ROMÂNIA
ACADEMIA TEHNICĂ MILITARĂ

TEZĂ DE DOCTORAT

CONTRIBUȚII PRIVIND MONITORIZAREA SECURITĂȚII REȚELELOR DE CALCULATOARE

Ing. Nicu-Sebastian NICOLĂESCU

Conducător ştiinţific: Prof. Dr. Ing. Victor-Valeriu Patriciu

Bucureşti
2011

MULȚUMIRI

Adresez mulțumirile cuvenite tuturor celor care, direct sau indirect, prin discuțiile, sugestiile şi expertiza oferită au contribuit la realizarea acestui demers ştiințific şi m-au susținut în finalizarea lui.

Doresc să exprim cele mai sincere mulțumiri şi recunoştință domului Prof. Dr. Ing. Victor-Valeriu Patriciu, conducătorul ştiințific al tezei mele de doctorat, pentru încrederea acordată, precum şi pentru sprijinul deplin şi îndrumarea oferite pe tot parcursul programului de studii doctorale.

Mulțumesc domnului Conf. Dr. Ing. Iustin Priescu, din cadrul Universității „Titu Maiorescu", evaluarea acestei lucrări, precum şi pentru sugestiile de cercetare, încurajările primite şi suportul logistic oferit de-a lungul întregii noastre colaborări.

Mulțumesc domnului Conf. Dr. Ing Ion Bica, şeful catedrei „Calculatoare şi Sisteme Informatice Militare" din cadrul Academiei Tehnice Militare, pentru orientările oferite, precum şi evaluarea critică a acestei lucrări.

Doresc să adresez mulțumiri Prof. Dr. Florentin Smarandache (University of New Mexico, USA), Dr. Pascal Djiknavorian (Université Laval, Quebec, Canada) şi Prof. Dr. Arnaud Martin (Université de Rennes, Franța) pentru sprijinul acordat în aprofundarea aspectelor teoretice a Teoriei Dezert-Smarandache, pentru permisiunea oferită de a utiliza bibliotecile Matlab de fuziunea datelor, documentarea anumitor module, precum şi sprijinul oferit în depanarea anumitor funcții ce au trebuit readaptate.

In cele din urmă, doresc sa aduc mulțumiri familiei pentru susținerea, înțelegerea şi timpul acordat pe durata întregii perioade de studiu.

CUPRINS

Prefață

Odată cu migrarea pe Internet a tot mai multor activități ale societății contemporane, a apărut şi necesitatea unei alte abordări a securității sistemelor IT. Dacă în urmă cu un deceniu securitatea informatică era în mare parte orientată spre produse, având un caracter preponderent defensiv şi reactiv, abordările de succes actuale tratează securitatea ca un proces continuu ce încorporează elemente de natură tehnologică, procedurală şi umană.

Obiectivul acestei teze este de a oferi un studiu aprofundat asupra problematicii complexe a monitorizării securității în sisteme şi rețele de calculatoare, a amenințărilor din spațiul virtual, a tehnologiilor ce pot fi utilizate în construirea soluțiilor de monitorizare, de a identifica şi evalua practicile şi procedurile necesare în implementarea şi operarea unor astfel de soluții, precum şi de a evalua noi modele teoretice cu scopul de a adresa anumite limitări existente în soluțiile tehnologice actuale.

Pentru a conferi o aplicabilitate ridicată rezultatelor cercetării, cadrul de studiu al problematicii, tematica abordată, precum şi construirea modelelor de evaluare a noilor teorii a fost centrată în jurul nevoilor şi problemelor tipice organizațiilor care au o componentă de operare în spațiul digital.

Omul a făcut Internet-ul după chipul şi asemănarea sa.
- Autor Necunoscut

INTRODUCERE

În 2001, Lawrence K. Gershwin (National Intelligence Officer pentru Ştiinţă şi Tehnologie în cadrul US National Intelligence Council) afirma că „tehnologiile informaționale reprezintă cea mai importantă transformare globală de la începutul revoluției industriale (mijlocul secolului al 18-lea)" [GER01]. La acel moment afirmația mi s-a părut forțată, însă după 10 ani în care am asistat la proliferarea accentuată a tehnologiilor informaționale în toate domeniile vieții sociale, şi în toate colțurile lumii, la influența acestora asupra unor procese majore (globalizarea economică, comerțul electronic, externalizarea pe scară largă a resurselor umane) sau evenimente din domenii cât mai diverse (unul de ordin recent fiind „Primăvara arabă din 2011"), înclin să-mi reconsider opinia inițială.

Utilizarea pe scară largă a tehnologiilor informaționale, a determinat apariția unui nou spațiu de desfăşurare a multora dintre activitățile umane - numit adesea *spațiul virtual* (cyberspace). Elementele de ordin infracțional şi confruntațional ale lumii fizice nu au făcut excepție la această transpunere a activităților în spațiul virtual, proliferarea activităților malițioase fiind înlesnită de limitările structurale existente la nivelul arhitecturii Internet-ului, precum şi de un şir neîntrerupt de vulnerabilități datorate unor factori precum: existența unui segment important de utilizatori Internet care încă ignoră măsuri elementare de securitate a sistemelor pe care le folosesc, adoptarea de către organizații a unor practici de securitate limitate sau ineficiente, complexitatea crescută a aplicațiilor, considerente de piață ce determină companiile producătoare de software de a livra soluțiile cât mai rapid, limitând astfel timpul de testare, precum şi adoptarea de soluții ce sacrifică securitatea pentru a oferi simplitate în utilizare.

Securitatea sistemelor şi rețelelor este un element fundamental pentru funcționarea Internet-ului, ea permițând totodată transformarea acestuia dintr-un proiect de cercetare academic, într-o infrastructură de bază a societății zilelor noastre. Dependența de tehnologiile informaționale a creat noi categorii de vulnerabilități pentru alte componente ale infrastructurii sociale, iar un atac major asupra Internet-ului va crea nu numai întreruperi în ceea ce priveşte comunicațiile, ci va avea implicații şi asupra altor infrastructuri critice (transporturi, energie, bancară, etc.). De aceea, securitatea infrastructurii Internet-ului a căpătat atenție deosebită în toate zonele sociale (academic, media, corporații, militar, politic, etc.).

În ciuda progreselor făcute în zona securizării tehnologiilor Internet, marea majoritatea a soluțiilor de securitate, bazate exclusiv pe suport tehnologic, a continuat să fie în continuare ineficace, realizându-se treptat că *securitatea în spațiul virtual* este în esență *o problemă umană*. Astfel, practici de securitate pe care societatea umană le-a desăvârşit de-a lungul istoriei sale au început să fie transpuse şi în spațiul virtual.

Definirea Problemei

Datorită complexității şi dinamicii schimbărilor pe planul tehnologiilor IT, precum şi a creşterii diversității şi complexității amenințărilor la adresa oricărei organizații conectate la Internet, strategiile de securitate construite exclusiv pe mecanisme de protecție sunt sortite eşecului. Abordarea securității ca *proces*, şi dintr-o perspectivă *proactivă*, orientată spre identificarea şi alertarea timpurie asupra potențialelor amenințări, sau atacurilor aflate în faze inițiale, poate oferi timpul necesar elaborării unui răspuns eficace înainte ca organizația să fie afectată.

Asigurarea eficacității oricărui gen de proces (inclusiv procesul de securitate), presupune adesea definirea şi implementarea unei componente care să urmărească constant evoluția procesului, astfel încât să se poată efectua în timp util corecții şi actualizări ca răspuns la schimbările ce au loc în mediul de operare.

Pe baza analizei datelor oferite de rapoartele Verizon Data Breach din ultimii ani, se poate determina faptul că majoritatea breşelor de securitate sunt rezultatul ignoranței sau al tratării securității ca „produs" (odată achiziționat, se aşteaptă să funcționeze pe o durată îndelungată fără intervenție). Spre exemplu, în raportul din 2011 se arată că 86% dintre atacuri au fost descoperite de o terță parte, 96% puteau fi evitate prin implementarea de controale de securitate de nivel simplu sau intermediar, iar în 83% din cazuri atacatorul a profitat de existența unor anumite de deficiențe de securitate [Ver10].

O abordare procesuală care să asigure o vizibilitate asupra componentelor cu relevanță în procesul de securitate, este *monitorizarea securității*. Aceasta se defineşte ca fiind abilitatea de a colecta, şi analiza în timp util evenimentele şi informațiile de securitate disponibile la nivelul organizației, atât din surse interne şi externe, în scopul elaborării unui răspuns eficace la amenințări şi atacuri.

Ca şi în cazul altor componente ale procesului de securitate, pentru o implementare şi utilizare adecvată şi eficientă a monitorizării securității, organizația trebuie să elaboreze în prealabil o politică de monitorizare, şi un program de monitorizare care va gestiona elementele de ordin tehnologic, procesual şi organizațional implicate în procesul de monitorizare a securității.

Deşi anumite elemente ale procesului de monitorizare au fost prezentate în literatura de specialitate de-a lungul ultimilor ani, există limitări în ceea ce priveşte interoperabilitatea tehnologiilor de detecție, procesele de evaluare a eficienței controalelor folosite, integrarea tehnologiilor şi proceselor, abordarea unitară a surselor cu relevanță de securitate, şi eficiența analizei evenimentelor de securitate când datele au un grad ridicat de incertitudine. Toate acestea au constituit motive întemeiate în alegerea temei de cercetare ştiințifică şi pentru elaborarea tezei de doctorat.

Abordarea în prezent a *monitorizării securității în rețele şi sisteme de calcul* reprezintă un subiect foarte bine ancorat în tendințele, relevante pe plan mondial, din domeniul larg al *securității informaționale*. Este printre primele teze de doctorat din lume care se ocupă exclusiv de domeniul monitorizării securității, din perspectiva complexității şi a unor cerințe ridicate, specifice programelor moderne de cercetare ştiințifică.

Metodologia de cercetare

Pentru elaborarea tezei de doctorat s-a folosit următoarea *metodologie de lucru*: s-au studiat numeroase articole, documentații, standarde, cărți etc. cu factor de impact ridicat şi de actualitate, care analizează şi descriu multiple aspecte din sfera monitorizării securității.

S-au tratat *subiecte neabordate* în literatura de specialitate de la noi din țară, cât şi din străinătate (de exemplu, *elaborarea unui cadru pentru definirea de metrici de securitate a rețelelor şi sistemelor din perspectivă organizațională,* sau *cercetarea aplicabilității în domeniul monitorizării securității a teoriilor matematice ce tratează fuziunea datelor cu incertitudine ridicată*), s-au preluat cât mai multe surse bibliografice, s-a făcut o unificare terminologică şi o structurare a lor, obținându-se în final o abordare complexă şi unitară, utilizată în definirea conceptului de monitorizare a securității. Acestei abordări i s-au adăugat actualizări şi completări, îmbunătățiri şi contribuții originale (prezentate în capitolul 6), o parte experimentală care cuprinde construirea modelului de testare, generarea traficului de testare, elaborarea programelor de procesare a datelor, scheme şi grafice, precum şi studii de caz referitoare la monitorizarea spațiului de amenințări în Internet.

Rezultatele obținute au fost posibile şi datorită activității intense de cercetare în domeniul securității informatice desfăşurate în laborator, a participării şi comunicării la numeroase conferințe şi manifestări ştiințifice, a efectuării unor cursuri de pregătire şi de specializare în străinătate la firme şi institute de prestigiu, precum şi colaborării permanente cu personalul academic din Academia Tehnică Militară precum şi alte institute de cercetare şi învățământ superior din România, Canada, Franța şi SUA.

Principalele *direcții de cercetare ştiințifică* abordate în cadrul tezei au fost:

- Elaborarea unui cadru de studiu al problematicii diverse şi complexe legată de monitorizarea securității
- Starea actuală de securitate în Internet: terminologia de securitate şi monitorizare a securității, analiza spațiului de amenințări şi vulnerabilități, clase şi scheme de atac;
- Politici şi procese de securitate: programul de monitorizare a securității, cadrul de metrici de evaluare a stării de securitate, oportunități pentru îmbunătățirea proceselor de securitate
- Tehnologii de monitorizare a securității: tehnologii de detecție, de scanare a vulnerabilităților, verificare a conformării cu politica de securitate, spațiul de amenințări, oportunități de îmbunătățire a tehnologiilor
- Arhitecturi de monitorizare: Integrarea multiplelor componente tehnologice, şi procesuale, considerente asupra generării evenimentelor de securitate, colectării şi formatării, datelor analiza şi prezentarea datelor, răspunsul la incidentele
- Posibilități de utilizare a noi modele matematice pentru a adresa limitări ale tehnologiilor curente în procesarea datelor de securitate ce prezintă un nivel ridicat de incertitudine şi conflict.

Organizarea tezei de doctorat

Teza de doctorat, elaborată pe parcursul a peste 180 de pagini, debutează cu această secțiune introductivă, urmată de 5 capitole dedicate unor aspecte tehnologice şi procesuale implicate în procesul de monitorizare a securității, şi se încheie cu o evaluare finală a rezultatelor şi contribuțiilor, cu un capitol de concluzii, precum şi cu bibliografia utilizată. Lucrarea conține peste 220 de referințe bibliografice circumscrise temei, precum şi o listă cu cele mai semnificative lucrări realizate şi publicate de autor în domeniul tezei, în număr de 21. De menționat faptul că, unele dintre aceste lucrări s-au bucurat de o apreciere deosebită din partea comunității ştiințifice internaționale până în prezent, fiind citate în 2 teze de doctorat, 4 teze de master, şi 9 articole publicate în jurnale şi reviste de specialitate.

Capitolul 1 este dedicat stării actuale de securitate în Internet. În prima parte se definesc conceptele generale de securitate şi relațiile dintre acestea, după care se prezintă clasele majore de vulnerabilități şi fazele tipice prin care un atacator compromite un sistem. În continuare se descriu activitățile asociate fiecărei faze de compromitere detaliindu-se tehnicile de scanare, clasificarea atacurilor, precum şi modul de desfăşurarea a acestora. În finalul capitolului 1 se defineşte componenta de monitorizare a securității, precum şi rolul şi locul său în cadrul procesului de securitate. În acest capitol se propun următoarele contribuții: definirea unui cadru pentru detecția intruziunilor şi a procesului de monitorizare asociat acestuia, schematizarea atacurilor tipice pe bază de mesaje de poştă, analiza comparativă a tehnicilor de scanare utilizate în propagarea viermilor în Internet

Capitolul 2 vizează metodologia de creare a unui program de monitorizare a securității plecând de la analiza managementului de risc în organizație. Sunt prezentate elemente precum stabilirea strategiei de monitorizare, stabilirea de măsurători şi metrici, precum şi politici de securitate specifice fiecărui nivel din organizație. Capitolul 2 continuă cu prezentarea procedurilor de răspuns la incidente precum şi de revizuire şi actualizare pe o bază continuă a procesului de monitorizare a securității. În cadrul acestui capitol se propun următoarele contribuții: Elaborarea unui cadru pentru definirea de metrici de securitate, definirea şi evaluarea unui cadru pentru partajarea informațiilor de intruziune la nivel global, precum şi definirea unui model de monitorizare completă a securității ce include toate elementele cu relevanță pentru procesul de securitate.

Capitolul 3 prezintă clasele de tehnologii de monitorizare disponibile în acest moment pentru implementarea un program de monitorizare completă a securității la nivelul securității. Se continuă apoi cu prezentarea tehnologiilor de scanare a vulnerabilităților şi tehnologiile de detecție a intruziunilor bazate pe anomalii, semnături, metode hibride, precum şi pe analiza fişierelor de jurnalizare, monitorizarea integrității fişierelor şi sistemelor. În partea finală a capitolului 3 sunt tratate tehnologii specifice de monitorizare pentru rețele mari având ca scop identificarea amenințărilor majore pentru infrastructura Internetului. Capitolul se încheie cu un studiu de caz asupra monitorizării amenințărilor din spațiu virtual pe bază de date provenind din surse publice. Se propun următoarele contribuții: sintetizarea şi elaborarea unei evaluări asupra tehnologiilor de culegere a datelor utilizate în procesul de monitorizare a securității, elaborarea unui studiu comparativ şi a unei caracterizări structurale a tehnologiilor de detecție a intruziunilor şi a implementărilor de sisteme IDS, evaluarea tehnicilor de urmărire a

atacurilor DDoS, precum şi un studiu de caz pentru analiza spațiului de amenințări pe baza datelor publice oferite de sistemele de monitorizare globală în Internet.

Capitolul 4 este dedicat arhitecturii de monitorizare a securității stabilită pe baza modelelor OSSIM, Counterpane şi MCI Sentry. Se descriu componentele de bază ale arhitecturii: surse de evenimente, colectoare, baza de date cu mesajele de securitate în format comun şi baza de cunoştințe, precum şi modulele de analiză şi aplicațiile pentru suportul răspunsului la incidentele de securitate identificate. Concomitent cu descrierea fiecărei componente se prezintă şi considerații cu privire la performanțele şi limitările acestora precum şi aspecte legate de integrarea diverselor componente şi tehnologii. O atenție deosebită în acest capitol se acordă tehnicilor de corelație care sunt utilizate în modulele de analiză ale arhitecturii. În cadrul acestui capitol se propun următoarele contribuții: elaborarea unei arhitecturi generice de monitorizare a securități, precum şi a unui set de considerații pentru faza de implementare a arhitecturii, elaborarea unui studiu asupra tehnicilor de corelație a datelor în procesul de monitorizare a securității, studiul şi evaluarea amenințărilor şi riscurilor la adresa arhitecturii de monitorizare.

Capitolul 5 este destinat studierii de noi modele matematice pentru adresarea mai eficientă a cazurilor în care datele de monitorizare prezintă un grad ridicat de incertitudine sau conflict. Se prezintă un cadru de identificare a imperfecțiunii datelor din sfera monitorizării securității plecând de la clasificarea imperfecțiunii informațiilor realizată de Smet. Apoi, se introduc modele matematice precum Teoria Dempster-Shafer şi Teoria Dezert-Smarandache (TDSm) pentru fuziunea informațiilor ce prezintă un grad ridicat de incertitudine. În partea finală a capitolului 5 se urmăreşte verificarea aplicabilității TDSm în eficientizarea detecției intruziunilor în condiții de incertitudine ridicată. Pentru aceasta s-a construit un model experimental în care date de trafic legitim şi atac sunt generate în regim controlat. Acestea sunt observate de un sistem IDS (Snort), care la rândul său generează alerte cu priorități diferite. Pe baza acestor alerte se creează evenimente asociate unui spațiu de discernământ şi care se combină pe baza a diferite reguli de fuziune (Shafer, PCR5, DSmH). Validarea a constant în verificarea concordanței între realitate şi rezultatul generat de pe baza regulilor de fuziune, precum şi rapiditatea de detecție a schimbărilor care apar în mediu. În cadrul acestui capitol se propun următoarele contribuții: construirea unui cadru de identificarea imperfecțiunii datelor în sfera monitorizării securității, studiul în premieră al DSmT în vederea utilizării în domeniul monitorizării securității, precum şi crearea unui model experimental de evaluare a aplicabilității TDSm în zona monitorizarea securității.

Capitolul 6 prezintă o sinteză a rezultatelor ştiințifice şi a contribuțiilor obținute în perioada de pregătire a doctoratului şi de elaborare a tezei.

Capitolul 7 este dedicat analizei îndeplinirii obiectivelor propuse, prezintă concluziile finale rezultate, precum şi direcțiile viitoare de continuare a cercetării în domeniul securității monitorizării şi a altor domenii de securitate conexe.

Motto: *Daca iţi cunoşti inamicul şi pe tine, nu trebuie să te îngrijorezi de rezultatele a o sută de bătălii.*
- Sun Tzu

CAPITOLUL 1

SECURITATEA ACTUALĂ ÎN INTERNET

Datorită importanței crescute a activităților desfăşurate în spațiul virtual, securitatea informațională a atras o atenție sporită atât din partea cercetătorilor în domeniu, a organizațiilor conectate la Internet, dar şi a mediilor de informare în masă. Schimbările constante în plan tehnologic, au generat adesea interpretări variate ale conceptelor şi terminologiei de securitate.

În acest capitol se vor prezenta concepte generale de securitate şi o descriere a spațiului de vulnerabilități şi amenințări tipice la adresa organizațiilor şi utilizatorilor ce operează în spațiul virtual.

1.1 Concepte generale de securitate

Asemenea tuturor domeniilor de securitate, securitatea în spațiul virtual operează cu următoarele concepte: amenințări, vulnerabilități, riscuri, bunuri, etc. Aceste concepte generale, precum şi relațiile dintre ele sunt ilustrate în figura 1.1 [CC99].

În contextul securității în spațiul virtual, o *amenințare* poate fi definită ca fiind prezența unui potențial eveniment care ar putea avea efecte negative prin violarea unui mecanism de securitate. *Vulnerabilitatea* se defineşte ca fiind o slăbiciune a infrastructurii sau sistemului ce poate permite violarea securității. *Riscul* reprezintă gradul de pericol sau probabilitatea de pierderi sau distrugere, a informațiilor proprietare şi/sau a sistemelor de calcul utilizate în procesarea, transmiterea şi stocarea acestor date. *Bunurile* reprezintă entități (cum ar fi: hardware, software, date, personal uman, etc.) pe care organizația sau utilizatorul le valorizează şi care constituie ținta unui atac [Pfl11].

Agenții de amenințare provin din surse multiple şi au motive, obiective, capabilități dintre cele mai variate. Aceştia pot fi: angajați ai organizației, servicii de spionaj, hackeri, grupuri extremiste şi teroriste, grupuri de activism, grupuri de crimă organizată, competitori, etc.. Un *atac (*sau *incident de securitate)* în spațiul virtual este materializarea unei amenințări, şi reprezintă acțiunea ilegală, neautorizată, sau inacceptabilă, care implică un sistem de calcul sau o rețea de calculatoare, prin care o entitate internă sau externă compromite aşteptările de securitate ale utilizatorului sau organizației [Man03].

Formalizarea modului de identificare a vulnerabilităților şi evaluarea riscului, a măsurilor

(controalelor) luate pentru a contracara amenințările din spațiul virtual şi minimizarea riscurilor, stabilirea membrilor organizației cu atribuții în procesul de implementare, se vor regăsi într-un set de documente ce definesc *politica de securitate*. Politica de securitate este mijlocul prin care o organizație asigură managementul implementării şi eficacitatea securității [Jon10].

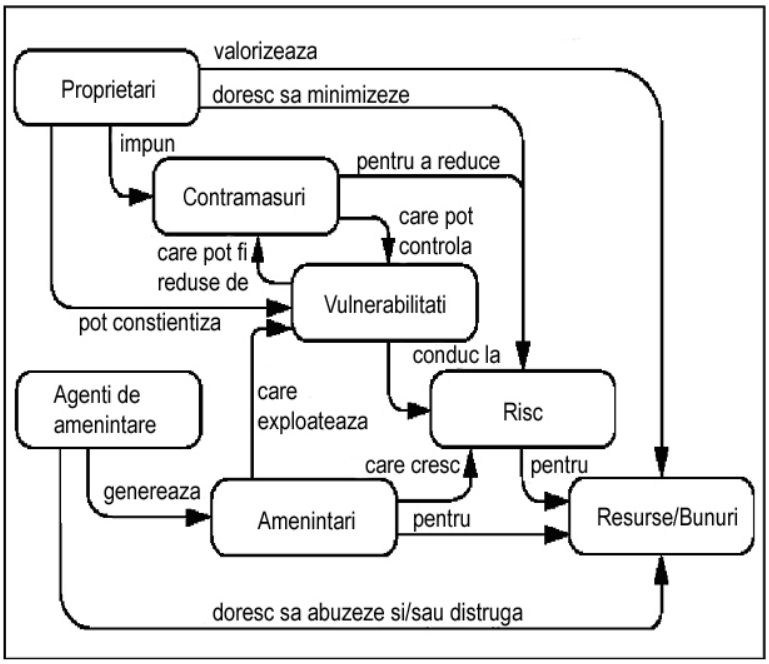


Figura 1.1 - Concepte de securitate conform CCIMB-99-031 [CC99]

1.2 Vulnerabilități în rețele şi sisteme de calcul

Vulnerabilități există în orice rețea sau dispozitiv incluzând rutere, swich-uri, stații client sau server, şi chiar dispozitive de securitate [Gre11]. Vulnerabilitățile pot fi datorate *configurației*, *politicii de securitate, utilizatorilor* şi *tehnologiei* [PNN10]. Vulnerabilitățile tehnologice sunt datorate deficiențelor structurale de securitate la nivelul suitei de protocoale de comunicație TCP/IP sau a implementărilor acestora, deficiențelor de securitate în sistemele de operare sau ale echipamentelor de rețea. Administratorii de sistem şi de rețea trebuie să cunoască problemele specifice de configurație pentru echipamentele şi sistemele pe care le gestionează pentru a fi create intrări în politica de securitate pentru verificarea configurațiilor. Managementul necorespunzător al politicii de securitate (actualizări incorecte sau neefectuate la timp) conduce la riscuri sporite.

1.2.1 Protocoalele de comunicație TCP şi UDP

Protocoalele de comunicație în Internet au fost proiectate pentru a permite o comunicare simplă şi rapidă între sisteme, fără a încorpora elemente de securitate. Referitor la acest aspect, unul din creatorii Internetlui, Vint Cerf (în prezent Vice President & Chief Internet Evangelist la Google), a menționat: ”dacă aş avea posibilitatea să proiectez rețeaua din nou, aş încorpora capabilități de autentificare automată astfel încât pachetele de la sursă către destinație să aibă semnătura digitală a utilizatorului. Aceasta nu s-a putut face atunci [când am proiectat Internet-ul] deoarece tehnologia nu exista.” [Cerf04]

Primul nivel de atac presupune descoperirea serviciilor existente în rețeaua țintă. Aceasta implică o serie de tehnici disponibile atacatorului pentru a obține informații despre rețeaua vizată cu ar fi [PPN05-02]:

- *Sondări ping* (ping sweeps) – sondarea unui grup de adrese IP pentru a determina stațiile active
- *Scanări TCP/UDP* – prezentate pe larg în secțiunea 1.4
- *Identificarea sistemului de operare* – Dorită particularităților de implementare a stivei de protocoale de către fiecare producător, pe bază analizei pachetelor TCP schimbate cu o stație, se poate determina tipul de sistem de operare şi eventual versiunea acestuia. Această informația poate fi utilă atacatorului în a înțelege rolul sistemului respectiv, şi serviciile ce pot rula pe acesta.

1.2.2 Posibilitatea de manipulare a datelor din pachetul IP

Deoarece adresa sursa din pachetul IP nu este folosită în procesul de rutare către destinație, atacatorul poate falsifica (spoof) această informație şi abuza maşina țintă ascunzându-şi identitatea. Acest tip de vulnerabilitate este exploatată cu predilecție de atacurile de tip Denial of Service (DoS).

1.2.3 Proiectări de soluții neadecvate ce permit scurgeri de informații

Acesta este cazul integrării unor tehnologii pentru a adresa adesea nevoi de eficientizare în organizație, dar care pot genera noi vulnerabilități.

Un exemplu în acest sens este accesibilitatea informațiilor director. Pentru a valida legitimitatea adresei destinatar din mesajele de poştă, multe organizații au integrat serviciile ce rulează pe stațiile gateway (ce recepționează poşta) cu serviciile director (cum ar fi LDAP/Active Directory) ale organizației. Dacă adresa destinatarului este validă, mesajul este acceptat spre livrare. Dacă adresa nu există, expeditorul este notificat despre acest lucru. Atacurile de culegere a informațiilor director - DHA (Directory Harvest Attacks) exploatează această vulnerabilitate prin trimiterea de mesaje către o listă posibilă de adrese de poştă din domeniul țintă. Pentru mesajele pentru care nu se primeşte notificarea de invaliditate a adresei se poate asuma că sunt legitime, putând fi folosite într-un viitor atac. O soluție pentru acest tip de vulnerabilitate ar fi ca serverul să proceseze mesajele cu adresă invalidă, însă aceasta are ca rezultat un volum din ce în ce mai mare de procesare pentru organizație [PPN06-02].

1.2.4 Vulnerabilități la nivelul protocoalelor de nivel aplicație

De-a lungul timpului au fost semnalate o serie de vulnerabilități în protocoalele native de poştă electronică (SMTP, IMAP şi POP), Web (HTTP), cum ar fi: susceptibilitate ridicată la atacurile de tip dicționar (POP şi IMAP), transmiterea traficului de date şi autentificare în clar (vulnerabilitate exploatată de sniffere), lipsa unui mecanism nativ de autentificare pentru SMTP (exploatat de atacurile de tip SPAM şi phishing), existența încă pe scară largă a multor servere SMTP configurate să accepte mesaje de la orice utilizator (open relay), şi nu în ultimul rând o suită de bug-uri în diferitele implementări ale acestor protocoale (exploatate adesea de atacurile de tip buffer overflow) [PPN04] .

1.2.5 Vulnerabilități la nivelul sistemelor de operare

Sistemele de operare de tip Windows suportă o largă gamă de servicii, metode şi tehnologii lucru în rețea. Multe din aceste componente sunt implementate ca Programe de Control a Serviciilor aflate sub controlul unui Manager de Control al Serviciului ce rulează sub numele de Services.exe. Vulnerabilitățile în aceste servicii care implementează funcționalități ale sistemului de operare reprezintă una din cele mai întâlnite căi de abuzare a stațiilor ce rulează sisteme Windows.

Vulnerabilitățile de tip buffer overflow exploatabile de la distanță continuă să fie o problema serioasă de securitate care afectează serviciile Windows. O parte din serviciile sistem de bază oferă interfețe clienților din rețea prin mecanismul RPC (Remote Procedure Calls). Alte servicii Windows implementează interfețe de rețea pe baza altor protocoale, inclusiv a celor standard cum ar fi SMTP, NNTP, HTTP, etc. Multe din aceste servicii pot fi exploatate de sesiuni de tip anonim (sesiuni cu nume utilizator şi parolă nule) pentru a executa cod cu privilegii ”SYSTEM” [PPN05-01].

Produsele inițiale Windows aveau activate implicit multe din aceste servicii pentru a asigura o convenienţă utilizatorilor cu cunoştinţe limitate. Însă aceste servicii, adesea neutilizate de cei mai mulți dintre utilizatori, aduc riscuri de securitate suplimentare.

În ceea ce priveşte sistemele UNIX/Linux, acestea includ în configurația inițială un număr de servicii standard care pot fi exploatabile datorită configurării inadecvate.

1.2.6. Vulnerabilități la nivelul serviciilor de infrastructură ale Internetlui

Un exemplu de serviciu critic pentru infrastructura Internetlui este DNS. Acesta găzduieşte înregistrările de tip MX utilizate în rutarea mesajelor de poştă către domeniul destinație, cât şi înregistrări de tip adresă ale altor sisteme ce oferă servicii de rețea (Web, autentificare, VPN). DNS ca multe alte protocoale de bază ale Internetlui datează din perioada inițială caracterizată de încredere mutuală. Acest model de încredere nu mai este de actualitate, iar tranzacțiile DNS pot fi viciate de atacuri de tip: cache poisoning, domain hijacking, şi redirecție man-in-the-middle [PPN09].

Unele din metodele propuse de autentificare a mesajelor de poştă cum ar fi Sender Policy Framework (SPF), SenderID, Domain Keys, Cisco Identified Internet Mail au la bază verificarea domeniului destinatarului utilizând serviciul DNS în actuala formă sau modificată. Pentru a limita cazurile de impersonare a serverelor de web, se recomandă utilizarea certificatelor de securitate, securizarea serviciului DNS, etc. Totuşi sunt multe organizații care încă nu folosesc astfel de soluții.

1.2.7 Vulnerabilități la nivelul aplicațiilor

Outlook Express este aplicația client de poştă instalată pe toate versiunile de sisteme Windows. Vulnerabilitățile în acest produs pot fi exploatate pe baza următorilor vectori de atac [PN06]:

Atacatorul poate trimite într-un mesaj de poştă un document Office maliții care este rulat de client. Acest vector de atac este exploatat de viruşi şi de o anumită categorie de viermi (worms).

Atacatorul poate rula un server de ştiri (News) care trimite răspunsuri malițioase pentru a genera buffer overflow în aplicațiile client de poştă.

Vulnerabilitățile la nivelul clienților de navigare (IE, Firefox, Google Chrome, etc) pot fi exploatate în cazul în care utilizatorul accesează locațiilor web ce conțin scripturi (JavaScript, PHP, ASP) ce implementează astfel de exploatări. Google (ce rulează principalul motor de căutare) realizează o scanare a conținutului paginilor indexate, însă posibilitatea de acces indirect (prin alte site-uri) permite eludarea acestui mecanism de protecție.

De-a lungul timpului au fost identificate vulnerabilități afectând mai toate categoriile reprezentative de aplicații utilizate în Internet cum ar fi: cele de accesare conținut media (Adobe Flash), aplicațiile de transmitere mesaje instant (Yahoo! Messenger, AOL Instant Messenger, MSN Messenger, Jabber, Trillian, Skype, Google Talk sau IRC), şi chiar aplicațiile antivirus (AhnLab, Avast!, AVIRA, BitDefender, ClamAV, Computer Associates, F-Secure, Kaspersky, Mcafee, Sophos, Symantec, Trend Micro sau ZoneAlarm). Chiar dacă aceste vulnerabilități nu vizează în mod direct securitatea serviciilor de bază în rețea, prin preluarea controlului asupra stațiilor afectate de acest gen de vulnerabilități, securitatea altor servicii poate fi compromisă.

1.2.8 Configurarea necorespunzătoare a aplicațiilor şi sistemelor

Vulnerabilitățile în configurarea echipamentelor, aplicațiilor şi sistemelor de operare pot fi clasificate după cum urmează [PPN06-01]:

- *Configurații implicite.* Majoritatea aplicațiilor şi sistemelor ajung la utilizatorii finali având o configurație ce urmăreşte o funcționalitate cât mai sporită şi utilizare cât mai simplă. Din păcate acest gen de configurații expun sistemul la riscuri considerabile. Practica a arătat că stațiile sau ruterele wireless de casă în configurațiile inițiale poate fi compromise în foarte scurt timp.
- *Parole administrator nule sau implicite.* Multiple teste de vulnerabilitate au arătat că un număr surprinzător de mare de sisteme şi aplicații atât în rândul rețelelor de organizație cât şi în rândul utilizatorilor de casă suferă de această problemă.
- *Erori de administrare.* Necunoaşterea sau simple erori umane pot conduce la situații în care aplicația, sau sistemul sunt configurate necorespunzător. Odată cu răspândirea pe scară largă a accesului utilizatorilor la conexiuni de bandă largă şi construirea de mini rețele de casă, există riscul ca un număr mare dintre sistemele şi rețele necorespunzător administrate să intre sub controlul atacatorilor, putând fi folosite pentru atacul asupra altor rețele.

1.2.9 Factorul uman

Realitatea a demonstrat în repetate rânduri că oamenii nu conştientizează îndeajuns importanță informațiilor pe care le dețin şi sunt neglijenți în ceea ce priveşte protecția acestora. Intruziunile de natură non-tehnică ce se bazează în principal pe interacțiunea umană şi urmăresc inducerea în eroare a utilizatorilor în scopul încălcării procedurilor de securitate uzuale fiind cunoscute în literatura de specialitate sub numele de *inginerie socială*.

Agenții de amenințare determinați (cum ar fi cei care operează în sfera spionajului industrial) posedă cunoştințe ale psihologiei umane şi abilitați comunicaționale

deosebite ce pot exploata vulnerabilitățile factorului uman pentru a obține informații greu accesibile prin mijloace exclusiv tehnice. Experții de securitate estimează că pe măsură ce societatea devine din ce în ce mai dependentă de informații, ingineria socială va rămâne cea mai importantă amenințare la adresa oricărui sistem de securitate. Protecția presupune conştientizarea utilizatorilor asupra valorii informațiilor, instruirea în ceea ce priveşte mijloacele de protecție şi a modului în care inginerii sociali operează. Utilizarea pe scară largă a rețelelor de socializare (cum ar fi Facebook, MySpace), înlesneşte culegerea de informații personale, permițând elaborarea de atacuri direcționate de culegere de informații.

1.3 Fazele de compromitere

Pentru a detecta intruziunile, trebuie înțelese acțiunile necesare pentru compromiterea unei ținte. Cele cinci faze descrise în continuare reprezintă o modalitate prin care un atacator poate prelua controlul asupra unei victime. Scenariul prezentat mai jos urmăreşte atacurile generate din afară care sunt mult mai frecvente şi reprezintă o problema majoră pentru organizații [PPN07-01]. Conform raportului annual despre breşele de date analizate de firma Verizon în 2010, 92% dintre acestea au fost generate de agenți externi organizației.

Recunoaşterea – reprezintă procesul de validare al conectivității, verificare a serviciilor active şi identificare a aplicațiilor vulnerabile. Atacatorii care verifică vulnerabilitatea unui serviciu înainte de a căuta să exploateze ținta, au o mai mare probabilitate de succes. Recunoaşterea ajută atacatorul în planificarea atacurilor într-o manieră cât mai eficient posibilă. Recunoaşterea poate fi condusă prin mijloace tehnice precum şi non-tehnice cum ar fi obținerea de informații incorect distruse, sau de la persoane din interior dornice să ofere informații. Dintre tehnicile de colectare prealabilă de informații despre țintă din surse publice se amintesc:

- Căutări avansate pe web, forumuri – un exemplu în acest sens este utilizarea de opțiuni avansate ale motoarelor de căutare pentru a beneficia de scurgeri de informații (de exemplu: utilizarea opțiunii **allintitle: "index of /" site:.mta.ro** la o căutare Google) datorate erorilor de postare sau management a documentelor în organizația țintă.
- Rețele de socializare - în cazul în care ținta este o persoană
- Interogări DNS – utilizând aplicații simple precum nslookup.
- Interogări Network Information Centers (NICs) - bazele de date WHOIS
- Sondarea SMTP - simpla trimitere a unui email la o adresă inexistentă în domeniul țintă oferă adesea informații utile despre rețeaua vizată.

Exploatarea – reprezintă procesul de utilizare neautorizată, subversivă sau de creare de breşe în serviciile de pe stația țintă.

Preluarea controlului – reprezintă faza în care atacatorul caută să obțină capabilități suplimentare asupra țintei. În timp ce unele exploatări conduc către obținerea de privilegii de nivel superuser, altele oferă doar acces la nivel utilizator. Atacatorii caută să găsească modalități pentru a obține privilegii mai mari pe stația țintă. De asemenea, atacatorul va urmări ştergerea informațiilor din fişierele de log, adaugă conturi neautorizate şi distruge orice informație (procese, fişiere) care evidențiază prezența sa ilegitimă. Unii atacatori pot instala şi mijloace de comunicare cu exteriorul (*back doors*).

Consolidarea – are loc când atacatorul comunică cu victima prin intermediul *back door*lui. *Back door*-ul poate lua forma unui serviciu de ascultare la care atacatorul se conectează. Odată ce sunt amplasate canalele de comunicație acoperite între atacator şi victimă, abilitatea sistemelor de detecție sau a analistului de securitate de a detecta astfel de trafic este pusă la mare încercare. În această fază atacatorul are control complet asupra țintei, singurele limitări sunt impuse de dispozitivele de filtrare a traficului din rețea între atacatori şi victime.

Abuzul – reprezintă materializarea obiectivului atacului. Aceasta poate fi: furtul de informație, construirea unei baze de atac către alte stații din organizație, sau orice altceva ce atacatorul urmăreşte.

Faza de compromitere	**Descriere**	**Probabilitatea de detecție**	**Avantaje de partea atacatorului**	**Avantaje de partea apărării**
Recunoaşterea	Enumerare stații, servicii şi versiuni de aplicație	Medie către mare	Atacatorii efectuează descoperiri de stații şi servicii pe durata de timp îndelungată utilizând caracteristici normale de trafic	Atacatorul se desconspiră prin diferențele între traficul lor şi traficul utilizatorilor legitimi
Exploatarea	Accesul neautorizat, subversiv sau breşe în servicii	Medie	Atacatorii pot exploata serviciile utilizând criptare sau masca traficul de exploatare	Exploatările nu apar ca trafic legitim, iar sistemele IDS au semnăturile pentru a detecta majoritatea atacurilor
Preluarea controlului	Instalarea de aplicații pentru a obține privilegii suplimentare şi / sau să-şi mascheze prezența	Mare	Criptarea poate ascunde conținutul aplicațiilor instalate	Traficul dinspre serverul victimă către exterior poate fi supravegheat şi identificat
Consolidarea	Comunică prin intermediul unei back door, în mod uzual, un canal acoperit	Mică către medie	Având control total asupra ambelor capete de comunicație activitatea atacatorului este limitată doar de controlul de acces al traficului oferit de dispozitivele aflate în calea de comunicație	Pe baza profilelor de trafic se pot determina caracteristici atipice corespunzătoare utilizării unui back door de către atacator . Sistemele de detecția intruziunilor pe stații pot identifica activități în această fază
Abuzul	Furtul de informații, deteriorarea unui bun, sau compromiterea întregii organizații	Mică către medie	Odată ce operează pe o ”maşină de încredere”, activitățile atacatorului sunt mult mai dificile de observat	Analiştii cu abilități superioare pot determina devieri de la caracteristicile de trafic ale sistemelor interne

Tabel 1.1 – Detectarea intruziunilor pe durata fazelor de compromitere

1.4 Tehnici de scanare a rețelelor şi sistemelor

Scanarea reprezintă una din activitățile de bază ale fazei de recunoaşte prin care atacatorul urmăreşte identificarea sistemelor active şi accesibile din exterior, precum şi a serviciilor pe care le oferă, folosind diverse metode şi teste de scanare a porturilor, de detectare a sistemului de operare. Tipurile de informații colectate în urma scanării se referă la [PNN10]:

- Serviciile TCP/UDP ce rulează pe fiecare sistem identificat
- Arhitectura sistemului
- Adresele IP ale sistemelor accesibile via Internet
- Tipul sistemului de operare.

Atacatorul va căuta ca prin volumul şi structura traficului de scanare generat să nu atragă atenția administratorilor de securitate şi sistem din organizația țintă.

