**] [1:884:2] WEB-CGI formmail access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:54.411065 152.63.146.6:3309 -> 192.168.100.4:80
TCP TTL:52 TOS:0x0 ID:15383 IpLen:20 DgmLen:285 DF
*****AP*** Seq: 0x85C51FDB Ack: 0xC0D4B803 Win: 0x16D0 TcpLen: 32**
TCP Options (3) => NOP NOP TS: 59974615 372988
[Xref => http://www.securityfocus.com/bid/1187]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0172]
[Xref => http://www.whitehats.com/info/IDS226]

[**] [1:871:2] WEB-CGI survey.cgi access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:58.609416 152.63.146.6:3310 -> 192.168.100.4:80
TCP TTL:52 TOS:0x0 ID:32890 IpLen:20 DgmLen:295 DF
*****AP*** Seq: 0x8B55C63C Ack: 0xC624745D Win: 0x16D0 TcpLen: 32**
TCP Options (3) => NOP NOP TS: 59983434 381809
[Xref => http://www.securityfocus.com/bid/1817]

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0936]

Din logurile emise de Snort, observăm ca în data de 1 iunie, au existat o serie de alerte CGI, pentru IP-ul sursa 152.63.146.6. Alertele indică faptul că este posibil sa fie vorba despre un atac provenit de la acest IP, deoarece aceste scripturi au vulnerabilități, care, prin exploatare, pot permite execuția de acțiuni cu control la distanta.

Regulile Snort care au declanșat aceste alerte sunt:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI phf access";flags: A+; uricontent:"/phf"; nocase; reference:bugtraq,629; reference:arachnids,128; reference:cve,CVE-1999-0067; classtype:attempted-recon; sid:886; rev:3;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI formmail access";flags: A+; uricontent:"/formmail"; nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172; reference:arachnids,226; classtype:attempted-recon; sid:884; rev:2;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI survey.cgi access";flags: A+; uricontent:"/survey.cgi"; nocase; reference:bugtraq,1817; reference:cve,CVE-1999-0936; classtype:attempted-recon; sid:871; rev:2;)

Aceste tipuri de erori declanșează numai când apar anumite șiruri de caractere în URL și sunt cunoscute în sisteme de detecție a intruziunilor pentru rata lor foarte mare de fals pozitiv. Analizate independent de celelalte sisteme, nu ne putem da seama daca aceste încercări de acces au fost asociate cu alte încercări de acces legitime. Putem bănui că aceste acțiuni fac parte dintr-un atac, deoarece este foarte puțin probabil ca aceste scripturi CGI să fie accesate prin încercări de conectare indirect, cum a fost indicat de către porturile sursă efemere. În orice caz, nu putem ști cu siguranță dacă încercările au avut succes sau nu. Știm doar ca au avut loc.

Informații oferite de logurile IDS-ului:

Cine	152.63,146.6
Ce	3 conectări http la rețeaua 192.168.100.0/24 cu încercări de acces la scripturi CGI: phf, formmail și survey.cgi. Nu se cunoaște dacă scripturile au fost accesate. Nu exista alte loguri legate de acest IP, deci nu putem evalua dacă acesta este un fals pozitiv, însă putem sa spunem ca este improbabil ca aceste scripturi CGI sa fie accesate intr-o perioada atât de scurtă de timp.
Când	1 iunie la ora 06:08:50
Unde	În rețeaua companiei DMZ (zona demilitarizată)
De ce	Scripturile phf, formmail și survey.cgi sunt scripturi exploatabile, care permit acțiuni cu control la distanta

Serverul WEB Apache va emite următoarele loguri:

Loguri de acces:

152.63.146.6 - - [01/Jun/2013:06:08:50 -0400] "GET /cgi-bin/phf HTTP/1.0" 404 304 "-" "Lynx/2.8.5dev.2 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a"

152.63.146.6 - - [01/Jun/2013:06:08:54 -0400] "GET /cgi-bin/formmail HTTP/1.0" 404 309 "-" "Lynx/2.8.5dev.2 libwww-FM/2.58 SSL-MM/1.4.1 OpenSSL/0.9.6a"

152.63.146.6 - - [01/Jun/2013:06:08:58 -0400] "GET /cgi-bin/survey.cgi HTTP/1.0" 404 311 "-" "Lynx/2.8.5dev.2 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a"

Loguri de eroare:

[Sat Jun 1 06:08:50 2013] [error] [client 152.63.146.6] script not found or unable to stat: /var/www/cgi-bin/phf

[Sat Jun 1 06:08:54 2013] [error] [client 152.63.146.6] script not found or unable to stat: /var/www/cgi-bin/formmail

[Sat Jun 1 06:08:58 2013] [error] [client 152.63.146.6] script not found or unable to stat: /var/www/cgi-bin/survey.cgi

Logurile de eroare cat și cele generate de serverul WEB indică faptul că în data de 1 iunie la ora 06:08, au existat încercări de acces ale scripturilor CGI phf, formmail și survey,cgi în subdirectorul cgi_bin, de la IP-ul sursa 152.63.146.6. Logurile de eroare indică faptul că aceasta activitate a generat aceste erori pentru ca scripturile nu erau operaționale pe server. Nu au mai existat alte conexiuni http de la acest IP, deci activitatea pare a fi de exploatare de vulnerabilități.

Informații oferite de logurile serverului WEB:

Cine	152.63,146.6, probabil un Unix sau Linux care folosește Lynx v2.8.5dev.2
Ce	3 conectări http la rețeaua 192.168.100.0/24 cu încercări de acces la scripturi CGI: phf, formmail și survey.cgi. **Aceste scripturi nu au fost accesate, pentru ca nu exista pe server**. Nu exista alte loguri legate de acest IP, deci probabil este un atac care încearcă exploatare de vulnerabilități CGI
Când	1 iunie la ora 06:08:50
Unde	În rețeaua companiei DMZ (zona demilitarizata)
De ce	Scripturile phf, formmail și survey.cgi sunt scripturi exploatabile, care permit acțiuni cu control la distanta

Analiza corelativa.

În exemplul studiat am observat că analiza individuală a sistemelor de securitate instalate în rețea nu oferă o imagine completă a atacului, ci doar porțiuni din puzzle. Pentru a determina cu siguranță dacă aceste încercări fac parte dintr-un atac real, administratorul de sistem trebuie sa analizeze logurile provenite de la fiecare sistem și sa facă o corelare între acestea. Metodologia corelativă pe care o efectuează administratorul de securitate poate fi simulată de către corelatorul de evenimente prin reguli predefinite. În cazul în care astfel de incidente apar zilnic în număr repetat, este esențial ca această analiză să fie făcută de un sistem care anulează situațiile de fals pozitiv, adică acelea în care nu exista un atac real, cu toate ca logurile unui singur sistem alertează ca este.

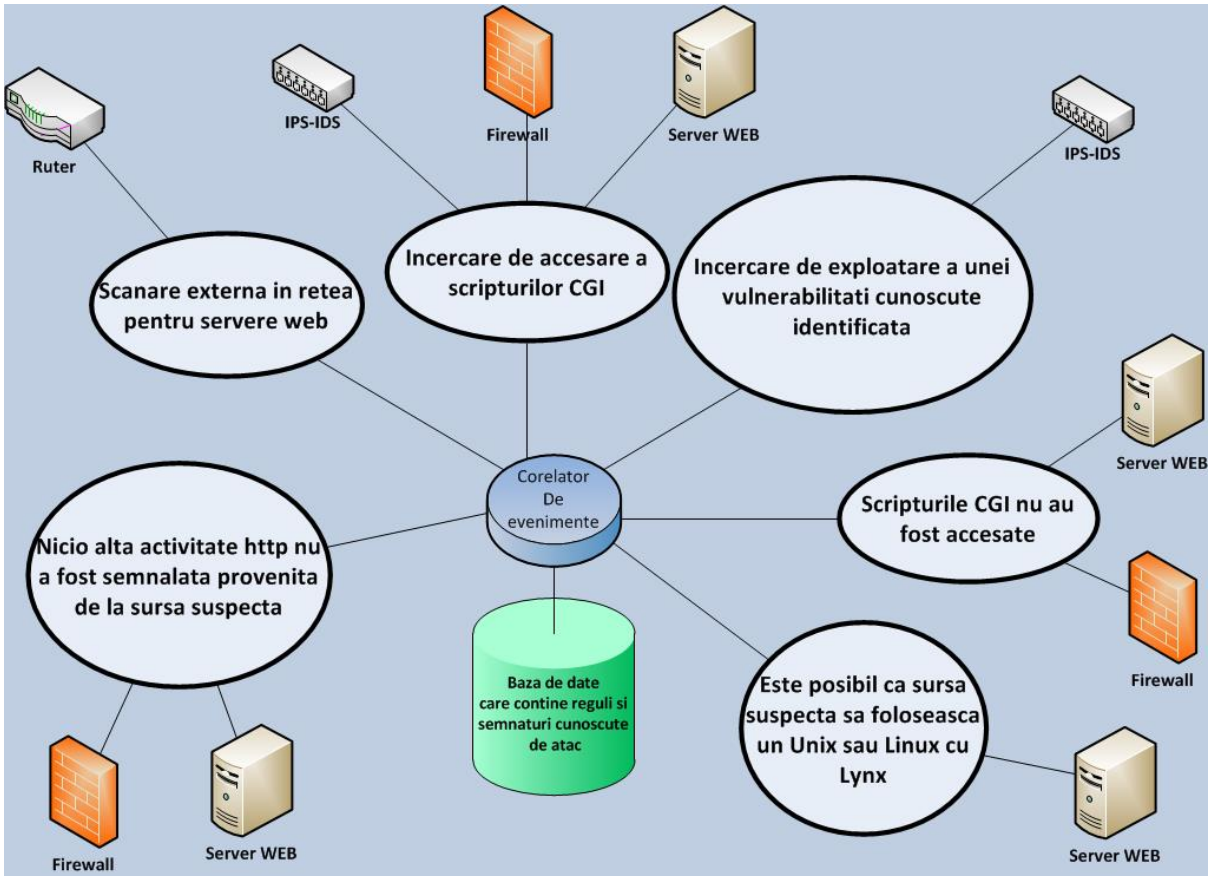

Fig. 0.7 Analiza corelativă a unui atac informațional extern

5.3 Securizarea corelatorului de evenimente

Securizarea corelatorului este un aspect foarte important, deoarece acesta este cel mai important sistem de alertă și în unele cazuri, poate avea putere de decizie instantă pentru luarea unor acțiuni, cum ar fi blocarea traficului de la un anumit host care încearcă un atac.

Analizând secvențele de atac obișnuite prin care atacatorii încearcă să exploateze sisteme ținta, se observă că de cele mai multe ori, aceștia încearcă să obțină drepturi suplimentare, pentru a putea accesa resurse și sisteme la care aceștia nu au acces. Pentru a combate acest mod de atac, propun ca pentru fiecare drept suplimentar primit de către un administrator, trebuie ca acest drept sa treacă printr-un filtru de management de identitate. Spre exemplu, pentru persoanele care au drept de adăugare sau ștergere de reguli în corelator, trebuie urmat un workflow definit de un sistem de Identity Management. În Fig. 3.17, se observă modul în care este acceptată o cerere de permisiuni pentru un administrator nou sau unul cu drepturi restrânse. Nicio entitate reprezentată printr-un sistem sau persoană nu va putea câștiga drepturi, dacă acest workflow nu este respectat.

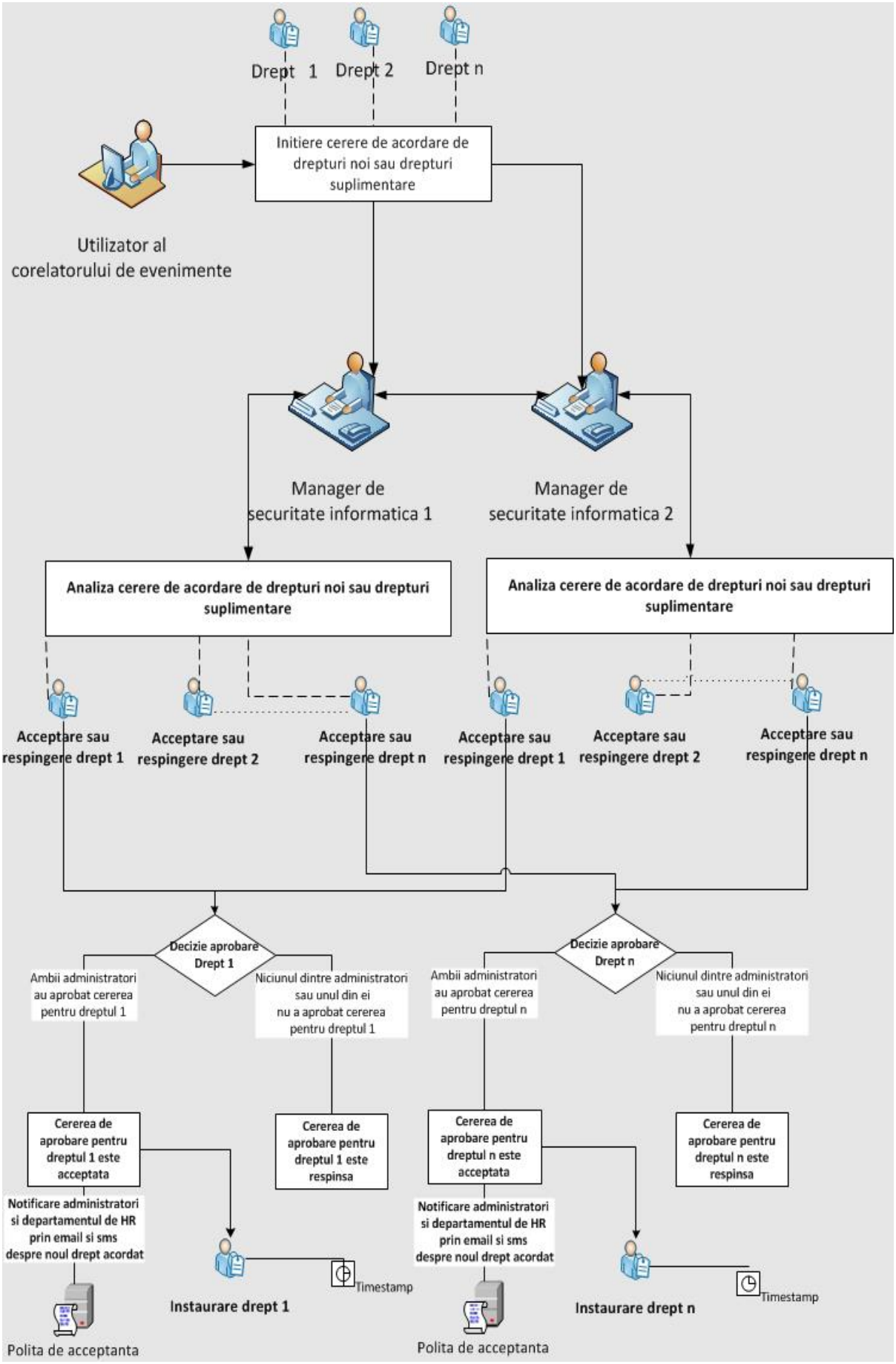

Fig. 0.8: Model pentru aprobarea cererilor de acordare de permisiuni pentru persoanele care au acces la corelator

6. Solutie de criptare care asigură integritate, confidențialitate și non-repudiere sigure

Criptografia asigură confidențialitatea datelor, prin criptarea unui mesaj utilizând chei asociate cu un algoritm. Cheia utilizată trebuie sa fie secretă ambelor entități, problema cea mai mare fiind managementul cheilor și menținerea lor secretă. Criptografia are la bază codificarea mesajelor prin substituirea unui bloc cu altul, după anumite reguli și proceduri.