1.4.1 Tehnici de scanare a porturilor TCP

Porturile TCP accesibile pot fi identificate prin scanarea adreselor IP țintă. Următoarele tipuri de scanare a porturilor TCP sunt folosite atât de atacatori în faza de recunoaştere, cât şi de organizații pentru identificarea propriilor vulnerabilități:

1.4.1.1 Metode de scanare standard

Aceste metode permit identificarea cu acuratețe a porturilor şi serviciilor active, dar sunt uşor de identificat şi jurnalizat. Organizațiile le folosesc în mod curent pentru detectarea propriilor vulnerabilități.

1.4.1.1.1 Scanare TCP connect

Se trimit pachete de sondare SYN la portul ce verifică. Dacă sistemul verificat răspunde cu un pachet ce are SYN şi ACK setate, atunci portul este deschis. Dacă portul este închis, se recepționează direct un pachet RST/ACK. Conexiunea se stabileşte prin trimiterea de un pachet ACK de către sistemul ce efectuează scanarea.

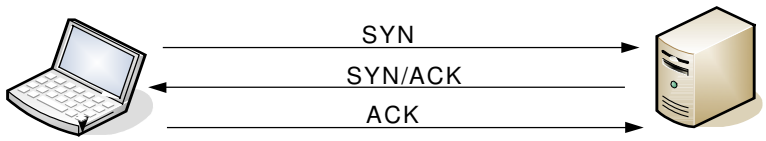


Figura 1.2 - Rezultatul scanării TCP connect atunci când un port este deschis

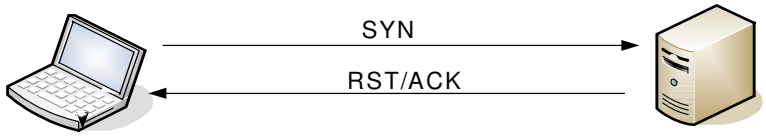


Figura 1.3 - Rezultatul scanării TCP connect atunci când un port este închis

Scanarea standard TCP connect este o cale sigură pentru a identifica serviciile de rețea accesibile. Dezavantajul este că acest tip de scanare este “zgomotos”, şi este evitat de atacatorii experimentați.

1.4.1.1.2 Scanare SYN semi-deschisă (half-open)

Această metodă diferă de cea precedentă prin trimiterea unui pachet RST (pentru a reseta conexiunea) în cel de-al treilea pas al fazei de stabilire a conexiunii. Deoarece adesea conexiunile nestabilite complet nu sunt jurnalizate de stațiile țintă, atacatorii pot utiliza acest gen de scanare. În figurile de mai jos este prezentat schimbul de pachete între 2 sisteme când este lansată o scanare de acest tip, atât în cazul unui port deschis cât şi în cazul portului închis.

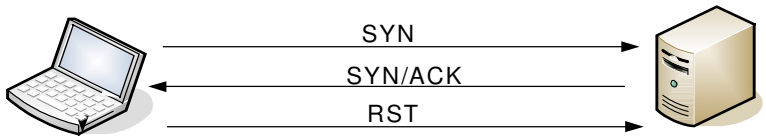


Figura 1.4 - Rezultatul scanării half-open SYN flag atunci când un port este deschis

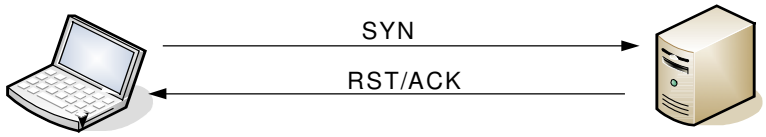


Figura 1.5 - Rezultatul scanării half-open SYN flag atunci când un port este închis

Scanarea SYN este rapidă şi sigură, dar necesită privilegii de acces la stațiile Windows şi Unix.

1.4.1.2 Metode de scanare TCP invizibilă

Metodele de scanare invizibile implică analiza proceselor ce au loc pe stiva TCP/IP a maşinii țintă şi răspunsul la pachetele cu anumiți biți setați. Asemenea tehnici nu sunt eficiente la descoperirea porturilor deschise pe anumite sisteme de operare, dar furnizează un anumit grad de discreție şi uneori nu sunt jurnalizate.

1.4.1.2.1 Scanare inversă TCP

RFC 793 stabileşte că dacă un port este închis pe o stație, atunci trebuie trimis un pachet RST/ACK pentru a reseta conexiunea. Pentru a folosi acest lucru se trimit pachete sondă cu diferiți biți de stare TCP setați către fiecare port al maşinii țintă. Există trei tipuri de configurații a biților de flag, folosite în mod curent [McN07]:

- Sondare FIN (bitul TCP FIN setat)
- Sondare XMAS (biții TCP FIN, URG, şi PUSH setați)
- Sondare NULL (fără biți de stare TCP fără flaguri TCP setate;

Conform standardul RFC, dacă nu este primit nici un răspuns de la portul maşinii țintă, atunci portul este deschis sau stația este inactivă. Pentru toate porturile închise de pe maşina țintă, sunt recepționate pachete RST/ACK. Totuşi implementările stivei TCP/IP

pe anumite sisteme de operare (cum sunt cele din familia Microsoft Windows) nu urmează complet standardul RFC 793 în acest sens, şi deci nu există răspuns RST/ACK la o încercare de conectare pe un port închis. În schimb, această tehnică este eficientă în cazul sistemelor de operare de tip UNIX.

1.4.1.2.2 Scanare ACK

O tehnică mai discretă de scanare este cea de a identifica porturile TCP deschise prin trimiterea unui volum de pachete de sondare ACK către diferite porturi ale staţiei ţintă şi analizarea informaţiilor din antetul pachetelor RST recepţionate.

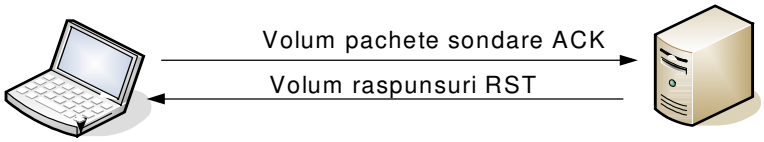


Figura 1.6 - Pachetele sondă ACK sunt trimise la diferite porturi

Există două tipuri de tehnici de scanare ACK care implică [McN07]:

- Analiza câmpului TTL (time-to-live) al pachetelor recepţionate - porturile deschise vor fi cele pentru care câmpul TTL este mai mic decât valoarea maximă a TTL din şirul de pachete RST recepţionate
- Analiza câmpului WINDOW al pachetelor recepţionate – porturile deschise vor avea câmpul WINDOW diferit de 0.

Avantajul acestui tip de scanare este că detecţia sa este foarte dificilă, însă datorită faptului că se bazează pe particularităţi ale implementării stivei TCP/IP, nu are aplicabilitate largă .

1.4.1.3 Metode de scanare TCP fabricată (spoofed)

Aceste metode de scanare permit ca pachetele de sondare să fie trimise prin intermediul staţiilor vulnerabile pentru a ascunde adevărata sursă care încearcă scanarea reţelei. Un important avantaj al acestor metode este că pot permite accesul la configuraţia firewalllui prin intermediul staţiilor de încredere, dar care sunt vulnerabile.

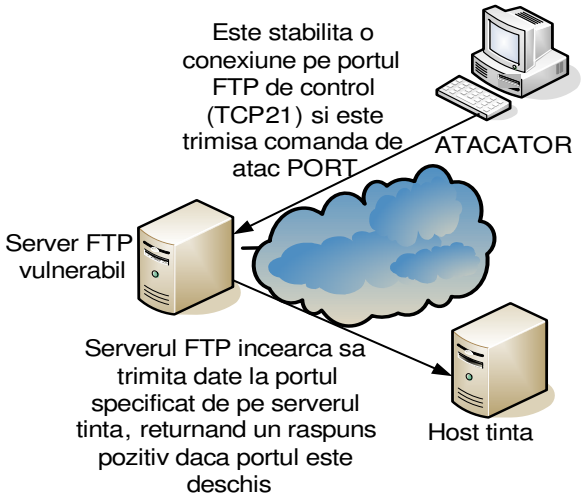


Figura 1.7 - Scanarea porturilor prin FTP

1.4.1.3.1 Scanare FTP

Multe servere FTP manipulează conexiunile folosind comanda PORT care permite transferul datelor la stația şi portul specificat. Dacă există şi un director pe care se poate scrie, atunci atacatorul poate introduce o serie de comenzi şi alte date într-un fişier şi apoi le transmite la o anumită stație şi port. Spre exemplu cineva poate face upload unui mesaj email spam, pe un server FTP vulnerabil, şi apoi mesajul este trimis la portul SMTP al serverului de email țintă [Nma--].

1.4.1.3.2 Scanare Proxy

Configurația incorecta a unor stații poate permite utilizarea lor ca agenți în expedierea cererilor de scanare. Deoarece această soluție este consumatoare de timp, atacatorii preferă adesea să realizeze atacul asupra țintei direct de pe stația proxy.

1.4.1.3.3 Scanare pe baza de sniffer

Elementul ce determină eficiența acestui tip de scanare este configurarea interfeței de rețea a stației în modul promiscuous, după care se ascultă răspunsurile pe segmentul de rețea. Exista două mari avantaje ale utilizării acestei metode de scanare[Ore08]:

- Daca atacatorul capătă privilegii de administrator asupra unei maşini din acelaşi segment de rețea cu stația ținta, sau cu firewall-ul care protejează ținta, se pot trimite pachete TCP de la o adresa IP aleatoare din rețea pentru a identifica stațiile de încredere şi a obține accesul la firewall.
- Daca atacatorul are acces la un segment mare de rețea partajată, poate realiza scanare fabricată în numele stațiilor din segmentul respectiv la care nu are acces, sau care nu există, pentru a scana eficient rețele la distanță într-un mod distribuit şi invizibil.

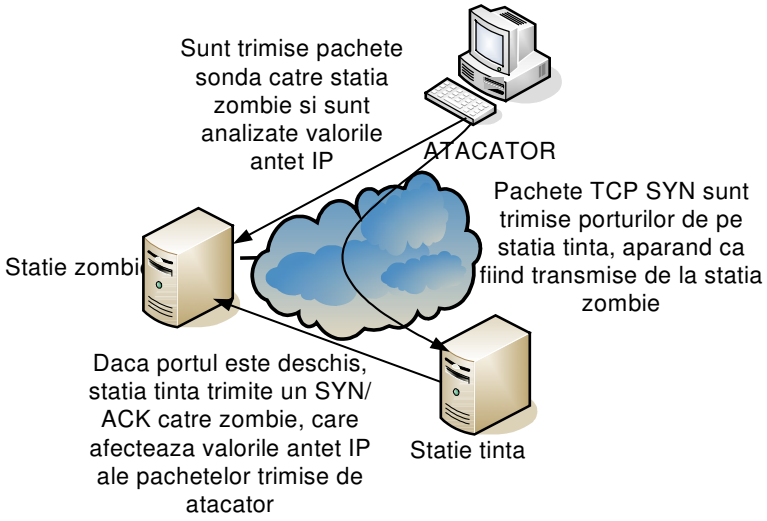


Figura 1.8 - Scanarea antetului IP şi părțile implicate

1.4.1.3.4 Scanarea antetului IP

Scanarea antetului IP este o tehnică de scanare care implică abuzarea implementărilor stivei TCP/IP în majoritatea sistemelor de operare. Sunt implicate trei stații [Ore08]:

- Stația zombie care este o maşină din Internet
- Stația țintă care va fi scanată
- Stația de scanare, sondează printr-o secvență de pachete stația zombie, iar pe baza modificărilor în numerele de secvență ale pachetelor recepționate se poate deduce dacă porturile pe stația țintă sunt deschise

1.4.2 Scanarea porturilor UDP

Deoarece UDP este un protocol fără conexiune, exista doar două căi de enumerare eficientă a serviciilor de rețea UDP de-a lungul unei rețele IP [Nma--]:

- Trimiterea pachetelor UDP către toate cele 65535 porturi UDP, şi apoi aşteptarea mesajului "ICMP destination port unreachable" pentru a identifica porturile UDP care nu sunt accesibile;
- Folosirea clienților specifici serviciului UDP (snmpwalk, dig, tftp) pentru a trimite datagrame UDP către serviciile de rețea UDP țintă şi apoi aşteptarea răspunsului pozitiv;

În figurile de mai jos sunt prezentate pachetele UDP şi răspunsurile ICMP generate de stații când porturile sunt deschise sau închise. Scanarea porturilor UDP este o scanare de tip invers în care porturile deschise nu răspund.

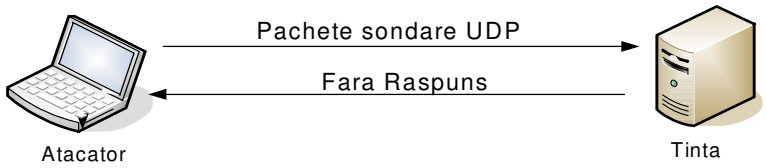


Figura 1.9 - Rezultatul scanării inverse UDP când un port este deschis

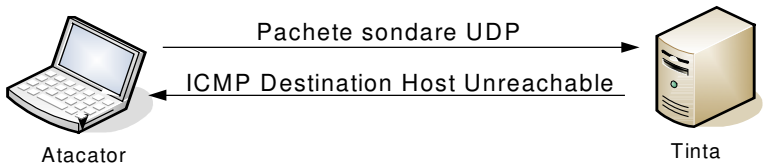


Figura 1.10 - Rezultatul scanării inverse UDP când un port este închis

1.5 Atacuri asupra rețelelor şi sistemelor de calcul

Toate resursele organizației (infrastructura de rețea, servicii, aplicații, date, utilizatori) sunt expuse diverselor amenințări din spațiul virtual. În funcție de resursa vizată, atacurile se pot împărți în următoarele categorii [PPN06-02]:

- *atacuri asupra infrastructurii* (rețele şi sisteme) - cuprinde atacurile DoS, propagările epidemice ale viermilor
- *atacuri asupra serviciilor şi aplicațiilor* - cuprinde infecțiile cu malware (viruşi, viermi, troieni) în scopul distrugerii sau furtului de date, sau preluării controlului asupra resurselor de pe stațiile client.

- *atacuri asupra utilizatorilor* - vizează exploatarea factorului uman pentru a determina utilizatorul să execute acțiuni care contravin procedurilor de securitate (de exemplu, prin răspunderea la mesajele de tip hoax, sau cele comerciale de tip SPAM), sau a induce utilizatorul în eroare asupra identității transmițătorului mesajului în scopul obținerii de informații confidențiale (de exemplu, mesajele de tip phishing)

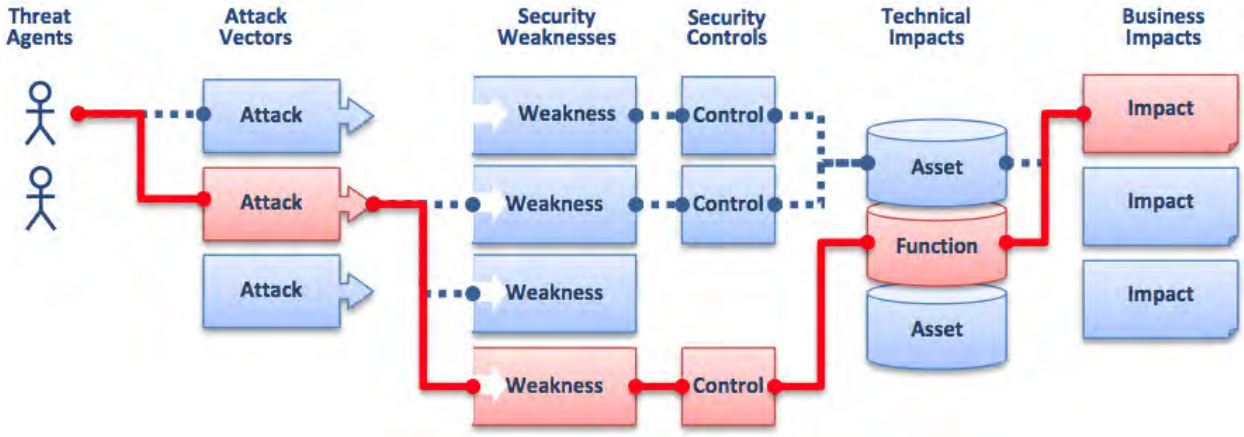


Figura 1.11 - Căi tipice de atac [OWA11]

1.5.1 Atacuri asupra infrastructurii

Câteva din trăsăturile Internetlui care creează premise pentru atacurile asupra infrastructurii sale de rețea sunt [Oik06]:

- **Securitatea în Internet are un grad de interdependență ridicat**: Nivelul de susceptibilitate la acest gen de atacuri al oricărui sistem conectat la Internet depinde în mare măsură de starea de securitate la nivel global Internet, şi nu de nivelul de securitate local.
- **Controlul în Internet este distribuit**: Cu un management distribuit şi politici locale de funcționare, este foarte greu de implementat un mecanism de securitate la nivel global, iar datorită considerentelor de confidențialitate a datelor, este adesea imposibil de investigat caracteristici de trafic peste mai multe rețele.
- **Resurse Internet limitate**: Fiecare entitate din Internet (stație, rețea, serviciu) are resurse limitate care pot fi consumate relativ rapid în condițiile unui nivel de cereri ridicat. Practic, în absența unei defensive, orice atac DDoS, sau propagarea epidemică a unui vierme va avea succes dacă reuşeşte să achiziționeze un număr suficient de stații agent.
- **Puterea celor mulți este mai mare decât puterea celor puțini**: Acțiunile simultane şi coordonate ale atacatorilor vor avea câştig de cauză dacă au resurse mai mari decât victimele.
- **Resursele şi sursele de informații nu se regăsesc la aceeaşi locație**: Paradigma de comunicație ”end-to-end” a determinat ca majoritatea informațiilor legate de asigurarea serviciului să fie disponibile la nivelul stațiilor finale, în timp

ce lărgimea de bandă este o caracteristică a legăturii fizice între rețele. Astfel, atacatorii pot utiliza resursele abundente de bandă ale rețelelor intermediare (de ISP) pentru a trimite mesaje către o victimă cu o capacitate mai redusă.

- **Lipsa unui mecanism de contabilitate**: Se presupune că valoarea câmpului ”adresă sursă” din pachetul IP reprezintă valoarea adresei IP a stației care a generat pachetul. Această aserțiune nu este validată sau impusă în nici un punct al traseului de la sursă către destinație, creând premisele de falsificare a adresei sursă numită şi ”address spoofing”. Aceasta oferă atacatorului posibilitatea de a scăpa de răspunderea acțiunilor sale, precum şi un mijloc de a realiza atacuri mai puternice (vezi DDoS prin reflexie – RDDoS, cum ar fi atacul Smurf).

1.5.1.1 Atacuri DoS

Atacurile de tip „denial of service” (DoS) sunt parte integrantă din realitatea Internetului de astăzi. Obiectivul atacului este de a împiedica utilizatorii legitimi de a accesa sistemul victimă sau resursele rețelei. Inițial, atacurile de acest tip au constituit o formă de *vandalism* asupra serviciilor Internet, însă cu timpul au devenit mai rafinate, vizând anumite grupuri de utilizatori. Câteva exemple ilustrative sunt: atacul asupra infrastructurii Estoniei [Naz07-2], atacul asupra site-urilor de socializare (Twitter, Facebook), atacul asupra site-ului Wikileaks [Par10].

În literatura de specialitate, există mai multe clasificări ale atacurilor DoS în funcție de factori cum ar fi: gradul de automatizare, tipul de vulnerabilitate exploatată, modul de efectuare a atacului, mecanismele de comunicare utilizate de atacatori [Mir02]. Lucrarea de față prezintă două tipuri de clasificări: după gradul de indirectare între atacator şi victimă, şi după tipul resursă exploatată.

În funcție de gradul de indirectare între atacator şi victimă atacurile DoS se clasifică după cum urmează.

A. Atacuri DoS directe

Atacurile directe sunt forma cea mai simplă de generare a unui atac, prin care atacatorul trimite cereri de serviciu către victimă cu o frecvență foarte mare pentru a-i epuiza unele din resursele cheie (CPU, memorie, bandă). Aceasta conduce la refuzul de servicii pentru clienții legitimi ai victimei.

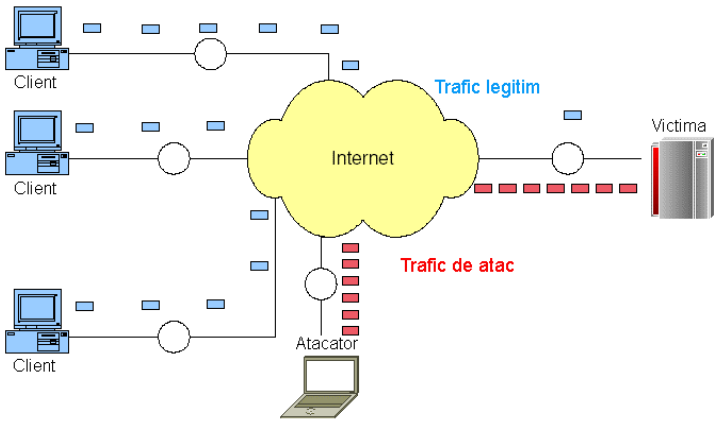


Figura 1.12 - Scenariu de atac DoS direct

B. Atacuri DoS distribuite (DDoS)

Un atac de tip DoS distribuit (DDoS) este un atac coordonat pe scară largă asupra disponibilității serviciilor oferite de sistemul victimă sau resursele rețelei lansat indirect prin intermediul mai multor stații Internet compromise. Serviciile atacate sunt cele ale „stației victime primare" în timp ce sistemele compromise utilizate în lansarea atacului sunt adesea numite „victime secundare". Utilizarea victimelor secundare în desfăşurarea unui atac DDoS oferă atacatorului posibilitatea de a realiza un atac pe scară mai largă şi cu efecte distructive mult mai mari, şi face mult mai dificile operațiile de identificare a atacatorului inițial [Mir04].

Un atac DDoS utilizează mai multe sisteme în lansarea unui atac DoS coordonat împotriva uneia sau mai multor ținte.

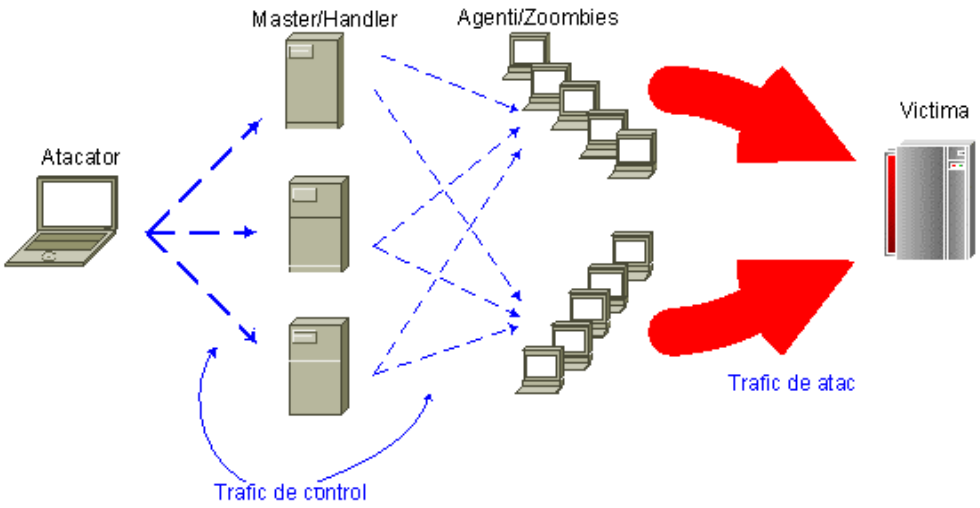


Figura 1.13 - Scenariu de atac DDoS

C. Atacuri DoS bazate pe reflectori (RDoS)

Detecția atacurilor poate fi îngreunată prin utilizarea reflectorilor în distribuirea traficului DoS. În esență, agenții nu vor trimite cererile către țintă, ci către nişte intermediari, numiți *reflectori*. Un reflector este orice stație IP care va răspunde la orice pachet trimis către el (un exemplu de reflector este un server web). Dacă adresa țintei este pusă ca adresă sursă în pachetului trimis de agent către reflector, răspunsul reflectorului va fi trimis către țintă. Prin utilizarea acestui mecanism se măreşte numărul de indirectări între atacator şi țintă, şi se realizează o dispersie a surselor de atac (orice maşină accesibilă în mod public poate fi utilizată ca reflector), ceea ce îngreunează depistarea atacatorului [Pei04].

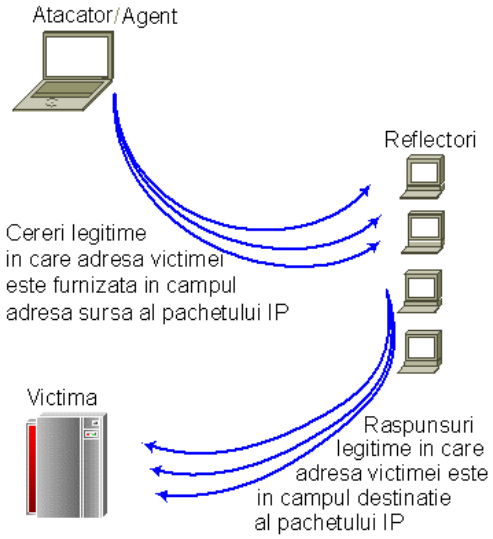


Figura 1.14 - Scenariu de atac RDoS/RDDoS

1.5.1.2 Atacuri DoS asupra rețelelor

Acestea sunt atacuri simple de efectuat ce consumă lărgime de bandă prin inundare (flooding). Obiectivul atacatorului este de satura legăturile de rețea pentru a prăbuşi ruter-ele şi switch-urile sau inundarea cu trafic peste posibilitățile de prelucrare. Din nefericire, uneltele necesare pentru un asemenea atac sunt disponibile pe Internet şi chiar utilizatorii fără experiență le pot folosi cu succes.

Atacurile de inundare copleşesc resursele victimei prin volumul lor. Deoarece pachetele de atac pot fi de orice tip, pot avea orice conținut, iar volumul mare de trafic împiedică o analiză detaliată a traficului, strategia pentru contracararea acestui tip de atac presupune ca detecția şi blocarea traficului de atac cât mai aproape de surse, ceea ce implică o conlucrare între furnizorii de servicii Internet.

A. ICMP Flood

Acest atac constă din trimiterea unui număr mare de pachete ICMP către victimă. Aceasta nu poate ține pasul cu volumul de informație primit şi poate observa o degradare a performanței. Implementări ale acestui tip de atac se găsesc în următoarele unelte DDoS: TFN, Stacheldraht, Shaft, TFN2K [Har09].

B. Smurf Flood

Atacul Smurf este o variantă de ICMP flood în care un pachet ICMP_ECHO_REQUEST având valoarea adresei sursă setată cu adresa stației țintă este trimis către o adresă de broadcast. RFC pentru ICMP specifică că nu trebuie generate pachete ICMP_ECHO_REPLY către adresele de broadcast, însă multe sisteme de operare şi producători de rutere nu au încorporat această cerință implementările lor. Ca urmare, stația țintă va primi pachete ICMP_ECHO_REPLY de la toate stațiile din rețea [Sin10]. Astfel de atacuri sunt numite atacuri cu amplificare sau cu reflexie. Implementări ale acestui tip de atac se găsesc în următoarele unelte DDoS: TFN, Stacheldraht, TFN2K.

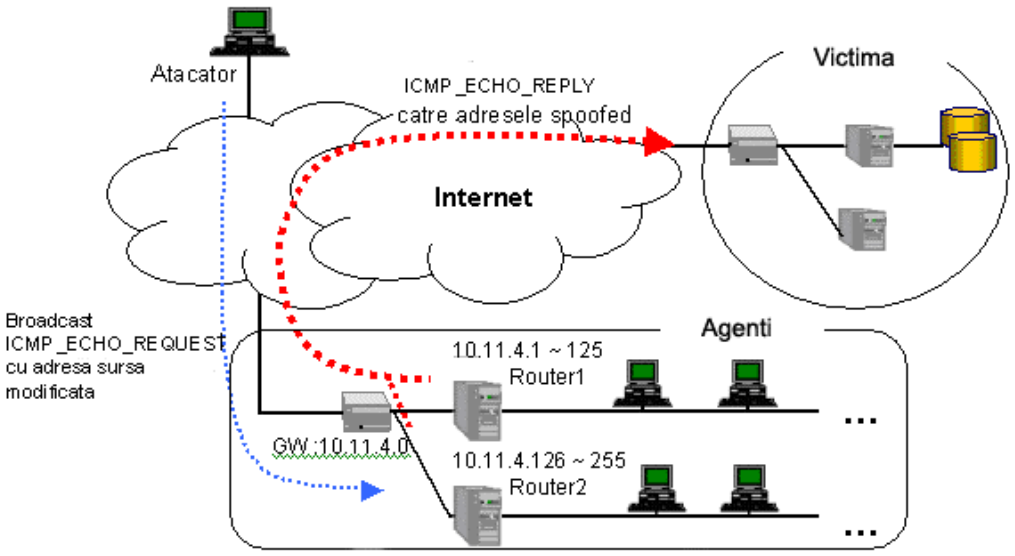


Figura 1.15 - Scenariu de desfăşurarea a unui atac de tip Smurf flood

C. UDP Flood (Fraggle)

Acest atac este posibil datorită naturii protocolului UDP care nu este orientat pe conexiune. Din moment ce nu este necesar nici un dialog în prealabil, un atacator poate trimite pachete către porturi aleatoare ale sistemului vizat. Victima va aloca resurse pentru determinarea aplicațiilor care ascultă porturile pe care sosesc date, iar când realizează că nici o aplicație nu face acest lucru, va trimite ca răspuns un pachet ICMP. Dacă numărul de pachete aleatoare este suficient de mare există posibilitatea ca sistemul să aibă probleme. Implementări ale acestui tip de atac se găsesc în următoarele unelte DDoS: Trinoo, TFN, Stacheldraht, Shaft, TFN2K, Trinity.

D. Chargen

Acest atac este o variantă a atacului de tip UDP Flood şi foloseşte portul 19 (chargen) al unui sistem intermediar folosit ca amplificator. Atacatorul trimite un pachet UDP fals către un sistem intermediar care la rândul său răspunde cu un şir de caractere victimei, pe portul său echo. Victima trimite înapoi un ecou al şirului primit şi bucla creată consumă rapid banda dintre victimă şi sistemul intermediar. Implementări ale acestui tip de atac se găsesc în următoarele unelte DDoS: TFN, Stacheldraht, Shaft, TFN2K.

E. E-mail bombing

„E-mail bombing” înseamnă trimiterea unui număr mare de mesaje electronice către un server cu scopul de a epuiza spațiul de pe disc şi lățimea de bandă. Cu excepția atacului UDP, restul se pot evita prin măsuri luate la nivelul sistemului de operare. Atacul UDP este dificil de contracarat întrucât există o multitudine de aplicații care ascultă la o multitudine de porturi. Filtrarea cu ajutorul firewall-urilor ar avea un impact puternic asupra funcționalității iar acest preț nu îl vor plăti foarte mulți utilizatori.

1.5.1.3 Atacuri DoS asupra sistemelor

Acestea sunt atacuri care epuizează o resursă cheie a sistemului determinând fie incapacitatea acestora de a servi corespunzător cererile legitime ale utilizatorilor, fie

întreruperea totală a funcționării sistemului. Atacurile exploatează vulnerabilități structurale ale protocoalelor de comunicație TCP/IP, sau vulnerabilități ale sistemului de operare, sau aplicațiilor rulate pe stația victimă prin trimiterea de pachete având un tip sau conținut special.

Deoarece vulnerabilitățile pot fi exploatate în mod frecvent prin utilizarea unui număr redus de pachete, atacurile de vulnerabilitate au un volum de trafic scăzut. Aceste caracteristici (pachet de tip special şi volum redus), simplifică strategia de tratare atacurilor de vulnerabilitate: detecția pe bază de semnături a pachetelor speciale, şi aplicarea de patch-uri pe sistemul victimă.

A. TCP SYN

Atacul de tip TCP SYN este posibil datorită schimbului de mesaje de la începutul protocolului TCP. Un client trimite o cerere (SYN) către un server, anunțându-şi intenția de a porni o conversație. La rândul său, serverul desemnează o intrare în tabela cu conexiuni pe jumătate deschise şi trimite înapoi un mesaj de acceptare (SYN,ACK), semnalizând astfel disponibilitatea sa. În acest moment clientul trebuie să răspundă cu un pachet SYN-ACK ACK pentru a putea începe comunicația de fapt. Un atacator ar putea să nu trimită niciodată această confirmare, cauzând umplerea tabelei de conexiuni, cererile legitime ulterioare fiind astfel blocate [Sin10].. Implementări ale acestui tip de atac se găsesc în următoarele unelte DDoS: TFN, Stacheldraht, Shaft, TFN2K, Trinity.

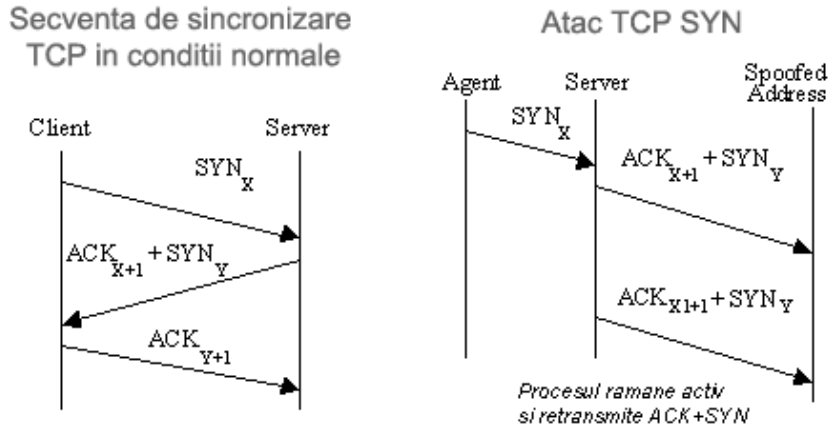


Figura 1.16 - Schimbul normal de mesaje în crearea unei conexiuni TCP (a).

Atacul de tip TCP SYN (b)

B. PUSH-ACK

Conform protocolului TCP, pentru a minimiza activitățile auxiliare asociate transferului de date, segmentele TCP sunt păstrate în stiva TCP şi trimise către destinație când stiva se umple. Totuşi, prin trimiterea unei cereri cu bitul PUSH=1, se poate forța receptorul să descarce conținutul stivei înainte ca aceasta să se umple. Atacatorul poate exploata această potențială vulnerabilitate de protocol prin trimiterea de pachete PUSH, care este posibil să genereze probleme chiar în condițiile de încărcare de trafic moderată [McN07]. Implementarea unui astfel de atac se regăseşte în uneltele DDoS mstream şi Trinity.

C. Shrew

Pin exploatarea gradului de determinism şi de omogenitate din implementarea mecanismului de evitare a congestiei TCP/IP, atacul urmăreşte crearea de întreruperi periodice şi de scurtă durată cu scopul de a sincroniza stările fluxurilor TCP şi de a forța protocolul să intre repetat în starea ”transmission timeout”.

Efectul resimțit de utilizatorii legitimi va fi un atac DoS, dar realizat cu un volum de trafic foarte mic, neobservabil de către mecanismele de detecție pentru atacurile DoS clasice.

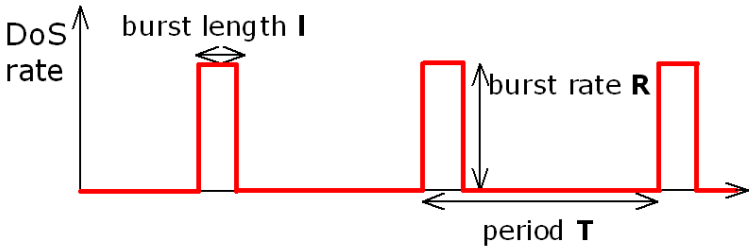


Figura 1.17 - Modul de operare al unui atac de tip Shrew

- l ~ RTT (timpul dus-întors al unui pachet în rețea)
- T ~ min(RTO) unde RTO (retransmission timeout) este timpul de aşteptare pentru retransmiterea segmentului TCP.

Conform [RFC 2998], RTO se defineşte pe baza formulei *RTO=SRTT+4*RTTVAR* unde, SRTT (smoothed round-trip time) este media RTT, iar RTTVAR (round-trip time variation) este dispersia RTT. Experimentele au arătat că aceste tipuri de atac poate genera o pierdere aproximativă a throughputlui de 87.8% până să fie detectate. O posibilă soluționare ar fi ca protocolul să aleagă între manieră nedeterministă minRTO [Sun08].

D. Ping of Death

Acest atac constă în trimiterea unui pachet ICMP mult mai mare decât pachetul maxim IP, şi anume 64 KBytes. La destinație, unele implementări nu pot decodifica pachetul, cauzând prăbuşirea sau reboot-ul sistemului. Vulnerabilități în implementările stivei TCP/IP ale sistemelor Windows timpurii, sau ale aplicațiilor (un caz recent fiind vulnerabilitatea MS11-057 în Internet Explorer 9) pot favoriza condiții pentru acest gen de atac [MS11-01].

ce predispuneau la astfel de atac au fost documentate în acest gen de atac au fost adresate in IE9 probleme recente au fost găsit

E. Teardrop

Datorită implementării defectuoase, unele sisteme nu pot asambla fragmente de pachete care au deplasamente eronate. În loc să ignore elegant aceste pachete, aceste implementări blochează sau reboot-ează sistemul. O implementare a acestui tip de atac se regăseşte în unealta DDoS Trinity.

F. Land

Unele implementări TCP/IP cauzează blocarea sistemului când primesc pachete având aceeaşi adresa ca sursă şi destinație.

G. WinNuke

Acest tip de atac este specific sistemelor de operare Windows. Atacatorul trimite date aleatoare la un port anume, ceea ce cauzează blocarea sau reboot-ul sistemului.

1.5.1.4 Atacuri pe bază de viermi

În accepțiunea clasică, un "vierme" este un agent infecțios autonom cu replicare independentă, capabil de a identifica noi victime (ținte) şi a le infecta prin intermediul rețelei. [Sta02]

Cu timpul, denumirea de vierme a fost extinsă şi asupra altor categorii de agenți infecțioşi care, pentru a fi activați, necesită o acțiune tipică, simplă pe care utilizatorul o execută în mod frecvent în interacțiunea cu spațiul virtual (citirea email, utilizarea mediilor externe USB, etc.). Această extindere are la bază faptul că tehnologia este utilizată pe scară largă şi în mod cvasi-permanent, ceea ce face ca activitățile frecvente şi probabile ale utilizatorilor să determine o rată de propagare acceptabilă pentru atacator.

Motivele care stau la baza proliferării atacurilor bazate pe viermi sunt următoarele [Naz07-1]:

- *Convenienț*a oferită de gradul înalt de automatizare în descoperirea țintelor vulnerabile;
- *Viteza de penetrare* datorată auto-propagării;
- *Persistența* - practica a arătat cazuri de infectări cu Conficker chiar după luni de zile de la lansarea lor, în ciuda faptului că patch-urile erau disponibile de o bună perioadă de timp [Por09];
- *Acoperirea* - majoritatea cazurilor precedente au arătat o infectare la nivel global a Internetlui.

Procesul de livrarea a agenților infecțioşi pe sistemele victimă a evoluat în mod deosibit de-a lungul anilor. O schimbare majoră o reprezintă utilizarea mai multor vectori de propagare. Dacă spre exemplu Slammer [MOO03] a utilizat o singură vulnerabilitate pentru a se propaga, Stuxnet [Mat11] a utilizat tehnici multiple pentru propagarea sa (memorii externe USB, exploatarea a 4 vulnerabilități nepublicate şi a două existente folosite în propagarea altor viermi precum Conficker [Por09]).

1.5.1.4.1 Structura viermelui

Structura unui vierme prezintă următoarele categorii de componente de bază [Naz03]:

- *Recunoaşterea* (sau scanarea) – Această componentă este responsabilă pentru descoperirea stațiilor din rețea care pot fi compromise prin metode cunoscute de vierme.
- *Atac* - Acesta este utilizată pentru a lansa atacuri împotriva unui sistem țintă identificat valorificând vulnerabilități de tip: "buffer overflow", "string formatting", interpretări eronate ale Unicode, sau configurații greşite.

- *Comunicație* - Nodurile din rețeaua de stații infectate pot comunica între ele. Această componentă oferă viermelui interfața prin care pot fi trimise mesaje între noduri sau către o locație centrală.
- *Comandă* – De îndată ce o stație este compromisă, viermele poate rula comenzi operaționale utilizând această componentă. Elementul de comandă furnizează interfața prin care un nod din rețeaua de stații infectate poate genera sau primi comenzi.
- *Culegere de informații* – oferă informațiile necesare pentru a putea contacta alte noduri infectate ale rețelei de stații controlate de vierme.

Fenotipul, sau comportamentul observabil al viermelui, este discutat în adesea în contextul celor mai ”vizibile” componente: cea de scanare şi cea de atac. Aceste două componente sunt necesare în orice implementare de vierme care se propagă pe scară largă, în timp ce toate celelalte componente sunt opționale.

Prin utilizarea şi a celorlalte trei componente, se poate conferi viermelui capacități sporite cum ar fi: generarea de atacuri distribuite de tip DDoS, monitorizarea activității la tastatură, sau controlul stației compromise (BotNet) [Bot11].