Cerințele pe care practica le impune metodelor criptografice sunt următoarele:

- **Asigurarea confidențialității**, care presupune condiția ca nicio persoana sa nu poată citi mesajul criptat cu excepția destinatarului
- **Asigurarea integrității datelor**, care presupune protejarea datelor la alterare sau manipularea de către persoanele neautorizate. Manipularea datelor reprezintă procesele de inserare de date adiacente, întârzieri sau substituiri ale datelor.
- **Asigurarea autentificării precise**, care presupune posibilitatea de identificare a sursei și a entității care a trimis mesajul sau informația
- **Asigurarea non-repudierii**, care presupune prevenirea negării unor angajamente sau a unor acțiuni ulterioare, adică cel care trimite mesajul nu poate să nege că acesta l-a trimis mai târziu.

6.1. Metoda de criptare hibridă pentru criptarea datelor în companii mari.

Din cauza dezavantajelor metodelor clasice de criptare, cum ar fi timp de criptare mare și posibilitatea de posesie a cheilor de criptare pentru persoane neautorizate [21], propun o noua metoda de criptare care asigură integritatea și confidențialitatea datelor[117]. Cheile de criptare sunt stocate în store-ul sistemului de operare, împreună cu certificatele entităților. Dacă se obține acces la această magazie, atunci o persoană neautorizată poate exporta și folosi aceste chei, semnându-se drept altă persoană sau entitate. De asemenea, există viruși specializați care vizează furtul de certificate și chei ale entităților. De aceea, trebuie avut în vedere modul de gestionare a cheilor. Metoda propusă de mine combina criptarea simetrică cu cea asimetrică, cu semnătura digitală și funcțiile hash. Toate metodele au puncte slabe, dar și funcționalități puternice. Criptarea cu cheie secretă este foarte rapidă, însă gestionarea cheii este dificilă, deoarece trebuie transmisă intr-un mod sigur. Criptarea asimetrică este o metoda consumatoare de timp, procesele de criptare și decriptare fiind folosite doar pentru transmiterea cheilor secrete și pentru criptarea documentelor.

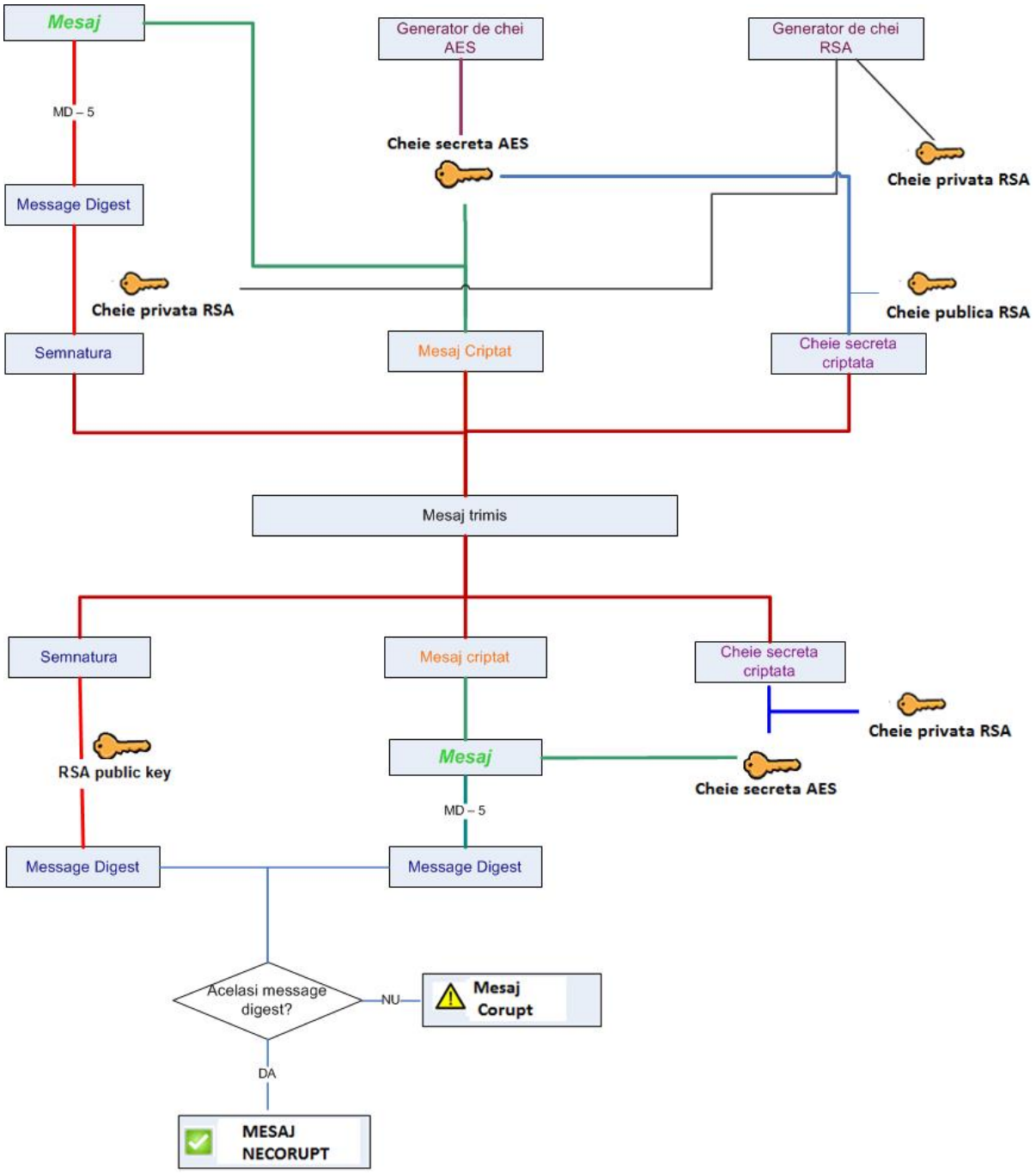

Fig. 6.1 Metoda hibridă de criptare a datelor

Modelul de funcționare a metodei hibride de criptare a datelor este:

1. Hashul mesajului original este semnat digital
2. Cheia de criptare simetrică este folosită pentru a coda mesajul original. Cheia secretă este obținută folosind un generator de chei și este schimbată periodic
3. Cheia privată folosită pentru a cripta cheia simetrică este codată folosind algoritmul RSA, dar cu chei diferite
4. Cheia privată codată este atașată mesajului criptat împreună cu semnătura digitală

Pentru semnătura digitala folosim algoritmul DSA sau RSA. În acest algoritm hash-ul mesajului este criptat folosind cheia privata RSA. Aceasta criptare reprezintă semnătura si este atașata mesajului. Este evident ca acesta abordare este una greșita deoarece:

- Semnătura textului cifrat are aceasi lungime ca si corespondentul în text liber, deci mărimea mesajului este dublata, consumând cantități mari de banda si spațiu de stocare
- Criptarea prin chei publice are viteza mica de execuție si plasează încărcări computaționale uriașe pe procesorul computerului, deci pot fi afectate si degradate semnificativ performantele computerelor
- Criptarea întregului conținut de informație produce cantități mari de text cifrat, care poate fi folosit pentru criptanaliza, în special atacuri de text liber, în care parți din pachetele criptate, cum ar fi headerele emailurilor sunt cunoscute de atacator.

7. Soluție pentru tratarea cazurilor de pierdere sau furt al laptopurilor în companii

Cele mai bune metode de protecție vizează atingerea urmatoarelor obiective:

- informația stocata pe laptop să fie total inaccesibila persoanelor neautorizate
- folosirea dispozitivelor GPS pentru a identifica locația laptopului dispărut
- Recuperarea laptopului și restaurarea modului de funcționare

7.1 Mijloace de declanșare a unei condiții suspicioase a unui laptop

Exista foarte muti declanșatori ai ridicării suspiciunii condiției unui laptop, în cazul în care acesta nu a fost deja declarat pierdut sau furat. În oricare dintre aceste cazuri, laptopul intra în modul de furt. Acesti declansatori sunt:

- Încercari excesive de autentificare
- Timpul de autentificare inaintea bootarii expiră – în momentul în care utilizatorul nu se autentifica în intervalul de timp stabilit de către departamentul IT.
- Laptopul nu comunica cu serverul central în intervalul de timp specificat de către departamentul IT, chiar daca laptopul are sau nu are conectivitate la rețea (declansatorrul este implementat în hardware)
- Serverul companiei trimite o „pilulă de otravă" prin intermediul unei rețele LAN sau wireless, în momentul în care sistemele reconciliază sau în momentul în care laptopul este declarat pierdut de către angajat
- Serverul companiei poate trimite „pilula de otrava" prin intermediul unui mesaj text SMS prin intermediul unei rețele 3G, daca laptopul dispune de un modem 3G.

7.3 Masuri luate după ce declanșatorul unei condiții suspicioase a unui laptop a fost activat

După ce declanșatorul a fost activat, laptopul este dezactivat, prin blocarea procesului de bootare la nivel de hardware. Sistemul nu va boota de pe un hard drive, drive secundar, drive USB, CD, DVD sau alte dispozitive periferice. Prin luarea acestei măsuri, dispozitivul va deveni inutil, fără a permite persoanelor rău intenționate sa-l revândă. Aceasta metoda intra în acțiune doar daca laptopul furat dispune de o conexiune la internet și daca serverul central poate transmite laptopului sa intre în mod de furt. Această metodă nu este neapărat cea mai eficientă din punct de vedere al integrității datelor, deoarece șansele ca laptopul și persoana care a comis infracțiunea să fie găsite scad considerabil și implicit și aflarea gradului de risc la care compania a fost expusă prin pierderea integrității datelor.

Altă măsură existentă luată în momentul declarării unui laptop ca fiind în stare de furt este blocarea informației esențiale, chiar dacă aceasta este criptată sau nu. Chiar dacă persoana rău intenționată are acces la credențialele de criptare cum ar fi chei sau informații criptografice stocate în sistem, „pilula de otrava" trimisa de către serverul de control al companiei le dezactivează, devenind ineficiente în încercările de decriptare sau criptare a datelor. Credențialele de criptare pot fi restaurate doar de către departamentul IT al companiei.

Laptopul este capabil sa trimită informații privind locația exactă în care acesta se află, către serverul central. Acesta trimite coordonatele de latitudine și longitudine prin intermediul unui SMS prin intermediul unei rețele 3G, însă doar dacă dispune de un dispozitiv 3G instalat.

Daca laptopul este recuperat, departamentul IT poate restaura funcțiile laptopului prin intermediul unei parole de acces, a unui token sau a unui mesaj SMS peste o rețea 3G. Nu există nicio garanție că datele nu sunt compromise.

7.4 Măsuri de precauție luate împotriva pierderii laptopurilor. – propunere personală

Sistemul trebuie sa îndeplinească următoarele funcții:

- Sa dețină posibilitatea de a activa o alarmă zgomotoasa pe laptop
- Sa dețină posibilitatea de a activa o alarmă pe dispozitivul mobil
- Sa introducă laptopul în stare de furt, în cazul în care aceasta este indusa de către proprietar la momentul constatării dispariției sau în cazul validării unor condiții predefinite de risc
- Sa închidă automat sesiunea activă în cazul în care este validată o condiție de distantă maximă prestabilită atinsă între laptop și dispozitiv și sa avertizeze utilizatorul despre schimbările de stare ale laptopului în cazul în care acestea au loc în lipsa lui. Acest sistem împiedică accesul neautorizat la laptop și la datele care sunt stocate sau pot fi accesate prin intermediul lui.
- Indicarea distanței intre laptop și dispozitiv
- Răspunderea laptopului la comenzile proprietarului transmise prin intermediul dispozitivului mobil
- Alertarea proprietarului și a serverului central cu privire la posibilele amenințări

Pentru măsurarea distantei intre dispozitive am ales tehnologia Bluetooth LE (Bloototh Low Energy), tehnologie suportata de majoritatea dispozitivelor care dețin wireless începând cu anul 2013. BLE, denumit si Bluetooth Smart este o tehnologie dezvoltata de Bluetooth Special Interest Group, conceputa în special pentru aplicații în sănătate, fitness, securitate si industriile home entertainment. În comparație cu tehnologiile Bluetooth clasice, BLE a fost conceput sa reducă consumul de putere, menținând raza de comunicare similara cu cele clasice. Acesta folosește aceasi frecventa radio de 2.4 GHz, ceea ce permite dispozitivelor dual-mode sa folosească o singura antena.

Toate profilele de aplicații de pe dispozitive mobile care folosesc energie scăzuta sunt bazate pe GATT(Generic Attribute Profile), care permite trimiterea si primirea unor piese mici de date cunoscute ca atribute pe un fir de energie scăzută. Bluetooth 4.0 furnizează consum de putere scăzut, cu banda mai mare de transfer. Modelul software pe care îl expune BLE se bazează pe API-uri (Application Programming Interface), care specifică modul în care componentele software interacționează intre ele.

Distanța maximă de acțiune a tehnologiei Bluetooth Low Enery este de 50 de metri, ceea ce este suficient pentru scopul nostru de a măsura proximitatea intre laptop si dispozitiv.

Starea de alerta la care se găsește sistemul la un moment dat trebuie setat de către utilizator. Aceasta stare de alerta este definită de mediul în care se găsesc proprietarul și laptopul la un moment dat de timp. Astfel putem distinge trei zone de alertă:

- **Zona de muncă** – această zonă este definită de spațiul în care proprietarul își desfășoară activitatea zilnică și are în vedere faptul că laptopul poate fi lăsat nesupravegheat intenționat. În această zonă sunt active alertele care privesc depășirea distanței medii dintre dispozitive și închiderea automată a sesiunii active a laptopului, în cazul în care aceasta nu a fost realizată de către proprietar.
- **Zona de transport** – această zonă vizează situațiile în care laptopul este transportat și are predefinită o distanta între dispozitive foarte mica, deoarece se considera ca laptopul ar trebui sa fie în permanență în proximitatea proprietarului. Valoarea implicita a distantei intre dispozitive este de 5 metrii.
- **Zona de inactivitate** – este definită de situațiile în care laptopul este considerat a fi depozitat într-o zonă relativ sigură: locuința proprie, camera de hotel și are ca modul de alarma cazul în care laptopul își schimbă locația. În acele cazuri, laptopul este considerat a fi în situație de risc.

Utilizatorul trebuie sa aibă posibilitatea să schimbe zona de alertă prin intermediul dispozitivului mobil.

Dacă utilizatorul este în zona de muncă, acesta trebuie să pre-configureze acțiunile pe care sistemul trebuie sa le efectueze automat în funcție de distanțele predefinite între dispozitive. Dacă este depășită raza minimă de proximitate, sesiunea activă a laptopului trebuie sa fie dezactivată și sistemul instalat pe laptop trebuie să verifice dacă laptopul este securizat fizic cu un dispozitiv de blocare fizică (chain lock sau alte dispozitive de securizare fizică). Această măsură de securitate este una standard implementată în companii, însă se bazează strict pe vigilența angajaților. Sistemul de securizare fizică este reprezentat de un fir metalic cu cifru care trebuie străbătut de un voltaj foarte slab pentru a se putea determina daca acesta se afla în mod activ sau pasiv. În momentul în care sistemul antifurt se găsește în mod activ, iar curentul slab este întrerupt, se consideră că firul metalic a fost tăiat, iar laptopul intră automat în stare de furt. Dacă laptopul nu este securizat cu un astfel de sistem, utilizatorul primește o alertă pe dispozitivul mobil. Daca este depășită o rază de proximitate mare între cele două dispozitive, sistemul trebuie să avertizeze utilizatorul despre aceasta situație, iar daca utilizatorul ignora această avertizare, iar raza de acțiune creste considerabil, laptopul este introdus automat în stare de furt, iar sistemul avertizează utilizatorul și serverul centrat despre situația generată.