1.5.1.4.2 Identificarea țintelor

În funcție de strategia folosită pentru aflarea țintelor se identifică următoarele tipuri de scanări [PPN05-01]:

- *Scanarea uniformă* – când un vierme nu posedă cunoştințe despre localizarea stațiilor vulnerabile în Internet, cea mai simplă soluție este de a scana aleator întregul spațiu de adrese pentru a găsi victime. Această strategie de scanare a fost folosită de viermi precum Code Red, Slammer, Conficker, Witty, Sasser [Moo03] [Fse04-2][PPN05-03].
- *Scanare de tip listă țintă (hit list)* – este tipul de vierme care posedă o listă cu adrese IP ale anumitor stații vulnerabile din Internet. Un astfel de vierme scanează şi infectează mai întâi toate stațiile vulnerabile definite în hit-list, iar apoi scanează aleator întregul spațiu Internet pentru a infecta şi alte stații vulnerabile. Acesta este doar un model teoretic, neexistând o implementare practică până în acest moment. [Zou03]
- *Scanare topologică* - se bazează pe adresele identificate pe stația victimă pentru a determina noile ținte de scanare. Un exemplu în acest caz îl constituie primul vierme propagat în masă – Morris.
- *Scanare metaserver* – informația de identificare a stațiilor țintă este obținută prin interogarea altor sisteme sau aplicații. Viermele Santy a utilizat Google pentru a identifica serverele web care rulau phpBB [Fse04-1]
- *Scanare pasivă* – se aşteaptă ca potențiale victime să contacteze sursa de scanare. Foarte greu de depistat. O implementare de acest tip a fost viermele Gnuman care opera ca nod Gnutella [Smi09]
- *Scanarea de tip divide-et-impera* - un vierme cu scanare uniformă poate utiliza o strategie de tip divide-et-impera astfel încât stațiile infectate vor scana şi infecta stații vulnerabile localizate în spații de adrese IP diferite
- *Scanarea de tip preferință locală* – urmăreşte scanarea adreselor IP din vecinătatea propriei adrese cu o probabilitate mai mare decât adresele dintr-un spațiu mult mai îndepărtat. În cazul în care viermele are dificultăți în a scana o

rețea aflată în spatele unui firewall, dar se aduce o stație infectată în zona protejată de firewall, acest tip de scanare va permite compromiterea rapidă a tuturor stațiilor vulnerabile din acea rețea locală. Un astfel de tip de scanare a fost utilizat de viermi precum Code Red 2, şi Nimda [Che03]

- *Scanarea secvențială* - odată ce o stație vulnerabilă este infectată, viermele selectează mai întâi o adresă IP de la care va începe o scanare secvențială. Blaster este un exemplu tipic de vierme care a utilizat această scanare
- *Scanarea direcționată* – se utilizează în realizarea de atacuri selective în care obiectivul atacatorului este scanarea şi infectarea stațiilor din domeniul țintă. În acest sens, de interes pentru atacator este de propagare a viermelui în domeniul țintă, şi nu de numărul de stații vulnerabile care sunt infectate în Internet. Un exemplu de vierme ce utilizează această scanare în anumite faze ale propagării sale este Stuxnet [Mat11]

1.5.1.4.3 Evaluarea strategiilor de scanare

Analiza impactului strategiilor de scanare asupra modului de propagare arată că [PPN05-01]:

- Scanarea de tip preferință locală sporeşte viteza de propagare a viermelui când stațiile vulnerabile nu sunt uniform distribuite. Probabilitatea optimă pentru scanarea de tip preferință locală creşte când scanarea locală este aplicată în subrețele mari.
- Când stațiile vulnerabile sunt uniform distribuite, scanările de tip divide-et-impera, cea secvențială şi cea uniformă, sunt echivalente în ceea ce priveşte numărul total de stații infectate în orice moment.
- Utilizarea preferinței locale în selectarea punctului de start al unei scanări secvențiale determină o scădere a vitezei de propagare a viermelui.
- În cazul în care densitatea de stații vulnerabile în domeniul țintă (raportul dintre numărul de stații vulnerabile şi cel al adreselor IP din domeniu) este mai mare decât alte domenii, atunci folosirea unei scanări direcționate va creşte viteza de propagare pe domeniul țintă față de o scanare uniformă.

Pe baza acestor rezultate, este important ca în proiectarea sistemelor defensive să se caute prevenirea atacatorului de la identificarea unui număr mare de adrese IP de stații vulnerabile, sau obținerea unor informații legate de spațiul de adrese alocat sau utilizat, care să permită reducerea spațiului de scanare [PPN05-03].

Un sistem de monitorizare şi protecție împotriva atacurilor lansate de viermi, trebuie să acopere un număr de blocuri de adrese IP suficient distribuite, pentru a avea o imagine corectă a modului de propagare a viermilor ce folosesc o scanare neuniformă (în special în cazul unei scanări secvențiale ca cea folosită de Blaster).

1.5.1.4.4 Tehnici anti-detecție ale viermilor

Pentru ca un vierme să afecteze o populație cât mai mare, atacatorii au la dispoziție două opțiuni [PPN05-01]:

- Utilizarea unei strategii în care propagarea în faza inițială să fie mai rapidă decât timpul necesar pentru generarea semnăturilor pentru firewall-uri, menite să

limiteze propagarea (cum a fost cazul propagărilor Core Red, Conficker, Witty, Sasser).

- Utilizarea de tehnici care să asigure o vizibilitate redusă pentru a evita detecția pe o perioadă cât mai îndelungată (cum a fost cazul propagării Stuxnet) [Mat11]. Această vizibilitate redusă poate fi obținută prin tehnici cum ar fi:
  - ♦ scanarea lentă - marea majoritate a soluțiilor de detecție a propagării utilizate de furnizorii Internet vizează protecția împotriva propagărilor epidemice, astfel că mecanismul de monitorizare al organizației țintă va trebui să fie capabil să detecteze astfel de situații.
  - ♦ polimorfism şi criptare – vizează auto modificarea sau criptarea pentru a evita detectoarele bazate pe semnătură
  - ♦ amestecarea – schimbarea comportamentului când trece prin zona sistemelor IDS prezentând caracteristici similare traficului curent, sau comportament normal
  - ♦ DoS asupra sistemelor IDS sau asupra personalului de securitate – se realizează prin producerea de trafic de diversiune pentru supraîncărcarea IDS (forțarea acestuia să genereze semnături inutile, să învețe noi atacuri), şi a personalului de securitate (care să analizeze un volum mare de alerte caracterizare un grad ridicat de confuzie).

1.5.2 Atacuri asupra aplicațiilor şi serviciilor

Dacă, atacurile inițiale în sisteme vizau cu precădere exploatarea unor vulnerabilități cunoscute în sisteme de operare, protocoale de comunicație sau serviciile de rețea clasice, în ultima perioadă se observă o specializare a atacatorilor şi creatorilor de malware, ce dezvoltă în mod constant metode noi şi ingenioase pentru a neutraliza îmbunătățirile aduse securității sistemelor actuale.

Atacurile din această categorie exploatează vulnerabilități ale sistemului de operare, sau ale aplicațiilor rulate pe stația victimă cu scopul de a prelua controlul asupra serviciilor, sau compromite integritatea şi confidențialitatea datelor procesate. Majoritatea vulnerabilităților ce creează premisele unor astfel de atacuri sunt cele de tip buffer-overflow, şi cele de proiectare a aplicațiilor (insuficiențe în definirea şi implementarea mecanismelor de autentificare, autorizare, şi manipularea datelor).

Atacurile asupra aplicațiilor au cunoscut o creştere deosebită în ultima perioadă. Un raport publicat de HP în 2010 estimează că aproximativ 70% din totalul atacurilor sunt îndreptate asupra aplicațiilor Web [SEC11]. Cele mai importante tipuri de atac asupra aplicațiilor Web sunt :[OWA11]

- *Atacurile Cross Site Scripting (XSS)* - au loc când serverul preia datele de la utilizator şi le trimite înapoi browserului, fără ca acestea să fie validate. XSS permite atacatorilor să redirecționeze paginile victimei, să execute scripturi în browserul victimei, aceştia putând ulterior să intercepteze sesiuni de utilizator, să introducă viermi, etc.
- *Erori de injectare (Injection Flaws)* - în special injecția de tip SQL, sunt comune în aplicațiile web. Injectarea se produce atunci când datele furnizate de utilizator sunt trimise la un interpret ca parte a unei comenzi sau a unei interogări. Atacatorul păcăleşte interpretorul determinându-l să execute comenzi sau schimbarea de date în mod eronat.

- *Execuția malițioasă a fişierelor* - Codul vulnerabil la includerea externă a fişierelor (Remote File Inclusion) permite atacatorilor să includă cod şi date ostile, rezultând atacuri devastatoare. Execuția malițioasă a fişierelor afectează scripturile PHP, XML şi orice cadru (Framework) care accepta fişiere (sau nume de fişiere) de la utilizator.
- *Expunerea referințelor directe* - O referință directă la un obiect are loc atunci când un dezvoltator expune o referință la un obiect intern cum ar fi un fişier, director, record de baze de date, sau cheie, un URL sau parametru dintr-un form. Atacatorii pot manipula aceste referințe pentru a accesa alte obiecte fără autorizație.
- *Cross Site Request Forgery (CSRF)* - Un atac CSRF forțează browser-ul victimei autentificate deja să trimită o cerere de pre-autentificate la o aplicație web vulnerabilă, care apoi forțează browserul victimei să efectueze o acțiune în beneficiul atacatorului.
- *Scurgerile de informații şi manipularea incorectă a erorilor* - Aplicațiile pot oferi, fără a se dori, informații despre configurare, modul intern de lucru, etc. Atacatorii pot folosi aceste informații pentru a sustrage date de pe serverul în cauză, sau pentru a lansa atacuri mai importante.
- *Compromiterea autentificării şi a managementului sesiunii* - Conturile şi sesiunile sunt de multe ori protejate insuficient. Atacatorii pot compromite parole, chei, sau sesiuni pentru a-şi asuma identitatea altor utilizatori.
- *Stocarea nesigură a datelor criptografice* - Aplicațiile web folosesc rar funcțiile criptografice în mod corespunzător pentru a proteja datele şi conturile. Atacatorii folosesc datele slab protejate pentru furt de identitate şi alte infracțiuni, cum ar fi fraudarea cărților de credit.
- *Comunicații nesecurizate* - În mod frecvent aplicațiile nu criptează traficul din rețea pentru a proteja transferul de date cu grad de confidențialitate sporit. Aceasta deschide posibilitatea ca sesiunea sa fie interceptata (cu ajutorul unui sniffer de exemplu).
- *Imposibilitatea de a restricționa accesul URL* - Frecvent, o aplicație protejează anumite date sau funcționare ce se doreşte a fi secretă doar prin prevenirea afişării de link-uri sau URL-uri pentru accesul utilizatorilor neautorizați. Atacatorii pot utiliza această slăbiciune pentru a accesa şi de a efectua operațiuni neautorizate prin accesarea acelor adrese URL în mod direct.

1.5.3 Atacuri asupra utilizatorilor

Ingineria socială poate implica trucuri atât psihologice cât şi tehnologice pentru a câştiga încrederea țintei. Din perspectiva psihologică, atacatorul poate exploata câteva caracteristici ale comportamentului uman pentru a creşte şansele ca victima să execute acțiunile dorite de atacator. Unele trăsături de comportament ce pot fi exploatate de atacatori sunt: dorința de conformitate, dorința de a fi de ajutor, lipsa de experiență, curiozitatea. Aceste trăsături de comportament sunt adesea exploatate de atacurile de tip phishing prin utilizarea de tehnici de înşelăciune.

Dintre trucurile de ordin tehnic utilizate de atacuri precum Phishing-ul sau cele bazate pe malware se menționează: imitarea adreselor de email, mascarea URL-urilor frauduloase, clonarea site-urilor. Pentru a exploata ignoranța utilizatorilor cu privire la modul de funcționare a tehnologiilor de protecție, site-urile clonă prezintă indicatori de

securitate fictivi (icoana specifică conexiunii criptate), sigle ale autorităților de certificare precum Verisign.

În paragraful următor se vor descrie scheme tipice de atac pe bază de mesaje de poştă, al căror obiectiv este în principal determinarea utilizatorului de a executa acțiunea dorită de atacator.

1.5.4 Scheme tipice de atacuri pe bază de mesaje de poştă

Schemele prezentate în continuare conțin paşii urmați atât de atacator cât şi de victimă pentru ca atacul să se încheie cu succes. Schemele arată şi modul în care tehnologiile disponibile la ora actuală pot fi utilizate pentru a reduce vulnerabilitatea la diferitele clase de atacuri.

Resursele sau condițiile pe care atacatorul încearcă să le obțină sunt reprezentate prin dreptunghiuri, iar acțiunile atacatorului şi victimei sunt prezentate prin săgeți. Cazul în care atacul este anihilat se reprezintă prin starea "*Atacul eşuează*", iar în cazul în care se materializează, starea finală este colorată distinctiv.

Datorită dimensiunii şi complexității schemei de atac, aceasta a fost împărțită în patru secțiuni (1.18-1.21). Prima secțiune (1.18) cuprinde fazele de atac comune tuturor vectorilor de atac. Fiecare din vectorii de atac (ce vizează cu precădere atacurile asupra sistemelor client şi utilizatorilor) sunt prezentați în diagrame separate. Aceşti vectori de atac sunt [PPN06-02]:

- *Instalarea de software malițios*. Software-ul malițios este categoria de cod instalat în sistem, de regulă fără ştirea utilizatorului, şi cu intenția de a compromite confidențialitatea, integritatea sau disponibilitatea datelor, aplicațiilor sau sistemului de operare de pe stația victimă.
- *Inducerea în eroare* a utilizatorului ce recepționează mesajul pentru a urma anumite instrucțiuni.
- *Utilizarea de spyware* pentru a intercepta comunicațiile legitime ale victimei. Spyware-ul este categoria de software care colectează în secret informații despre activitatea utilizatorului (conturi şi parole tastate, adrese web vizitate, etc.) care apoi sunt-transmise în exterior.

Atacurile încep cu un mesaj destinat victimei (utilizator, sau server de poştă). Atacatorul obține adresele de poştă utilizând o varietate de surse şi tehnici (generare semi-aleatoare, explorarea Internetului, liste de adrese, atacuri DHA anterioare, etc.). Mesajele ce vizează atacuri asupra infrastructurii sunt construite astfel încât să exploateze vulnerabilități ale SMTP, sistemelor de operare şi configurației sistemelor client şi server. Mesajele de atac ce vizează utilizatorul sunt construite astfel încât receptorul să creadă că ar putea fi legitime şi trebuie deschise. O configurare corespunzătoare a aplicației server de poştă, a sistemului de operare pe server şi a infrastructurii de protecție (firewall) poate bloca cea mai mare parte a atacurilor de tip DoS şi DHA. Filtrarea conexiunilor SMTP poate asigura controlul asupra încercărilor de inundare cu mesaje prin limitarea ratei de trimitere către server per transmițător. În mod asemănător, filtrarea de conținut (antispam) poate bloca o mare parte a mesajelor nelegitime. Odată ce mesajul este deschis de utilizator, conținutul său trebuie să fie îndeajuns de realistic pentru a determina receptorul să execute paşii doriți de atacator.

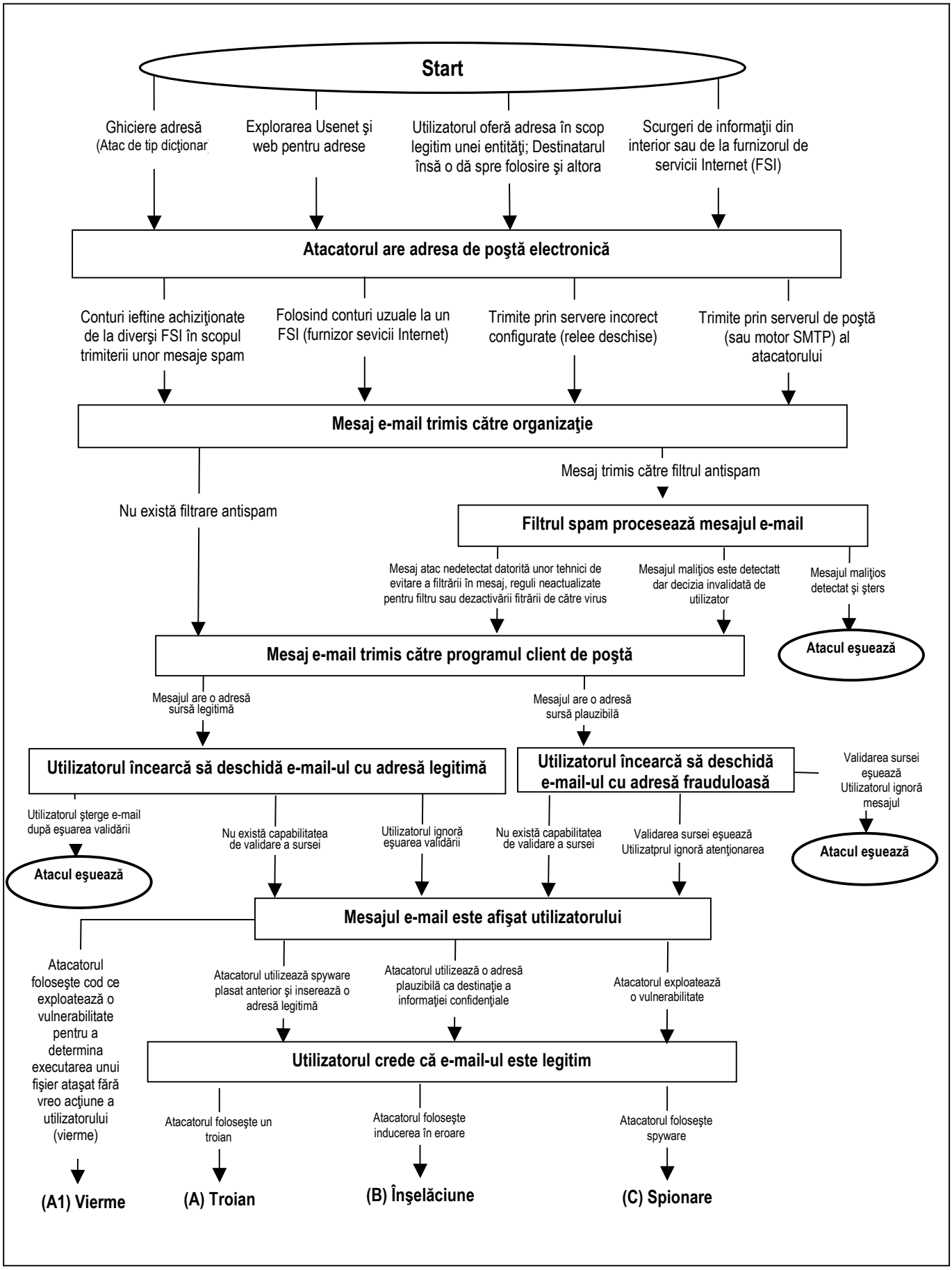


Figura 1.18 - Metode comune de atac folosind mesajele e-mail

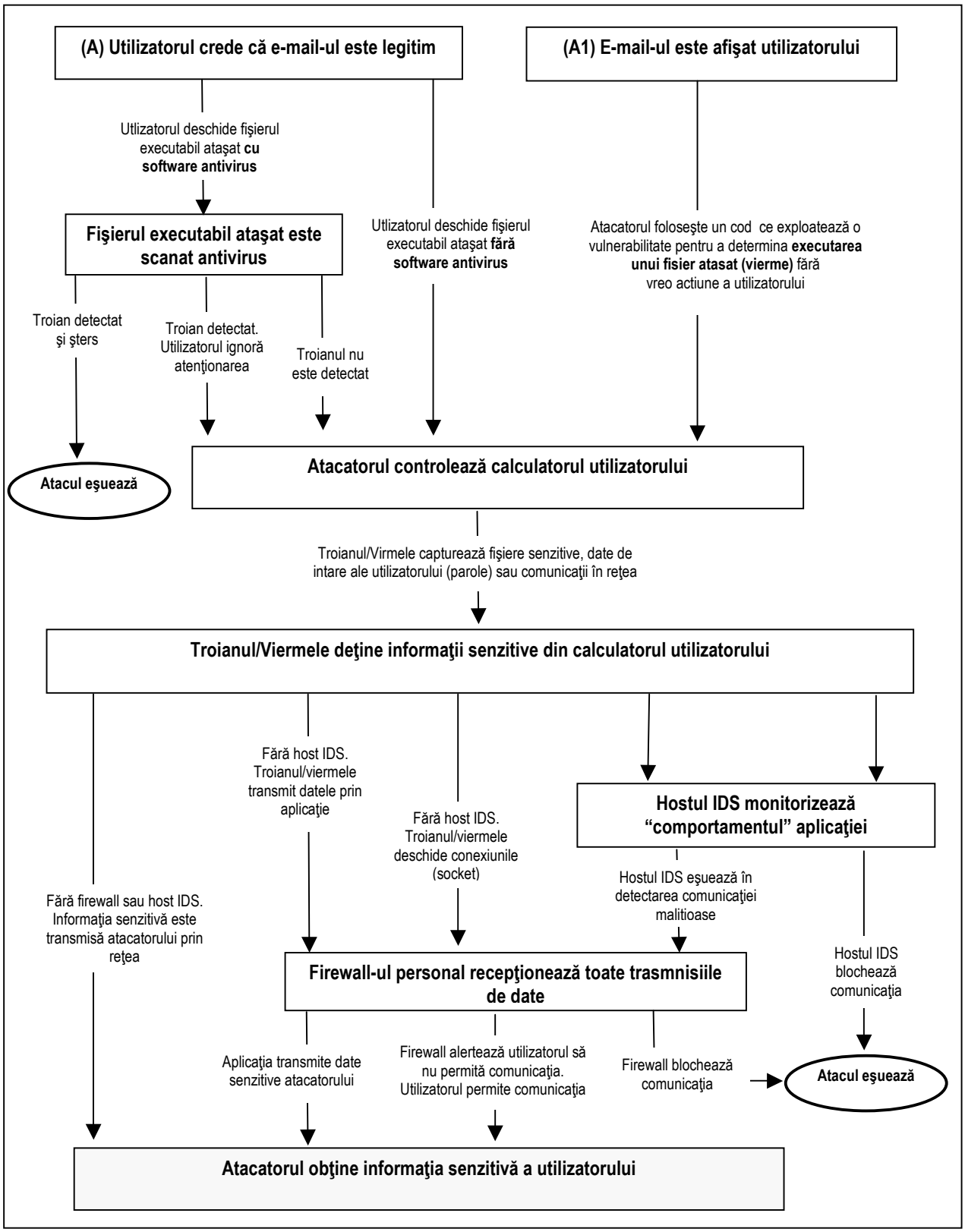


Figura 1.19 - Tipuri de atacuri ale viermilor şi troienilor

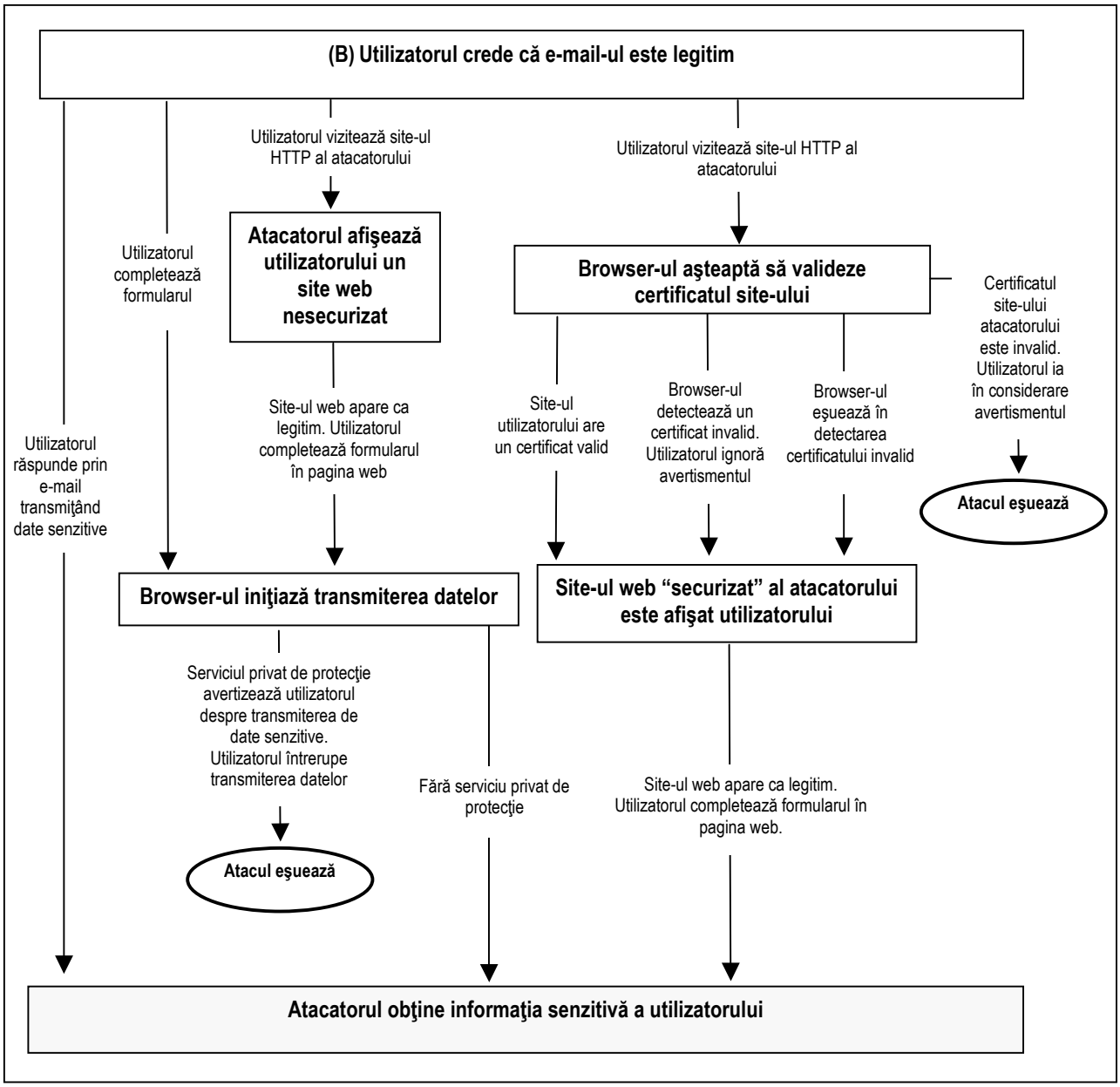


Figura 1.20 - Atacatorul înşeală pentru a obține încrederea utilizatorului

Figura 1.19 descrie continuarea secvențelor de atac din figura 1.18 prin transmiterea unui fişier ataşat ce prezintă în aparență elemente de utilitate pentru victimă (cum ar fi: imagini, screen saver, vedere electronică, etc.), dar care instalează cod malițios în scopul preluării controlului asupra sistemului victimei. Sistemele antivirus şi IDS locale joacă un rol important în blocarea multora din aceste scenarii de atac.

Figura 1.20 prezintă continuarea secvenței de atac din figura 1.18 ce se bazează exclusiv pe înşelarea încrederii utilizatorului. Singura vulnerabilitate vizată de acest tip de atac este cea umană. Atacatorul mizează pe legea probabilistică a numerelor mari trimițând mesajul la un număr mare de utilizatori în speranță că un număr din aceştia vor fi convinşi de legitimitatea acestuia şi vor urma direcțiile dorite de atacator. În cazul în care atacatorul foloseşte HTTPS, SSL (Secure Socket Layer) oferă protecție doar dacă utilizatorul ia în considerare avertismentul asupra invalidității certificatului. Aplicațiile comerciale ce oferă servicii private de protecție, pot fi de ajutor prin avertizarea utilizatorului când acesta este pe punctul de a trimite informații confidențiale către destinații îndoielnice.

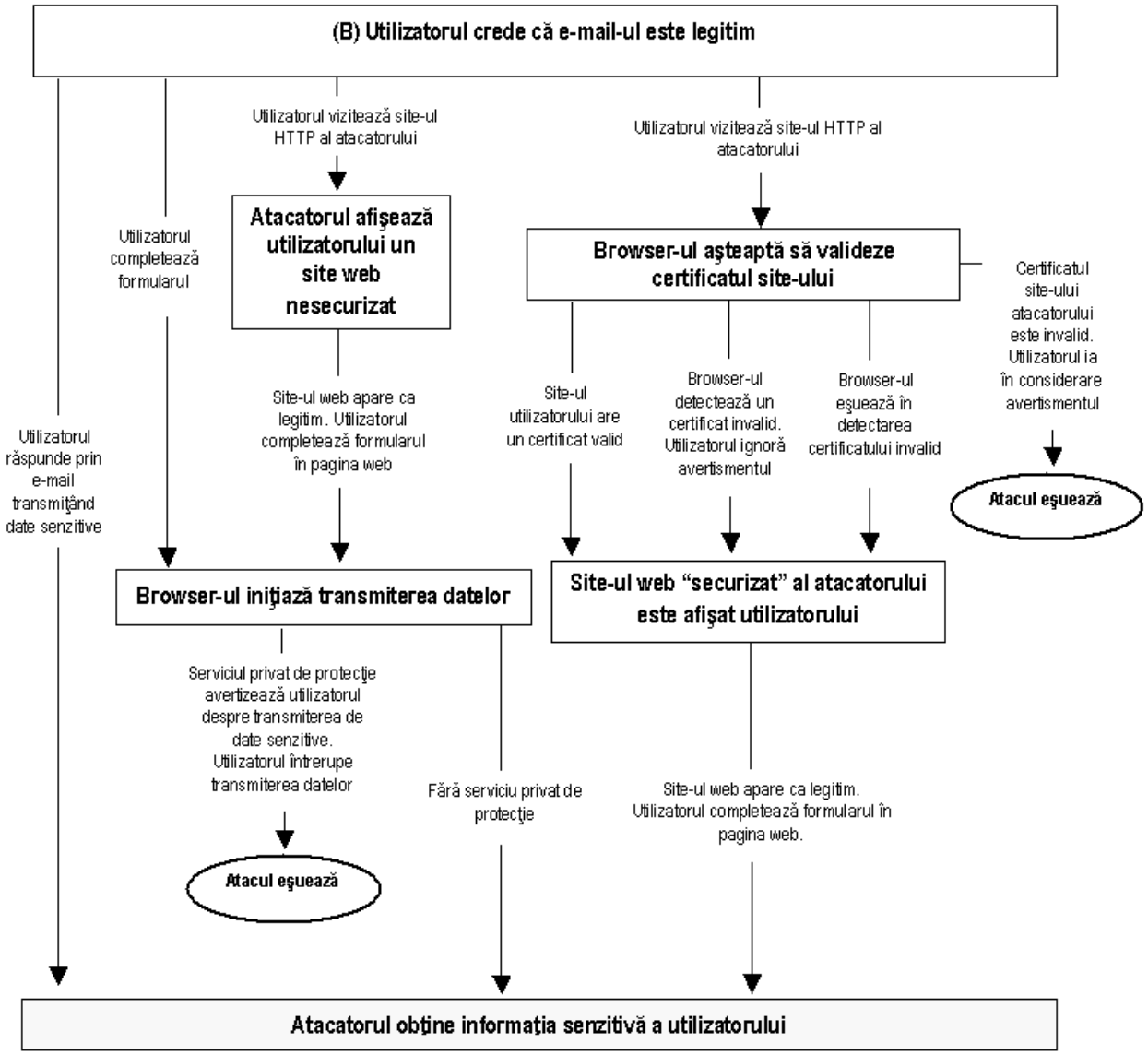


Figura 1.21 – Atacuri pe bază de spyware pentru culegere de informații

Figura 1.21 arată modul în care atacatorul poate obține informații confidențiale despre victimă şi activitățile acesteia prin instalarea de aplicații de tip spyware pe maşina victimei. Aceasta poate fi realizată prin intermediul unui atac prealabil cu Troian sau vierme, sau alte mijloace. Acest tip de software poate fi adesea detectat de programe anti-spyware specializate, cât şi de multe din programele antivirus comerciale. În plus, aplicațiile locale de tip firewall şi IDS pot adesea preveni programul spyware să transmită informații confidențiale în exteriorul sistemului.

1.5.5 Metodologii de clasificare a atacurilor

Clasificarea atacurilor în spațiul virtual se poate face după mai multe criterii cum ar fi: modul de desfăşurare, vulnerabilitatea exploatată, obiectivul atacului, motivația atacatorului, impactul şi implicațiile atacului, resursa atacată, elementele de securitate afectate. [Kja05] [Han05] [Sim10]

Plecând de la taxonomia prezentată in figura 1.22 [Sim10], se propune ca în procesul de evaluare şi analiză a noilor amenințări să se utilizeze un model de clasificare ce încorporează şi un atribut specific monitorizării securității. Acesta va indica zona în care intruziunea se va putea detecta (în cazul în care mecanismul de protecție eşuează), precum şi procesele conexe cadrului de securitate necesare pentru implementarea mecanismului defensiv (de exemplu: managementul patch-urilor). O abordare formală are rolul de a oferi o perspectivă consistentă care ia în calcul toate aspectele de interes ale organizației. O exemplificare a utilizării modelului propus pentru evaluarea atacurilor este ilustrată în tabelul 1.2. Organizațiile cu cerințe speciale de securitate (armată, servicii secrete, corporații, etc) care doresc o caracterizare mai detaliată a atacurilor, pot construi un cadru formal de modelare a amenințărilor plecând de la structurile de VerIS descrise în secțiunea 2.4.5.

ID Grup	Nume	Vector	Impact Operaţional	Impact Informaţie	Ţinta	Mecanism Defensiv	Zona Monitorizare
100	Conficker A	Buffer Overflow	Instalare vierme	Întrerupere	SO Windows (Server, XP)	Soluţie temporară: Buletin furnizor Remediere: Patch	IDS Reţea (NIDS) Control Management Patch
100	Conficker B	USB	Instalare vierme	Întrerupere	SO Windows (Server, XP)	Soluţie temporară: Buletin furnizor Remediere: Patch	IDS Staţie (HIDS) Control Management Patch
100	Conficker B	Buffer Overflow	Instalare vierme	Întrerupere	SO Windows (Server, XP)	Soluţie temporară: Buletin furnizor Remediere: Patch	IDS Reţea (NIDS) Control Management Patch

Tabel 1.2 – Model de evaluarea a atacurilor

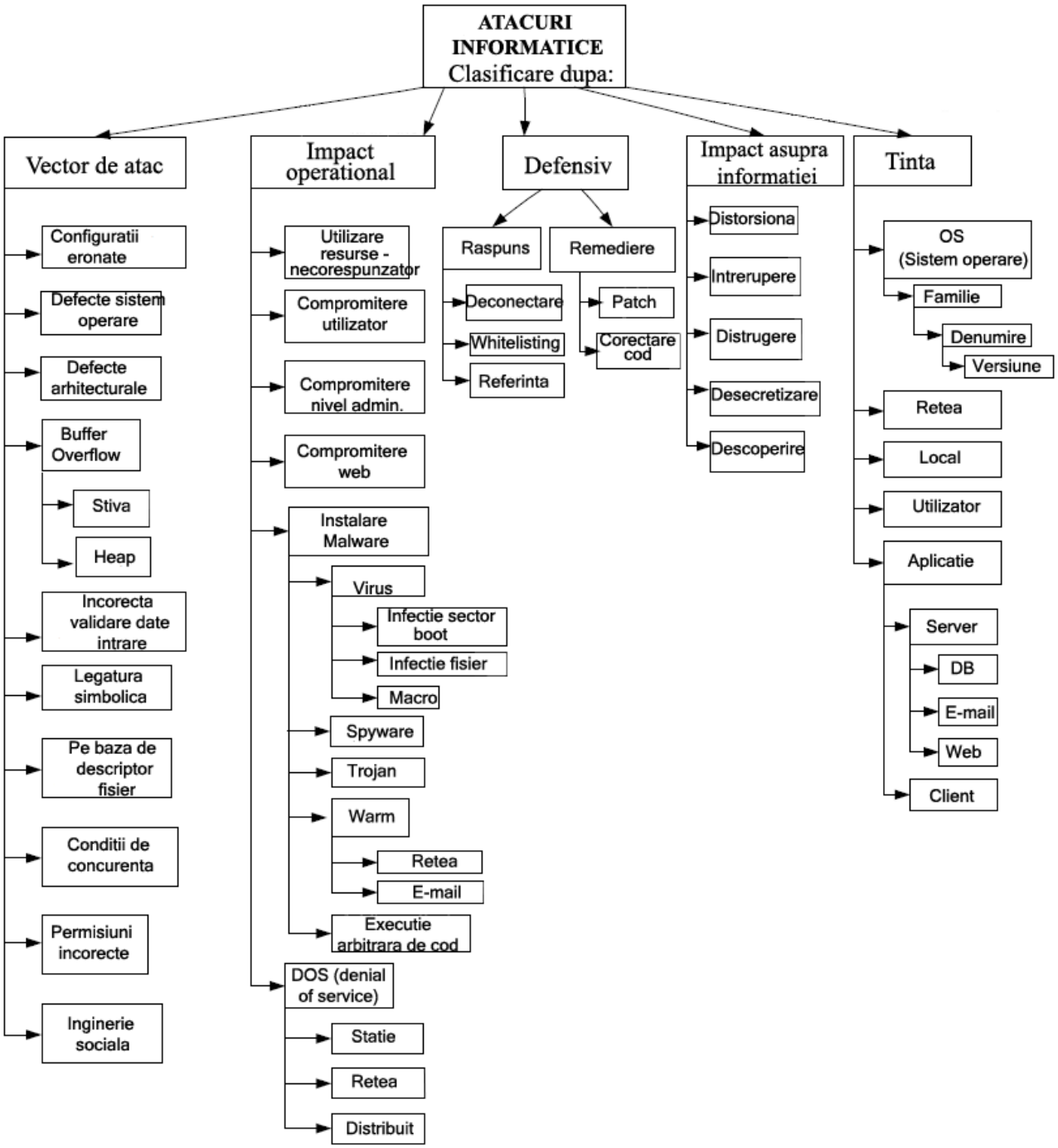


Figura 1.22 - Clase de atacuri [Sim10]

1.6 Componenta de monitorizare şi procesul de securitate

1.6.1 Indicatori şi avertismente

Manualul armatei americane [USA95] defineşte *indicatorii şi avertismentele* (*IA*) ca fiind ”monitorizarea strategică a evenimentelor mondiale pe plan militar, economic şi politic pentru a asigura că acestea nu reprezintă un precursor către activități ostile sau contrare intereselor USA.” Aşadar IA este procesul de monitorizare strategică care analizează indicatori şi produce avertismente.

După cum se poate observa, în *accepțiunea clasică* IA este orientat către amenințări. În acest context se defineşte *monitorizarea securității* ca fiind procesul de colectare, analiză şi investigare a indicatorilor şi avertismentelor pentru detecția şi răspunsul la intruziuni (violări ale politicii de securitate) [PPN06-01].

Cu timpul, pentru eficientizarea procesului de monitorizare şi pentru determinarea stării de securitate de ansamblu la nivelul întregii organizații, scopul monitorizării a fost extins şi asupra categoriilor de date asociate altor concepte de securitate cum ar fi vulnerabilități, agenți de amenințare, controale de securitate, etc [PPN07-01].

Pe baza acestei abordări, se defineşte IA de natură digitală în *accepțiune extinsă* ca fiind "monitorizarea strategică informațiilor disponibile la nivelul resurselor interne (trafic de rețea, fişiere log de pe sisteme, activitate utilizatori, etc.) cât şi externe (buletine de securitate, starea generală de securitate, studii de cercetare asupra noilor clase de amenințări) pentru a adresa într-o manieră proactivă şi anticipativă riscurile şi amenințările la adresa organizației."

Indicatorii se pot defini ca fiind acțiuni observabile sau percepute care confirmă sau neagă intențiile şi capabilitățile agenților de amenințare. În domeniul monitorizării securității, indicatorii sunt adesea concluziile oferite de produsele securitate, cum ar fi alertele generate de sistemele IDS. *Avertismentele* sunt rezultatul interpretării de către analistul de securitate a indicatorilor. Analiştii evaluează indicatorii generați de produsele de securitate şi transmit avertismente către factorii de decizie [PPN07-01].

În domeniul monitorizării securității, sunt elemente distincte, responsabile pentru colectarea şi interpretarea indicatorilor, precum şi transmiterea avertismentelor către factorii de decizie, şi anume:

- *Produsele* efectuează *colectarea*. Un produs este o componentă software sau hardware al cărei scop este de a analiza pachetele din rețea.
- *Oamenii* efectuează *interpretarea*. În timp ce produsele pot oferii concluzii preliminare despre starea de securitate, oamenii sunt necesari pentru a oferi contextul. Determinarea contextului necesită plasarea rezultatelor oferite de produs într-o perspectivă adecvată, dată de natura mediului în care produsul operează.
- *Procesele* determină *transmiterea informației către factorii de decizie*. Factorii de decizie sunt persoanele care au autoritatea, responsabilitatea şi capabilitatea de a răspunde la potențialele incidente.

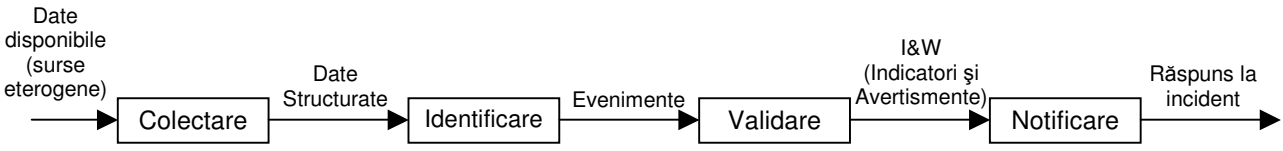


Figura 1.23 – Proces generic de monitorizare a securității

1.6.2 Procesul de securitate

Mitch Kabay, fost director al departamentului de educație din cadrul International Computer Security Association, menționa în 1998 că ”*securitatea este un proces* de menținere a unui nivel acceptabil de risc perceput, şi nu o stare finală” [Kab98].

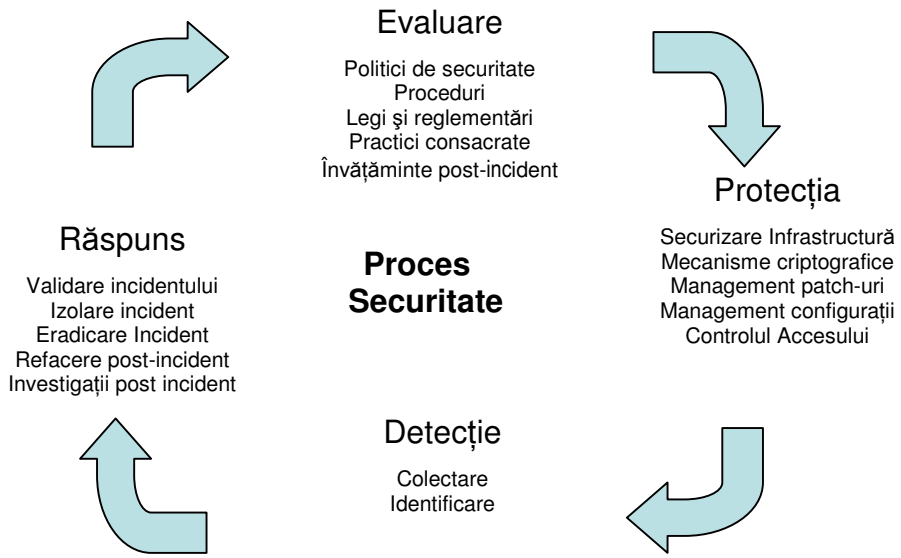


Figura 1.24 – Procesul de securitate pe baza BS7799-2/ISO27001 [ISO--]

Procesul de securitate cuprinde următoarele patru mari componente: evaluarea, protecția, detecția şi răspunsul [BPN09].