7.5 Măsuri de control al daunelor și de recuperare a laptopurilor pierdute – propunere personală

Propunerea personală pentru a proteja un laptop de companie conține 5 pași:

1. Toate datele utilizatorului sunt salvate în timp real pe un server specific al companiei. Acest aspect este tratat de către un software de backup care realizează backup incremental sau diferențial de fiecare dată când angajații sunt în interiorul spațiului de lucru al companiei, sau în momentul în care aceștia se conectează din exteriorul companiei la aplicațiile si resursele acesteia prin intermediul unei conexiuni VPN(Virtual Private Network). Această etapă este foarte importantă, pentru că oferă disponibilitatea companiei de a renunța la datele stocate pe un laptop pierdut și pot fi implementate masuri de distrugere a datelor existente pe acestea. Al doilea beneficiu este ca restaurarea datelor pe un alt laptop împiedică atragerea costurilor provenite din lipsa activității utilizatorului care a pierdut laptopul.

2. Folosirea unui sistem de alertă și control care comunică cu laptopul pentru a avertiza proprietarul acestuia despre amenințările și situațiile de risc posibile, sau pentru a instaura masuri de management al daunelor (dezactivarea sesiunii active, activarea automată a modului de furt), în cazul în care sunt activați anumiți declanșatori.
3. Instaurarea de metode de criptare a hardului și metode de sincronizare hardware a laptopului cu hardul astfel încât acestea sa fie nefuncționale unul fără celalalt. În cazul în care ambele metode sunt instaurate, șansele de utilizare a laptopului fără cunoașterea cheilor de criptare este nula.
4. Laptopul este urmărit cu ajutorul unul dispozitiv GPS instalat în interiorul laptopului, alimentat de bateria principală sau de o baterie auxiliară, care funcționează chiar dacă laptopul nu este pornit. Dispozitivul GPS are rolul de emițător și poate fi localizat prin intermediul unei interfețe web securizate în timp real. Alegerea unei interfețe web pentru localizarea laptopului are avantajul că oferă utilizatorului disponibilitate mărită datorita locațiilor diverse din care poate fi accesată în timp scurt.
5. După recuperarea laptopului, datele pot fi restaurate folosind backup-urile incrementale sau diferențiale stocate în serverul central al companiei.

Backup-urile incrementale sau diferențiale reprezintă soluții mult mai bune pentru realizarea copiilor de rezerva a datelor zilnice ale angajaților, deoarece durează mult mai puțin decât backup-urile complete și astfel pot fi realizate zilnic. Un backup complet este necesar o data pe săptămână sau o data pe lună. Backup-ul incremental include doar fișierele care au fost schimbate de la ultimul backup complet, prin verificarea bitului de arhiva, un indicator care se schimba de fiecare dată când un fișier este schimbat, mutat sau copiat. După ce backup-ul incremental copiază fișierele marcate, șterge bitul de arhivă de pe hardul computerului.

Cea mai bune soluții pentru protejarea integrității datelor o reprezintă împerecherea hard-disk-ului cu laptopul, astfel încât niciunul să nu funcționeze fără celalalt. Aceasta soluție impune criptarea hardului. Acest lucru este util, deoarece în majoritatea cazurilor, hard disk-ul este scos din laptop și informațiile sunt extrase prin bootarea prin intermediul unui alt hard. În momentul extragerii hard-disk-ului din laptop, serverul central nu poate trimite „pilula cu otravă” și este posibil ca laptopul sa fie în alta locație în momentul în care acesta este identificat cu ajutorul dispozitivului GPS. De aceea este important ca persoanele rău intenționate sa fie descurajate să separe cele doua dispozitive unul de celalalt.

7.6 Ideile noi comparate cu soluțiile existente

Masurile existente luate în cazurile de laptopuri pierdute sau furate nu dau garanția că datele stocate pe acestea pot fi recuperate. Recuperarea lor are loc doar dacă laptopul este recuperat, iar autorul faptei nu a avut acces la date. Realitatea demonstrează că majoritatea hard-disk-urilor sunt extrase din laptopuri după momentul furtului pentru că hoții nu pot trece peste măsurile de securitate implementate pe acestea. Deoarece nu exista acces la software-ul care comunică cu serverul central, „pilulele cu otrava” nu pot fi lansate, iar laptopurile nu mai pot fi recuperate. Soluția de backup incremental sau diferențial garantează că datele sunt accesibile în permanență, indiferent de statusul laptopului.

Privind metodele de prevenire a pierderii laptopului sau a furtului de date, majoritatea metodelor implementate de către companii consista în securizarea acestora cu sisteme antifurt (chain lock) cu cifru. Nu exista nicio metoda care avertizează proprietarul laptopului în timp real despre starea laptopului. Metoda prezentată permite proprietarului sa seteze diferite stări ale mediului în care laptopul se află, pentru a putea fi avertizat cu privire la folosirea malițioasă sau eventualele situații de risc.

CONCLUZII

C.1. CONCLUZII GENERALE

Mediul de afaceri actual este un mediu competitiv care se bazează pe informație pentru a evolua și pentru a supraviețui. Măsurile de securitate implementate sunt în conformitate cu gradul de risc aferent expunerii datelor sau a sistemelor la amenințări și vulnerabilități și urmăresc reducerea costurilor provenite din evenimente neprevăzute. Acțiunile de prejudiciere provenite din compromiterea integrității sau furtul de informație evoluează odată cu măsurile de prevenire a acestora, de aceea niciodată un sistem nu poate fi considerat total sigur. Măsurile expuse prin care se încearcă controlul sau minimizarea pierderilor sunt doar încercări de a face fată acestor amenințări.

Studiile efectuate relevă faptul ca cele mai mari amenințări sunt cele în care intervine factorul uman, în special neglijența sau intențiile rele ale angajaților (pierderea dispozitivelor mobile care conțin date sensibile, furtul de proprietate intelectuală sau necontrolarea și ne-securizarea informației care părăsește compania). De aceea, trebuie îmbunătățite metodele prin care datele sunt transmise în exteriorul companiei: îmbunătățirea metodelor de criptare și îmbunătățirea controlului la datele copiate sau transmise prin soluții de tip DLP și îmbunătățirea metodelor de securizare a dispozitivelor mobile.

Analizând după gradul de risc ridicat de amenințări, am constatat ca cele mai periculoase sunt amenințările la nivelul logic, iar cele mai importante metode de securitate a datelor au la baza metode de criptare, prin care se asigură canale securizate de comunicare și protecție a datelor stocate. Din cauza faptului ca metodele actuale de stocare și gestionare a certificatelor care conțin cheile de criptare pot fi exploatate de către persoane rău intenționate sau viruși, consider ca aceasta este o arie care trebuie îmbunătățită prin stocarea datelor biometrice ale proprietarului certificatelor în interiorul acestora. În acest mod, se poate crește gradul de securitate pentru datele și informațiile critice, iar persoanele rău intenționate sunt descurajate, deoarece nu poseda caracteristica fizică a proprietarului și nu pot exploata sistemul.

Pentru a putea trata în timp real amenințările interne și externe, trebuie impusă o soluție care monitorizează toată activitatea informațională a companiei. Corelatorul de evenimente colectează informații de la diferite sisteme și le corelează pentru a identifica amenințări cu grad sporit de risc, având capabilitatea de a lua măsuri în timp real și de a avertiza persoanele care tratează tipul de caz de amenințare apărut. Acesta este mult mai eficient decât echipele de securitate bazate pe resurse umane pentru a răspunde amenințărilor, deoarece acesta ia decizii în timpul apariției amenințării, spre deosebire de echipele de securitate informațională constituite din administratori de securitate, care efectuează o analiză post-incident.