Evaluarea – reprezintă pregătirea pentru celelalte trei componente. Este menționată ca o componentă separată deoarece vizează în principal politici, proceduri, legi, regulamente, aspecte bugetare, atribuții manageriale, precum şi evaluarea tehnică a propriei posturi de securitate. Eşuarea în a cuprinde unul din aceste elemente va afecta operațiile ulterioare. Evaluarea presupune stabilirea controalelor de securitate pentru limitarea riscurilor organizației.

Protecția – reprezintă aplicarea contramăsurilor pentru a reduce probabilitatea de compromitere. Un alt termen echivalent în literatura de specialitate este „ *prevenirea*”, deşi realitatea a dovedit că prevenirea poate eşua. Monitorizarea securității nu este o componentă activă a strategiei de control a accesului, însă o bună prevenire contribuie la realizarea unui monitorizări mult mai eficace.

Detecția – reprezintă procesul de identificare a intruziunilor (violări ale politicii de securitate) sau a incidentelor de securitate. Elemente ale procesului de monitorizare, cum ar fi colectarea şi identificarea, se vor regăsi în această componentă.

Răspunsul – reprezintă procesul de validare a rezultatelor detecției şi paşii luați pentru remedierea intruziunilor. Activitățile din această categorie includ aplicarea de patch-uri şi devirusare, precum şi urmărirea şi chemarea în justiție a vinovaților. Abordările anterioare urmăreau restaurarea funcționalității componentelor afectate de atac; cele mai recente urmăresc şi remedieri de natură legală prin colectarea dovezilor necesare unor acțiuni juridice împotriva atacatorului.

1.6.3 Elementele procesului de monitorizare

Elementele procesului de monitorizare a securității se vor regăsi în componentele de detecție şi de răspuns ale procesului de securitate şi sunt descrise în continuare conform [PN08].

Colectarea – este procesul de culegere a datelor care permit observarea, detecția, prevenirea amenințărilor şi vulnerabilităților de securitate cunoscute, precum şi managementul diferitelor aspecte ale controalelor de securitate implementate pentru a adresa acele amenințări şi vulnerabilități.

Identificarea – este procesul de recunoaştere a evenimentelor suspecte. Activitatea din organizație din perspectiva securității este structurată la nivel de evenimente care sunt clasificate după cum urmează:

- *Legitime* – activități conforme politicii şi controalelor de securitate
- *Suspecte* – activități atipice la prima vedere (de exemplu: fragmente de pachete), dar care nu afectează bunurile sau resursele organizației. În cele mai multe cazuri, aceste activități sunt conforme cu politica de securitate
- *Maliționase* – activități neconforme cu politica de securitate care pot afecta negativ securitatea organizației. Atacurile de orice tip sunt cuprinse în această categorie

Identificarea se poate realiza prin intermediul unor măsuri de ordin tehnic şi non-tehnic. Măsurile de ordin tehnic se regăsesc în produse (cum ar fi cele de detecție a intruziunilor şi de monitorizare a securității), în timp ce măsurile de ordin non-tehnic se bazează pe observații umane cum ar fi: administratori care identifică un nou proces ce rulează pe server sau utilizatori ce raportează că stațiile personale se comportă ”atipic”. Aceste măsuri nu trebuiesc ignorate, deoarece reprezintă adesea mijlocul prin care se detectează atacatorii foarte buni. Tot personalul organizației ar trebui să cunoască modul de raportare a unor astfel de situații suspecte către grupul de răspuns la incidente.

Validarea – este procesul de asociere a unei categorii preliminare de incident evenimentelor identificate în procesul anterior [USAF96].

- Categoria I – Acces neautorizat la nivel root/admin.
- Categoria II – Acces neautorizat la nivel utilizator
- Categoria III – Încercare de acces neautorizat
- Categoria IV – Atac Denial of Service (DOS) reuşit
- Categoria V – Violare de politică de securitate, sau practică de securitate necorespunzătoare
- Categoria VI – Activitate de recunoaştere, sondare sau scanări
- Categoria VII – Infecție cu viruşi (vierme)

Notificarea – este procesul prin care se furnizează rezultate de analiză factorilor de decizie (interni sau externi) pentru a răspunde incidentului. Nu toate IA vor fi clasificate ca incidente şi trimise către factorii de decizie. În majoritatea cazurilor, notificarea reprezintă primul pas al planului de răspuns la incident, recomandându-se organizațiilor să aibă proceduri clare în acest sens.

Motto: *Nu cele mai puternice sau inteligente specii supraviețuiesc,*
ci cele care se adaptează cel mai bine la schimbare.

- Charles Darwin

CAPITOLUL 2

PROCESE ŞI POLITICI DE MONITORIZARE

Securitatea informațiilor este un proces dinamic care trebuie să răspundă eficient noilor vulnerabilități, amenințări, precum şi schimbărilor constante care au loc în arhitectura, sau mediul operațional al organizației. O abordare exclusiv tehnologică, sau fără suportul întregii organizații va conduce la soluții incomplete care nu adresează nevoile de ansamblu ale organizației. O soluție de succes presupune utilizarea unui proces structurat ce integrează securitatea informației şi activitatea de management al riscului în ciclul de viață al dezvoltării sistemelor [PNCN09].

Monitorizarea securității informațiilor la nivelul organizației se defineşte ca fiind procesul de menținere în mod constant a atenției asupra securității informaționale, vulnerabilităților şi amenințărilor, cu scopul de a oferi suport deciziilor legate de managementul riscului la adresa organizației. Obiectivul este de a realiza monitorizarea în mod constant a securității rețelelor şi sistemelor informaționale ale organizației şi de a răspunde prin acceptarea, evitarea, transferul sau adresarea riscurilor atunci când sunt schimbări [PN08].

2.1 Procesul de management al riscului.

Managementul riscurilor la adresa rețelelor şi sistemelor de calcul reprezintă o componentă fundamentală a programului de securitate informatică a fiecărei organizații.

Principalul obiectiv al procesului de management al riscului este de a proteja organizația, precum şi capacitatea acesteia de a-şi îndeplini activitățile. De aceea procesul de management al riscului este o funcție esențială a procesului de management al organizației, şi nu neapărat o funcție tehnică realizată de experții IT, care operează şi gestionează aceste sisteme [PPIN08-01].

Abordarea bazată pe risc a managementului sistemelor informaționale va avea un grad ridicat de eficiență atunci când este integrată în ciclul de viață al dezvoltărilor sistemelor (System Development Lifecycle-SDLC). SDLC este un proces pe mai multe etape care începe cu inițierea, analiza, proiectarea, dezvoltarea şi implementarea sistemelor informatice, continuă cu operarea, şi se finalizează cu încheierea ciclului de viață al sistemului [NIST-SP 800-64, NIST-SP 800-18, NIST SP 800-39].

Managementul riscului organizațional este un element cheie în programul de securitate informațională a organizației, şi oferă un cadru eficace pentru selectarea controalelor de securitate corespunzătoare fiecărui sistem informațional (controale de securizare necesare protejării indivizilor, operațiilor şi bunurilor organizației).

Abordarea bazată pe risc în ceea ce priveşte selecția şi specificațiile controalelor de securitate va avea în vedere eficacitatea, eficiența, şi constrângerile de natură legislativă, politică organizațională, standarde, reglementări sau alte cerințe venite din partea managementului executiv al organizației [PPIN08-02].

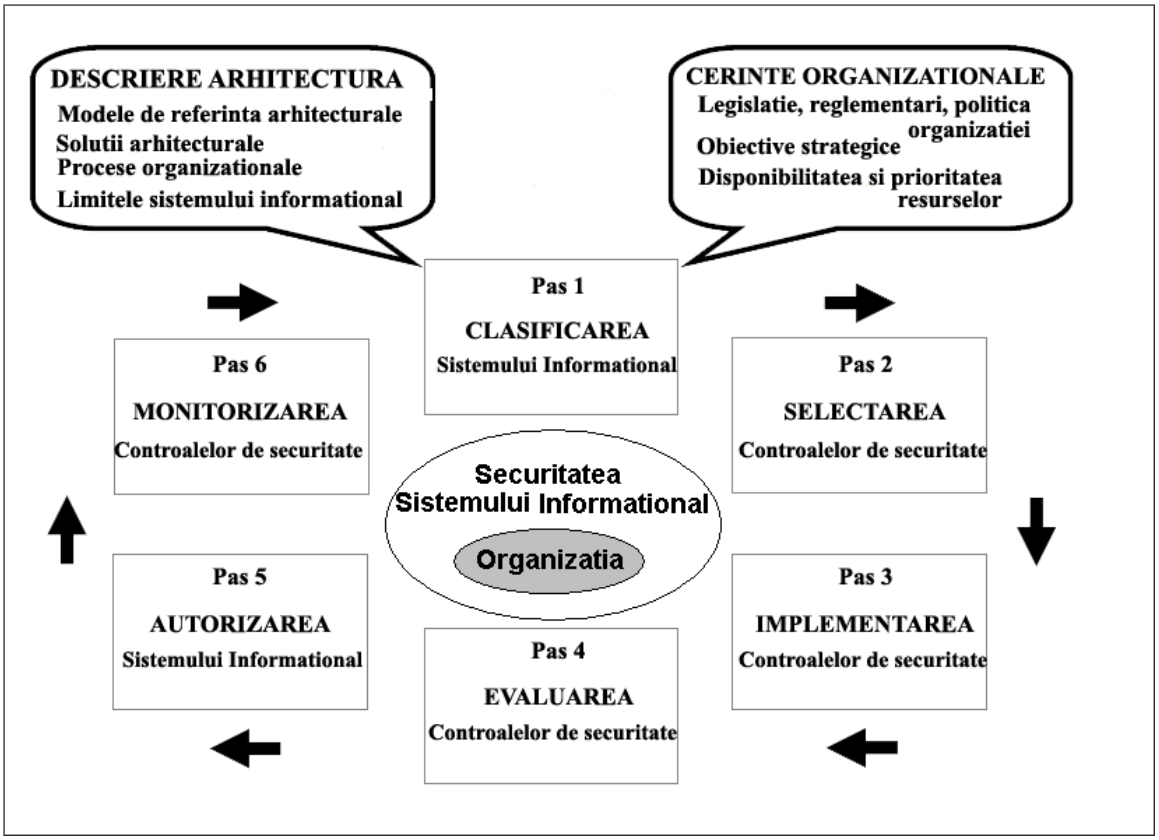


Figura 2.1 - Cadru de management al riscului conform NIST SP 800-30

Următoarele activități legate de managementul riscului organizațional (cunoscut ca şi cadru de management al riscului) sunt definitorii pentru implementarea unui program de securitate informațională eficace şi pot fi aplicate atât pentru sistemele existente cât şi cele ce vor fi create [BPN09].

- Clasificarea sistemelor informaționale şi a informațiilor procesate, memorate şi transmise de acel sistem pe baza analizei impactului asupra operațiilor organizației. [NIST SP 800-60; FIPS 199].
- Selectarea unui set inițial cu controale de securitate de bază (baseline) pentru sistemul informațional realizat pe baza clasificării de securitate efectuată anterior; adaptarea şi suplimentarea controalelor de securitate de bază pe măsura nevoilor având în vedere evaluarea riscului de către organizație şi a condițiilor specifice locale. [FIPS 200; NIST SP 800-53].
- Implementarea controalelor de securitate şi documentarea modului de amplasare în sistemele informaționale şi a mediului de operare [NIST SP 800-70; NIST SP 800-100].

- Evaluarea controalelor de securitate utilizând proceduri corespunzătoare pentru a determina dacă au fost implementate în mod corect, dacă operează conform planului stabilit şi produc rezultatele anticipate în ceea ce priveşte îndeplinirea cerințelor de securitate pentru sistem [NIST SP 800-53A].
- Autorizarea operării sistemului informațional având la bază determinarea riscului la adresa operațiilor, bunurilor, indivizilor precum şi a altor organizații ca rezultat al operării sistemului respectiv, precum şi obținerea deciziei în termeni de acceptabilitate a acestui risc [NIST SP 800-37].
- Monitorizarea şi evaluarea în mod constant a controalelor de securitate selectată pentru sistemul respectiv, incluzând evaluarea eficacității, documentarea modificărilor efectuate asupra sistemului sau mediului în care operează acesta, efectuarea de analize de impact a securității asupra schimbării modificărilor asociate, şi raportarea stării de securitate a sistemului către persoanele responsabile din organizație [NIST SP 800-53A, NIST SP 800-37, NIST SP 800-137].

Monitorizarea controalelor de securitate este una din componentele cadrului de management al riscului [NIST SP 800-37]. Obiectivul programului de monitorizare este de a determina dacă setul de controale de securitate identificate ca fiind necesare, şi apoi implementate pentru un sistem informațional, îşi mențin eficacitatea în timp, având în vedere dinamica amenințărilor, tehnologiilor, precum şi schimbările care apar în organizație. Monitorizarea reprezintă o activitate importantă în evaluarea impactului de securitate al unui sistem informațional ce decurge din modificări planificate sau neplanificate în spațiul hardware, software, mediu de operare (incluzând spațiul de amenințare).

2.2. Model de monitorizare a securității la nivelul întregii organizații

Menținerea unei perspective actualizate asupra nivelului de securitate şi al riscurilor la nivelul întregii organizații este o activitate foarte complexă, care necesită implicarea întregii organizații (de la managementul executiv care oferă strategia şi până la nivel individual, în ceea ce priveşte dezvoltarea, implementarea şi operarea diferitelor sisteme ce suportă activitățile de zi cu zi) [PPIN08-01].

Figura 2.2 prezintă o abordare pe mai multe nivele a monitorizării securității din perspectivă organizațională. Deciziile legate de toleranța riscului care au fost luate la nivel executiv vor determina politica de monitorizare definită la nivelul 1, procedurile la nivelul 2 şi activitățile de implementare de la nivelul 3.

2.3 Considerații generale asupra politicilor de securitate

Politicile de securitate sunt fundația infrastructurii de securitate. Fără acestea, organizația nu poate fi protejată împotriva atacurilor de securitate, a disputelor juridice, şi publicității negative. O politică de securitate este un document sau set de documente care stabilesc practici, proceduri şi controale în scopul de a proteja resursele organizației, de a reduce probabilitatea incidentelor de securitate şi minimizarea impactului asupra organizației în cazul în care au loc, de a reducere sau elimina expunerea juridică față de angajați sau alte organizații [PNCN09].

O politică are menirea să influenţeze şi să determine decizii şi acţiuni. Standarde cum ar fi BS7799-2/ISO27001, ISO17799/ISO27002, RFC 2196 şi RFC 2504 pot fi utilizate ca punct de plecare în elaborarea unei politici de securitate solide pentru organizaţie. De exemplu, Controlul A.10.8 al standardului BS7799-2 stabileşte cerinţele pentru organizaţii de a dezvolta şi implementa o politică de securitate, precum şi controale în scopul reducerii riscurilor de securitate create de sistemul de poştă. În mod similar, standardul ISO17799 identifică un număr de riscuri de securitate specifice serviciului de poştă.

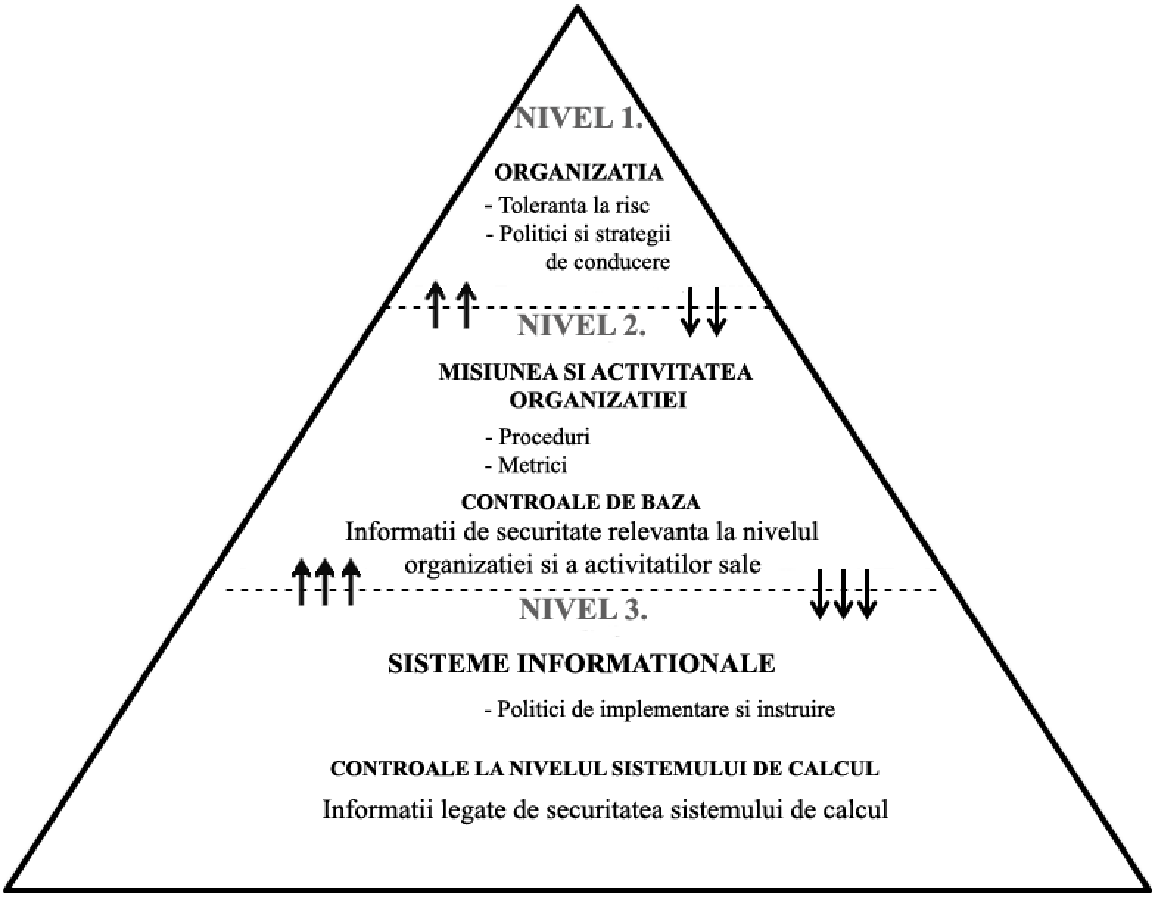


Figura 2.2 - Monitorizarea securităţii din perspectivă organizaţională [NIST SP 800-137]

În general o politică de securitate defineşte [Wol05]:

- Obiectivele de securitate: proprietăţile de confidenţialitate, integritate şi disponibilitate aşteptată de la sistem
- Regulile de securitate care sunt impuse mecanismelor care pot modifica starea de securitate a sistemului, pentru a garanta proprietăţile de securitate.

În elaborarea politicii de securitate a organizaţiei se vor lua în considerare următoarele aspecte [Lig06][Ort98][Ou04] [ISA00] [Kil03][BPN09]:

- *Consistenţa politicii* – aceasta trebuie să garanteze că plecând de la o stare de securitate nu se poate ajunge într-o stare de insecuritate fără violarea regulilor de securitate. Dintre cauzele care pot determina inconsistenţe se amintesc: conflicte între regulile funcţionale din cadrul sistemelor, obiective de securitate contradictorii, conflicte între regulile de securitate ale specificaţiilor de sistem, conflicte între regulile funcţionale şi obiectivele de securitate.

- *Cunoaşterea potenţialilor atacatori* - aceasta presupune identificarea motivaţiilor acestora, estimarea acţiunilor acestora şi a pagubelor pe care le pot produce. Măsurile de securitate nu pot face imposibil atacul, şi de aceea scopul principal stabilirea de controale de securitate care să depăşească abilitatea şi motivaţia atacatorului.
- *Costul* resurselor necesare implementării, menţinerii, precum şi al impactului asupra altor activităţi şi procese ale organizaţiei.
- *Cultura organizaţiei* - Este important ca organizaţiile să dezvolte şi adopte o politici care să reflecte cultura organizaţiei şi oferă totodată nivelul de securitate corespunzător riscurilor evaluate. Multe politici sunt dezvoltate utilizând şabloane sau exemple generice din alte organizaţii. Politicile de securitate nepotrivite culturii şi practicilor de activitate din organizaţie conduc adesea la nerespectarea lor pe scară largă.
- *Realismul şi suportul conducerii* - Politicile trebuie să fie realiste şi sprijinite explicit de către conducere. De acea, stabilirea unui program de monitorizare centrat în jurul organizaţiei şi misiunii sale, va avea asigurat suportul conducerii. Înainte de publicare, vor trebui adresate toate problemele şi aspectele legate de gradul de acceptare din partea utilizatorilor, precum şi costurile asociate schimbărilor sistemelor şi practicilor curente.
- *Culturalizarea politicii* – Securitatea este un comportament care se învaţă. Dacă utilizatorii nu conştientizează valoarea unei politici, nu o vor găsi necesară, şi astfel nu o vor urma. Utilizatorii vor trebui să înţeleagă o politică înainte de a li se cere să se conformeze acesteia. Un program de instruire eficace ar trebui să includă notificări prealabile asupra politicii din partea grupurilor responsabile cu elaborarea, şi implementarea acesteia. De îndată ce este publicată, se vor prezenta măsurile de monitorizare a conformării utilizatorilor şi perioada în care va intra în vigoare. Este importantă explicarea detaliată a procedurilor de obţinere a exceptărilor de la politică şi a raportării încălcării acesteia. Programul de instruire trebuie să includă notificări periodice către utilizatori şi management asupra problemelor de neconformitate până când acestea sunt rezolvate.
- *Urmărirea conformării şi măsuri disciplinare* – Odată cu politica este necesară şi elaborarea procedurilor de monitorizare a conformării şi a măsurilor disciplinare în caz de neconformare. Aceste proceduri de monitorizare au rolul de a detecta şi rezolva interpretările eronate sau încălcările politicii. Procedurile de management a incidentelor trebuie să adreseze modul de investigare şi colectare de evidenţe, şi cazul în care trebuie implicate autorităţile legale. Datele asupra gradului de conformare, excepţii şi violări trebuie comunicate în mod regulat conducerii asigurându-se atât informarea cât şi sprijinul acestora.

2.4 Procesul de implementare a unui program de monitorizare

O strategie bine definită de monitorizare a securităţii informaţionale adresează evaluarea controalelor de securitate, monitorizarea stării de securitate şi raportarea stării de securitate dintr-o perspectivă decizională orientată în jurul riscurilor. Elementele programului de monitorizare a securităţii sunt [PPN07-01] [PPIN08-01]:

- Definirea strategiei de monitorizare bazată pe toleranţa la risc ce asigură o vizibilitate asupra bunurilor, vigilenţă asupra vulnerabilităţilor, şi utilizează informaţii legate de ameninţări actuale sau în curs de cristalizare.
- Stabilirea de măsurători, şi metrici care [PPIN08-02] [PPN06-05]:

- ♦ determină starea de securitate a organizației
- ♦ detectează schimbările în infrastructura informațională a organizației
- ♦ detectează schimbările în mediile de operare
- ♦ mențin vizibilitate asupra bunurilor
- ♦ asigură un grad ridicat de informare asupra vulnerabilităților
- ♦ oferă informații asupra amenințărilor
- ♦ asigură eficiența controalelor de securitate într-o manieră care suportă operarea în limitele de toleranță de risc stabilite.

- Implementarea programului de monitorizare pentru a colecta datele necesare pentru metricile predefinite şi raportarea celor identificate; automatizarea colectării, analizei şi rapoartelor unde acest lucru este posibil.
- Analiza datelor colectate, raportarea celor identificate şi determinarea răspunsului corespunzător. În acest caz poate fi necesară colectarea de informații adiționale pentru a suplimenta datele de monitorizare existente.
- Răspunsul tehnic, managerial şi operațional pentru adresarea incidentelor sau acceptarea, transferul sau evitarea riscului.
- Revizuirea şi actualizarea programului pe o bază continuă, ajustând strategia de monitorizare, eficientizând capacitățile de măsurare pentru a creşte vizibilitatea asupra bunurilor şi vulnerabilităților; crearea de controale de securitate în organizație bazate pe datele de monitorizare; creşterea rezilienței organizaționale.

2.4.1. Definirea strategiei de monitorizare

Orice efort sau proces în suport al monitorizării securizării, trebuie să înceapă prin definirea unei strategii de monitorizare globale acoperind aspecte tehnologice, procesuale, procedurale, operaționale şi de personal uman. Elementele care vor fi luate în considerare în stabilirea strategiei sunt [PPN07-01] :

- Aspectele de toleranță a riscului în organizație
- Măsurători şi metrici pentru a oferi indicații edificatoare asupra stării de securizare la toate nivelele organizaționale
- Verificarea pe o bază continuă eficacitatea controalelor de securitate
- Menținerea vizibilității asupra inventarului cu bunuri ale organizației
- Controlul asupra schimbărilor prin managementul inventarului şi configurației
- Managementul proactiv al impactului asupra securității în cazul schimbărilor
- Vizibilitatea şi informarea asupra spațiului vulnerabilităților şi amenințărilor
- Necesitatea organizației de a stabili priorități şi a menține riscul în limitele de toleranță acceptate.

Un program eficace de monitorizare începe cu dezvoltarea unei strategii care adresează cerințele de monitorizare, şi activitățile la fiecare nivel organizațional descris în figura 2.2. În funcție de organizație pot exista suprapuneri între sarcinile şi activitățile efectuate la fiecare nivel. Fiecare nivel monitorizează metricile de securitate pentru a determina eficacitatea controalelor stabilite, şi frecvența de evaluare.

Eficacitatea controlului de securitate poate fi considerată ca o metrică de securitate în sine şi poate avea astfel asociată o frecvență de monitorizare a stării [PPIN08-02].

2.4.1.1 Strategia de monitorizare la nivel organizațional şi al misiunii sale

Responsabilii cu evaluarea riscului vor determina riscul de toleranță organizațional la nivel general precum şi strategia de adresare a riscului în contextul organizațional. Strategia de monitorizare şi programul sunt dezvoltate şi implementate pentru suportul managementului de risc în concordanță cu toleranța la risc a organizației. În mod uzual, strategia de monitorizare la nivelul organizației este dezvoltată la nivel organizațional, cu proceduri generale de implementare elaborate la nivelul misiunii sale.

Această informație este comunicată personalului de la toate nivelele, şi se va reflecta în politicile şi procedurile nivelelor misiune, şi sistem.

La nivelul organizației (management executiv) şi al misiunii (operațiilor) strategia de monitorizare poate include politici şi proceduri în suportul acesteia cum ar fi [NIST SP 800-137] :

- Politica de definire a metricilor cheie
- Politica pentru modificări şi întreținerea strategiei de monitorizare
- Politica şi procedurile pentru evaluarea eficacității controalelor de securitate
- Politica şi procedurile pentru monitorizarea stării de securitate
- Politica şi procedurile pentru raportarea stării de securitate (asupra eficienței controlului şi stării de monitorizare
- Politica şi procedurile pentru evaluarea riscurilor şi de obținere a informațiilor asupra amenințărilor
- Politica şi procedurile pentru managementul configurațiilor
- Politica şi procedurile pentru analiza impactului de securitate
- Politica şi procedurile pentru implementare şi utilizarea aplicațiilor la nivelul organizației
- Politica şi procedurile pentru stabilirea frecvențelor de monitorizare
- Politica şi procedurile pentru determinarea dimensiunii eşantionului şi populațiilor ce fac obiectul monitorizării
- Proceduri pentru determinarea măsurilor de securitate şi a evaluării riscurilor.
- Model pentru raportarea stării de securitate
- Politica şi procedurile pentru instruirea personalului implicat în monitorizarea securității. Instruirea include managementul şi utilizarea aplicațiilor, recunoaşterea şi răspunsul la incidente şi alerte pe baza metricilor, indicându-se când riscul depăşeşte riscurile acceptabile.

2.4.1.2 Strategia de monitorizare la nivelul sistemelor informaționale

Are la bază determinarea riscurilor asociate operării fiecărui sistem sau porțiune de infrastructură. Strategia şi programul de monitorizare la nivelul sistemului sunt dezvoltate şi implementate pentru suportul managementului de risc la nivelul întregii organizații, şi nu doar la nivel sistem, în concordanță cu riscul de toleranță asociat sistemului, cât şi celui organizațional.

Informația de securitate la acest nivel include evaluarea datelor legate de controalele de securitate la nivel sistem şi metricile obținute pe baza acestor controale de securitate. Grupurile şi departamentele care operează sistemele stabilesc strategia de monitorizare la nivel sistem luând în considerare factori tehnologici, arhitecturali,

specifici mediului de operare, dar şi cerinţele, politicile, procedurile şi modelele stabilite la nivelul organizaţional şi al celei de misiune [PPN06-03].

În general, strategia şi programul este definit la nivelul organizaţional şi al misiunii sale, iar politicile de implementare specifice sistemelor sunt dezvoltate la nivelul de bază.

Monitorizarea la nivel sistem va adresa monitorizarea controalelor de securitate din punct de vedere al eficacităţii, monitorizarea stării de securitate şi a raportării celor identificate.

Dacă iniţial monitorizarea stării de securitate viza identificarea ameninţărilor (detecţia intruziunilor), conceptul a fost ulterior extins şi către alte zone din sfera securităţii IT cum ar fi: monitorizarea conformării cu politica de securitate, monitorizarea eficacităţii controalelor de securitate, monitorizarea vulnerabilităţilor controalelor, etc [PPN09]

O soluţie de monitorizare completă, care va putea oferi informaţii de starea securităţii cat mai apropiate de realitate, va trebui să acopere toate aspectele de securitate prezentate în figura 2.3 cum ar fi [PNCN09].:

- Ameninţări – clasa de monitorizare ce urmăreşte detecţia atacurilor (de exemplu: sistemele IDS), şi constituie latura preponderent reactivă a soluţiei complete de monitorizare a securităţii
- Vulnerabilităţi - clasa de monitorizare ce urmăreşte identificarea sistemelor vulnerabile (de exemplu: scanere de vulnerabilităţi), şi constituie o componentă preponderent proactivă a monitorizării securităţii
- Controale - clasa de monitorizare ce urmăreşte gradului de conformare cu politica de securitate şi eficacitatea controalelor de securitate implementate. Aceasta constituie o componentă preponderent proactivă a monitorizării securităţii.
- Resurse - clasa de monitorizare ce urmăreşte realizarea şi menţinerea unui inventar actualizat al resurselor organizaţiei, configuraţiei, gradului curent de utilizare şi operare a acestora (de exemplu: sisteme de management de reţea, monitorizarea utilizare server, etc.). Aceasta constituie o componentă de suport a monitorizării securităţii.
- Risc - clasa de monitorizare ce urmăreşte evaluarea în timp real a riscului prezentat de intruziuni, pentru a ajuta la o mai bună prioritizare a răspunsului. Această este o componentă preponderent reactivă a soluţiei complete de monitorizare a securităţii. Un exemplu în acest sens ar fi componenta monitorizare a riscului utilizată de soluţia de monitorizare OSSIM (Open Source Security Information Management) [PPN08].
- Agenţi de ameninţare – este clasa care are rolul de a anticipa noi categorii de ameninţări, evoluţia acestora. Un exemplu în acest sens ar fi: monitorizarea forumurilor, site-urilor de socializare precum şi a altor resurse publice. Acest gen de clasă de monitorizare este prezentă în procesele de tip cyber intelligence.

Ca element de bază, eficacitatea tuturor controalelor de securitate este evaluată în concordanţă cu planul de securitate al sistemului şi cu metode specifice descrise în NIST 800-53A. Frecvenţa de evaluare este determinată de operatorii de sisteme pe baza cerinţelor primite de la toate cele trei niveluri.

Informaţia de securitate de la nivel sistem este utilizată pentru a determina starea de securitate la toate cele trei niveluri.

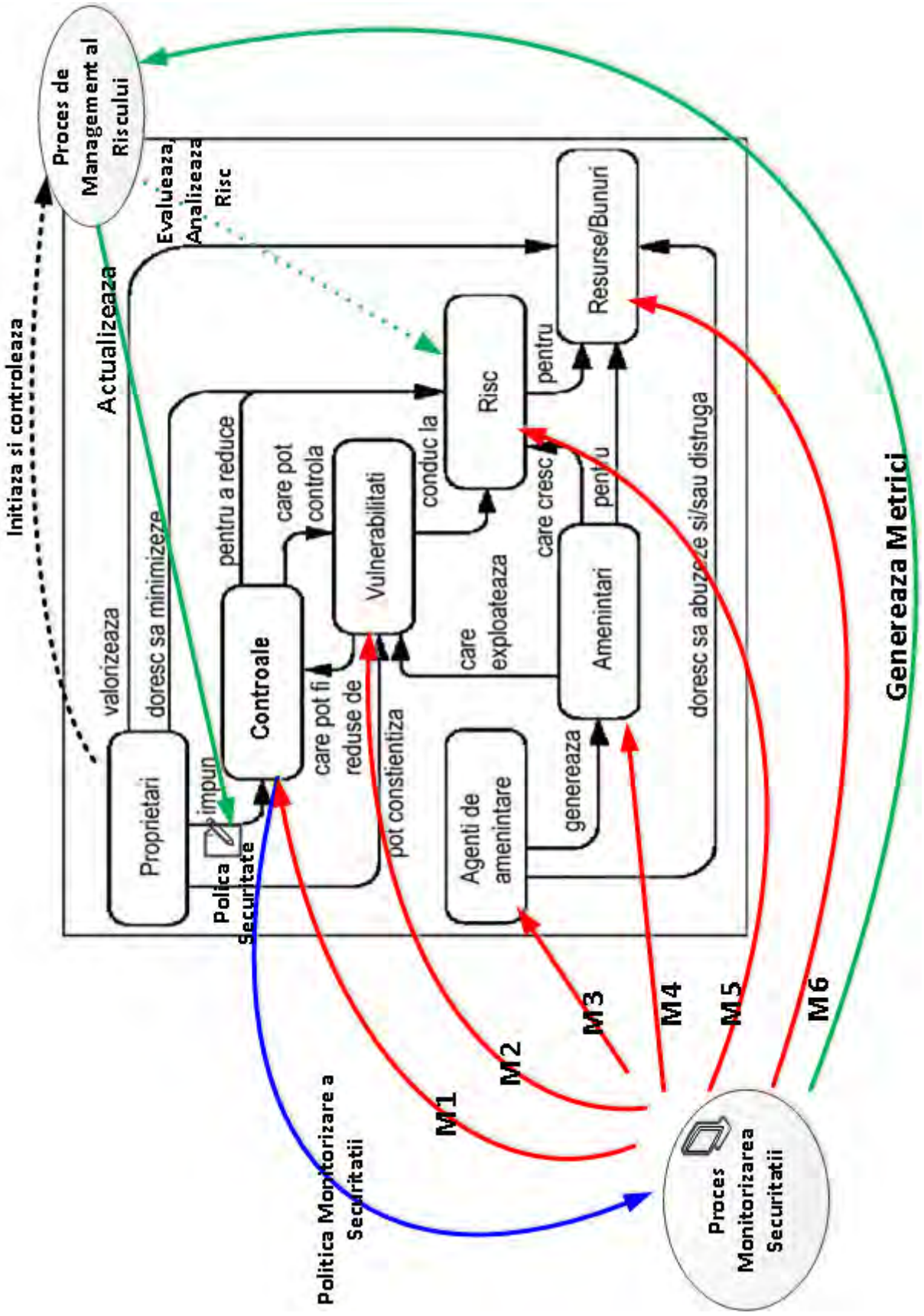


Figura 2.3 Relația dintre procesul de monitorizare a securității şi cel de management al riscului

2.4.2 Stabilirea de măsurători şi metrici

Asemenea oricărui alt proces, managementul efectiv al securității nu poate avea loc dacă aceasta nu poate fi ”măsurată”. Implementarea unor metrici de securitate este importantă pentru determinarea nivelului curent de securitate, pentru evaluarea eficienței controalelor de securitate implementate, pentru dezvoltarea unor proceduri operaționale adecvate, dar şi pentru suportul eforturilor de cercetare în domeniul securității [PPN06-05].

Acest subiect capătă o importanță în contextul în care organizațiile trebuie să se alinieze unor norme şi reglementări în domeniul asigurării securității care să demonstreze eforturi luate în direcția protejării datelor, cât şi în contextul economic actual în care resursele financiare sunt limitate. [SOX06]

În activitatea de măsurare a securității se utilizează următorii termeni definiți după cum urmează [DoD09]:

Definiție: **Măsurătoare** reprezintă date colectate care cuantifică o singură dimensiune a obiectului supus măsurătorii. Un exemplu în acest sens este numărul de vulnerabilități al unei aplicații.

Definiție: **Măsurarea** reprezintă procesul de efectuare de măsurători.

Definiție: **Metricile** (în literatura se utilează ca sinonim şi termenul de **măsură**) sunt măsurători care au fost structurate ca informație cu relevanță pentru procesul de elaborare a deciziilor.

Organizațiile determină măsurătorile şi metricele pentru evaluarea şi controlul riscului organizației.

Metricile sunt dezvoltate pe baza datelor de la nivel sistem astfel încât să rezulte informații cu relevanță pentru procesul de management de risc organizațional cât şi în contextul misiunii şi operațiilor sale. Metricile colectate la nivelul sistemelor şi rețelelor pot fi agregate iar informațiile relevante pentru factorii de decizie pot fi extrase pe baza acestora.

Măsurătorile includ toate informațiile cu relevanță de securitate din evaluări şi monitorizare obținute pe baza unor procese automatizate precum şi informații obținute pe cale manuală. Dacă măsurătorile reprezintă rezultatele la un moment dat de timp ale unor parametri măsurabili, metricile oferă o imagine mai completă (constând de regulă din câteva măsurători, valori de referință şi alte informații care oferă context de interpretare a măsurărilor).

Câteva exemple de măsurători sunt :

- Numărul şi severitatea vulnerabilităților identificate şi remediate
- Numărul componentelor neautorizate dintr-o rețea
- Activitatea autorizată
- Procentul de computere configurate corespunzător
- Procentul de sisteme care au testat planuri de situații de urgență
- Număr de angajați care sunt la curent cu cerințele programelor de instruire.

Câteva exemple de metrici sunt :

- Limitele de toleranță a riscului pentru organizație,
- Scoruri de risc asociat cu o anumită configurație sistem
- Scorul de securitate a unei arhitecturi ce urmează a fi creată în contextul arhitecturii existente şi a nevoilor organizaționale.

Un set corespunzător de metrici va fi **orientat către un obiectiv** şi va avea următoarele caracteristici [NIST800-33]:

- Specifică
- Măsurabilă
- Comparabilă
- Determinabilă
- Repetabilă şi
- Dependentă de timp.

2.4.2.1 Standarde şi metodologii pentru elaborarea metricilor de securitate

Codurile de practică şi standardele de securitate sunt utile ca un prim punct de plecare în definirea şi implementarea unui program de metrici în organizație. Acestea vizează cu precădere stabilirea de seturi de controale, însă modul de măsurare a calității şi aplicabilității acestor controale nu face obiectul acestora. [BS 7799, ISO 17799, NIST SP 800-33][BPN09]

SECMET (Security Metrics Consortium) a fost înființat pentru definirea unor metrici de securitate standard pentru companii şi a facilita adoptarea acestora de către factorii de decizii din companii. Un alt efort de standardizare este condus de MWG (Metrics Work Group) din cadrul ISSEA (International Systems Security Engineering Association). Acest grup este însărcinat totodată şi cu dezvoltarea de metrici pentru SSE-CMM (System Security Engineering-Capability Maturity Model). SSE-CMM a adoptat metodologia NIST SP 800-55 pentru dezvoltarea metricilor de securitate şi proces.

Grupul a propus 22 de arii de proces pentru dezvoltarea de metrici grupate în două secțiuni şi anume: practici de bază de securitate, şi practici de bază pentru proiecte şi organizații.

Între timp, organizațiile legislative din mai multe țări au elaborat proiecte şi reglementări care necesită măsurători în domeniul securității IT (HIPAA- Health Insurance Portability and Accountability Act, FISMA- Federal Information Security Management Act, The Data Protection Directive 95/46/EC a Parlamentului European).

Cele mai importante metode utilizate în dezvoltarea metricilor de securitate sunt:

- metodologia de evaluare a performanțelor IT (coordonată de Departamentul Apărării USA), care are următoarele componente: capabilități, nivel atribut şi metrici specifice.
- model bazat pe capabilități - un produs al SSE-CMM şi adresează capabilități funcționale cum ar fi: protecție, detecție şi răspuns.
- model orientat către rolul utilizatorilor (stakeholders) - abordează problematica metricilor din perspectiva rolului organizațional al utilizatorilor (responsabilitatea, interesul şi acțiunile acestora).

Dificultatea în procesul de definire şi elaborare a metricilor de securitate constă în formularea şi modelarea matematică a acestora. Metricile trebuie să fie de asemenea uşor de obținut şi de validat, şi să acopere toate dimensiunile securității IT incluzând organizația, componenta tehnologică precum şi pe cea operațională.

2.4.2.2 Metrici pentru evaluarea vulnerabilităților de securitate

Multe din strategiile de evaluare şi validare a securității sunt încă axate exclusiv pe proceduri de tip scanări de vulnerabilități, teste de penetrare, sau alte mijloace de identificare a deficiențelor în implementarea controalelor de securitate legate de protecția bunurilor organizației. Eficiența unor astfel de implementări este limitată în contextul numărului mare şi a frecvenței ridicate de noi vulnerabilități.