În cazul criptării, pentru a securiza canalele de comunicație și datele stocate, se implementează algoritmi de criptare hibrizi cu chei de criptare cat mai mari, însă problema majora se afla la modul de gestiune a cheilor de criptare, care pot fi expuse prin anumite procedee. De aceea, cea mai eficientă metodă este de generare în timp real al unei chei simetrice si transferul acesteia securizat către sistemul sau persoana destinatar.

În cazul laptopurilor, costurile generate de expunerea datelor pot aduce un prejudiciu suficient încât compania sa-și piardă credibilitatea pe piață sau să se găsească în insuficiența să acopere daunele provocate. De aceea este foarte important sa fie asigurată incapacitatea de expunere a acestor informații altor persoane decât cele autorizate și să se asigure recuperarea datelor în cazul în care acestea sunt pierdute.

C.2. CONTRIBUȚII ORIGINALE

În cadrul acestei teze am definit problemele principale legate de securitatea informațională din cadrul companiilor și toate evenimentele implicate de acestea. Studiul se bazează pe incidente petrecute în contextul actual si pe masuri actuale care contracarează sau minimizează impactul pe care aceste incidente le proiectează asupra companiilor.

Pentru acoperirea punctelor esențiale în atingerea scopului de asigurare a securității informaționale, am propus o arhitectura de securitate informațională structurata pe trei niveluri:

- nivel fizic, care privește masuri de securitate fizica în data center sau în interiorul locațiilor care stochează sisteme informaționale ale companiilor cum ar fi:
  - asigurarea securității si funcționalității serverelor intr-o maniera eficienta si continua
  - securizarea cablului de rețea, pentru a împiedica interceptarea pachetelor transmise prin intermediul acestora, de către persoane neautorizate
- nivel logic, care vizează:
  - tehnici de securitate informationala la nivel de aplicație
  - permisiuni de acces
  - politici de securitate
  - tehnici de criptare sau alte tehnici de asigurare a confidențialității si integrității datelor
  - sisteme de detecție si prevenire a intruziunilor
- nivel administrativ, care implica asigurarea securității informaționale prin implementarea unor constrângeri si proceduri de securitate la nivelul tehnologiilor si resurselor umane ale companiei, cum ar fi:
  - folosirea de calculatoare fără unități de disc
  - efectuarea de backup-uri incrementale sau diferențială la intervale regulate pentru datele din companie
  - implementarea si asigurarea funcționalității a sistemelor de rezervă, care preiau sarcinile celor principale, în cazul în care acestea sunt indisponibile, sau funcționează deficitar
  - implementarea de soluții de Data Loss Prevention, care monitorizează si controlează fluxul de informații sensibile pentru companie, cu rolul de a împiedica pierderea sau diminuarea atributelor de integritate si confidențialitate a datelor în mod intenționat sau neintenționat

Pentru asigurarea unei securități informaționale cat mai eficiente, după ce sistemele de securitate informationala au fost integrate si implementate corect în infrastructurile software si hardware ale companiei, am folosit sisteme de management al evenimentelor și de securitate a informației, care corelează evenimentele din sistem provenite din loguri înregistrate de sistemele de securitate si alte sisteme cu factor de risc din companie si pot genera alerte de securitate în timp real, pe baza unor reguli de corelare predefinite. Pentru a înțelege modul de funcționare si aplicabilitatea pe care acestea o oferă în maparea pe sistemele de securitate existente, am expus:

- rolul corelatoarelelor de evenimente în securitatea informationala
- modul de utilizare
- viteza de corelare si de recepție a logurilor
- scalabilitate sistemelor de corelare de evenimente în condițiile extinderii infrastructurii hardware sau a măririi volumului de date care trebuie corelate

- etape premergătoare corelării, necesare pentru a putea fi posibilă aplicarea regulilor de corelare, cum ar fi:
  - Transmiterea logurilor de la sistemele de securitate instalate către un sistem centralizat care face agregarea tuturor evenimentelor din cadrul companiei intr-un singur sistem de monitorizare si control
  - Normalizarea logurilor, tradusa prin transformarea structurii si sintaxei tuturor logurilor intr-un singur format, pe care corelatorul îl poate interpreta
  - Reducerea volumului de date care trebuie analizate, exprimat prin eliminarea logurilor duplicate din sistem, reducerea dimensiunii logurilor prin tehnici de arhivare si comprimare
  - Generarea de evenimente prin cumulul si corelarea altor evenimente, pentru a transmite o informație generalizată si succintă
  - Prioritizarea logurilor, astfel încât sa fie evidențiate si trimise către regulile de corelare cele care au factor de risc superior
- Sisteme care pot fi integrate cu corelatorul de evenimente cu factor de risc si rolul lor în securitatea informationala a companiei

În cadrul acestei teze de doctorat am propus reguli de corelare pentru evenimente cu factor de risc, pentru scenarii reale din interiorul companiilor. Regulile de corelare sunt aplicate folosind un corelator de evenimente, care adună loguri de la sisteme de securitate multiple, cum ar fi Firewall, Router, sistem DLP, Active Directory, Sistem de Detecție și Prevenire a Intruziunilor, etc. Am insistat pe securitatea internă din companii și pe tratarea cazurilor în care acțiunile angajaților ar putea duce la prejudicii serioase pentru companie din perspectiva pierderii confidențialității sau integrității datelor. Pentru a avea efect, regulile de corelare trebuie sa primească informații concrete despre evenimentele cu factor de risc. În primul rând trebuie efectuate doua procese prin care se generează evenimente cu factor de risc pentru confidențialitatea datelor:

- Identificarea si categorisirea datelor cu caracter sensibil pe niveluri de confidențialitate
- Definirea regulilor pentru angajații cu statut special:
  - Angajat în preaviz
  - Angajat în concediu
  - Angajat în practica
  - Angajat venit de la concurență

Pentru evidențierea eficienții pe care corelatoarele de evenimente o au în fața unor astfel de amenințări am expus scenarii prin care angajații pot pune în pericol integritatea si confidențialitatea datelor:

- In primul scenariu, un angajat cu statut special încearcă sa trimită date cu caracter sensibil în internet, încearcă sa copieze un volum mare de date pe o unitate de stocare externa, sau încearcă sa trimită informații confidențiale prin intermediul poștei electronice. Corelatorul de evenimente ia acțiunea de a dezactiva contul de Active Directory al angajatului, care, prin urmare, nu mai are posibilitatea de a folosi resursele companiei
- In al doilea scenariu, un angajat care figurează ca nu se afla fizic în companie si nu are drept de acces de la distanta la resursele companiei, se autentifica în Active Directory cu setul sau de credentiale. Corelatorul de evenimente ia acțiunea de a dezactiva contul de Active Directory al angajatului, care, prin urmare, nu mai are posibilitatea de a folosi resursele companiei

Pentru securizarea mediilor de transmisie între sisteme, cât și pentru securizarea datelor transmise în exteriorul companiei, am propus o metoda de criptare care asigură

integritatea, confidențialitatea și non-repudierea datelor. Prin combinarea diferitelor tehnici de criptografie, aceasta abordare oferă o soluție pentru combaterea punctelor slabe expuse tehnicilor de criptare:

- Managementul cheilor: generarea cheilor, stocarea cheilor, transmiterea cheilor sunt expuse riscurilor
- Timpul de criptare este mare
- Asigurarea tuturor atributelor de siguranța a datelor nu este realizata simultan:
  - Integritate
  - Disponibilitate
  - Confidențialitate
- Non-repudierea nu este asigurata

Metoda propusa asigura:

- Integritatea datelor – folosind funcția de hash
- Autentificare si autenticitate – folosind semnătura digitala prin criptare asimetrica DSA
- Confidențialitatea datelor folosind algoritmul de criptare simetrica AES (Advanced Encryption Standard)
- Viteza de criptare mare – folosind AES
- Protejarea cheilor prin generator propriu de chei si prin transferul sigur al cheilor secrete prin criptare asincrona

Metoda asigură integritatea și confidențialitatea datelor, aducând certitudinea destinatarului că mesajul este nealterat, prin verificarea message digest-ului (hash-ul mesajului) și că mesajul nu poate fi descifrat de către altă persoană în afara de el, datorită algoritmului de criptare cu cheie secretă, pe care doar el o poate decripta. Aceasta metoda este o metoda de criptare foarte puternică și datorită generării periodice a cheii secrete la fiecare încercare de reconciliere între expeditor și destinatar.

Pentru securizarea informațiilor stocate pe dispozitivele mobile sau care pot fi accesate prin intermediul acestora, am propus o soluții de prevenire și soluții de control al daunelor pentru astfel de situații. Soluția vizează propunerea unui sistem de comunicare între un sistem wireless hardware instalat pe laptop și un dispozitiv mobil de dimensiuni reduse de tip ceas de mana, smartphone, breloc sau pager.

Sistemul trebuie sa îndeplinească următoarele funcții:

- Sa dețină posibilitatea de a activa o alarmă zgomotoasa pe laptop
- Sa dețină posibilitatea de a activa o alarmă pe dispozitivul mobil
- Sa introducă laptopul în stare de furt, în cazul în care aceasta este indusa de către proprietar la momentul constatării dispariției sau în cazul validării unor condiții predefinite de risc
- Sa închidă automat sesiunea activă în cazul în care este validată o condiție de distantă maximă prestabilită atinsă între laptop și dispozitiv și sa avertizeze utilizatorul despre schimbările de stare ale laptopului în cazul în care acestea au loc în lipsa lui. Acest sistem împiedică accesul neautorizat la laptop și la datele care sunt stocate sau pot fi accesate prin intermediul lui.
- Indicarea distanței intre laptop și dispozitiv
- Răspunderea laptopului la comenzile proprietarului transmise prin intermediul dispozitivului mobil
- Alertarea proprietarului și a serverului central cu privire la posibilele amenințări

Pentru securizarea informatiilor stocate si manipulate de dispozitive mobile ale companiilor, cum ar fi laptopurile, propun o serie de metode care vizează reducerea impactului generat de furt sau pierdere a acestora în 5 pași:

1. Toate datele utilizatorului sunt salvate în timp real pe un server specific al companiei. Acest aspect este tratat de către un software de backup care realizează backup incremental sau diferențial de fiecare dată când angajații sunt în interiorul spațiului de lucru al companiei, sau în momentul în care aceștia se conectează din exteriorul companiei la aplicațiile si resursele acesteia prin intermediul unei conexiuni VPN(Virtual Private Network). Această etapă este foarte importantă, pentru că oferă disponibilitatea companiei de a renunța la datele stocate pe un laptop pierdut și pot fi implementate masuri de distrugere a datelor existente pe acestea. Al doilea beneficiu este ca restaurarea datelor pe un alt laptop împiedică atragerea costurilor provenite din lipsa activității utilizatorului care a pierdut laptopul.
2. Folosirea unui sistem de alertă și control care comunică cu laptopul pentru a avertiza proprietarul acestuia despre amenințările și situațiile de risc posibile, sau pentru a instaura masuri de management al daunelor (dezactivarea sesiunii active, activarea automată a modului de furt), în cazul în care sunt activați anumiți declanșatori.
3. Instaurarea de metode de criptare a hardului și metode de sincronizare hardware a laptopului cu hardul astfel încât acestea sa fie nefuncționale unul fără celalalt. În cazul în care ambele metode sunt instaurate, șansele de utilizare a laptopului fără cunoașterea cheilor de criptare este nula.
4. Laptopul este urmărit cu ajutorul unul dispozitiv GPS instalat în interiorul laptopului, alimentat de bateria principală sau de o baterie auxiliară, care funcționează chiar dacă laptopul nu este pornit. Dispozitivul GPS are rolul de emițător și poate fi localizat prin intermediul unei interfețe web securizate în timp real. Alegerea unei interfețe web pentru localizarea laptopului are avantajul că oferă utilizatorului disponibilitate mărită datorita locațiilor diverse din care poate fi accesată în timp scurt.
5. După recuperarea laptopului, datele pot fi restaurate folosind backup-urile incrementale sau diferențiale stocate în serverul central al companiei.

C.3. PERSPECTIVE DE DEZVOLTARE ULTERIOARĂ

Mecanismele de securitate propuse sunt limitate doar de incapacitatea administratorilor de securitate de a anticipa metodele de exploatare a vulnerabilităților sistemelor din interiorul companiilor. Deoarece modelul de securitate exploatat în aceasta teză se bazează pe corelare de evenimente, rolul administratorului este de a instaura cat mai multe reguli de corelare, pentru a acoperi toate scenariile în care ar putea apărea un incident de securitate informațională. În aceasta arie se poate extinde foarte mult plaja de reguli instaurate. Este indicat ca toate alertele de securitate cu grad de risc mare sa fie analizate, chiar daca nu a fost compromis niciun sistem, deoarece prin investigare se pot descoperi vulnerabilități neacoperite prin reguli sau politici de securitate.

Metoda de criptare prezentata în capitolul 4 poate fi integrata în protocoale de comunicație, sau poate fi folosita pentru a extinde securitatea obținută prin infrastructura cu chei publice (PKI).

Soluția de prevenire a pierderii laptopurilor sau de securizare a acestora se poate materializa prin dispozitivul de control al stării în care se găsește laptopul, sau printr-o aplicație de telefon, în cazul în care acesta dispune de funcție GPS sau alta funcție de măsurare a proximității.

Bibliografie

[1] *T. Peltier*, Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management, ISBN 0-8493-1137-3, 2013

[2] *M. Harkins*, Managing Risk and Information Security, 2012

[3] *A Calder*, information Security Based on ISO 27001/ISO 27002: A Management Guide

[4] *M. Stanciu, A. Oprea,* Sistem de detecţie şi prevenire a intruziunilor într-o reţea, 2013

A. Spadaro, Event correlation for detecting advanced multi-stage cyber-attacks, 2013

[5] *Aron Warren,* Setting up Splunk for Event Correlation în Your Home Lab,Noiembrie 2013

[6] Intelligent IT operations; Making IT smarter with advanced event correlation and management; Hewlett-Packard Development Company; 4AA2-7408ENW, 2012

[7] *Mazda A. Marvasti, Arnak V. Poghosyan, Ashot N. Harutyunyan, Naira M. Grigoryan*, An Anomaly Event Correlation Engine: Identifying Root Causes, Bottlenecks, and Black Swans în IT Environments, Wmware Technical Journal 2013

[8] *Gary C. Kessler*, „An overview of Cryptography", 28 Apr. 2013

[9] *Tim de Chant,* The boring and exciting life of biometrics, 18 june 2013

[10] RSA Laboratories- Chryptographic tools; secțiunea 2.1.5.;

[11] *Anton A. Chuvakin, Kevin J. Schmidt*, „Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management „ Decembrie 13, 2013, ISBN-10: 1597496359 | ISBN-13: 978-1597496353 | Ediția: 1

[12] National Institute of Standards and Technology. (2010). National Vulnerability Database (NVD) National Vulnerability Database (CVE-2010-2075).

[13] *Peter Zadrozny, Raghu Kodali,* „Big Data Analytics Using Splunk: Deriving Operational Intelligence from Social Media, Machine Data, Existing Data Warehouses, and Other Real-Time Streaming Sources",22 Mai 2013

[14] PwC. Cybercrime: Protecting against the growing threat. Events & Trends Vol. 256. Martie 2012, pp. 6-18

[15] *Salah, Saeed, Maciá-Fernández, Gabriel și Díaz-Verdejo, Jesús E.* „A model-based survey of alert correlation techniques. 2013, Computer Networks, Volume 57, Issue 5, pp. 1289-1317

[16] *Vaishnavi, Vijay and Kuechler, William.* „Design Science Research în Information Systems. Design science research în information systems and technology". [Online] Septembrie 30, 2011.