Pentru a determina urgența şi prioritatea de răspuns la vulnerabilități, organizațiile au nevoie de modele care să ia în calcul severitatea acestora. CVSS (Common Vulnerability Scoring System) este un model care oferă un scor al gradului de risc şi severitate al vulnerabilității. Scorul este determinat pe baza unor metrici care acoperă trei categorii distincte care pot fi măsurate cantitativ şi calitativ:

1. Metricile de bază conțin atribute care sunt intrinseci fiecărei vulnerabilități şi nu variază în funcție de timp sau mediu.
2. Metricile temporale conțin caracteristici ale vulnerabilității care se modifică pe durata de viață a vulnerabilității.
3. Metricile de mediu conțin acele caracteristici care sunt legate de o anumită configurație a implementării din mediul utilizatorului.

Setul de metrici utilizat în CVSS a fost identificat pe baza unui compromis între uşurința utilizării, acurateței şi acoperirea în detaliu, obținut după testări extensive a multiple seturi de vulnerabilități reale în diferite medii utilizator. [CVSS-09]

A. Metricile de bază

Setul de metrici de bază care acoperă trăsăturile de bază ale unei vulnerabilități sunt:

- **Vector de acces (VA)** - măsoară dacă vulnerabilitatea este exploatabilă local sau la distanță. Valorile posibile sunt {local, la distanță}
- **Complexitatea accesului (CA)** - măsoară gradul de complexitate al atacului necesar pentru exploatarea vulnerabilității odată ce atacatorul are acces la sistemul țintă. Valorile posibile sunt {mare, mică}
- **Autentificarea (A)** - măsoară dacă atacatorul trebuie să fie autentificat de sistemul țintă pentru a putea exploata vulnerabilitatea. Valorile posibile sunt: {necesară, nenecesară}
- **Impactul de confidențialitate (IC)** - măsoară impactul asupra confidențialității în cazul unei exploatări cu succes a vulnerabilității pe sistemul țintă. Valorile posibile sunt {fără impact, parțial, complet}.
- **Impactul de integritate (II)** - măsoară impactul asupra integrității în cazul unei exploatări cu succes a vulnerabilității pe sistemul țintă. Valorile posibile sunt: {fără impact, parțial, complet}
- **Impactul de disponibilitate (ID)** - măsoară impactul asupra disponibilității în cazul unei exploatări cu succes a vulnerabilității pe sistemul țintă. Valorile posibile sunt: {fără impact, parțial, complet}

- **Impactul de bias (prejudecată) (IB)** - permite acordarea unei ponderi mai mari unuia dintre cele trei metrici menționate anterior în detrimentul celorlalte două. Valoarea poate fi :
  - Normală - IC, II, ID, au aceeaşi pondere
  - Confidențialitate - dacă IC are pondere mai mare decât II şi ID
  - Integritate - dacă II are pondere mai mare decât IC şi ID
  - Disponibilitate - dacă ID are pondere mai mare decât IC şi II

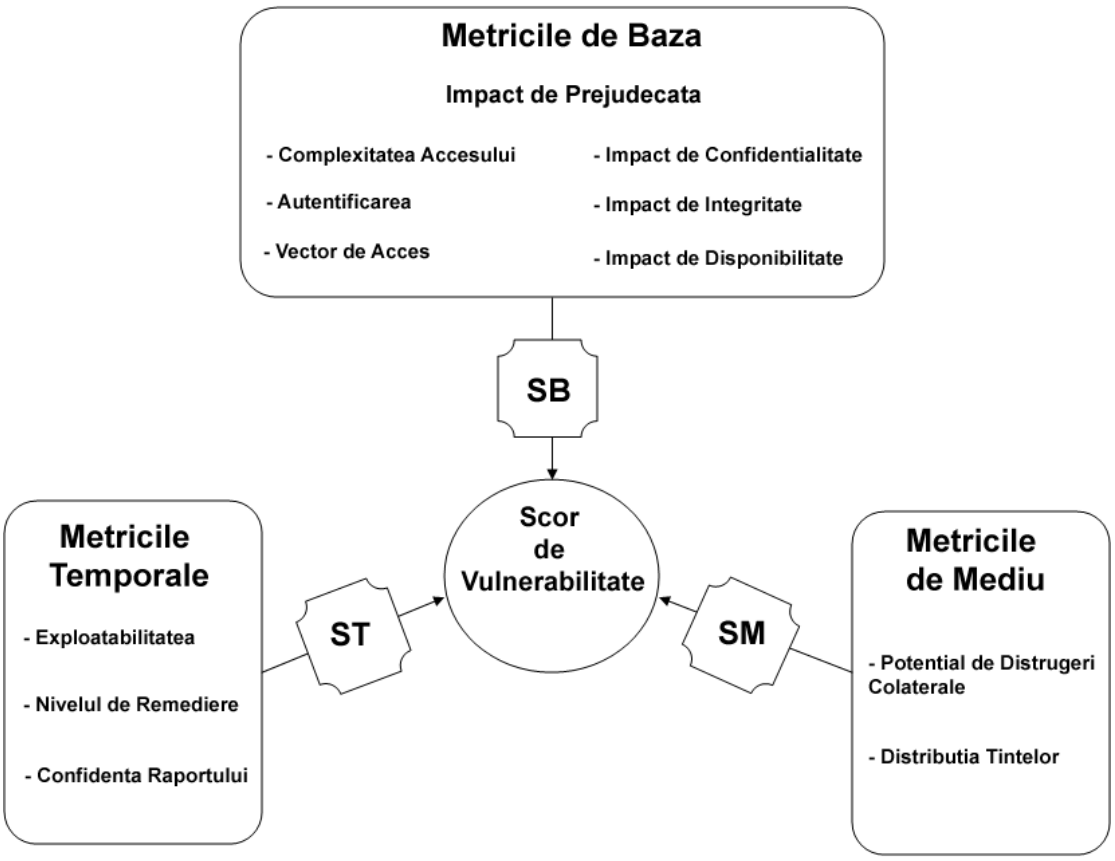


Figura 2.4 Model de evaluare a vulnerabilităților de securitate

B. Metricile temporale

Metricile temporale reprezintă trăsăturile dependente de timp ale vulnerabilității şi anume:

- **Exploatabilitatea (E)** - măsoară complexitatea procesului de exploatare a vulnerabilității pe sistemul țintă. Valorile posibile sunt: {nedovedită, în stadiu de validare a conceptului, funcțională, mare}.
- **Nivelul de remediere (NR)** - măsoară nivelul de disponibilitate a unei soluții. Valorile posibile sunt: {rezolvare permanentă, rezolvare temporară, soluție de moment, şi nedisponibilă}.
- **Confidența raportului (CR)** - măsoară gradul de confidență în existența vulnerabilității şi credibilitatea raportării acesteia. Valorile posibile sunt: {neconfirmată, neverificată, şi confirmată}.

C. Metricile de mediu

Metricile de mediu reprezintă trăsături specifice configurației implementării şi mediului de existență a vulnerabilității:

- **Potențial de distrugeri colaterale (PDC)** - măsoară potențialul de pierdere a unui echipament, distrugerea proprietății, pierderi de vieți sau accidente umane Valorile posibile sunt: {fără, scăzut, mediu, mare}.
- **Distribuția țintelor (DT)** - măsoară mărimea relativă a domeniului sistemelor țintă susceptibile la vulnerabilitate Valorile posibile sunt: {fără, scăzut, mediu, mare}.

Elaborarea scorului se face pe baza combinării tuturor valorilor metricilor pe baza formelor specifice prezentate mai jos :

1. **Scorul de bază (SB)**- este calculat de furnizor după cum urmează :

```
SB= round(10 * VA* CA *A * ((IC * IBC) + (II * IBI) + (IA * IBA))
```

Odată ce acesta este publicat, scorul de bază (SB) nu se va mai modifica şi va reprezenta fundația care va fi modificată de metricile temporare şi mediu. Scorul de bază are ponderea cea mai mare în scorul final şi reprezintă nivelul de severitate a vulnerabilității.

2. **Scorul temporal (ST)-** este calculat de furnizori după cum urmează :

```
ST= round(SB * E *  NR * CR)
```

şi permite introducerea factorilor de reducere a scorului vulnerabilității şi va fi reevaluat la intervale de timp specifice pe durata de viață a vulnerabilității. Acest scor reprezintă gradul de urgență al vulnerabilității la un moment dat de timp.

3. **Scorul de mediu (SM)**- este calculat în mod opțional de organizațiile utilizator şi ajustează cele două scoruri anterioare pe baza următoarei formule :

```
SM= Round((ST + ((10-ST) * PDC)) * DT)
```

Acest scor reprezintă o valoare la un moment dat de timp reprezentativă pentru un mediu anume. Organizația ar trebui să utilizeze acest scor, SM, pentru a prioritiza răspunsul la vulnerabilitate în cadrul mediului respectiv.

CVSS diferă de alte sisteme de scor a vulnerabilităților cum ar fi Microsoft Threat Scoring System, Symantec Threat Scoring System, Cert Velnerability Scoring sau Sans Critical Vulnerability Analysing Scale Rating) prin faptul că oferă un cadru deschis de clasificare a vulnerabilităților într-o manieră consistentă, cât şi posibilitatea de personalizare a acestora pentru fiecare mediu utilizator. Pe măsură ce CVSS se maturizează aceste metrici pot fi extinse sau ajustate pentru a-l face cât mai precis, flexibil şi reprezentativ pentru modul de adresare a claselor de vulnerabilități şi a riscurilor asociate cu acestea.

2.4.2.3 Metrici pentru evaluarea controalelor de securitate în sistemele informaționale

În multe organizații, măsurătorile legate de securitatea sistemelor informaționale sunt conduse adesea de echipe multiple care acționează în mod dependent pentru definirea, colectarea şi analiza metricilor tehnice.

Aceste metrici includ vulnerabilitățile identificate în scanările de rețea, raportarea incidentelor, estimarea pierderilor cauzate de evenimentele de securitate, rata de descoperire a defectelor de securitate în noile aplicații software, alerte ale sistemului de intruziune, numărul de emailuri infectate de viruşi interceptate, şi altele.

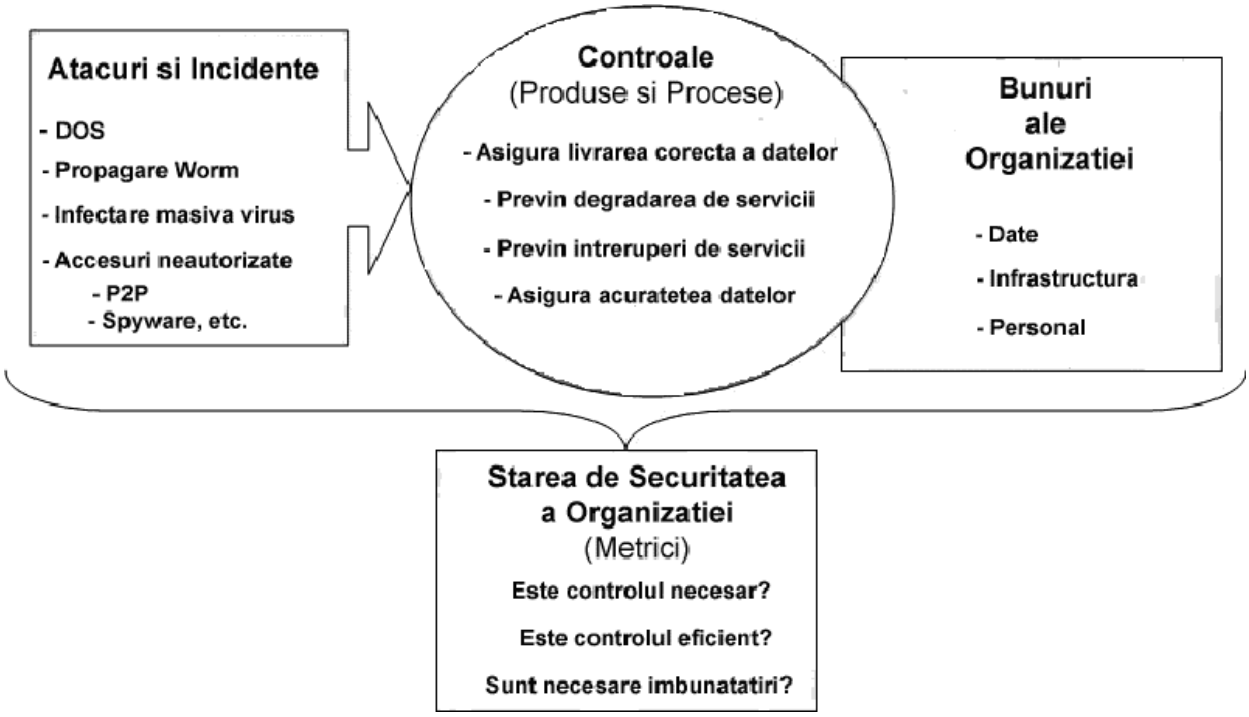


Figura 2.5 Model de securitate bazat pe metrici [PPN06-05]

Metricile de securitate descrise în această secțiune vizează integritatea şi disponibilitatea rețelei şi sistemelor. Alte aspecte precum valoarea bunurilor informaționale sau costul pierderilor, nu fac subiectul analizei.

În contextul unui model orientat pe rolul avut în organizație (Modelul stakeholders), utilizatorii vor urmări diferite aspecte legate de securitatea sistemelor.

Managementul de nivel executiv, ce corespunde nivelului organizațional şi misiune din figura 2.1 şi este responsabil cu performanțele de nivel general ale organizației, va fi interesat de capacitatea sistemului de a asigura suportul operațiilor organizației şi misiunilor acesteia. Având autoritatea de a aloca resurse (atât financiare cât şi de personal) pentru a adresa problemele de securitate a sistemelor şi infrastructurii, aceştia vor fi interesați în a avea răspunsul la următoarele întrebări:

- Gradul de securitate al organizației comparativ cu al altora similare din acelaşi domeniu de activitate
- Evoluția în timp a securității sistemelor
- Eficiența investițiilor efectuate în domeniul securității sistemelor şi infrastructurii
- Costurile şi consecințele când se consideră asumarea riscurilor asociate unor noi vulnerabilități.

Un exemplu de metrici de securitate la nivelul managementului ar fi:

- *Nivelul de serviciu al sistemelor* - procentul de disponibilitate a serviciilor sistemelor măsurat pe durata unui interval de timp specificat, precum şi evoluția acestuia.
- *Nivelul serviciului de rețea* - procentul de disponibilitate a serviciilor rețelei măsurat pe durata unui interval de timp specificat, precum şi evoluția acesteia.
- *Nivelul de satisfacere al cerințelor de business* - procentul de nevoi de business satisfăcute de infrastructura şi sistemele existente.
- *Numărul de compromiteri* - număr de incidente pe durata unei perioade date, în care rețeaua sau sistemele au fost compromise
- *Impactul compromiterilor asupra organizației* - pentru fiecare incident, numărul de ore, timpul şi personalul afectat de degradarea sau întreruperile cauzate de rețea, sisteme sau serviciile de aplicații.
- *Costurile şi beneficiile investițiilor* - costurile directe şi indirecte, precum şi beneficiile ca urmare a investițiilor legate de securitatea sistemelor

Echipa de securitate pentru rețea şi sisteme este în mod uzual responsabilă cu definirea controalelor de securitate şi este interesată de modul în care programele, procedurile şi politicile de securitate rezolvă cerințele impuse în acest sens.

- Dacă sistemele responsabile pentru compromitere erau conforme cu politica de securitate?
- Ce schimbări ar trebui făcute la politica şi procedurile de securitate?
- Dacă politica nu îşi atinge scopul ce aspecte comportamentale trebuie modificate la nivelul politicii pentru atingerea obiectivelor?
- Ce tehnologii ar putea ajuta prevenirea unor compromiteri viitoare?
- Care a fost impactul tehnic al compromiterii?

Echipa de securitate operațională este responsabilă cu menținerea unui nivel de securitate în limitele prevăzute de politica de securitate şi de regulă utilizează în decursul activităților de zi cu zi următoarele seturi de metrici:

- *Structura vulnerabilități* - este numărul cumulativ de vulnerabilități identificate în organizație clasificate după echipamentele conforme şi neconforme cu politica de securitate
- *Încercări de intruziune* - este numărul de încercări de intruziune
- *Încercări de acces neautorizat* - este procentul de accese neautorizate pentru diferite servicii de rețea sau sisteme
- *Rapoarte de conformitate detaliată* - este numărul de utilizatori şi echipamente conforme cu fiecare element al politicii de securitate
- *Impactul de compromitere* - va măsura utilizatorii afectați (datorată serviciului degradat, întrerupt), nivelul de date pierdut, modificat sau distrus; numărul de echipamente compromise; degradarea performanțelor rețelei şi sistemelor.
- *Scanări suspecte de porturi* - număr de scanări suspecte din organizație, timp de remediere, care este timpul între descoperirea compromiterii şi încheierea remedierii.

2.4.3 Implementarea programului de monitorizare

2.4.3.1 Categorii de date utilizate în procesul de monitorizare

Un prim pas al fazei de implementare constă în identificarea categoriilor de date care pot fi colectate şi utilizate în procesul de elaborare a metricilor definite. În cele mai multe cazuri, aceste categorii de date sunt [PPN06-02] [PPN07-01][PNCN09]:

- *Datele de trafic complete* - reprezintă totalitatea pachetelor de trafic colectate de senzori. În marea majoritate a cazurilor, acest tip de date reprezintă ”materia primă” pentru sistemele IDS de rețea. Totodată, ele sunt utilizate pentru analiza detaliată a alertelor, validarea intruziunilor, şi investigații post incident. Analiza şi corelațiile stabilite pe baza acestui date tip sunt de natură să confirme cu exactitate modul de operare a unui atac, precum şi validarea răspunsului implementat. Înregistrările complete de trafic prezintă două trăsături care le fac valoroase:
  - *granularitatea* (accesul la fiecare bit al pachetului de date face posibilă determinarea intruziunilor care nu ar fi posibil de detectat prin alte mijloace, cum ar fi utilizarea de către atacator a unei aplicații de canal ascuns) şi
  - *relevanța aplicației* (accesul la informația disponibilă nivelului aplicație permite o mai bună înțelegere a interacțiunii între cele două entități atunci când aceasta nu este criptată).
- *Datele de sesiune* - reprezintă sinteza schimbului de pachete între două stații. Elementele de bază ale datelor de sesiune includ: adresele IP şi porturile sursă/destinație, timpul de start al sesiunii şi o măsură a volumului de informații transferat pe durata sesiunii. Spre deosebire de sistemele IDS care urmăresc identificarea unei semnături sau anomalii, aplicațiile de colectare a datelor de sesiune vizează identificarea şi arhivarea tuturor sesiunilor vizibile senzorilor. Pe măsură ce încărcarea de trafic creşte, analiza acestui tip de date reprezintă cea mai simplă metodă pentru a urmările mişcările atacatorilor şi succesiunea acestora în timp. Deoarece adesea, colectarea datelor complete de trafic este imposibil sau foarte greu de realizat pentru legăturile de mare viteză, datele de sesiune reprezintă cea mai bună aproximare a conversației între două entități din rețea.
- *Datele statistice* – reprezintă o sinteza a traficului de rețea pe o perioadă mai mică sau mai mare de timp. Asemenea celor două tipuri de date prezentate anterior, şi acest tip de date este *neutru* din punct de vedere al conținutului comunicației între stații. Datele statistice pot fi de două categorii: *statistici descriptive* (rezultate ale agregării datelor de trafic complete într-o manieră clară şi coerentă, cum ar fi statisticile disponibile pe rutere) şi *statistici deduse* (unde rezultatele analizei efectuate asupra unui eşantion de populație reprezentativ, sunt extinse la întreaga populație).
- *Datele de pe sisteme* - sunt fişierele de jurnalizare generate de sistemele de operare, sau de aplicații (email, web, etc) ce rulează pe aceste sisteme, statistici despre încărcarea sistemelor, accesul utilizatorilor la resurse.
- *Alerte IDS* – Alertele sunt rezultatul unui proces prealabil de procesare şi analiză efectuat de sistemele IDS asupra datelor de trafic vizibil acestora (în cazul IDS de rețea) sau a datelor disponibile pe sisteme în cazul IDS de sistem. Pentru detectarea unor planuri de intruziune pe scară largă, este necesară corelarea tuturor datelor disponibile (alerte IDS din mai multe segmente de rețea ale

organizației, rutere, jurnale firewall, fişiere de log de pe staţii, date de sesiune şi date de trafic complete).

- *Date vulnerabilități* – sunt date generate de sistemele proprii de detecție a vulnerabilităților. Pot fi în format fişier, însă cele mai multe organizații au console pentru managementul şi prezentarea acestora
- *Notificări de neconformitate* – sunt generate de sistemele de monitorizate ce urmăresc gradul de conformare a staţiilor din organizație cu politica internă sau cu alte reglementări (de exemplu: sistemele ce procesează plăți electronice pe cărți de credit trebuie să se conforme unor practici şi standarde de domeniu cum are fi PCI (Payment Card Industry)
- *Date activitate utilizatori* – pentru minimizarea riscului anumite organizații monitorizează activitatea utilizatorilor cu privilegii sporite. De asemenea, având în vedere senzitivitatea datelor utilizate în procesul de monitorizare a securității, se recomandă monitorizarea activității personalului şi verificarea periodică a cazierului juridic a personalului implicat în acest proces
- *Date management a rețelei* – sunt date generate de sistemul de management ale rețelei care poate oferi indicații asupra activităților atipice din rețea.
- *Date alarme proactive ale sistemelor* – pot fi date statistice de timp real generate în organizațiile mari pe baza alarmelor de monitorizare a aplicațiilor din organizație (de exemplu: alarme simultane sau în volum neobişnuit al sistemelor de procesare a tranzacțiilor de business specifice)

2.4.3.2 Implementarea tehnică a soluției de monitorizare

O descriere detaliată a tehnologiilor de monitorizare ce pot fi utilizate pentru implementarea programului de monitorizare este descrisă în capitolul 3, iar modul de integrare a diverselor componente, precum, corelarea şi raportarea este descrisă în capitolul 4.

2.4.4 Răspunsul la incidentele de securitate

Incidentul reprezintă o violare a politicilor şi procedeelor de securitate ale organizației. Pentru a detecta şi răspunde eficace la aceste încălcări ale politicilor de securitate, este necesar ca organizația să dispună de politici şi proceduri de răspuns la incident.

2.4.4.1 Componentele procesului de tratare a incidentelor

Ghidul de tratare a incidentelor de securitate în sisteme de calcul NIST SP 800-61 prezintă principalele faze ale procesului de răspuns în caz de incidente:

1. ***Prepararea*** - Organizațiile trebuie să ia măsuri prealabile pentru a răspunde eficace în caz de incident. Acțiunile care se recomandă în această fază sunt:
   - Dezvoltarea de politici şi proceduri de tratare a incidentelor
   - Realizarea unui program de instruire şi exerciții periodice cu orientare specifică
   - Stabilirea în avans a unei echipei de răspuns la incidente (ERI) care va fi responsabilă pentru coordonarea răspunsurilor organizației în caz de incident
   - Stabilirea mai multor mecanisme de comunicare în scopul asigurării coordonării între membrii ERI, personalul tehnic, conducerea organizației chiar şi în cele mai nefavorabile situații.

2. ***Detecția şi analiza*** - În cazul unor incidente de tip ce afectează infrastructura de rețea (cum ar fi atacuri DOS, sau pe bază de viermi) o detecție şi validare în cel mai scurt timp este necesară pentru a evita contaminarea pe scară largă.

   O detecție cât mai rapidă poate ajuta organizația să minimizeze impactul incidentului, micşorând considerabil timpul şi costurile de refacere. Acțiunile ce se recomandă în această fază sunt [CBU--][DOE--]:

   - Monitorizarea buletinelor de notificare publicate de organizații cum ar fi US CERT (Computer Emergency Response Team), US DOE-CIAC (US Department of Energy Computer Incident Advisory Capability)
   - Monitorizarea alertelor şi evenimentelor de securitate produse de diverse controale tehnice cum ar fi: firewalls, IDS, antivirus, fişiere jurnal de pe sisteme (web, email, etc) etc.
   - Evaluarea datelor de incident din sursele inițiale cum ar fi rapoartele utilizator, sau ale personalului IT, şi controalele tehnice pentru a avea o înțelegere completă a mecanismului de intruziune .
   - Construirea unui set de aplicații ce va fi utilizat în identificarea intruziunii, şi a altor activități de analiză
   - Stabilirea unui set de criterii de prioritizare pe baza căruia se identifică nivelul corespunzător de răspuns pentru incidentele ce afectează rețeaua şi sistemele organizației.
3. ***Izolarea*** - Această fază vizează limitarea incidentului în vederea suprimării intruziunii. În cazul incidentelor de tip malware (viruşi, viermi) izolarea are două componente majore: stoparea propagării (compromiterii de noi sisteme) şi prevenirea efectuării de alte daune pe sistemele deja compromise. În adresarea incidentului, este important ca organizația să decidă asupra metodelor de izolare ce vor fi utilizate în faza inițială a răspunsului. Organizațiile vor trebui să aibă strategii şi proceduri disponibile pentru a lua deciziile legate de izolarea incidentului care să reflecte nivelul de risc acceptabil pentru organizație. Politicile organizaționale trebuie să stabilească clar persoana autorizată să ia decizii majore de izolare a incidentului şi circumstanțele aferente. Recomandările specifice acestei faze includ următoarele:

   - Identificarea stațiilor compromise de incident. Pentru organizațiile mari trebuie stabilite în prealabil metodele şi tehnicile de identificare a stațiilor din rețea
   - Dacă este cazul, şi este posibil, se vor oferi utilizatorilor instrucțiuni pentru a identifica dacă stațiile client au fost compromise şi măsurile ce ar trebui luate. Totuşi, organizațiile nu trebuie să se bazeze exclusiv pe utilizatori chiar şi în cazul izolării incidentelor care afectează organizația pe scară largă.
   - Dacă software-ul malițios nu poate fi identificat şi izolat prin actualizarea softwarelui antivirus, organizațiile trebuie să fie pregătite să utilizeze alte mijloace pentru izolare. Organizațiile trebuie să fie în măsură să trimită eşantioane de cod malițios furnizorului de aplicație pentru analiză, precum şi să contacteze organizațiile de răspuns la incidente şi furnizorii de antiviruşi atunci când este necesară consultarea în legătură cu modul de adresare a noilor amenințări.
   - Pentru izolarea incidentului, organizația trebuie să fie pregătită chiar şi pentru întreruperea totală sau blocarea serviciilor utilizate de programul malițios, inclusiv a aplicațiilor şi serviciilor de bază (web, e-mail, etc).
   - Organizația trebuie să fie în măsură să răspundă problemelor create de alte organizații ca urmare a dezactivării propriilor lor servicii în răspuns la un incident.

- Dacă situația o impune, organizația va dispune restricții suplimentare de conectivitate pe o durată limitată (de exemplu: suspendarea accesului la Internet, dezactivarea de porturi, rerutarea traficului, punerea în carantină a stațiilor compromise)

4. ***Eradicarea*** - Principalul obiectiv al acestei faze este eliminarea amenințării. Spre exemplu, în cazul atacurilor de tip malware se urmăreşte ştergerea aplicației malware din sistemele compromise. Pentru atacurile de tip DoS, obiectivul este blocarea completă a traficului de atac. Datorită necesității unor eforturi de eradicare relativ mari, organizațiile trebuie să fie pregătite să utilizeze concomitent diverse combinații de tehnici de eradicare în situații variate. Organizațiile trebuie sa aibă în vedere desfăşurarea prealabilă de activități de instruire care stabilească nivelul de aşteptare pentru eforturile de eradicare şi refacere în caz de incident.
5. ***Refacerea*** - Principalele aspecte ale acestei faze sunt restaurarea funcționalității şi a datelor pentru sistemele afectate de incident, şi ridicarea restricțiilor de conectivitate impuse pe durata fazei de izolare. Organizațiile trebuie să aibă în considerare scenariile cele mai nefavorabile şi modul de restaurare (spre exemplu: reinstalarea de la zero a sistemelor compromise, sau pe baza unei versiuni salvate anterior). Ridicarea restricțiilor de conectivitate se face atunci când numărul de stații compromise, sau vulnerabile este suficient de mic, iar eventuale incidente secundare au consecințe reduse.
6. ***Activități post-incident*** - Deoarece incidentele de securitate ce afectează sistemele pot fi destul de costisitoare, este necesar ca organizația să analizeze atent incidentul pentru a lua măsuri de îmbunătățire a defensivei şi modului de tratare a incidentelor în scopul prevenirii unor situații similare. Pe baza acestor măsuri, se vor determina schimbări în politica de securitate, schimbări în configurațiile sistemelor, cât şi amplasarea de controale de detecție şi prevenire a unor amenințări de acest gen.

Datorită ritmului destul de ridicat al apariției de noi amenințări, organizațiile trebuie să stabilească capabilități robuste şi flexibile de prevenire şi tratare a incidentelor pentru a adresa atât amenințările actuale cât şi cele pe termen scurt, şi cu posibilități de modificare pentru a adresa amenințări viitoare pe termen lung [PPN06-02]. Această ”competiție” continuă între amenințări şi defensivă impune organizațiilor să fie la curent în privința celor mai noi amenințări şi a controalelor de securitate disponibile pentru contracararea lor.

2.4.4.2 Clasificarea incidentelor

Definirea unei cadru formal pentru clasificarea incidentelor va permite colectarea într-o manieră mai eficientă a elementelor caracteristice incidentului ceea ce va permite [CBU--]:

- O reacție mai rapidă la incidente
- O comunicare mai bună atât între membri echipei de răspuns la incidente, cât şi în relația cu organizațiile naționale la care se raportează incidentele.
- Posibilitatea de a analiza diferite tendințe şi genera statistici

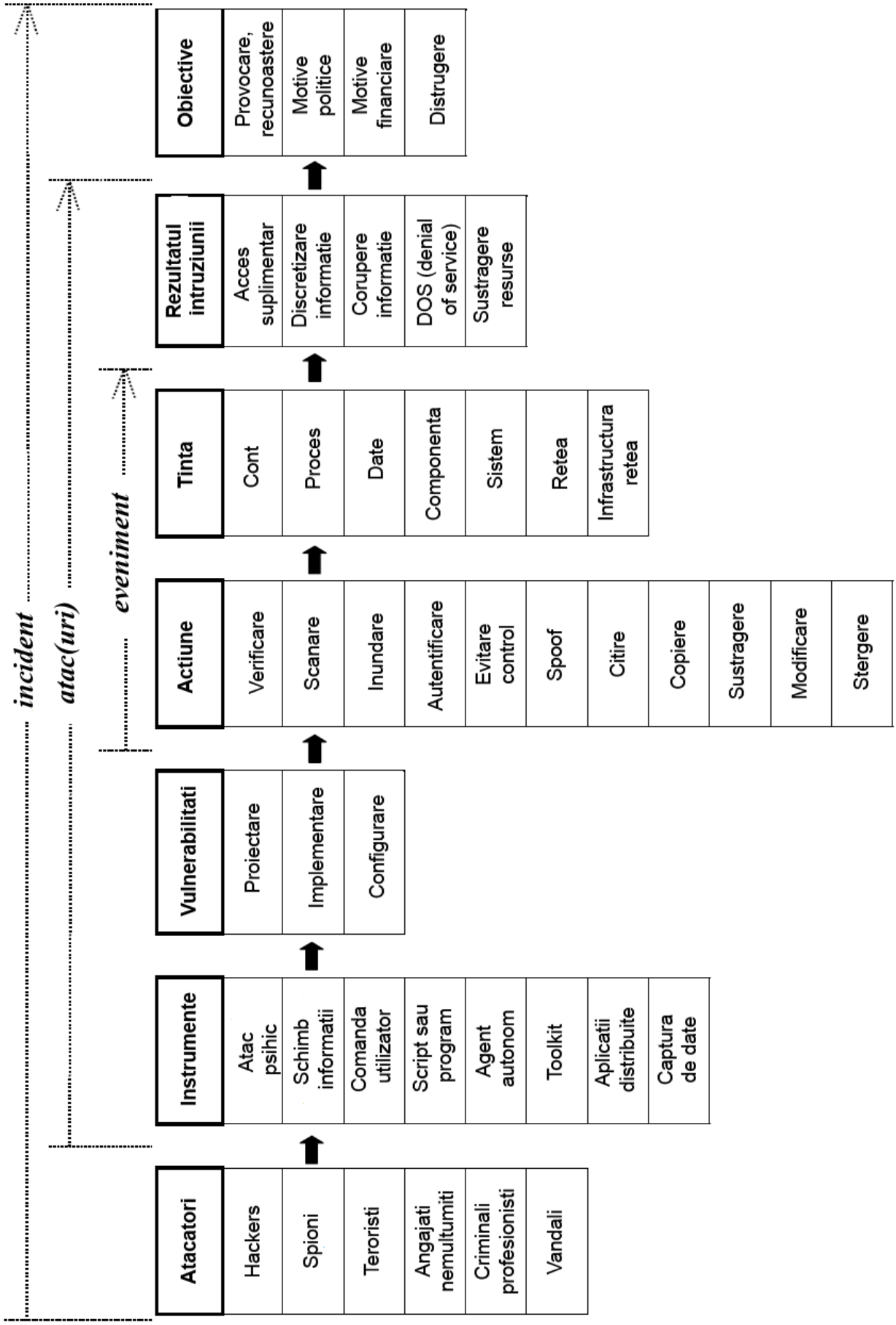


Figura 2.6 – Clasificarea incidentelor folosită de CERT US.

Organizațiile CERT naționale au create taxonomii pentru raportarea incidentelor, însă adopția a fost limitată doar la nivelul organizațiilor mari, din motive de complexitate, şi de resurse suplimentare necesare documentării detaliate asupra incidentului. Însă cea mai importantă utilitate a unor astfel de clasificări formale a fost de a oferi organizațiilor o mai bună înțelegere a terminologiilor precum şi un cadru eficient pentru construirea programelor de educare a personalului propriu.

2.4.5 Revizuirea şi actualizarea programului de monitorizare

Succesul unui program de monitorizare va fi determinat de o tratare procesuală acestuia, în care strategiile şi chiar programul în sine sunt reevaluate periodic, sau ca urmare a unor schimbări majore în organizație, în modul de operare al acesteia, sau în mediul în care aceasta acționează. Această reevaluare va asigura o operare care să țină seama de nivelele tolerabile de risc, relevanța metricilor utilizate, îmbunătățirea vizibilității asupra spațiului de amenințări, adresarea mai rapidă a vulnerabilităților, detecția şi răspunsul mai rapid la incidente.

Astfel, programul de monitorizare va trebui la rândul său monitorizat, astfel încât să opereze în concordanță cu obiectivele organizației, mediul operațional, şi amenințările momentului respectiv de timp.

Actualmente, multe organizații au implementat programe de răspuns la incidente, însă continuă să trateză atacurile ca evenimente singulare fără a colecta informații despre ele. Colectarea unor astfel de informații ar oferi posibilitatea de a analiza evoluția în timp a amenințărilor la adresa organizației, precum şi oportunitatea identificării unor riscuri structurale care să poată fi evaluate în procesul de analiză a riscului.

Pornind de la cadrul de lucru CERT (prezentat în secțiunea precedentă), compania Verizon a elaborat un cadru extins - VerIS (Verizon Incident Sharing) - ce permite colectarea şi analiza într-o manieră consistentă a informațiilor despre atacuri, astfel încât organizațiile să aibă o mai bună înțelegere a evenimentului, precum şi a impactului asupra organizației. Cadrul de lucru VerIS cuprinde patru secțiuni, fiecare captând aspecte diferite ale unui incident de securitate, şi anume [VER10]:

- *Aspecte demografice* - cum ar fi data incidentului, localizarea geografică, tipul activităților desfăşurate de organizație
- *Clasificarea incidentului* - fiecare incident (sau scenariu de amenințare) este modelat ca o serie de evenimente. Fiecare eveniment este descris pe baza unui model de amenințare ale cărui metrici (prezentate în figurile 2.7 –2.10) sunt grupate în următoarele categorii:
  - „*Asset*" – bunul valorizat şi protejat de organizație care a fost afectat
  - „*Agent*" – entitatea ale cărei activități au afectat bunul organizației
  - „*Action*" – activitățile efectuate sau declanşate de agent care au afectat bunul
  - „*Attributes*" – atributele de securitate ale bunului care au fost afectate
- *Descoperirea şi rezolvarea* - analizează evenimentele ce au urmat imediat incidentului şi concluziile rezultate. Metricile din această secțiune includ evoluția în timp a incidentului, modul în care incidentul a fost descoperit, resursele utilizate, controalele de securitate folosite şi dacă acestea au fost eficace
- *Clasificarea impactului* - detaliază pierderile directe de bunuri (date, sisteme, etc), întreruperi în operațiile organizației, costurile asociate răspunsului şi

refacerii, precum şi costurile indirecte (afectând imaginea organizației sau competitivitatea acesteia)

Utilizarea cadrului VerIS permite organizațiilor identificarea de trenduri pe baza cărora pot lua decizii de îmbunătățire a strategiilor şi tacticilor de securitate. Raportul de investigare a breşelor de date pe care Verizon îl produce anual (Verizon Data Breach Investigation Report), şi care este utilizat pe scară largă de comunitatea de securitate pentru a înțelege evoluția stării de securitate în Internet, utilizează date din răspunsurile la incident pe care Verizon le adresează şi care sunt structurate pe baza cadrului VerIS.

În mod tradițional evaluarea riscurilor are la bază scanările de vulnerabilități şi testele de penetrare, care testează în mod selectiv ceea ce se poate întâmpla. VerIS poate aduce o nouă dimensiune fazei de evaluare a procesului de management al riscului – cea bazată pe evidențe.

Asset		
Applications		
Enterprise application	Web application	Middleware
Servers and Systems		
Authentication server	DNS server	Payment switch/gateway
Backup server	Fax server	POS store controller
Chat/IM server	File server	Print server
Code repository	FTP server	Proxy server
Data warehouse	IDS/IPS server	Remote Access server
Database server	Log server	SCADA system
DHCP server	Mail server	Software distribution server
Directory server (LDAP, AD)	Mainframe	Terminal services server
Distributed Control System	Media server	Web server
Networks and NW Devices		
Private Branch Exchange (PBX)	Private WAN link/line	Hub
Demarcation point/device (ie, NID)	Public WAN link/line	Hardware security module (HSM)
Wiring closet	Mobile broadband network	IDS/IPS sensor
LAN cabling/jack	Modem bank Wireless Access Point	Remote Terminal Unit (RTU)
Telephone network/line	VoIP appliance	Programmable Logic Controller
Storage Area Network (SAN)	Router	Firewall
Wireless LAN	Switch	
End-User Devices		
Desktop computer	Uncontrolled computer	PIN entry device/Card reader
Laptop computer	POS system/terminal	Telephone
Smartphone	Self-service kiosk	VoIP phone
Mobile phone	Automated Teller Machine (ATM)	Printer/copier/scanner/fax
PDA	Pay at the Pump terminal	User authentication device
Offline Data		
Backup tapes	Exported data	Hard disk drive
Disks (CDs, DVD, Diskettes)	Flash drives/cards	Media player/recorder
Documents		
People		
Executive/Upper Mgt	Janitorial staff	Finance/Accounting staff
Auditor	Security staff	End-User
IT Administrator	Human resources staff	Partner
Developer	Help desk staff	Customer
Maintenance staff		
Facilities		
Camera/video device	Physical barriers (win, doors)	Uninterruptible Power Supply (UPS)
Fire suppression system	Physical security system	
HVAC system	Power infrastructure	Utilities infrastructure

Figura 2.7 - Model de amenințare VerIS – Metrici categoria „Asset"

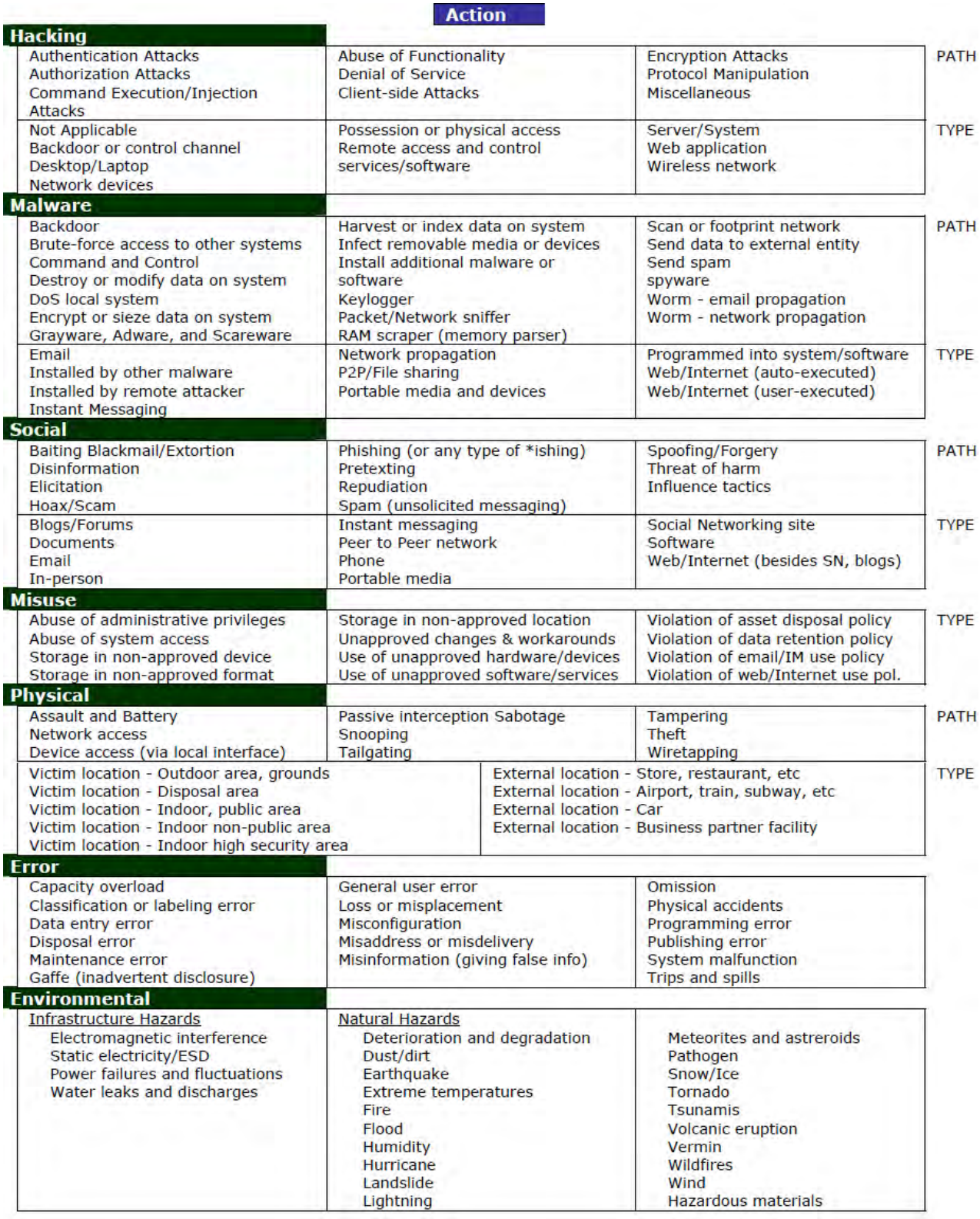


Figura 2.8 - Model de amenințare VerIS – Metrici categoria „Action”

Agent		
External		
Activist group Auditor Bot or Botnet Corporation	Customer (B2C) Force majeure Government	Maintenance/Construction crew Organized Criminal group Unaffiliated person(s)
Internal		
Auditor End-User Executive/Upper Mgt Finance/Accounting staff	Help desk staff Human resources staff Internal system or site IT/Security Admin	Janitorial staff Maintenance staff Security guard Software developer
Partner		
Auditor Data Processing and Analysis Hardware vendor Hosting provider Information/Content provider	Janitorial services Onsite IT management/support Security guard services Remote IT management/support Shipping/logistics provider	 Software as a Service provider Software developer/vendor Storage provider Telecommunications provider

Figura 2.9 - Model de amenințare VerIS – Metrici categoria „Agent”

Attributes		
Confidentiality	**Integrity**	**Availability**
Possession or Control	**Authenticity**	**Utility**

Figura 2.10 - Model de amenințare VerIS – Metrici categoria „Attributes”

Motto*: Nici o problemă nu poate rezista asaltului susţinut al gândirii.*
- Voltaire

CAPITOLUL 3

TEHNOLOGII DE MONITORIZARE A SECURITĂȚII

Există o multitudine de instrumente şi tehnologii disponibile pe care o organizație le poate folosi eficient şi eficace pentru obținerea, agregarea, analiza, şi raportarea datelor cu relevanță în procesul de monitorizare, începând de la nivelul componentelor individuale ale infrastructurii (echipamente de rețea, sisteme) şi până la nivelul managementului executiv cu atribuții de securitate.