[17] *Vries, Johannes A*, "An analysis framework to aid în designing advanced persistent threat detection systems"., 2012

[18] Verizon RISK Team. Data Breach Investigation Report. s.l. : Verizon Enterprise, 2012.

[19] *Ing. Cristian MARINESCU, Prof.Dr.Ing. Nicolae ŢĂPUŞ* ; "An Overview of the Attack Methods Directed Against the RSA Algorithm"; Revista Informatică Economică, nr. 2(30)/2004

[20] *Risto Vaarandi*, Tools and Techniques for Event Log Analysis, 2005

[21] *Arash Partow*, "General Purpose hash Function Algorithms"

[22] *Masashi Une and Masayuki Kanda,* "Year 2010 Issues on Cryptographic Algorithms", Lucrarea Nr. 2006-E-8, IMES, C.P.O BOX 203 Tokyo, 100-8630 Japan

[23] *Prof. Patrick McDaniel,* Network and Security Research Center Department of Computer Science and Engineering Pennsylvania State University, University Park PA – "Public-Key Cryptography and Attacks on RSA", 2010

[24] *X. Wang, and B. de Weger,* "Colliding X.509 Certificates," Cryptology ePrint Archive, 2005

[25] *Rodrigues, J. Roberts,*. "System security and personal help data protection", 2007

[26] *Gregory Braun,* " Crypto 2000" (*For Small to Medium Businesses*)

[27] Information Technology and Organizations: "Trends, Issues, Challenges and Solutions", volumul 1, 2003 Information Resources Management Association, International Conference,Philadelphia, Pennsylvania, USA,May 18-21, 2003

[28] *Ki Woong Park, Hyun Jin Choi, Kyu Ho Park*-"An Interoperable Authentication System using ZigBee-enabled Tiny Portable Device and PKI", International Conference on Next Generation PC

[29] *Daemen, Joan; Rijmen, Vincent.* "AES Proposal: Rijndael"

[30] *Nicolae Bârsan-Pipu, Ion Popescu, "*Managementul riscului – concepte- metode-aplicații.*"*, Editura Universității "Transilvania" din Brasov, 2003

[31] *Brynjolfsson, Erik and Yang, Shinkyu***,** Information Technology and Productivity: A Review *of the Literature,* 1996, Advances in Computers 43, pp. 179-214

[32] *Abbas, Haider* ,Addressing Dynamic Issues in Information Security Management. 2011, Information Management & Computer Security, Vol.19, pp. 5-24.

[33] World Economic Forum. *Global Risks 2012.* Cologny : Risk Response Network, 2012.

[34] PwC. Cybercrime: Protecting against the growing threat. *Events & Trends Vol. 256.* March 2012, pp. 6-18.

[35] *Sommestad, Teodor* ,Security mistakes in information system deployment projects. 2011, Information Management & Computer Security, Vol. 19 No.2, pp. 80-94.

[36] *Ren, Hanli, Stakhanova, Natalia and Ghorbani, Ali A*.,An online adaptive approach to alert correlation. Bonn : Springer-Verlag, 2010. Proceedings of the 7th international conference on Detection of intrusions and malware, and vulnerability assessment. pp. 153-172.

[37] *Debar, Hervé and Viinikka, Jouni.,*Security information management as an outsourced service. 2006, Information Management & Computer Security, Vol. 14 No.5, pp. 417-435.

[38] SecurityWeek. Worldwide IT Security Spending to Top $60 Billion in 2012, Says Gartner. *securityweek.com.* [Online] September 13, 2012. http://www.securityweek.com/worldwide-it-security-spending-top-60-billion-2012-says-gartner.

[39] GTISC and GTRI. *Emerging cyber threats report 2012.* Atlanta : Georgia Tech Cyber Security Summit, 2011.

[40] IDC. Security Products: Market Analysis. *IDC #231292, Volume: 1* . Framingham, MA, USA : s.n., November 2011.

[41] *A Comprehensive Approach to Intrusion Detection Alert Correlation.* Valeur, Fredrik, et al. 2004, IEEE Trans. Dependable Secur. Comput. 1, 3, pp. 146-169.

[42] *Alert Correlation for Extracting Attack Strategies.* Zhu, Bin and Ghorbani, Ali A. 2006, International Journal of Network Security, Vol.3, No.3, pp. 244–258.

[43] *Temporal and Spatial Distributed Event* . Jiang, Guofei and Cybenko, George. Boston : s.n., 2004. American Control Conference. pp. 996-1001.

[44] *M2D2: a formal data model for IDS alert correlation.* Morin, Benjamin, et al. Berlin : Springer-Verlag, 2002. RAID'02 Proceedings of the 5th international conference on Recent advances in intrusion detection . pp. 115-137.

[45] *A model-based survey of alert correlation techniques.* Salah, Saeed, Maciá-Fernández, Gabriel and Díaz-Verdejo, Jesús E. 2013, Computer Networks, Volume 57, Issue 5, pp. 1289-1317. 94

[46] *Asynchronous Alert Correlation in Multi-agent Intrusion Detection Systems.* Gorodetsky, Vladimir, Karsaev, Oleg and Samoil, Vladimir. St. Petersburg : Springer, 2005.

Computer Network Security, Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security.

[47] *Transactions on Systems, Man, and Cybernetics.* 1993, Vol. 23, 3, pp. 665-685.

[48] Sugeno, Michio. *Industrial applications of fuzzy control.* s.l. : Elsevier Science Ltd., 1985.

[49] *An Experiment in Linguistic Synthesis with a Fuzzy Logic Controller.* Mamdani, E. H. and Assilian, S. 1, International Journal of Man-Machine Studies, Vol. 7, pp. 1-13.

[50] Shafer, Glenn. *A Mathematical Theory of Evidence.* s.l. : Princeton University Press, 1976.

[51] *M. Une, M. Kanda*Cryptographic Algorithms", Discussion Paper No. 2006-E-8, IMES, C.P.O BOX 203 Tokyo, 100-8630 Japan

[52] *Learning attack strategies from intrusion alerts.* Ning, Peng and Xu, Dingbang. Washington D.C. : ACM, 2003. Proceedings of the 10th ACM conference on Computer and communications

[53] *Ponemon Institute,* 2013 cost of Data Breach Study: Global Analysis, 2013 https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[54] *Ponemon Institute,* 2011 Cost of Data Breach Study: United States, 2012 http://www.ponemon.org/library/2011-cost-of-data-breach-united-states

[55] *C. Hadnagy,* Social engineering: The Art of Human Hacking, John Wiley & Sons, 2010i

[56] *Bitdefender,* Amenințări cibernetice la adresa utilizatorilor din România, 2013 http://www.cert-ro.eu/files/doc/792_20131114101100057378900_X.pdf

[57] *J. Lyman,* SCO Hit with Another Denial-of-Service Attack, 2012

[58] *K. Roebuck,* Data Loss Prevention (DLP): High-impact Strategies – What You Need to Know: Definiions, Adoptions, Impact, Benefits, Maturity, Vendors, ISBN 1743045492, 9781743045497, Emereo Pty Limited, 2011

[59] *M. Vlădescu, G. Mateescu,* A hybrid approach of system security for small and medium enterprises: Combining different cryptography techniques , 2013, Computer Science and Information Systems (FedCSIS)

[60] *M. Vlădescu, G. Mateescu, V. Sgârciu*, The Design and Implementation of an Experimental Model for Secure Management of Personal Data Based on Electronic Identity Card and PKI Infrastructure, 2012, 14th IFAC Symposium on Information Control Problems in Manufacturing, INCOM

[61] *M. Vlădescu, G. Mateescu, V. Sgârciu*, The Design and Validation of an Experimental Model for the Secure and Efficient Medical Services based on PKI Infrastructures and Smart-Cards, 2012, 14th IFAC Symposium on Information Control Problems in Manufacturing, INCOM