3.1 Clase de tehnologii de monitorizare a securității

3.1.1 Tehnologii pentru culegerea directă a datelor

Tehnologiile de culegere directă a datelor sunt cele care permit observarea, detecția, prevenirea sau jurnalizarea amenințărilor şi vulnerabilităților de securitate cunoscute, precum şi managementul diferitelor aspecte ale controalelor de securitate implementate pentru a adresa acele amenințări şi vulnerabilități.

Clasele de tehnologii ce facilitează culegerea de date utilizate în procesul de monitorizare completă a securității sistemelor şi rețelelor organizației sunt [PPN09]:

- *Managementul vulnerabilităților* - Scanerele de porturi şi vulnerabilități sunt instrumente utilizate adesea de agenții de amenințare în faza de pregătire a atacurilor pentru identificarea de vulnerabilități ale echipamentelor din rețea, sistemelor de operare şi ale aplicațiilor uzuale. Organizațiile pot utiliza aceste instrumente pentru a identifica în mod proactiv gradul de expunere la vulnerabilități, identificarea versiunilor software neactualizate, cât şi pentru validarea conformității cu politica de securitate [NIST SP800-40v2].
- *Managementul patch-urilor* - Instrumentele de management al patch-urilor pot asista în identificarea automată a patch-urilor necesare pentru sistemele ce au fost identificate în prealabil având vulnerabilități, şi asistă administratorii de sistem în implementarea procesului de patch-ing [NIST SP800-40v2].
- *Managementul evenimentelor şi incidentelor* - Monitorizarea evenimentelor din sisteme sau rețele, şi analiza acestora pentru a identifica indicatori ai unor posibile intruziuni constituie baza detecției intruziunilor. Evenimente cu relevanță pentru procesul de securitate sunt disponibile în fişiere de jurnalizare şi traficul de rețea. Instrumentele în această categorie sunt: sniffere, sisteme IDS de rețea, sisteme IDS pentru stații, detectoare de intruziuni bazate pe fişiere de jurnalizare [NIST SP800-94] [NIST SP800-61] [NIST SP800-92].

- *Detecția Malware* - Oferă posibilitatea de a identifica şi raporta prezența de viruşi, troieni, spyware, sau a altor categorii de cod malițios pe sau destinat sistemului țintă. Organizațiile amplasează mecanisme de detecție Malware pe sistemele aflate în punctele de intrare/ieşire ale organizației : firewall, servere e-mail, servere web, servere de acces de distanță şi sistemele utilizator din rețea pentru a detecta şi şterge codul malițios transportat prin sistemul de poştă electronică, medii externe, sau acces web. Utilizate în conjuncție cu procedurile de management al configurației, precum şi controale de integritate a software-ului, mecanismele de detecție Malware, pot fi foarte eficiente în prevenirea execuției de cod neautorizat [NIST SP 800-83].
- *Managementul configurației* - Permite administratorilor să configureze şabloane de setări, să monitorizeze schimbări ale acestora şi să le restaureze atunci când este necesar. Managementul numeroaselor configurații întâlnite în sisteme şi elementele de rețea, a devenit imposibil de realizat utilizând metode manuale. Automatizarea soluțiilor de configurare precum şi a instrumentelor de scanare a configurației sistemelor, oferă abilitatea de a determina conformitatea cu o configurație de referință sigură [NIST SP 800-37].
- *Managementul rețelei* - Instrumentele din această categorie ajută la descoperirea stațiilor, inventarul acestora, controlul schimbărilor, monitorizarea performanțelor. Unele instrumente automatizează configurarea dispozitivelor şi managementul schimbării şi validează conformitatea dispozitivului cu politicile preconfigurate [NIST SP800-115].
- *Managementul inventarului de echipamente şi sisteme* – Instrumentele din această categorie (adesea combinând instrumente configurare a sistemelor, cele de management de rețea, sau a licențelor) ajută la menținerea inventarului, precum şi managementul modificărilor, hardware şi software din organizație [NIST SP 800-18].

3.1.2 Tehnologii pentru agregare şi analiză

Aceste tehnologii colectează date provenind de la unul sau mai multe controale de securitate, fie direct, fie prin intermediul tehnologiilor menționate în paragraful anterior, pentru a le corela, analiza şi reprezenta într-un format care să suporte luarea de decizii, sau evaluarea eficacității controlului [NIST SP 800-53]. Grupele de tehnologii reprezentative din această clasă sunt [PPN07-01]:

- *SIEM (Security Information and Event Management)* - Instrumentele SIEM sunt aplicații centralizate de management al fişierelor log sau al alertelor generate de sistemele IDS care permit agregarea, consolidarea, auditarea şi analiza înregistrărilor provenind din mai multe surse ale organizației. Produsele SIEM includ suport pentru mai multe tipuri de surse de înregistrări de audit cum ar fi: sisteme de operare, servere de aplicații, şi software de securitate. Serverul SIEM analizează datele provenind din surse multiple, corelează evenimentele şi identifică şi prioritizează pe cele mai importante dintre ele. Câteva produse din această categorie ar fi: Cisco MARS, HP OpenView, IBM Tivoli, OSSIM.
- *Console de management al securității* - Acest gen de instrumente consolidează şi comunică informația relevantă despre starea de securitate a organizației în timp real către personalul cu atribuții în zona managementului securității (administratori de sistem, personal de securitate, şi management executiv)

[NIST SP800-27]. Consola de securitate prezintă informații într-un format semnificativ şi uşor de interpretat.

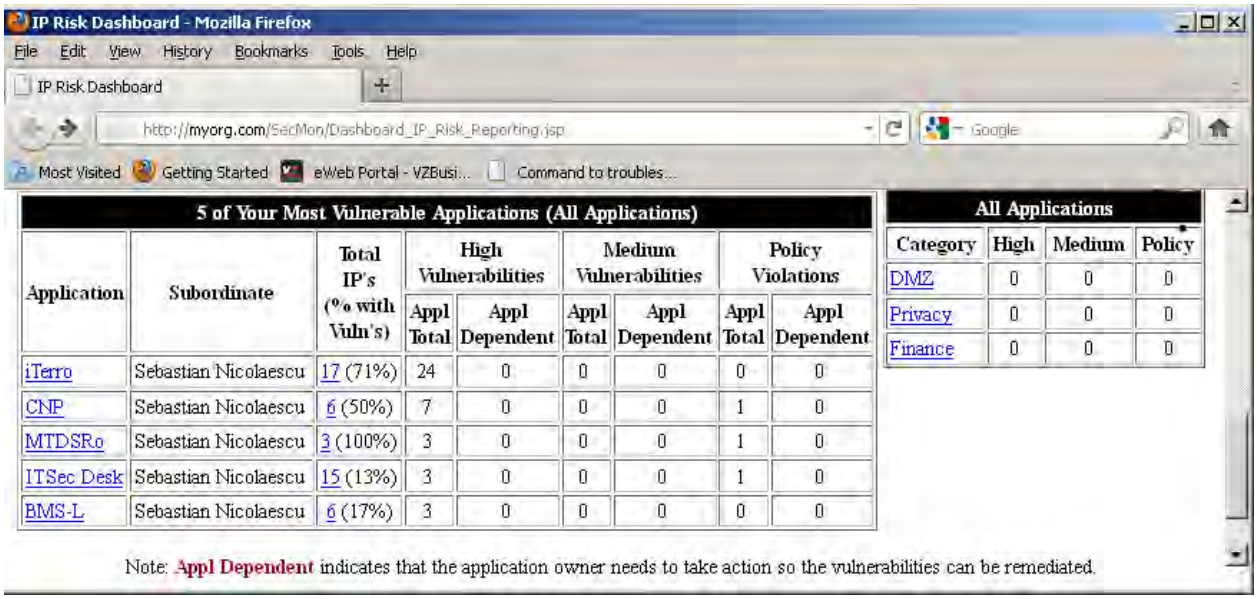


Figura 3.1 - Exemplu consolă de management a riscului (secțiunea vulnerabilități)

3.1.3 Tehnologii de automatizare

Automatizarea este o modalitate eficientă pentru a realiza o monitorizare cu caracter continuu în ceea ce priveşte captura, corelarea, analiza şi raportarea stării generale de securitate a organizației [NIST SP800-117].

Câteva exemple de activități de securitate automatizate includ :

- Scanarea vulnerabilităților şi aplicarea patch-urilor corespunzătoare.
- Activarea configurațiilor de securitate bazate pe setările din şablonul de securitate construit în prealabil
- Scanarea gradului de conformitate cu configurația de securitate predefinită
- Colectarea metricilor şi măsurătorilor de securitate şi raportarea acestora utilizând tehnologii de tip consolă.

Tehnologiile şi instrumentele prezentate în acest capitol, suportă o varietate de protocoale şi resurse permițând implementarea unor arhitecturi de monitorizare cu grad ridicat de interoperabilitate între componente.

3.2. Tehnologii de scanare a vulnerabilităților

Scanarea vulnerabilităților are la bază conceptul scanării de porturi. Scanerul de vulnerabilități identifică stațiile active şi porturile deschise pe acestea, furnizând însă şi informații cu privire la vulnerabilitățile asociate. Scanerele de vulnerabilități furnizează următoarele capabilități [NIST SP 800-115]:

- Identificarea stațiilor active din rețea
- Identificarea serviciilor active şi vulnerabile ale unei stații
- Identificarea sistemelor de operare şi a vulnerabilităților asociate acestora
- Identificarea setărilor eronate

- Stabilirea unei baze pentru testul de penetrare

Dintre beneficiile utilizării acestora de către organizație se amintesc [PNN10]:

- Reprezintă instrumente proactive pentru identificarea propriilor vulnerabilităților înaintea atacatorilor
- Oferă informații cu privire la modalitatea de eliminare a vulnerabilităților descoperite
- Reprezintă un mijloc relativ rapid şi uşor de utilizat cu ajutorul căruia se poate cuantifica gradul de expunere la vulnerabilități al organizației
- Identifică versiunile software ce trebuie actualizate, şi în conjuncție cu instrumentele de management al patch-urilor se determină actualizările necesare
- Validează conformitatea cu politica de securitate a organizației în ceea ce priveşte aplicațiile instalate, serviciile active, configurațiile sistemelor, etc.

Dintre limitările scanerelor de vulnerabilități se amintesc [PNN10]:

- Generează un volum de trafic de rețea mult mai mare scanerele de porturi, ceea ce necesită o planificare şi utilizare adecvată pentru a nu avea impact negativ asupra activităților operaționale ale organizației.
- Necesită actualizări constante ale bazei de date cu vulnerabilități pentru a putea recunoaşte vulnerabilitățile recente. Astfel, în alegerea scanerului de vulnerabilități trebuie avut în vedere frecvența cu care actualizările sunt disponibile
- Ineficiente în ceea ce priveşte detecția noilor tipuri de vulnerabilități

Pentru o organizație tipică, practicile de securitate operațională curente recomandă [NIST SP 800-40v2]:

- Scanarea de vulnerabilități a stațiilor la cel mult trei luni pentru sistemele fără importanță critică pentru organizație şi infrastructură, şi scanarea în regim continuu (monitorizarea permanentă) a sistemelor critice (firewall-urilor, baze de date, etc).
- Folosirea mai multor tipuri de scanere de vulnerabilități. O soluție poate fi o combinație de scaner comercial şi unul bazat pe surse deschise.

Rezultatele obținute în urma scanării vulnerabilităților trebuie documentate, iar deficiențele descoperite trebuie remediate după cum urmează:

- Actualizarea sau aplicarea de patch-uri de urgență sistemelor vulnerabile pentru eliminarea vulnerabilităților
- Deconectarea stațiile neautorizate şi dezactivarea serviciilor neutilizate
- Impunerea de controale de limitare a accesului la serviciile vulnerabile (la nivel de firewall, şi stație), în cazul în care remedierea necesită timp, iar serviciul nu poate fi oprit.
- Revizuirea controalelor de securitate pentru a asigura o rată de vulnerabilități scăzută

Unul din cele mai eficiente instrumente ce poate fi utilizat pentru scanarea de porturi şi care posedă şi elemente de bază în scanarea vulnerabilităților este Nmap [Nma--]. Nmap suportă o gamă variată de tehnici de scanare (ICMP, TCP, UDP), oferind totodată posibilități avansate de identificare a protocolului serviciilor, a adreselor IP,

scanare ascunsă, şi analize de filtrare a traficului. Scanările Nmap se desfăşoară în mai multe faze secvențiale după cum urmează :

- *Prescanări de scripturi* - motorul de scripting Nmap (MSN) utilizează o colecție de scripturi special destinate obținerii de informații adiționale despre sistemele țintă. Este activată de opțiunea –sC şi are loc doar când scripturile necesare sunt selectate (exemple de astfel de scripturi sunt: dhcp-discover şi broadcast-dns-service-discovery, care utilizează interogări de tip broadcast pentru a obține informații de la serviciile standard de rețea).
- *Enumerarea țintei* - pe baza specificatorilor de stație oferiți (poate fi combinație de DNS, adrese IP, notație CIDR), Nmap generează lista adreselor IP care vor fi scanate.
- *Descoperirea stațiilor* - scanarea începe prin descoperirea stațiilor active care astfel vor necesita o investigație mai amănunțită. Acest proces este numit descoperire stație (sau scanare ping). Nmap utilizează tehnici multiple de descoperire cum ar fi cereri ARP, sau combinații de interogări mai elaborate bazate pe TCP şi ICMP.
- *Rezoluția DNS inversă* - după determinarea stațiilor ce se vor scana, vor obține numele DNS inverse ale tuturor stațiilor active identificate de scanarea ping.
- *Scanarea porturilor* - este componenta principală a Nmap. Răspunsurile (sau lipsa de răspuns) asociate sondărilor trimise sunt utilizate pentru clasificarea stării porturilor (deschis, închis sau filtrat) de pe stația țintă.
- *Detecția versiunii* - pentru porturile care au fost deschise, Nmap poate trimite o varietate de probe pentru a determina versiunea de software care rulează pe stația țintă, verificând răspunsurile recepționate pe baza unei baze de date de semnături de servicii cunoscute.
- *Detecția sistemului de operare* - are la bază caracteristici specifice de implementare ale standardelor de rețea în diverse sisteme de operare. Pe baza măsurării acestei diferențe este adesea posibilă determinarea sistemului de operare care rulează pe stația țintă.
- *Traceroute* - Nmap conține o implementare optimizată de traceroute, identificând în paralel rutele de rețea pentru mai multe stații pe baza celor mai bune pachete de sondare generate în fazele de descoperire anterioare.
- *Scripturi de scanare* - majoritatea scripturilor motorului de scripting vor fi rulate în această fază, şi au ca rol detectarea vulnerabilităților serviciilor, identificarea de Malware, colectarea de informații adiționale din bazele de date şi alte servicii de rețea, precum şi detecția avansată a versiunii.
- *Rezultatele de ieşire* - Nmap colectează toate informațiile obținute şi le salvează într-un fişier sau le afişează pe ecran.

Nessus este un pachet de testare a vulnerabilităților ce poate realiza teste automate asupra unor rețele țintă, incluzând scanări ICMP, TCP şi UDP, testarea unor servicii de rețea (Apache, MySQL, Oracle, Microsoft IIS, şi altele), precum şi capacități de raportare a vulnerabilităților identificate [Nes--]. Nessus este unul dintre cele mai utilizate instrumente de scanare şi testare a rețelelor. Nessus are două componente (demon şi client) ce lucrează intr-o manieră distribuită permițând astfel un management şi control eficient. Rapoartele generate de Nessus sunt uşor de înțeles, concise conținând uneori alerte de tip “false pozitive”, astfel fiind necesar ca personalul de securitate să parcurgă manual raportul necesitând totodată un înalt nivel de cunoştințe şi experiență.

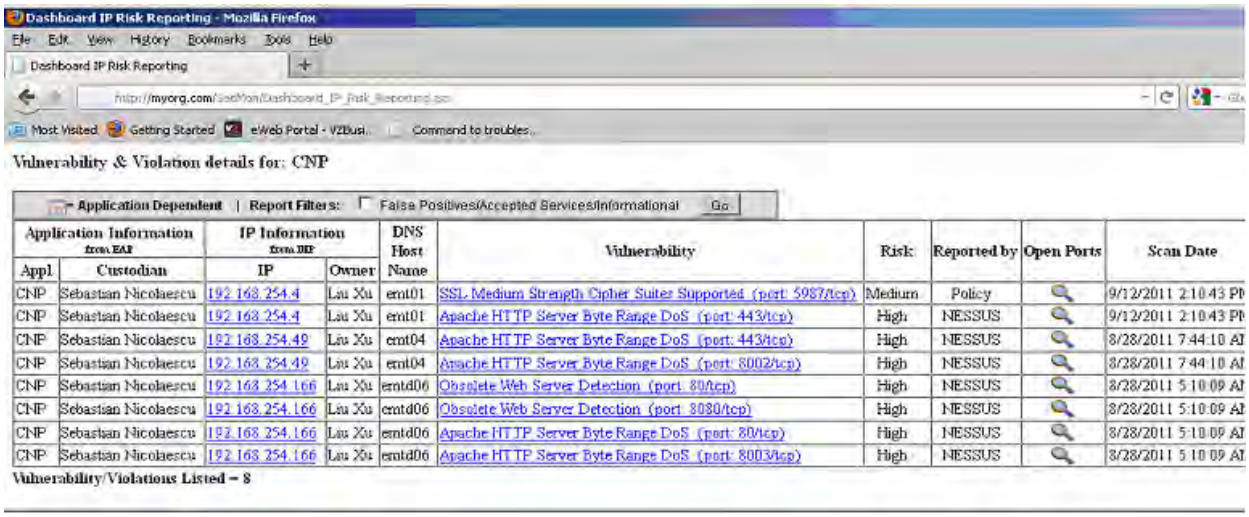


Figura 3.2 – Exemplu Ecran raport scanare Nessus

Metasploit Framework (MSF) este o platformă avansată de tip sursă deschisă pentru dezvoltarea, testarea şi utilizarea de programe de tip "exploatare". Inițial proiectul a pornit ca un joc de rețea, dar s-a dezvoltat pe parcurs devenind un instrument puternic folosit în testele de penetrare, dezvoltarea de programe de "exploatare" şi căutarea de vulnerabilități. Mediul şi scripturile de exploatare sunt scrise în Ruby şi pot rula pe aproape orice sistem de tip Unix şi Windows. Sistemul însuşi poate fi accesat şi controlat prin intermediul unui interpretor de comenzi sau a unei interfețe web [Met--].

Dintre pachetele comerciale, cel mai reprezentativ este eEye Retina [Eey--]. Acesta scanează vulnerabilitățile unei rețele dispunând de un sistem de management al remediilor prin care descoperă şi asistă la repararea tuturor vulnerabilităților de securitate cunoscute într-un sistem. Retina este uşor de configurat şi include instrumente avansate de raportare pentru a ajuta la izolarea şi sistematizarea remediilor necesare. În afară de faptul că dispune de cea mai completă bază de date de vulnerabilități cunoscute, Retina dispune şi de o tehnologie proprietară numită CHAM (Common Hacking Attack Methods) care emulează un comportament de tip hacker pentru penetrarea în adâncime a rețelei. În acest fel, Retina poate practic detecta vulnerabilități ascunse sau necunoscute anterior, oferind cunoştințele pentru o securizare mai bună a rețelei.

3.3 Tehnologii pentru detecția intruziunilor

Domeniul detecției intruziunilor a luat naştere odată cu documentul tehnic publicat de J. Anderson în 1980. Acesta propunea primul concept de detecție a anomaliilor în care informația de auditare putea fi folosită pentru identificarea abuzurilor ce aveau loc în sisteme [And80].

Principiul de operare al unui sistem de detecție a intruziunilor are la bază idea conform căreia activitățile în spațiul virtual (inclusiv cele asociate intruziunilor) nu se desfăşoară în vacuum, generând indicii şi urme. În multe cazuri, atacatorii „personalizează" sistemele compromise utilizând un set propriu de aplicații pentru a-şi consolida accesul (instalarea software captură activitate tastatură, spaming, activitate botnet, etc). În mod teoretic, un sistem de calcul are posibilitatea de a detecta astfel de modificări, iar

sistemele IDS încearcă să implementeze aceste capabilități şi să notifice asupra celor identificate.

Arhitectura de principiu a unui sistem pentru detecția intruziunilor (IDS) este prezentată în figura următoare.

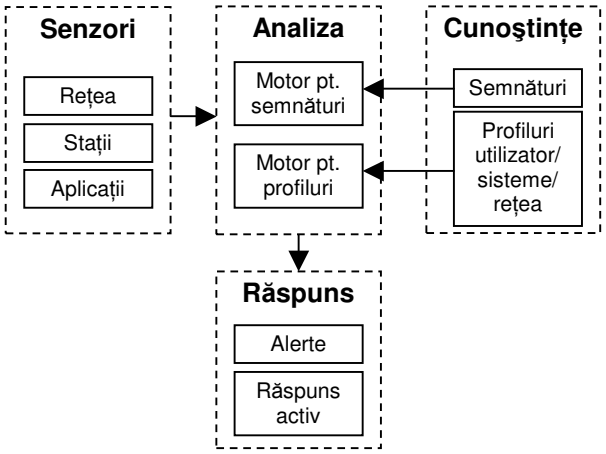


Figura 3.3 - Arhitectura generică a unui sistem IDS

În literatura de specialitate sunt disponibile mai multe clasificări ale sistemelor IDS, cele mai importante fiind după *proveniența datelor* şi după *tehnica de detecție* folosită.

În funcție de *proveniența datelor* utilizate în procesul de detecție (ceea ce dictează în mod implicit şi amplasarea acestora), soluțiile IDS se clasifică în *HIDS* (IDS bazate pe informații provenind de la stații) şi *NIDS* (IDS bazate de datele de trafic din rețea).

Un sistem HIDS monitorizează starea stației precum şi aspecte ale comportamentului său dinamic cu scopul de a determina încercări de violare a politicii de securitate a sistemului respectiv. HIDS utilizează în general o bază de date securizată cu obiecte sistem şi atributele de referință asociate acestora (permisiune, dimensiune, date modificare, etc.). În procesul de monitorizare se compară atributele curente ale obiectelor cu cele de referință, din baza de date.

Un sistem NDIS monitorizează pachetele de date din rețea (Snort, Bro), sau statisticile de trafic furnizate de echipamentele din rețea sau alte aplicații (Novell Analyzer, Microsoft Network Monitor) pentru a determina indicatori asupra activităților suspecte cum ar fi: scanări, propagări de viermi, atacuri DoS, etc..

În multe implementări de sisteme IDS comerciale, se combină aspecte specifice HIDS şi cele NIDS, aceste implementări fiind numite şi *NNIDS* (IDS de nod de rețea). NNIDS operează ca un NIDS hibrid la nivel de stație ce procesează traficul destinat către maşina respectivă. Aceste soluții hibride adresează limitările de vizibilitate ale NIDS clasic în ceea ce priveşte traficul de rețea criptat, oferind totodată o monitorizare eficientă la nivelul serviciilor (Web, SMTP, SSH, etc.) pentru identificarea încercărilor de violare a specificațiilor protocoalelor de nivel aplicație [PPN07-01] .

În funcție *tehnica de detecție* folosită, sistemele IDS au fost în mod tradițional grupate în două clase mari: sisteme bazate pe anomalii şi cele bazate pe semnături. În timp, o serie de noi tehnici au fost recunoscute în literatura de specialitate şi anume:

monitorizarea integrității, monitorizarea fişierelor de jurnalizare, tehnici capcană (honeypot), şi tehnicile hibride. [Ame10] [Pfl11]

În continuare se vor descrie tehnologii reprezentative de detecție a intruziunilor pe baza tehnicilor folosite.

3.3.1 Analiza fişierelor de jurnalizare

Analiza fişierelor de jurnalizare, denumită adesea în literatura comercială de specialitate LIDS (detecție de intruziuni bazată pe fişiere de jurnalizare) poate fi utilizată pentru a detecta utilizări necorespunzătoare ale sistemelor, sau violări ale politicii de securitate.

3.3.1.1 Soluții de analiză offline

Anumite soluții realizează analiza fişierelor de jurnalizare (log) pe o durata de timp şi generează rapoarte care pot fi evaluate ulterior de personalul de administrare sau de securitate. Acest gen de soluții rulează în mod uzual zilnic şi sunt benefice în identificarea evenimentelor pentru o analiză mai aprofundată de timp real. Rapoartele oferă de asemenea informații statistice care ajută în evaluarea tendințelor (detectarea de anomali). Totuşi aceste soluții au limitări în ceea ce priveşte adresarea situațiilor ce necesită un răspuns imediat. De exemplu, dacă un server web este inaccesibil, este necesar un răspuns imediat, iar identificarea acestei probleme pe baza acestui tip de soluție este inadecvată.

Logwatch este o soluție ajustabilă care analizează fişierele specificate de utilizator pe baza unor criterii alese de acesta şi generează rapoarte. Aplicația constă într-un set de scripturi Perl şi filtre care sunt simplu de configurat. Aceste criterii sunt furnizate ca opțiuni în linia de comandă. Soluția poate fi utilizată pentru analiza fişierelor de jurnalizare a programelor uzuale (cum ar fi Apache, sendmail, etc.), dar poate fi uşor configurată pentru a interpreta şi jurnalele altor categorii de aplicații [Log--].

SLAPS-2 (System Log Analysis & Profiling System 2) este o colecție de programe Perl utilizate pentru filtrarea fişierelor de jurnalizare sistem ce se colectează pe un server central. Aplicația produce o serie de rapoarte de analiză a operării sistemului care pot fi trimise prin email către o listă de utilizatori specificați. Această soluție adresează şi aspecte legate de rotația fişierelor de jurnalizare utilizate în decursul analizei [Sla--].

3.3.1.2 Soluții de analiză online

Analiza de timp real constă în acele soluții care rulează permanent şi monitorizează unul sau mai multe fişiere de jurnalizare. Aceste soluții au avantajul generării în timp real de alerte când sunt detectate anumite evenimente, însă cele mai multe dintre soluții sunt limitate în ceea ce priveşte adresarea situațiilor atipice.

SWatch (Simple Watchdog) a fost una din primele soluții create pentru monitorizarea fişierelor de jurnalizare. Aceasta filtrează datele care nu satisfac soluția de filtru, şi efectuează asupra datelor rămase un set de acțiuni specificate de utilizator. Când se identifică o linie în fişierul de jurnal care satisface condiția specificată de utilizator o poate salva, sau notifica administratorii. Soluția oferă suport pentru executarea unui set de acțiuni, cât şi pentru ignorarea evenimentelor duplicate. Deoarece examinează

secvențial evenimentele, funcția de corelație temporară lipseşte în acest caz [Swa--].

Logsurfer este o soluție mai eficientă care permite schimbarea dinamică a regulilor în timp sau în funcție de contextul evenimentelor identificate. Soluția permite o multitudine de opțiuni ce asigură un grad ridicat de flexibilitate, cum ar fi: specificarea de excepții, setare de timeout pentru reguli, specificarea de secvențe de identificare care pot fi ignorate, trimiterea rezultatelor prin email către anumite maşini, etc. *Logsurfer+* este o extensie care permite generarea de alerte când se detectează lipsa de mesaje şi permite de asemenea specificarea unui număr minim de evenimente care trebuie identificate pentru a genera o alertă. Această ultimă facilitate poate fi folosită pentru identificarea stărilor anormale, însă este necesară o evaluare prealabilă din partea utilizatorului pentru determinarea acestui prag de anomalie. [Dan--]

SEC (Simple Event Correlator) este o soluție bazată pe surse deschise, independentă de platformă care poate fi utilizată pentru corelarea de evenimente. Oferă un mod flexibil de introducere a datelor (pipeuri numite, intrare standard STDIN, sau nume fişiere normale) [Sec--]. Se utilizează o listă de reguli pe baza cărora se caută potriviri în liniile de intrare. O regulă SEC are următorul format [Ris05]

- Condiție de potrivire a evenimentului – sunt exprimate ca expresii regulare şi rutine Perl
- O listă de acțiuni - care vor fi efectuate în cazul satisfacerii condiției de potrivire. Dintre tipurile de acțiuni se amintesc: creare de contexte, invocarea unor programe externe, resetarea corelațiilor active.
- O valoare booleană - care controlează aplicabilitatea regulii la un moment dat de timp.

La momentul aplicării unei reguli se poate specifica un nume de context, permițându-se astfel corelarea evenimentelor pe bază de context.

Deşi are reguli statice, SEC oferă operații de corelare de nivel ridicat cum ar fi: potriviri explicite de perechi şi numărarea operațiilor. Spre exemplu, pe baza regulii SingleWithThreshold se poate contoriza numărul de apariții al unui eveniment A pe durata unui interval de timp dat, iar contorul este comparat cu o valoare de prag specificată în regulă. În cazul în care contorul depăşeşte valoarea de prag, o acțiune se va executa.

OSSEC este un sistem HIDS complex ce oferă şi servicii de analiză a fişierelor de jurnalizare. Această aplicație efectuează procesarea fişierelor log în trei etape [Oss--]:

- *Predecodare* - extrage câmpuri cunoscute din fişierele log precum timpul evenimentului
- *Decodare* – folosind decoderi definiți de utilizator pentru a extrage informații relevante din fişierele de jurnalizare care vor fi folosite în procesul de analiză
- *Analiză* – efectuează operații de tip potrivire asupra informațiilor decodate pe baza unei structuri arborescente de reguli atomice sau compozite. Structura arborescentă asigură utilizarea în procesul de analiză numai a sub-regulilor relevante pentru procesul de detecție respectiv. De exemplu, dacă se analizează o intrare legată de un eveniment SSH, nu se va traversa prin sub-arborele de reguli pentru evenimente Apache.

Un exemplu de procesare pe baza OSSEC a unei intrări dintr-un fişier de evenimente SSH este ilustrat în continuare.

3.3.1.3 Exemplu utilizare OSSEC pentru analiza fişierelor

1. OSSEC primeşte fişier de log SSH cu următoarea intrare

```
#intrare din fişier log
Sep 14 17:32:06 mylinux sshd[1025]: Accepted password for root from
192.168.1.101 port 1618 ssh2
```

2. După predecodare se obțin următoarele informații

```
# Informația după pasul de pre-decodare
time/date -> Sep14 17:32:06
hostname -> mylinux
program_name -> sshd
log -> Accepted password for root from 192.168.1.101 port 1618 ssh2
```

3. Decoderul SSH implicit OSSEC este definit după cum urmează

```
# Exemplu decoder SSH

   <decoder name="sshd">
      <program_name>^sshd</program_name>
   </decoder>

   <decoder name="sshd-success">
      <parent>sshd</parent>
      <prematch>^Accepted</prematch>
      <regex offset="after_prematch">^ \S+ for (\S+) from (\S+) port
      </regex>
      <order>user, srcip</order>
   </decoder>
```

4. După decodare informația arată după cum urmează

```
# Informația după pasul de decodare
time/date -> Sep14 17:32:06
hostname -> mylinux
program_name -> sshd
log -> Accepted password for root from 192.168.1.101 port 1618 ssh2
srcip -> 192.168.1.101
user -> root
```

5. Se defineşte regula de analiză 133 prin care se doreşte generarea unei alerte în caz de conectare din exteriorul rețelei `192.168.254.0/24` la stația cu numele `mylinux`.

```
# Exemplu regula analiza
# atributul level reprezintă gradul de severitate

   <rule id = "111" level = "5">
      <decoded_as>sshd</decoded_as>
      <description>Logging every decoded sshd message</description>
   </rule>

   <rule id="122" level="7">
      <if_sid>111</if_sid>
      <match>^Failed password</match>
      <description>Failed password attempt</description>
   </rule>

   <rule id="133" level="18">
      <if_sid>111</if_sid>
      <hostname>^mylinux</hostname>
      <srcip>!192.168.254.0/24</srcip>
      <description>Problema! Cineva din exterior s-a conectat ca la
      serverul mylinux </description>
   </rule>
```

6. Prin aplicarea regulii 133 asupra informațiilor decodate, se va genera o alertă întrucât conexiunea SSH la stația `mylinux` s-a efectuat de la o adresă (`192.168.1.101`) externă.

OSSEC oferă o funcționalitate de bază acceptabilă datorită numărului mare de decodere şi reguli pentru serviciile de bază. De asemenea, oferă posibilități de extensie pentru analiza fişierelor de jurnalizare a aplicațiilor proprietare prin definirea de noi decodere şi reguli. Totuşi, prezintă limitări în ceea ce priveşte capacitatea de detecție a evenimentelor de tip necunoscut.

3.3.2 Monitorizarea integrității fişierelor

Această categorie de monitorizare este capabilă să identifice şi raporteze modificări neautorizate asupra fişierelor. Se utilizează pentru protecția fişierelor critice (fişiere binare aplicație, sau fişiere de configurare a aplicațiilor şi serviciilor) şi care se consideră a fi statice între activitățile de actualizare a sistemului sau a configurațiilor acestuia. Această tehnică stabileşte în prealabil o sumă de verificare a fişierelor care se stochează într-o bază de date, după care verifică integritatea fişierelor monitorizate prin recalcularea sumei de verificare şi compararea cu cea înregistrată inițial în baza de date. O implementare reprezentativă pentru această clasă o reprezintă aplicația *Tripwire* [Kim94], al cărei principiu de funcționare se regăseşte şi în alte implementări cum ar fi AFICK [Afi--], OSSEC [Ose--].

În primă fază se creează politica de monitorizare a integrității prin identificarea fişierelor şi directoarelor ce trebuie monitorizate, şi stabilirea regulilor de identificare a intruziunilor şi a nivelului de verificare a integrității sistemului - atributele de fişier ce vor fi monitorizate cum ar fi: dimensiune, id utilizator, id group, timp ultim acces, timp ultimă modificare, număr de legături, număr iNode, permisiuni, etc.. Apoi, se inițializează baza de date care păstrează informații despre starea de referință a fişierelor ce vor fi monitorizate [Kim94].

Pe durata monitorizării se va compara informația de referință (din baza de date) cu atributele de stare actuală ale fişierului, iar în caz de discrepanță se generează un raport sau o alertă.

Pentru o securitate sporită a mecanismului de monitorizare a integrității, *Tripwire* criptează şi semnează propriile fişiere utilizând două chei criptografice pentru a detecta dacă a fost compromis [Tri--]:

- Cheia de site - protejează fişierul de politică şi cel de configurare
- Cheia locală - protejează baza de date şi rapoartele de discrepanță generate.

Pe lângă utilitatea în descoperirea intruziunilor şi a breşelor de securitate, monitorizarea integrității fişierelor poate servi şi la eficientizarea altor procese din organizație cum ar fi managementul modificărilor şi asigurarea conformității cu politica de securitate [Tri10].

3.3.3 Monitorizarea integrității sistemelor (detecția rootkit)

Monitorizarea integrității sistemelor are ca obiectiv detecția aplicațiilor malițioase de tip rootkit. Această categorie de malware permite acces privilegiat şi permanent asupra unui sistem, ascunzând în acelaşi timp prezentă sa prin modificarea unor funcții de bază ale sistemului de operare sau a altor aplicații. În mod uzual, atacatorul va instala un rootkit în faza de preluare a controlului asupra sistemului, care îi va permite mascarea intruziunii, precum şi menținerea accesului privilegiat la sistem prin ocolirea mecanismelor normale de autentificare sau autorizare. Detecția rootkit-urilor este dificil de realizat, deoarece acestea sunt capabile să schimbe funcțiile sistemului care sunt utilizate în procesul de identificare a aplicațiilor malițioase. [But05]

Detectoarele de tip Rootkit existente în momentul de față rulează local pe sistemul monitorizat, în mod similar tehnologiilor de tip antivirus. Implementările comerciale actuale efectuează detecția pe baza tehnicilor descrise în această secțiune.

3.3.3.1 Detectoare bazate pe semnătură

Aceasta este cea mai simplă tehnică utilizată în principal de aplicațiile de tip antivirus. Identificarea rootkitlui se face pe baza semnăturii unice a acestuia cum ar fi o anumită secvență de octeți în memorie sau existența unor anumite fişiere din sistem.

Chkrootkit este un exemplu de implementare care identifică modificări efectuate asupra fişierelor din sistem precum şi modulelor kernel încărcabile prin identificarea anumitor secvențe de octeți. Se caută de asemenea prezența altor indicatori specifici cum ar fi modificări asupra unor fişiere de tip log [Chk--].

3.3.3.2 Detectoare bazate pe integritate

Această tehnică este utilizată pentru a crea o sumă de verificare a obiectelor (fişierelor, zone de memorie) care se stochează apoi într-o bază de date. Periodic integritatea acestor obiecte sistem se verifică prin recalcularea sumei de verificare şi compararea cu cea înregistrată inițial în baza de date. Avantajul acestei tehnici față de cea bazată pe semnătură constă în posibilitatea de a detecta tipuri necunoscute de rootkit. Implementările în care obiectele monitorizare sunt doar fişiere, corespund cazului descris în secțiune monitorizării integrității fişierelor (3.3.2).

SVV (System Virginity Verifier) este un verificator de integritate a memoriei care compară componentele Windows utilizate în mod frecvent (de exemplu tabelele de funcții IRP, IDT, SSDT) cu o stare anterioară de referință validă. Acesta utilizează de asemenea componente euristice pentru a contoriza numărul de evenimente fals pozitive generate de aplicații autorizate precum software-ul antivirus ce rulează pe sistem [Rut05-2].

3.3.3.3 Detectoare de tip crossview

Tehnica a fost propusă inițial de Microsoft în proiectul Ghostbuster [Wan05] şi permite detecția rootkit-urilor ascunse în diferite nivele între spațiul utilizator şi cel kernel prin combinarea unor seturi variate de interogări ce conferă perspective multiple asupra sistemului. Implementările existente au la bază două tipuri de scanări [Rut05-1]:

- Scanare *inside the box* - permite obținerea unei perspective de nivel utilizator prin interogarea API-urilor de enumerare OS, care se compară cu o altă perspectivă generată prin inspectarea directă a structurilor de date kernel. O diferență între rezultatele nivelului utilizator şi cel kernel indică prezența rootkit-ului între aceste 2 spații. Implementările Revealer (Microsoft) şi Blacklight (F-Secure) utilizează acest tip de scanare pentru detecția proceselor şi fişierelor ascunse.
- Scanare *outside the box* - compară rezultatul unei perspective de nivel kernel obținută pe sistemul verificat, cu rezultatul unei perspective similare, obținute pe un sistem neinfectat. O modalitate de a obține un sistem neinfectat este de a reboota sistemului monitorizat şi încărca un kernel neinfectat (utilizând un mediu extern). O diferență între aceste două perspective indică prezența rootkit-ului la nivel kernel. Eficacitatea acestei tehnici de detecție depinde în mare măsură de modul de implementare a soluției. O implementare pentru sisteme de tip Windows ce utilizează acest tip de scanare este Klister [Sec05].

3.3.3.4 Detectoare bazate pe comportament

Interceptarea apelurilor de funcții, mesajelor sau evenimentelor transferate între componentele software, poate constitui mijlocul prin care se poate modifica comportamentului sistemului de operare sau aplicațiilor. În literatura de specialitate, codul care se ocupă cu interceptarea apelurilor de funcții, mesajelor sau evenimentelor se numeşte hook.

VICE este un detector de rootkit pentru Windows care verifică punctele de interceptare ale proceselor din spațiul utilizator cât şi din cel kernel. VICE instalează un driver care scanează kernel-ul pentru identificarea elementelor de interceptare. Politica utilizată în căutarea punctelor de interceptare la nivel proces este bazată pe principiul conform căruia fiecare pointer de funcție trebuie să rezolve către o adresă de cod în spațiul procesului sau al kernelui. În căutarea punctelor de interceptare în spațiul kernel, VICE verifică următoarele structuri de date kernel [But04]:

- Tabelele IDT (Interrupt Descriptor Table) şi SSDT (System Service Descriptor Table) pentru a confirma că pointerii de funcție rezolvă către spațiul de cod kernel.
- Tabelele de funcții IRP (I/O Request Packet) în drivere şi verifică dacă acestea pointează către zone de cod din spațiul driverului, iar apoi,

- Tabele IAT(Import Address Table) şi EAT (Export Address Table) din spațiul procesului pentru a identifica prezența unui element de interceptare.

Totuşi VICE are o rată mare de alarme false, deoarece multe aplicații Windows încorporează în construcția lor principii de interceptare.

Patchtfinder utilizează o metodă de creare a profilului căii de execuție la momentul rulării. Idea acestei soluții are la bază observația că rootkitul trebuie să adauge cod la o anumită cale de execuție pentru efectuarea unor activități adiționale [Sec04]. Acesta utilizează trăsătura procesoarelor X86 de contorizare a numărului de instrucțiuni executate. Tehnica are câteva limitări în ceea ce priveşte:

- Performanțele sistemului - modul de execuție al procesorului va necesita oprirea rulării după fiecare instrucțiune şi apelarea unei rutine de întrerupere de serviciu pentru actualizarea contorul de instrucțiune.
- Acuratețea alertelor - metoda conduce către un comportament nedeterminist când este utilizată în sisteme de operare complexe (precum Windows) datorită întrepătrunderilor căilor de control, ceea ce conduce către alarme false [Rut04] .

3.3.4 Detecția intruziunilor cu sisteme capcană (honeypot)

Honey-pots reprezintă o tehnică flexibilă utilizată în principal de companiile de produse antivirus şi agenții guvernamentale pentru culegerea de informații despre noile tipuri de amenințări. În principiu, se monitorizează un spațiu de adrese neutilizat în activitatea normală (numit în literatura de specialitate şi “Black Hole”), iar identificarea de trafic destinat către acest spațiu reprezentând un atac în curs de desfăşurare.

Spre deosebire de sistemele de detecție clasice, al căror rol este de a identifica intruziuni în curs de desfăşurare pentru a le stopa, sistemele capcană au fost create pentru a capta atacurile direcționate asupra organizației, protejând sistemele reale şi oferind totodată informații despre atacatori şi metodele folosite. Performanța unui honeypot depinde de modul de adresare în cadrul implementării a unor probleme pe care le poate prezenta un astfel de sistem, cum ar fi [Coh05]:

Identificarea. Sistemele de tip capcană oferă mai multă sau mai puțină interacțiune şi pot răspunde mai multor obiective cum ar fi încetinirea propagării atacurilor pe bază de viermi, detectarea acceselor neautorizate, colectarea de informații despre atacatori. Valoarea sistemelor capcană este diminuată dacă identitatea lor reală este divulgată. Odată detectat, un atacator poate să evite sistemul capcană, sau să-l alimenteze cu informații false, derutante. Exceptând cazul când o organizație face cunoscut faptul că utilizează sisteme capcană pentru a descuraja atacurile asupra sistemelor sale, este important ca sistemul capcană să nu fie detectabil. Chiar dacă este identificat, el poate avea un rol în infrastructura de securitate, semnalând atacul asupra rețelei interne prin acționarea unei alarme. În cazul în care se doreşte mai mult decât atât, colectarea de informații despre atacator şi metodele folosite, programul pentru emularea capcanei trebuie modificat. Cu cât comportamentul sistemului „capcană” este modificat mai mult față de parametrii impliciți definiți de producător, determinând răspunsuri neaşteptate de atacatori, cu atât scad şansele ca identitatea acestuia să fie relevată.

Exploatarea. Chiar şi în cazul unor sisteme capcană cu interacțiune scăzută, ce nu oferă un sistem real ce poate fi compromis, ci emulează doar nişte servicii, există riscul ca aceste sisteme să fie compromise. Din acest motiv se impune o securizare maximă

sistemului de operare, pe care este instalată aplicația capcană, prin aplicarea patchurilor şi modificarea parametrilor impliciți de acces: servicii, conturi, parole, resurse partajate în rețea. Ca măsură suplimentară este recomandată instalarea unui firewall local pe maşina care rulează aplicația capcană. Sistemele capcană cu nivel ridicat de interacțiune, care oferă un mediu real la dispoziția atacatorilor trebuie protejate prin sisteme externe de protecție: limitarea benzii de comunicație, instalarea unui sistem de detectare a intruziunilor, monitorizarea atentă a tuturor acțiunilor întreprinse asupra sistemului capcană.

Relevanța. Majoritatea atacurilor, mai ales cele venite din exterior prin Internet sunt efectuate prin instrumente automate care încearcă să exploateze vulnerabilități publice. Aceste atacuri pot fi relativ uşor contracarate prin aplicarea unor măsuri elementare de securitate cum ar fie modificarea parametrilor impliciți de acces, instalarea unui firewall şi a unui sistem de detectare a intruziunilor. Amenințarea serioasă o prezintă atacurile lansate de persoane cu cunoştințe avansate, care au informații despre vulnerabilități încă nedescoperite de producătorii de software, şi pentru care nu există patchuri disponibile. Pentru a surprinde astfel de atacuri este necesară ajustarea particulară a sistemului „capcană" pentru fiecare tip de atac ce se doreşte a fi capturat. De exemplu, pentru a depista şi demonstra o eventuală fraudă de date (cum ar fi efectuarea unei copieri neautorizate de numere de cărți de credit), activitățile detectate de scanare a rețelei şi penetrarea sistemului de acces la serverul capcană nu identifică implicit şi tentativa de furt a datelor. Această tentativă de fraudă nu va fi captată dacă sistemul capcană nu simulează valoarea căutată de infractor: baza de date centrală a sistemului de cărți de credit. Rezolvarea acestui impediment, a lipsei de relevanță a informațiilor oferite de capcană, va necesita particularizarea sistemului capcană astfel încât să poată obține probe solide (şi din punct de vedere juridic) în ceea ce priveşte scopul atacatorului.

3.3.5 Detecția pe bază de anomalii

Detecția anomaliilor nu vizează intruziunile cunoscute, ci anormalități în traficul de rețea şi al comportamentului sistemelor. Construcția unui astfel de detector începe prin crearea unor cunoştințe (profiluri de metrici) a ceea ce înseamnă trafic normal, şi a pragurilor de deviație sau altor reguli pe baza cărora se vor genera alerte.

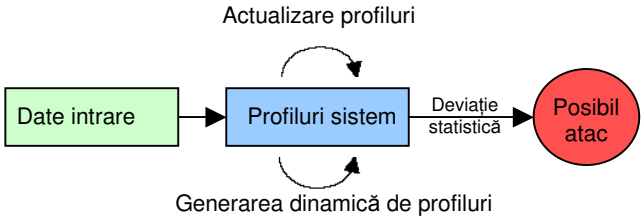
- 

Figura 3.4 - Modelul general al unui detector de anomalii

Sistemele de detecție bazate pe anomalii se clasifică după cum urmează:

A. Sisteme cu auto-instruire - sunt cele care pe baza observării traficului sau activității sistemului pe o durată mai lungă de timp sunt capabile să construiască profiluri a ceea ce reprezintă "normalitatea".

- **Serii atemporale** – reprezintă detectorii care modelează comportamentul normal al sistemului pe baza utilizării unui model stocastic care nu ia în calcul evoluția seriilor temporale.
  - **Modelarea regulilor** – sistemul studiază traficul şi formulează un set de reguli care descriu operarea normală a sistemului sau rețelei. În faza de detecție, sistemul aplică regulile şi generează alarmă în cazul unei deviații a caracteristicilor traficului observat față de setul de reguli.
  - **Statistici descriptive** – sistemul colectează într-un profil statistici simple, descriptive, mono-mod pe baza unor parametrii ai sistemului, şi construieşte un vector distanță pentru traficul observat şi profil. Dacă distanța este suficient de mare, sistemul va genera alarmă.
- **Serii temporale** – Acest model este mult mai complex, luând în considerare evoluția seriilor temporale. Exemple de astfel de tehnici ar fi: lanțuri Markov ascunse, rețele neurale artificiale, etc.
  - **Rețeaua neurală artificială** (RNA) – este un exemplu de modelare de tip ”black-box”. Traficul normal al sistemului este pus la dispoziția RNA, care ”învață” caracteristicile traficului normal. Ieşirea este aplicată traficului curent şi este utilizată pentru formarea deciziei legată de detecția intruziunii, sau este transmisă unui sistem expert de nivel superior pentru a lua decizia finală.

B. Sisteme programate – sistemele din această clasă necesită o entitate externă (utilizator, administrator, etc.) pentru a instrui sistemul să detecteze anumite evenimente ce caracterizează anomalii.

- **Statistici descriptive** – sistemele construiesc un profil de comportament normal statistic pentru parametrii sistemului prin colectarea de statistici descriptive pentru un număr de parametrii (de exemplu: număr de încercări de login eşuate, numărul de conexiuni de rețea, numărul de comenzi ce returnează erori, etc.)
  - **Statistici simple** – statisticile colectate sunt utilizate de componente de nivel superior pentru a lua decizia de detecție a intruziunii.
  - **Bazate pe reguli simple** – utilizatorul furnizează sistemului reguli simple pentru a fi aplicate statisticilor colectate.
  - **Bazate pe prag** – acesta este cel mai simplu exemplu de detector programat ce utilizează statistici descriptive. Odată ce sistemul a colectat suficiente date, utilizatorul poate programa praguri predefinite (sub forma unor intervale simple) pe baza cărora se vor genera alarme (de exemplu: numărul de încercări nereuşite consecutive > 3).
- **Interzice implicit** – idea de bază pentru această clasă este de a specifica în mod explicit circumstanțele în care sistemul observat operează într-o manieră de securitate sporită şi să raporteze toate deviațiile de la acest mod de operare ca intruziuni. Aceasta reprezintă o corespondența clară cu o politică de securitate de tip ”interzice implicit ceea ce nu e permis în mod explicit”.
  - **Modelarea seriilor de stare** – în acest caz, politica pentru operarea într-un mod de sporit de securitate este codată ca un set de stări. Tranzițiile între stări sunt implicit în model, şi nu explicit ca în cazul codării unei maşini de stare în shell-ul unui sistem expert. Ca în orice maşină de stare, odată ce se verifică o stare, motorul de detecție a intruziunii aşteaptă realizarea următoarei tranziții. Dacă acțiunea monitorizată (de exemplu: accese la fişier, deschiderea unor porturi de comunicație ce prezintă interes deosebit) solicită

o tranziție care nu este specificată în mod explicit, se va genera o alarmă. Motoarele de verificare a regulilor sunt simple, însă nu la fel de puternice ca în cazul unui sistem expert.

În continuare se prezintă o serie de sisteme de detecție bazate pe anomalii.

3.3.5.1 IDES – Sistem expert pentru detecția în timp real a intruziunilor

IDES este un sistem clasic pentru detecția intruziunilor, fiind şi unul din cele mai documentate [LJL88, LTG92]. Sistemul a fost dezvoltat de SRI International pentru a testa modelul [Den87]:

- Reprezintă utilizatori, sesiuni de login, şi alte entități ca o secvență ordonată de statistici $<q_{0,j}, .., q_{n,j}>$, unde $q_{i,j}$ (statistica i pentru ziua j) este un număr sau interval de timp.
- Comportamentul recent are preferință ridicată față de cel vechi
  - $A_{k,j}$ este suma valorilor ce determină metrica statisticii k în ziua j
  - $q_{k,l+1} = A_{k,l+1} - A_{k,l} + 2^{-rt} * q_{k,l}$, unde t este numărul de intrări de log sau timp total, iar r un factor ajustat experimental

Conceptul de bază care stă în spatele IDES este că utilizatorii au un comportament relativ stabil în timp atunci când îşi desfăşoară activitățile pe un sistem de calcul, iar comportamentul lor poate fi reprezentat pe baza unor diferite statistici. Activitatea curentă a sistemului este corelată cu profilul calculat, iar deviațiile sunt raportate drept intruziuni.

IDES procesează fiecare nouă înregistrare de audit pe baza profilurilor utilizator şi de grup. De asemenea, odată ce sesiune se încheie, aceasta este verificată pe baza profilurilor cunoscute.

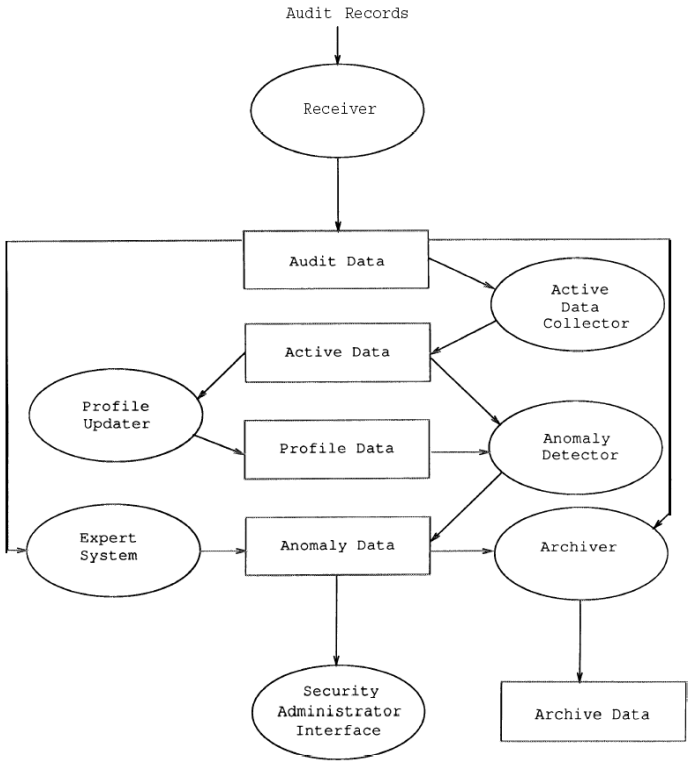


Figura 3.5 - Arhitectura IDES

3.3.5.2 Wisdom & Sense – Detecția activităților anormale în sesiuni de lucru pe stații

Sistemul utilizează o abordare unică în ceea ce priveşte modul de detecție a anomaliilor, prin studierea datelor de audit istorice pentru a produce reguli ce descriu tipul de comportament ”normal” (de aici şi denumirea de ”wisdom”). Aceste reguli sunt apoi introduse într-un sistem expert care evaluează datele de audit recente pentru a determina violări ale acestor reguli şi generează alerte când regulile indică comportament anormal („sense”) [VL89].

3.3.5.3 Computer Watch

Această aplicație a fost dezvoltată de Departamentul de Securitatea Sistemelor din cadrul AT&T ca un pachet adițional pentru System V/MLS (o versiune de UNIX sistem V în clasa de securitate B1 după Common Criteria).

Aplicația operează asupra datelor de audit şi oferă utilizatorului un sumar asupra activității sistemului, pe baza căruia acesta poate decide dacă este necesară investigarea statisticilor ce par anormale. Aplicația oferă şi mecanismele prin care se pot face interogări la date de audit pentru obținerea de detalii asupra activităților suspecte [DR90].

3.3.5.4 NADIR – Sistem automat pentru detecția abuzurilor şi intruziunilor în rețea

Dezvoltat la laboratorul național de la Los Alamos pentru uz intern (astfel că adresează probleme şi cerințe specifice acelei organizații), NADIR a fost implementat pe o stație SunSPARC utilizând un sistem de baze de date relațional Sybase.

Sistemul colectează date de audit de la trei tipuri de noduri de serviciu, care sunt apoi procesate înainte de a fi introduse în baza de date ca informație de audit. Fiecare înregistrare de audit introdusă în sistem corespunde unui eveniment specific şi conține următoarele informații: data şi timp, identificator de utilizator, eveniment, parametru de înregistrare, cod de eroare.

Sistemul determină săptămânal profiluri individuale ale utilizatorilor ce sintetizează comportamentul utilizatorului. Aceste profiluri sunt comparate pe baza unui set de reguli de sistem expert determinate pe baza următoarelor surse:

- Experți de securitate şi politica de securitate
- Analiza statistică a înregistrărilor de audit din sistem

Sistemul produce o serie de rapoarte despre activitatea sa, pe baza cărora se pot efectua investigații mai amănunțite. [JDS91, HJS+93]

3.3.5.5 Hyperview – Componentă de rețea neuronală pentru detecția intruziunilor

Acest sistem are două componente majore: un sistem expert uzual care monitorizează informația de audit pentru a identifica caracteristici pentru intruziunile cunoscute, şi o componentă bazată pe rețele neuronale (ARN) care învață adaptiv comportamentul utilizatorului şi generează alarme când informația de audit deviază de la comportamentul deja învățat.

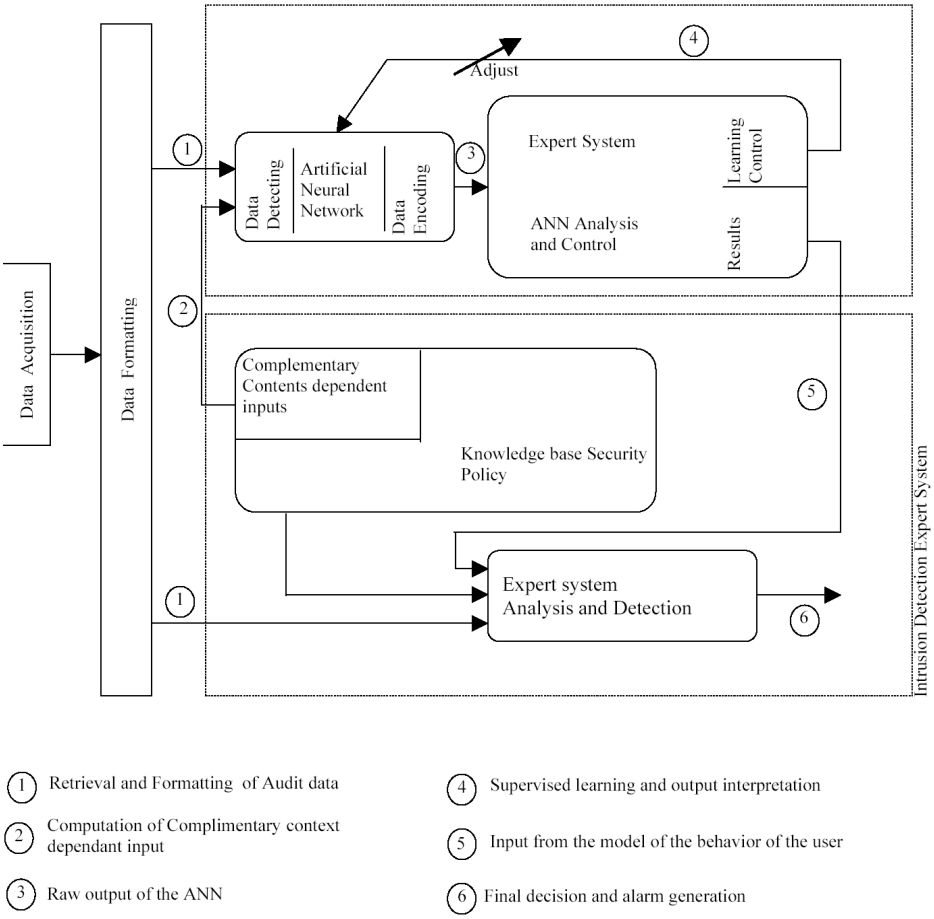


Figura 3.6 - Arhitectura Hyperview

Decizia de a utiliza ARN pentru a implementa funcția de detecție a anomaliilor pe bază statistică, se bazează pe următoarele ipoteze legate de caracteristicile informației de audit:

- informația de audit reprezintă o serie temporală multivariată, în care utilizatorul constituie procesul dinamic care emite o serie de evenimente ordonate secvențial.
- înregistrarea de audit care reprezintă un eveniment constă din două tipuri de variabile: variabile cu valori dintr-un set finit (de exemplu: nume de stații) şi variabile de valoare continuă (de exemplu: utilizarea CPU)

Seriile temporale au fost asociate intrărilor în ARN, iar o parte din ieşirile rețelei au fost conectate la intrare (ceea ce creează memoria internă în rețea). Între evaluări, datele din seriile temporale sunt introduse în rețea realizându-se ”percepția trecutului”.

ARN este conectată la două sisteme expert: unul monitorizează operarea, instruirea rețelei (prevenind învățarea eronată), şi evaluează ieşirea acesteia; iar celălalt scanează informația de audit pentru a identifica anumiți indicatori ai atacului. Decizia de generare a unei alerte se generează pe baza ieşirii din ambele sisteme expert [DBS92].

3.3.5.6 DPEM – Monitorizarea distribuită a execuției unui program.

Metodele de detecție prezentate anterior se bazează cunoaşterea caracteristicilor din atacuri precedente. Autorul acestui sistem propune o abordare diferită – detecția intruziunilor urmăreşte evoluția corectă a securității sistemului, sau mai precis, a aplicațiilor privilegiate ce rulează pe sistemul respectiv. DPEM [Ko96] citeşte specificațiile de securitate pentru un comportament acceptabil al aplicațiilor privilegiate, şi verifică dacă există violări ale specificațiilor de securitate în informația de audit.

Prototipul DPEM monitorizează execuția programelor într-un sistem distribuit prin colectarea de urme ale execuției de pe diverse stații. Arhitectura sistemului cuprinde următoarele componente: centralizator, un manager de specificații, dispeceri de urme, colectori de urme şi analizatori distribuiți pe stațiile din rețea.

3.3.6 Detecția bazată pe semnături

Detecția bazată pe semnături determină intruziunile pe baza cunoştințelor unui model al procesului intruziv şi a urmelor care trebuie lăsate în sistemul observat. Detectorii încearcă să determine intruziunile urmărind anumite indicii care au fost determinate în prealabil de proiectanții sistemului, fără a avea însă informații despre ceea ce ar însemna condițiile normale de trafic. Aceasta impune cerințe stricte asupra modelului naturii intruziunii.

O varietate de tehnici au fost utilizate pentru modelarea şi recunoaşterea caracteristicilor atacului: sisteme expert, analiza semnăturii, rețele Petri, analiza tranzițiilor de stare şi algoritmi genetici. Elementul comun al acestor tehnici îl reprezintă faptul că se încearcă reprezentarea caracteristicilor esențiale ale atacurilor cunoscute astfel încât variații ale atacului pot fi identificate. Orice ce nu este identificat ca atac, este considerat a fi normal.

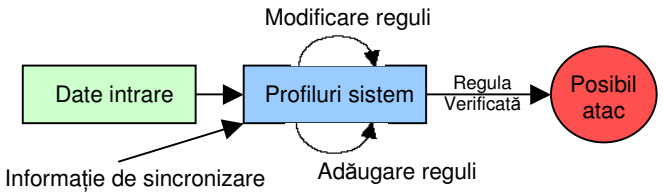


Figura 3.7 - Modelul general al unui detector pe bază de semnături

Sistemul de detecție este programat cu o regulă de decizie explicită, unde programatorul a pre-filtrat ”zgomotul” din spațiul de observare. Codul corespunzător regulii de detecție conține elemente de identificare clare care trebuie observate în cazul intruziunii.

Sisteme de detecție bazate pe semnături se clasifică după cum urmează:

A. Sisteme bazate pe modelarea stărilor – intruziunea este codificată ca un număr de stări diferite, fiecare din ele trebuind a fi prezente în spațiul de observare pentru a se considera că intruziunea are loc. Prin natura lor, acestea sunt modele de serii temporale pot fi grupate în două clase:

- **Tranziții de stare** – stările care alcătuiesc intruziunea formează un lanț simplu care trebuie să fie traversat de la un capăt la celălalt.
- **Rețele Petri** – stările formează o structură arborescentă generică, în care anumite stări preparatorii pot fi îndeplinite, indiferent de ordine şi de poziția în model.

B. Sistem Expert - este destinat să evalueze starea de securitate a sistemului pe baza unui set de reguli ce descrie comportamentul intruziv. Adesea, sunt utilizate aplicații de tip înlănțuire înainte (forward-chaining), considerate a fi o alegere potrivită pentru sistemele în care se introduc în mod constant evenimente de audit. Aceste sisteme expert oferă flexibilitate, permițând accesul utilizatorului la mecanisme foarte puternice cum ar fi unificarea. Aceste facilități vin adesea în detrimentul unei scăderi a vitezei de execuție în comparație cu metodele mai simple.

C. Sisteme bazate pe string matching – este o metodă simplă, de verificare a subşirurilor de caractere din fluxul de date transmis între sisteme. Avantajul său constă în simplitatea implementării şi se bazează pe algoritmii descrişi în paragraful 4.6.

D. Sisteme bazate pe reguli simple – sunt similare sistemelor expert puternice, dar nu sunt la fel de avansate. Au însă o execuție mai rapidă.

În continuare se prezintă o serie de sisteme de detecție bazate pe semnături.

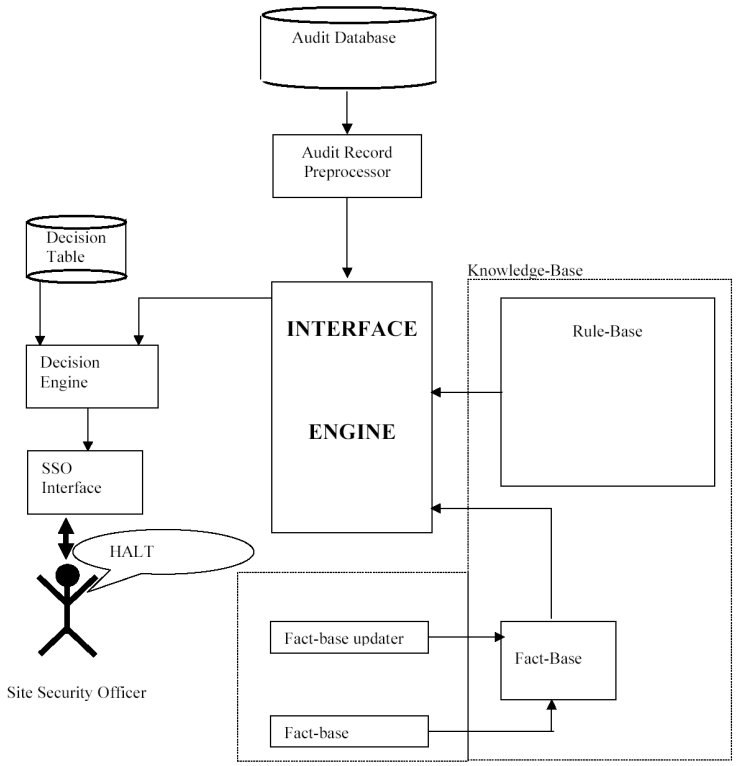


Figura 3.8 - Arhitectura USTAT

3.3.6.1 USTAT – Analiza tranzițiilor de stare [IKP95]

Analiza tranzițiilor de stare presupune că sistemul se află inițial într-o stare de securitate, iar ca urmare a penetrărilor, modelate ca tranziții de stare, poate ajunge într-o stare finală sinonimă cu compromiterea. Sistemul preia de la utilizator specificațiile

tranzițiilor de stare necesare pentru realizarea intruziunii, după care evaluează informația de audit în conformitate cu aceste specificații.

Utilizatorul specifică comportamentul intruziv pe care IDS ar trebui să-l detecteze ca o secvență de tranziții de stare specifice. Ipotezele de operare a acestui model bazat pe analiza tranzițiilor de stare sunt:

- Intruziunea trebuie să aibă efect vizibil asupra stării sistemului
- Efectul vizibil trebuie să fie recunoscut fără cunoştințe din exterior (cum ar fi identitatea adevărată a atacatorului)

Un impediment al modelului este că nu toate intruziunile îndeplinesc aceste condiții (de exemplu atacatorii care sunt impostori, ce utilizează un cont şi o parolă valide obținute în mod fraudulos).

Un exemplu de scenariu de penetrare UNIX BSD 4.2 ce poate fi utilizat de atacator să obțină privilegii administrative, şi diagrama de tranziții de stare corespunzătoare, sunt prezentate în tabelul şi figura următoare.

Pas	Comanda	Descriere
1	% cp /bin/csh /usr/spool/mail/root	Presupune ca nu există fişierul de mail pentru root
2	% chmod 4755 /usr/spool/mail/root	Creează un setuid file
3	% touch x	Creează un fişier gol
4	%mail root < x	Mail fişierul x către root
5	%/usr/spool/mail/root	Execută shell ce permite accesul root
6	Root %	

Tabel 3.1 – Scenariu de penetrare

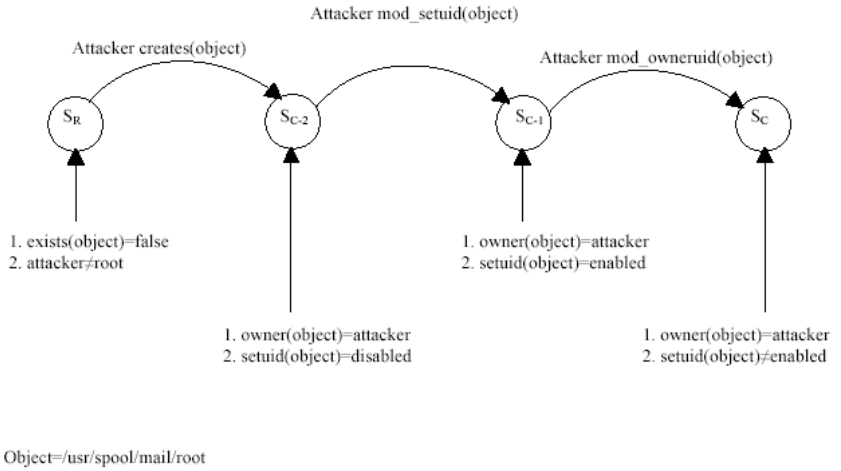


Figura 3.9 - Diagrama de tranziții de state corespunzătoare scenariului de atac din Tabelul 3.1.

3.3.6.2 IDIOT - Intrusion Detection In Our Time

Modelul sistemul se bazează pe rețele Petri colorate pentru detecția de intruziunilor. Autorii propun o abordare structurată în aplicarea tehnicilor bazate pe semnături în rezolvarea problemei detecției intruziunilor [Kum95].

Modelul presupune că atacul este caracterizat de următoarele trăsături:

- Existență : atacurile generează urme (fişiere, sau alte entități)
- Secvență : atacul cauzează câteva evenimente secvențial
- Ordine parțială: atacul cauzează două sau mai multe secvențe de evenimente care sunt în ordine parțială în coordonate temporale.
- Durată: are durată limitată în timp
- Interval: evenimentele sunt distanțate în timp

Modelul defineşte un eveniment ca fiind una sau mai multe acțiuni ce generează o singură înregistrare. Secvențele de evenimente pot fi întrețesute.

Rețeaua Petri va captura următoarele informații:

- Fiecare semnătură corespunde unui anumit CPA (Colored Petri Automaton)
- Nodurile sunt token-uri, arcele sunt tranziții
- Starea finală a semnăturii este cea de compromitere

Adăugarea de noi semnături se poate face în mod dinamic, iar ordonarea CPA-urilor permite stabilirea ordinii de verificare a semnăturilor de atac.

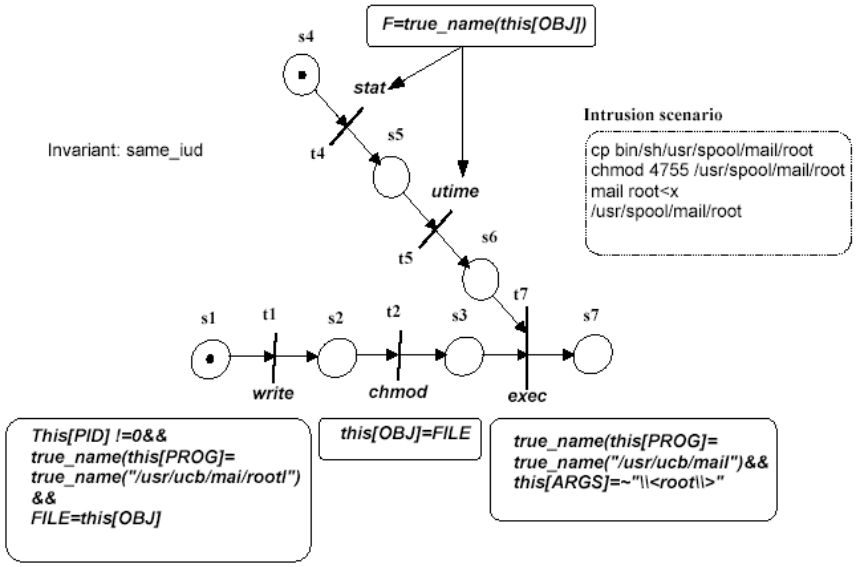


Figura 3.10 – Semnătură de intruziune reprezentată printr-o rețea Petri

3.3.6.3 Snort

Snort este o aplicație pentru analiza de pachete multimod care poate fi folosită ca: sistem de colectare şi procesare a pachetelor de trafic, sistem IDS, aplicație pentru investigații post-incident. Este foarte simplu (sursa are aproximativ 800kB), portabil (rulează pe majoritatea versiunilor de UNIX, Linux şi Windows), destul de rapid (are o probabilitate ridicată de detecție a atacurilor cunoscute în rețele de 1Gbps), configurabil (limbaj simplu pentru descrierea de reguli). Snort este totodată standardul de facto pentru IDS de rețea din surse deschise, fiind foarte bine documentat.

Versiunile Snort 2.x oferă o îmbunătățire a funcției de pattern-matching şi detecție prin utilizarea unor algoritmi mai performanți cum ar fi: Aho-Corasick sau Horspool.

Actualmente Snort oferă suport doar pentru protocoalele uzuale de nivel 2-4 din

rețelele TCP/IP (Ethernet, FDDI, Frame Relay, SLIP, PPP, ISDN, IP, ARP, TCP, UDP, ICMP), dar prin adăugarea de noi decodere de tip plug-ins

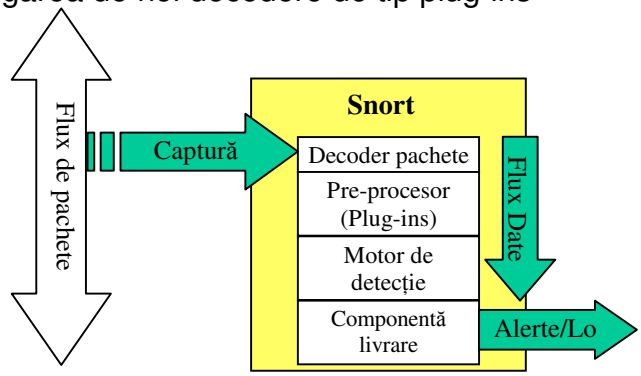


Figura 3.15 - Arhitectura Snort

Antet regulă	Opțiuni
Alert tcp 1.1.1.1 any -> 2.2.2.2	(flags: SF; msg: "SYN-FIN
Alert tcp 1.1.1.1 any -> 2.2.2.2	(flags: S12; msg: "Queso
Alert tcp 1.1.1.1 any -> 2.2.2.2	(flags: F; msg: "FIN

Figura 3.11 - Exemplu de regulă formulată de utilizator

3.3.6.4 OSSEC

OSSEC este un sistem de detecție care oferă servicii de tip analiză de fişiere de jurnal, verificare integritate, detecție Rootkit, alerte pe bază de timp şi răspuns activ. Arhitectural, soluția constă dintr-o serie de agenții care colectează şi transmit evenimentele către un server central. Aplicația suportă formate multiple de fişiere syslog, apache, snort, etc., iar evenimentele sunt procesate pe bază de reguli specificate în format XML.

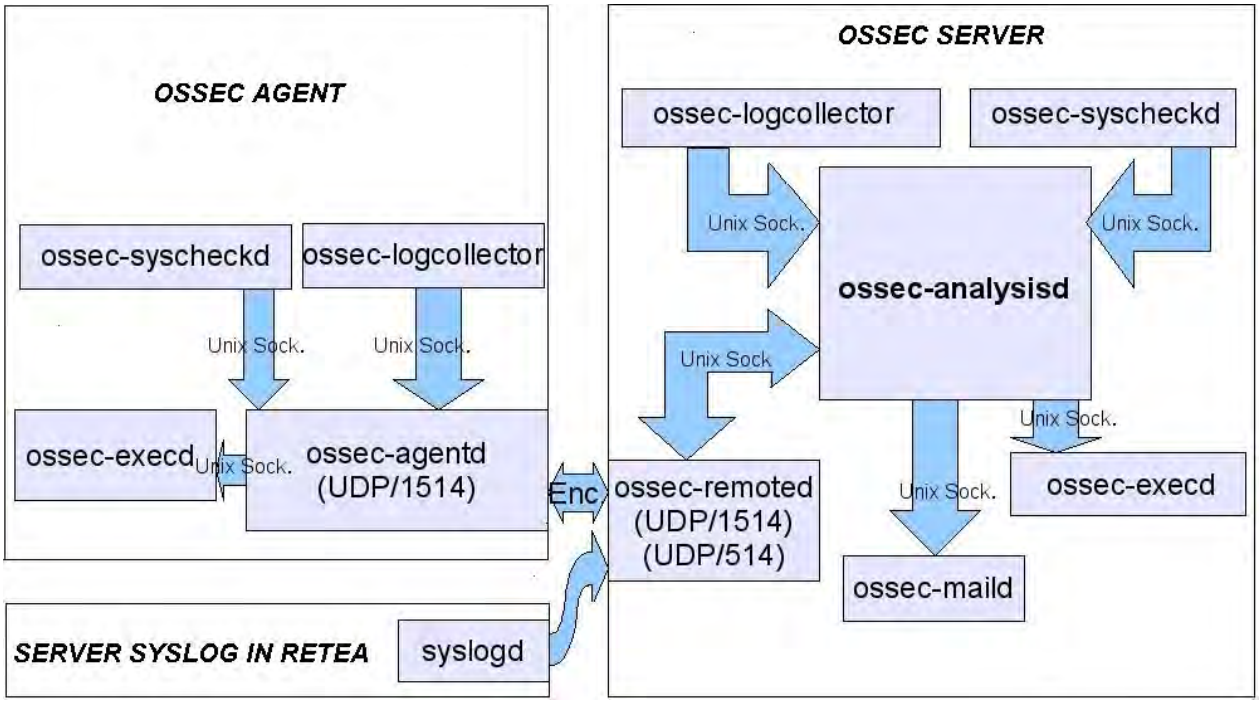


Figura 3.12 – Operarea OSSEC în modul server

OSSEC are două moduri de operare: client/server (pentru o analiză centralizată) şi local (când se monitorizează un singur sistem)

Procesele interne OSSEC sunt:

- Analysisd – este procesul principal, şi este responsabil cu analiza datelor
- Remoted – Recepționează fişierele de jurnalizare de la agenții ce rulează pe alte stații. Rulează implicit pe port UDP 1514, şi şi pentru comunicația cu agenții OSSEC, canalul este criptat (folosind algoritmul blowfish şi chei partajate) şi traficul comprimat (folosind zlib).Pentru compatibilitate extinsă, clienții tradiționali syslog
- Logcollector – consolidează fişierele log (syslog, evenimente Windows, fişiere text, etc)
- Agentd – expediază fişierele de jurnalizare către server-ul OSSEC. Canalul de comunicație dintre agent şi server este criptat (folosind algoritmul blowfish şi chei partajate), iar traficul este comprimat (folosind zlib).
- Maild – transmite alertele email către utilizatori
- Execd – Execută răspunsurile active asociate regulilor de detecție
- Monitord – monitorizează starea agenților, comprimă şi semnează digital fişierele de jurnalizare
- Ossec-control – efectuează managementul proceselor OSSEC cum ar fi pornirea şi oprirea lor.

3.3.6.5 RIPPER (Real Time Data Mining-based Intrusion Detection)

Idea centrală a acestui sistem este utilizarea programelor de audit pentru extragerea de informații detaliate ce descriu fiecare conexiune de rețea sau fiecare sesiune pe o stație, şi aplicarea programelor de data-mining pentru a învăța reguli care capturează comportamentul intruziv şi activitățile normale, şi care reguli pot fi utilizate pentru detecția pe bază de semnături şi cea de anomalii [Lee99].

Data-mining se referă în general la procesul de extragere de modele descriptive din volume mari de date şi utilizează o varietate de algoritmi din domeniul statisticii, pattern-matching, învățarea maşinilor şi baze de date.

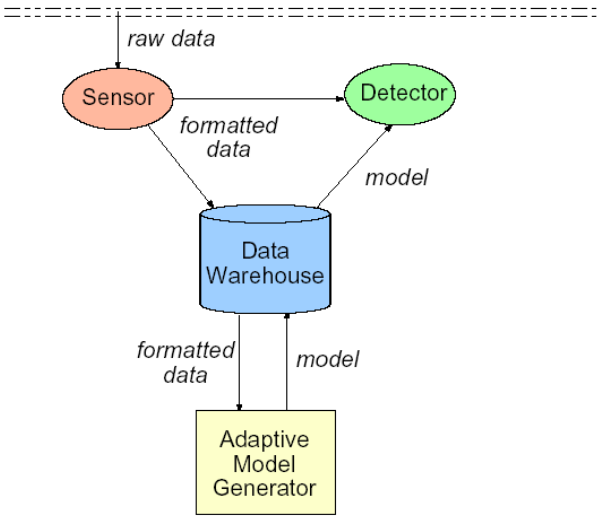


Figura 3.13 – Arhitectura RIPPER

3.3.7 Sisteme IDS Hibride

Sisteme din această categorie utilizează tehnici combinate (prezentate în secțiunile 3.3.5 şi 3.3.6) în procesul de detecție a intruziunilor. Majoritatea sistemelor comerciale actuale utilizează tehnici hibride de bazată pe anomalii şi semnături. Sistemele prezentate în această secțiune, au fost identificate pe baza reprezentativității conceptelor utilizate în tehnicile de detecție.

3.3.7.1 Haystack

Prototipul Haystack [Sma88] a fost conceput pentru detecția intruziunilor într-un sistem multi-user al US Air Force (Unisys 1100/60 mainframe ce rula OS/1100). Detecția intruziunilor se efectua pe baza detecției de anomalii şi de semnături. Detecția de anomalii era organizată în jurul a două concepte: modele utilizator definite pe baza comportamentului trecut al acestora, şi modele generice pentru grupe specifice de utilizatori ce definesc comportamentul acceptabil pentru utilizatorii grupului respectiv.

Modelul matematic utilizat de sisteme este următorul:

- $<A_0, .., A_n>$, unde A_i este statistica i (valoare sau interval de timp)
- Se definesc T_L şi T_U astfel încât 90% din valorile A_i Є $[T_L , T_U]$
- Sistemul calculează A_{n+1} şi generează anomalie dacă nu se verifică că A_i Є $[T_L , T_U]$.
- Se actualizează limitele T_L , T_U .

3.3.7.2 MIDAS: Sistem expert pentru detecția intruziunilor

MIDAS [SSHW88] a fost dezvoltat de National Computer Security Centre (NCSC) în cooperare cu SRI International în scopul detecției de intruziuni în mainframe-ul NCSC. MIDAS implementează o detecție a intruziunilor de tip euristic. Autorii au modelat sistemul plecând de la activitățile desfăşurate de un agent de securitate uman pentru a determina intruziunea pe baza analizei fişierelor de log.

MIDAS utilizează un sistem expert, P-BEST, (Production Based Expert System Toolset) pentru detecția intruziunilor. Baza de reguli este organizată pe două niveluri. Primul realizează deducția imediată a anumitor tipuri de evenimente cum ar fi ”numărul de încercări de login eşuate”, şi le asociază o categorie de suspiciune. Nivelul următor de reguli realizează procesarea acestor suspiciuni pe baza cărora decide declanşarea unei alarme.

3.3.7.3 NSM – Network Security Monitor

Acesta a fost primul sistem care a utilizat direct traficul de rețea ca sursă de date de audit şi este precursorul NSM actuale. NSM ascultă în mod pasiv traficul de rețea LAN şi deduce pe baza analizei acestuia caracteristicile comportamentul intruziv. [HDL+90, MHL94].

NSM are o arhitectură pe mai multe niveluri:

- *Nivelul conexiune* – este responsabil pentru studiul datelor din rețea şi încercarea de a forma perechi de canale de comunicație bidirecțională între grupe de stații.
- *Vectorul de conexiune* – grupează mai multe conexiuni

- *Sistem expert simplu* – utilizează ca intrare vectori conexiune, vectori stație, profiluri de trafic normal (volume de date între stații, protocoale utilizate), cunoştințe de protocol (telnet, sendmail) şi analizează datele pentru a determina indicii de comportament intruziv.

Datele sunt prezentate utilizatorului la consolă sub forma unei liste sortate ce cuprinde vectorul de conexiune şi un nivel de suspiciune determinată de sistemul expert. Rezultatele sunt arhivate într-o bază de date pentru suportul unor eventuale investigații ulterioare.

3.3.7.4 NIDES – Next Generation Intrusion Detection System

NIDES [AFV95] este succesorul proiectului IDES şi urmăreşte aceleaşi principii generale ca ultima versiune de IDES (are componentă solidă de detecție a anomaliilor, dublată de o componentă de sistem expert bazată pe semnături - PBEST).

NIDES este construit pe o arhitectură client-server, este modularizat, având interfețe bine definite între componente. Sistemul este centralizat, putând efectua analiza pe o anumită stație numită – *NIDES host*. *Stațiile țintă* colectează datele de audit din diverse surse cu informații de log de stație şi de rețea.

3.3.7.5 JiNao – Detecția scalabilă a intruziunilor pentru infrastructuri de rețea critice

Acest sistem [JCS97] are rolul de protecție a infrastructurii de rețea ce utilizează OSPF. Modelul de amenințare presupune că anumite entități care asigură rutarea pot fi compromise, cauzând stoparea sau deturnarea traficului.

Detecția intruziunilor este operată utilizând trei modele bazate pe: anomalii, semnături şi violări de protocol.

3.3.7.6 EMERALD – Event Monitoring Enabling Responses to Anomalous Live Disturbances

EMERALD [PV98] a fost conceput ca o arhitectură scalabilă, distribuită de detecție a intruziunilor pe stații şi în rețea. Arhitectura conține şi componente care permit sistemului să răspundă în mod activ în principal la amenințările ce vin din exteriorul organizației.

Arhitectura vizează o rețea de organizație largă, compusă din domenii cu relativă separație administrativă, şi cu niveluri de încredere diferite inter-domenii. Autorii propun un sistem distribuit care operează pe trei niveluri distincte:

- *Analiza de servicii* – ce acoperă abuzurile componentelor individuale şi serviciile rețelei în limitele unui domeniu. Obiectivul acesteia este de a simplifica şi descentraliza monitorizarea interfețelor de rețea ale unui domeniu în scopul identificării activităților care indică abuzuri sau anomalii semnificative în operare. Elementele de arhitectură care asigură această funcționalitate sunt *monitoarele de serviciu*, care realizează o analiză locală de timp real a infrastructurii (rutere, gateways) şi serviciilor (subsisteme privilegiate cu interfețe de rețea). Monitoarele pot interacționa în mod pasiv cu mediul (de exemplu: citirea fişierelor de log), sau activ (prin sondare în vederea obținerii de informații adiționale). Informația disponibilă la nivelul unui monitor local poate fi pusă la

dispoziția altor monitoare pe baza unui mecanism de comunicație bazat pe *subscripții*.

- *Analiza la nivel de domeniu* – acoperă abuzurile vizibile între servicii multiple şi componente. Un *monitor de nivel domeniu* este responsabil pentru monitorizarea unei părți sau a întregului domeniu. Acesta corelează informațiile de intruziune oferite de monitoarele de serviciu, oferind astfel o perspectivă mai bună asupra activități malițioase la nivelul domeniului. Monitoarele de domeniu îndeplinesc şi alte funcții cum ar fi: asigură reconfigurarea parametrilor sistemului, realizează interfața cu alte monitoare din afara domeniului şi raportează administratorilor amenințările la adresa domeniului.
- *Analiza de nivel organizație* – care vizează abuzurile coordonate asupra mai multor domenii. Monitoarele de organizație corelează rapoartele de activitate produse de un grup de domenii monitorizate şi vizează în principal amenințările de nivel global cum ar fi: atacuri DDoS şi viermi, atacuri repetate împotriva serviciilor de rețea interdomenii, precum şi atacuri coordonate din mai multe domenii asupra unui singur domeniu. Prin corelații şi publicarea către alte monitoare a rezultatelor de analiză, se realizează distribuirea la nivelul organizației a informației legate potențiale amenințări globale. Capacitatea sistemului de a realiza analiza evenimentelor inter-domenii este vitală în contextul unor atacuri pe scară globală, cum ar fi cele din clasa războiului informațional.

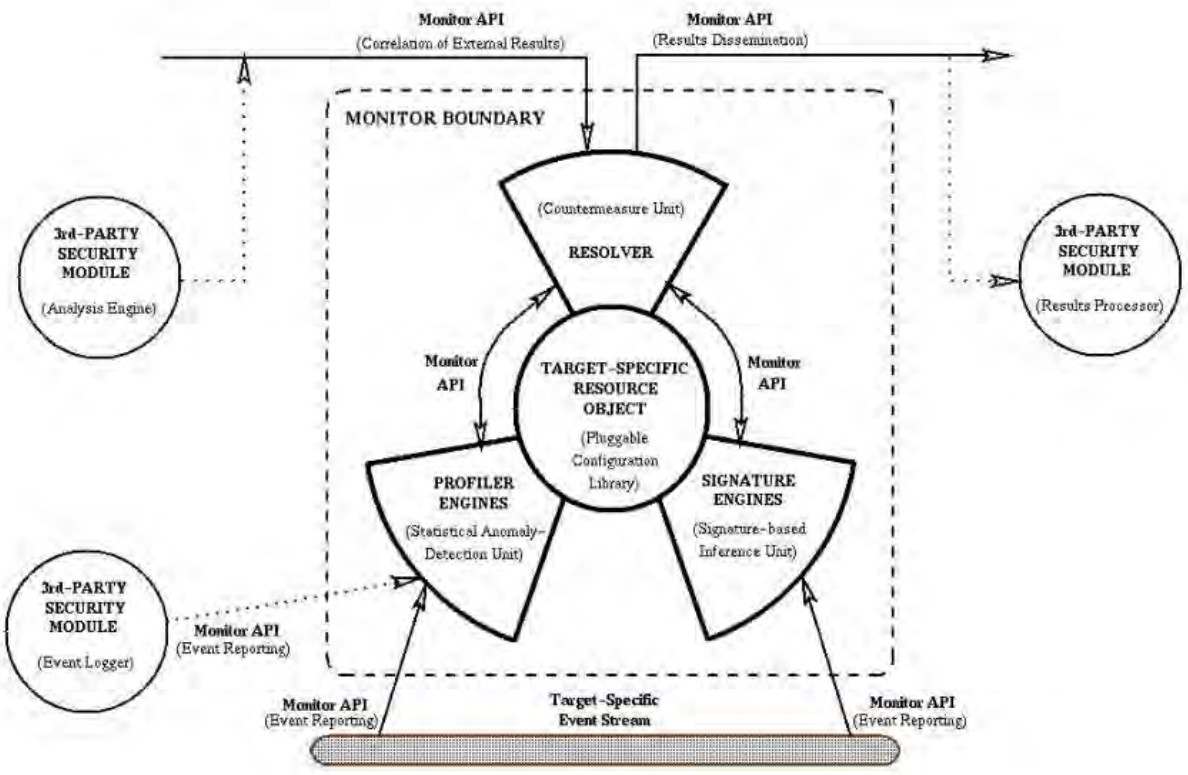


Figura 3.14 – Arhitectura generică a Monitorului EMERALD

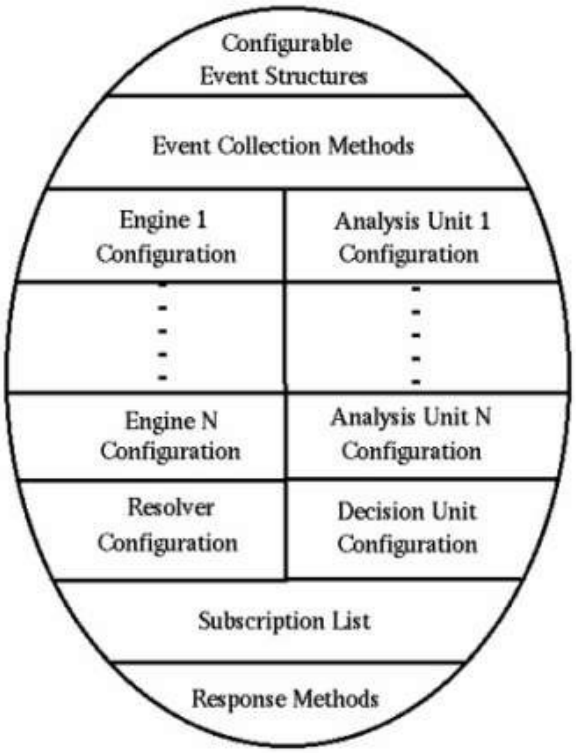


Figura 3.15 – Structura generica a obiectului resursă EMERALD

3.3.7.7 Bro

Bro este un sistem pentru detecția în timp real a intruziunilor în rețea prin monitorizarea pasivă a legăturii de rețea prin care se circulă traficul de atac [Pax88]. Obiectivele urmărite de autor în proiectarea acestui sistem au fost:

- Abilitatea sistemului de a realiza o monitorizare de volum mare
- Procesarea rapidă a pachetelor de intrare pe senzor astfel încât să se evite pierderea de date.
- Notificarea în timp real a utilizatorului asupra încercărilor de atac sau a atacurilor în curs de desfăşurare
- Separarea mecanismului de politică, făcând astfel posibilă actualizarea politicilor de securitate
- Sistemul va fi extensibil fiind posibilă adăugarea de cunoştințe despre tipuri noi de atac
- Sistemul va ajuta utilizatorul în a evita efectuarea de erori în procesul de specificare a politicii de securitate

Caracteristicile sistemului ar putea fi sintetizate după cum urmează:

- Componentele majore sunt: motorul de evenimente (de analiză a protocolului) şi interpretorul scripturilor de politici.
- Permite căutări pe bază de expresii regulate
- Poate analiza trafic în ambele direcții
- Poate detecta atacuri ce au loc pe durata mai multor faze
- Are un nivel de alarme false mai redus decât Snort

Lucrarea originală ce descrie Bro [Pax88] este prima care adresează şi problema atacurilor asupra monitorului şi a capacității acestuia de a rezista acestor atacuri.

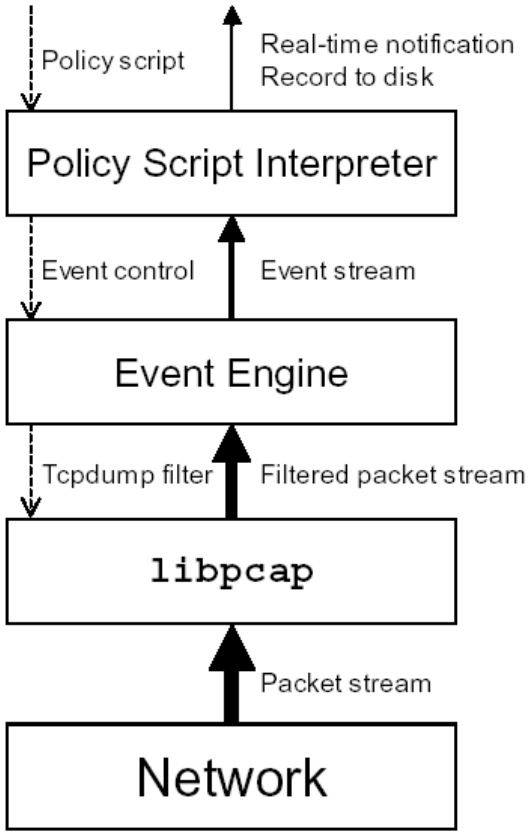


Figura 3.16 - Structura Bro

Pentru a ilustra modul în care Bro rezistă atacurilor, autorul împarte atacurile de rețea în trei categorii:

- Atacuri de supra-încărcare (sunt atacuri de tip DoS cu rolul de a provoca alterarea procesului de colecție prin pierderea de pachete de captură)
- Atacuri de blocare (sunt atacuri de tip DoS ce caută stoparea funcționalitatea monitorului sau a procesului de colecție ce rulează pe acesta)
- Atacuri de diversiune (atacuri ce urmăresc generarea de alarme false pentru a masca alte atacuri)

Anomalie	Auto-instruire	Serii atemporale	Modelare reguli	W&S
			Statistici descriptive	IDES, NIDES, EMERALD, JiNao,Haystack
		Serii temporale	Rețele Neurale Artificiale	Hyperview
	Programate	Statistici descriptive	Statistici simple	MIDAS, NADIR, Haystack
			Bazate pe reguli simple	NSM
			Prag	ComputerWatch
		Interzice implicit	Modelare serii de stare	DPEM, Bro
Semnătură	Programate	Modelare de stare	Tranziție de stare	USTAT
			Rețele Petri	IDIOT
		Sisteme expert		NIDES, EMERALD, MIDAS, DIDS
		String matching		NSM
		Bazate pe reguli simple		NADIR, Haystack, Bro, Snort, JiNao, OSSEC
Inspirate pe bază de semnături	Auto-instruire	Selectare automată a trăsăturilor		Ripper

Tabel 3.2 - Clasificarea tehnicilor de detecție utilizate de IDS prezentate în secțiunile 3.3.5-3.3.7

3.4 Tehnici de monitorizare a infrastructurii pentru organizații mari

Atacurile DDoS, propagarea epidemică a viermilor, precum şi utilizarea unui botnet de a atac o anume țintă pot paraliza chiar şi cele mai bine organizate rețele. Strategia pentru neutralizarea acestor amenințări presupune implementarea unor soluții de monitorizare care să acopere un spațiu de adrese mare, precum şi cooperarea între rețele. Acest paragraf abordează soluții de monitorizare ce se pot implementa în organizații mari, sau la nivelul furnizorilor de servicii Internet pentru a adresa potențialele atacuri la adresa infrastructurii de rețea.

3.4.1. Contracararea atacurilor generate de viermi Internet

Răspunsul la un atac lansat de un vierme presupune următoarele componente majore: detecția (de preferat a fi făcută cât mai timpuriu posibil), şi defensiva (vizează limitarea propagării şi neutralizarea viermelui). [Moo02]

Caracteristicile specifice ale propagării viermelui ce se vor fi monitorizate pentru a detecta prezența sa sunt [PPN05-03]:

- Volum substanțial de trafic similar (scanări, încărcătura de infecție)
- Volum ridicat de stații implicate
- Număr mare de sondări adrese nealocate

Detectarea atacurilor pe scară largă în Internet (atât cele DDoS şi a celor generate de viermi) se bazează pe sisteme IDS. Sistemele IDS bazate anomalii ale traficului identifică potențiale amenințări pe baza variațiilor dintre traficul curent şi un model de trafic în rețea pentru condiții normale. Deşi oferă o mai mare adaptabilitate, aceste tipuri de IDS au o rată ridicată de alarme false.

Considerând impactul asupra activității generale în Internet pe durata propagării epidemice a unui vierme, este necesară implementarea unor sisteme de detecție şi neutralizarea automată a atacurilor generate de viermi care trebuie sa satisfacă următoarele cerințe: [PPN05-01]

- Detectarea propagării viermilor în etape cât mai timpurii ale ciclului de manifestare pentru a-i putea anihila înainte de a scăpa de sub control.
- Generarea semnăturilor viermilor în mod automat pentru a reacționa şi neutraliza rapid propagarea acestora. O semnătură identifică caracteristicile comune ale unui vierme, suficiente pentru a-l identifica şi-l anihila.
- Sistemele de detecție a viermilor trebuie să aibă o rată redusă de alarme false, întrucât o alarmă falsă reprezintă de fapt interzicerea unui serviciu legitim. De aceea, trebuie realizat un compromis între o detecție rapidă şi o rată redusă de alarme false când se proiectează un sistem automat de detecție şi neutralizare a viermilor.

La nivelul furnizorilor de servicii sau al organizațiilor cu rețele mari, se poate efectua colectarea sondărilor trimise către adrese nealocate utilizând senzori distribuiți ce monitorizează traficul de intrare şi ieşire în diferite zone ale infrastructurii. Senzorii pentru traficul de intrare detectează pe cât posibil activitatea viermelui aflat în faza de scanare şi care încearcă să contacteze adrese dintr-un spațiu de rețea neutilizat (principiul este similar celui de ”Network telescop” prezentat de Moore[Moo02]). Acest

tip de senzori pot oferi informații despre activitatea viermelui la nivel global.

Senzorii pentru traficul de ieşire sunt plasați pe interfețele de ieşire ale ruterului care conectează rețeaua locală la Internet. Scopul unui astfel de monitor este de a identifica caracteristicile de scanare ale unui potențial vierme din traficul de ieşire. În cazul în care o stație din rețeaua locală este infectată, senzorii de ieşire pentru această rețea pot observa majoritatea traficului de scanare trimis către exterior de stația compromisă.

Figura 3.17 - Un sistem generic de monitorizare a atacurilor lansate de viermi

Pentru o avertizare timpurie asupra unui potențial atac lansat de vierme, datele observate de senzorii distribuite trebuie colectate şi transmise în timp real către un centru de avertizare (CA).

Un alt motiv pentru implementarea unui sistem distribuit de monitorizare, îl reprezintă faptul că acelaşi vierme poate arăta un comportament diferit, în funcție de particularitățile stației victimă. De exemplu, rata de scanare a lui Slammer este limitată de lărgimea de bandă pe care calculatorul infectat o are la dispoziție (utilizând protocolul UDP pentru propagare), pe când rata de scanare Conficker şi a altor viermi cu scanare uniformă este limitată de lărgimea de bandă a canalului de transmisie.

Informațiile colectate de senzori pe durata unui interval de timp de monitorizare, şi trimise către CA, sunt:

- Rata medie de scanare şi distribuția scanărilor (oferite de senzorii de ieşire)
- Numărul de scanări recepționate, precum şi adresele IP ale stațiilor care au trimit pachete de scanare (oferite de senzorii de ieşire)

CA colectează şi consolidează în timp real rapoartele de scanare generate de senzori pe parcursul fiecărui interval fiecare monitorizare. Pentru fiecare port TCP sau UDP, CA are un prag de alarmă de monitorizare a traficului nelegitim. Pentru procesarea acestor date se pot utiliza tehnici multiple.

Considerând propagarea exponențială care are loc în faza inițială, [Zou03] propune o strategia de detecție de identificare a unui *trend* în traficul de date prin activarea unui filtru Kalman care va estima rata de infecție pe baza informațiilor oferite de monitoare. Estimarea recursivă va continua până când valoarea estimată pentru parametrul ratei de infecție se stabilizează. Dacă rate de infecție estimată se stabilizează sau oscilează uşor în jurul unei valori constante pozitive, atunci s-a detectat prezența unui vierme. Dacă oscilează în jurul valorii zero, atunci traficul nelegitim identificat de senzori este interpretat ca zgomot .

3.4.2 Monitorizarea fluxurilor de comunicație pereche pentru detecția BotNet

Odată ce intruziunea a intrat în faza de consolidare, şansele de detecție pe baza NIDS sunt foarte limitate. Un astfel de caz îl reprezintă detecția stațiilor care sunt înrolate într-un botnet. Elementul caracteristic ce poate fi utilizat în detecția traficului botnet, îl reprezintă profilul de comunicație specific acestei structuri. Punctul de plecare îl constituie înțelegerea profilului de comunicație specific elementelor unui botnet [Bai09]. Pe baza acestui profil se construieşte un model de monitorizare a fluxurilor de comunicație în ambele sensuri între rețeaua proprie şi Internet pentru a determina indicii dialogului tipic botnet. În plus se pot corela alarmele IDS asociate traficului de intrare cu elemente specifice de comunicație în traficul de ieşire.

Una din cele mai eficiente implementări din această clasă de tehnologii este Bothunter [Gu07]. Aceasta modelează o secvență de infecție (I) pe baza unui tuplu de participanți şi a unei secvențe de dialog slab ordonate. I = <A,V,L,C,P,V',{D}>, unde

A– Atacator, V– Victimă, L– Locație încărcare soft, C– Server Comandă&Control, P– Punct coordonare P2P, V'– țintele de propagare ale victimei, {D}– Setul de secvențe de dialog pe fluxuri biderecționale

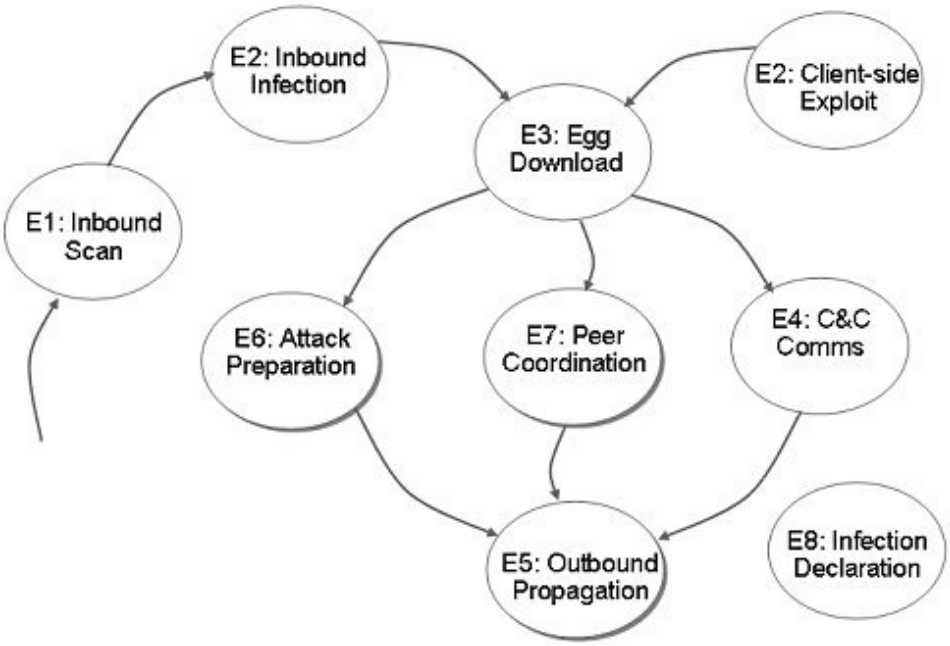


Figura 3.18 - Bothunter: Modelul ciclului de viață al infecțiilor (MCVI) [Bot11]

Componentele arhitecturii BotHunter sunt [Bot11]:

- *SLADE (Statistical payLoad Anomaly Detection Engine)* - implementează un modul simplu de analiză a încărcăturii în fluxurile de trafic de intrare, urmărind divergențe în distribuția octeților pentru protocoalele care sunt tipice intruziunilor pe bază de malware.
- *SCADE (Statistical sCan Anomaly Detection Engine)* - efectuează câteva scanări suplimentare de porturi tipice claselor malware atât pentru fluxurile de intrare cât şi cele de ieşire.

- *Corelatorul BotHunter* – pe baza unei diagrame interne de stări care defineşte MCVI, efectuează o corelație a elementelor de dialog din traficul de intrare şi a alarmelor de intruziune cu elemente dialogului din traficul de ieşire. Considerentele avute în procesul de corelație sunt [Gu07]:
  - Identificarea secvențelor de comunicație care sunt conforme cu MCVI
  - Elementele de trafic identificate a genera tranziții de stare nu trebuie să fie în ordine strică (ținând cont de întârzieri în rețea care pot afecta în mod diferit secvențele de pachete), trebuie să fie într-o anumită vecinătate temporală
  - Alerte de bot nu se generează doar pe baza elementelor de trafic externe, fiind nevoie de prezența elementelor de trafic interne.
  - Fiecare flux va avea un scor de încredere al infecției calculat pe baza elementelor de dialog asociate fiecărei stări.
- *Setul de semnături* - conține semnături de exploatări cunoscute de viermi, malware, scripturi, schimburi de mesaje C&C, scanări externe. Semnăturile provin din surse multiple cum ar fi: Bleeding Edge, comunitatea Snort, reguli specifice de bot Cyber-TA

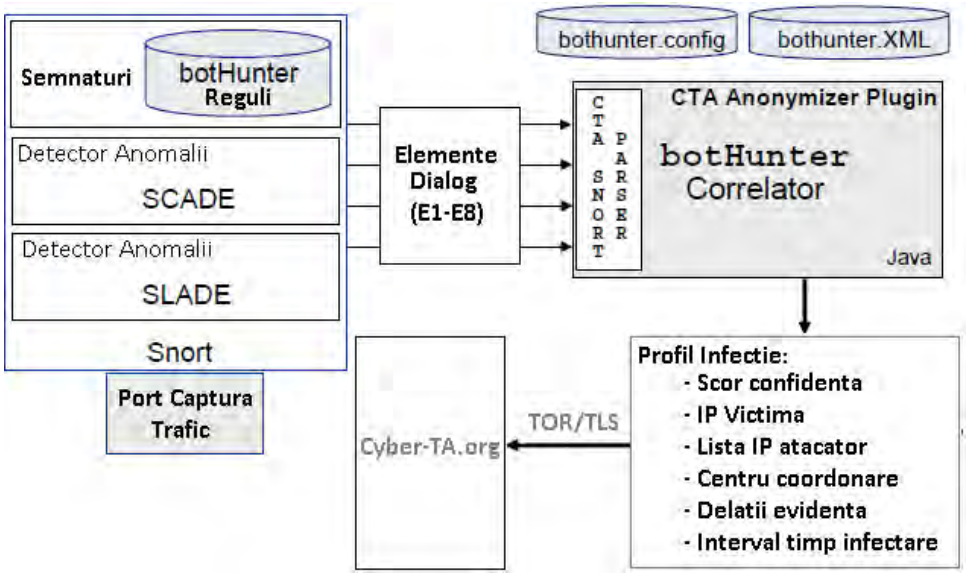


Figura 3.19 - Arhitectura Botnet [Gu07]

3.4.3 Urmărirea atacurilor DDoS

O strategie eficientă de combatere a atacurilor DDoS combină tehnici pentru adresarea următoarelor aspecte: prevenirea, detecția, urmărirea pachetelor fluxurilor sau traficului agregat creat de DDoS şi suprimarea atacurilor.

Măsurile de detecție şi urmărire a atacurilor DDoS pot fi împărțite în următoarele clase [PNB09]:

- *Marcarea pachetelor* - constă în suprascrierea unuia sau mai multor câmpuri ale antetului pachetului IP, pentru a păstra informații despre calea urmată de fiecare pachet de la sursă către destinație. Destinația va utiliza acest tip de informație pentru a reconstrui calea şi identifica atacatorul. Metodele bazate pe rescrierea pachetelor sunt relativ ineficiente împotriva atacurilor ce utilizează reflectori,

deoarece informația de marcare este pierdută la nivelul reflectorilor. Această clasă necesită funcții de calculare a căii ultrarapide în rutere, deoarece fiecare pachet trebuie marcat. Nu este demonstrat dacă funcțiile propuse sunt suficient de rapide pentru ruterele de backbone.

- *Controlul căii* - Spre deosebire de metodele cu marcare de pachete, aceste abordări bazate pe controlul căii presupun transmiterea de informații despre atacuri DoS în pachete adiționale. Aceste pachete ar trebui trimise la o rată mult mai scăzută decât pachetele de trafic manipulate de rutere. Spre deosebire de metoda anterioară, nu necesită schimbări în semantica câmpurilor existente în antetul pachetului. Aceasta este important deoarece rescrierea poate schimba semantica pachetelor. Prin creşterea numărului de căi între atacatori şi victimă, a ratei de trimitere a pachetelor, conținutul pachetelor, numărul de victime atacate simultan şi cantitatea de trafic legitimă generată de atacatori, probabilitatea ca victima să descopere locația reală a atacatorului scade prin reducerea diferențelor între traficul legitim şi cel de atac. Propunerile existente din această categorie se împart în două grupe: abordări bazate pe ICMP Traceback şi abordări bazate pe rutare (BlackholeRouting, CenterTrack)
- *Jurnalizarea pachetelor* - Metodele bazate pe marcarea pachetelor şi controlul căii pot fi păcălite de atacator, deoarece nivelul atacului trebuie să atingă o anumită limită pentru a putea determina calea dintre atacator şi victimă. Abordările bazate pe înregistrarea de pachete consideră un potențial pericol în fiecare pachet, şi de aceea trebuie înregistrat. Totuşi, colectarea şi procesarea tuturor pachetelor constituie o operație foarte complexă. De aceea, o serie de abordări vizează modul de sumarizare a traficului de pachete (DWARD, Multops, NetFlow, SPIE).

3.5. Monitorizarea spațiului de amenințări global pe baza resurselor publice

Una din componentele principale ale strategiei de securizare a Internetului o reprezintă monitorizarea amenințărilor de nivel global. Tehnicile reprezentative utilizate pentru monitorizarea spațiului de amenințări precum, precum şi o serie de exemple ilustrative a modului în care se poate efectua analiza pe baza acestor date publice sunt prezentate în cele ce urmează.

3.5.1 ”Network Telescope”

Network Telescope (numit adesea şi „darknet” sau „blackhole”) este o soluție de monitorizare a accesului la un spațiu larg de adrese IP rutabile care în condiții normale au un volum de trafic legitim foarte mic, inexistent, sau care poate fi uşor filtrat. Orice trafic atipic destinat spațiului de adrese monitorizat, poate fi interpretat ca un potențial atac. Această soluție este viabilă pentru observarea evenimentelor majore, la nivel global, în care atacul încorporează un grad ridicat de aleatorism în selectarea țintelor [Moo02-2]. Dacă conceptul inițial de telescop avea ca obiectiv doar capturarea traficului destinat spațiului de adrese neutilizat, implementări ulterioare (Internet Motion Sensors) încorporează un mecanism de răspuns limitat la traficul primit.

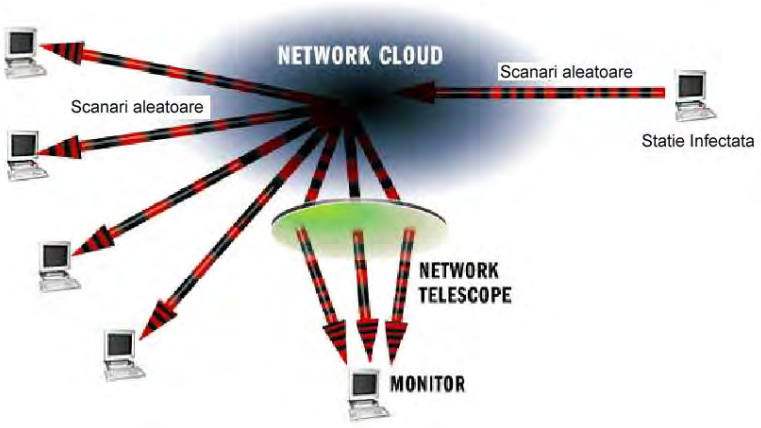


Figura 3.20 – "Network Telescope" utilizat de CAIDA

Pe baza acestui sistem s-au putut obține statistici despre atacuri de tip DDoS în desfăşurare (când telescopul recepționează de la victimă/victime un volum mare de pachete SYN-ACK), precum şi despre atacurile generate de propagarea viermilor (când telescopul recepționează un volum mare de cereri TCP SYN sau pachete UDP, şi care are un trend exponențial pe durata inițială de propagare a viermelui).

Utilitatea unei astfel de soluții constă în posibilitatea identificării unor atacuri majore în Internet la încă din fazele inițiale, de a estima potențialul impact, şi analiza evoluția ulterioară şi precum şi a mecanismelor aplicate pentru izolarea şi anihilarea atacului.

În procesul de utilizare şi interpretare a informațiilor oferite de o soluție telescop, trebuie să se aibă în vedere ipotezele şi limitările acestuia [Smi09]:

- Un telescop utilizând un spațiu de adrese distribuit va oferi o acuratețe mai ridicată în extrapolarea observațiilor locale la nivelul întregii infrastructuri Internet. Această soluție determină şi o implementare mai complexă, care trebuie să rezolve toate aspectele legate de sincronizare, de distribuția datelor, şi de interpretarea statistică a datelor deoarece, la un moment dat, nu toate rețele monitorizate au acelaşi grad de accesibilitate. Din păcate, soluțiile disponibile în acest moment (CAIDA, WAIL) utilizează preponderent spații de adresă continue. Extrapolarea observațiilor fiind aplicabilă doar în cazul atacurilor cu scanare uniformă a Internetlui
- Datorită congestiei, adesea telescopul va raporta cu întârziere scanările, iar aceasta va afecta şi rata de scanare estimată
- Prezență tehnologiei NAT (Network Address Translation) va avea ca urmare raportarea unui număr scăzut de adrese IP distincte. O soluție în acest sens ar fi utilizarea câmpului IP ID pentru anumite sisteme de operare.
- Scanările neuniforme (utilizând anumite preferințe cum ar fi cea de rețea locală – utilizată în cazul viermelui Stuxnet) limitează vizibilitatea telescopului.
- Limita de viață a stațiilor infectate. Modul de construcție a viermelui, precum impactul acțiunii viermelui sau al atacului DDoS asupra stației poate afecta modul de scanare. De exemplu, Code Red opreşte scanarea după o anumită perioadă, Witty afectează modul de operare a maşinii infectate care în timp devine indisponibilă, Stuxnet (utilizează o scanare direcționată, şi se autoşterge pentru a nu genera un volum de scanare ce poate atrage atenția)
- Erorile echipamentelor de măsură. Şi în cazul CAIDA, s-au putut observa intervale de timp în care colecția de date este afectată de întârzieri, congestie

3.5.2 Dshield/Internet Storm Center

Această abordare are la bază colectarea de fişiere de detecție a intruziunilor oferite de diferite organizații, care în momentul de față acoperă peste 500.000 adrese IP din peste 50 de țări. Această abordare asigură o mai bună distribuție asupra spațiului de monitorizare, însă diversitatea configurațiilor IDS utilizate de multiple organizații, poate genera probleme de interpretare atunci în cazul unor evenimente pentru care nu există reguli Snort în pachetul de bază [ISC--].

3.5.3 ATLAS (Active Threat Level Analysis System)

ATLAS este una din primele inițiativele care a avut ca obiectiv construirea unei rețele de analiză a amenințărilor la nivel global.

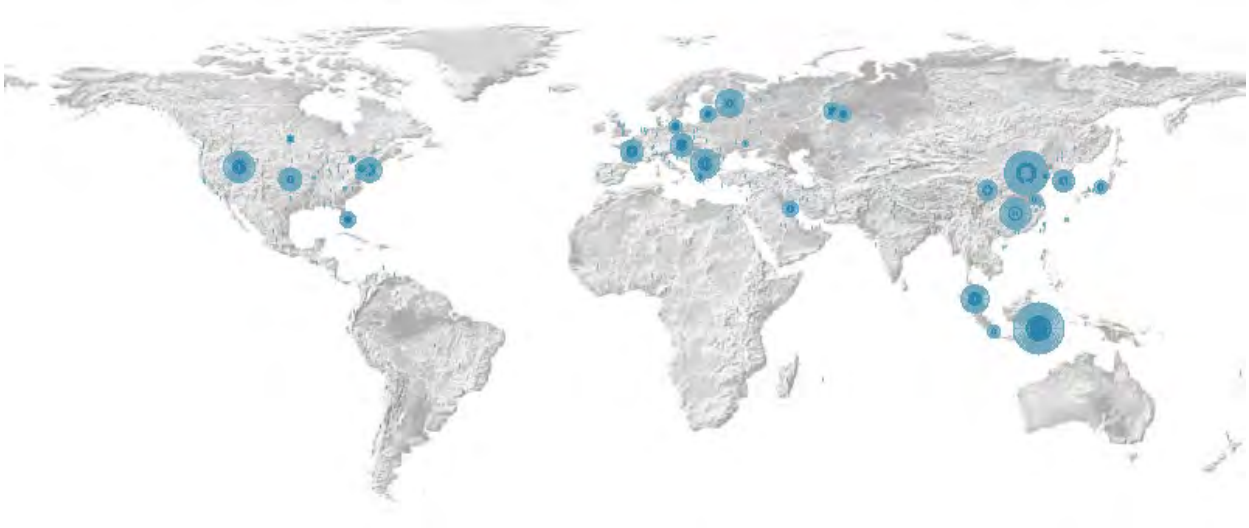


Figura 3.21 - Consola de monitorizare globala ATLAS – Distribuția geografica a atacurilor 23/09/2011 [Arb11-01]

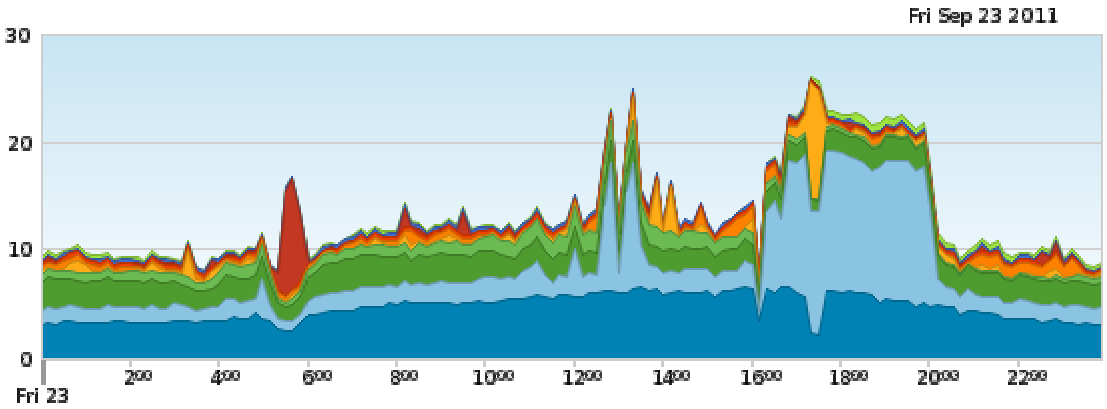
Datele sunt capturate prin utilizarea de senzori distribuiți global care rulează o serie de aplicații de captură şi analiză de date. Senzorii au capacitatea de a:

- Interacționa cu atacatorii pentru a determina „intențiile" acestora
- Captură de trafic complet şi analiza acestuia
- Caracterizarea traficului de scanare

Datele sunt apoi trimise la o locație centrală pentru analiză detailată şi prezentare la consolă.

Alte surse de date utilizate de ATLAS sunt:

- Trafic capturat de honeypots
- Fişiere log IDS
- Fişiere de scanare
- Statistici DoS la nivel Internet
- Ştiri şi rapoarte de vulnerabilitate
- Eşantioane de malware capturat
  - ♦ Date despre infrastructura de phishing
  - ♦ Date comanda şi control botnets



Key	Service	Attacks per subnet	Percentage
	TCP/445 (microsoft-ds)	640.98	31.0%
	TCP/80 (http)	515.81	24.9%
	UDP/1434 (ms-sql-m)	310.65	15.0%
	UDP/49550	125.23	6.1%
	UDP/5060 (sip)	71.32	3.4%
	TCP/5900	52.97	2.6%
	TCP/9988	46.30	2.2%
	TCP/3306 (mysql)	42.98	2.1%
	UDP/0	39.23	1.9%
	TCP/23 (telnet)	32.83	1.6%
	Other	190.51	9.2%

Figura 3.22 - Consola de monitorizare globala ATLAS – Distribuția după servicii a atacurilor 23/09/2011 [Arb11-02]

Acoperirea globală este în mare parte rezultatul FSA (Fingerprint Sharing Alliance), o alianță creată în 2005 şi care reuneşte furnizori de serviciu majori în Internet, care operează pe toate continentele. Programul FSA oferă participanților un mecanism prin care pot partaja uşor şi rapid informații despre atacuri între organizații, şi care adresează [FSA11]:

- Cerințele specifice de ordin legislativ
- Disponibilitatea datelor în timp real
- Vocabular comun de descriere a anomaliilor
- Modului de adresare a anomaliilor având în vedere complexitatea relațiilor între entitățile implicate

Un avantaj al acestei abordări de „amprentare" a anomaliilor este faptul că nu necesită investiții majore de infrastructură, putând fi văzută mai degrabă ca un limbaj standard care facilitează comunicarea de informații despre atac.

Informația de caracterizare a anomaliei de rețea observată de membru include contextul atacului şi informațiile de contact pentru centru de operare de rețea al părților implicate. Contextul atacului este un set de statistici care identifică în mod unic anomaliile de trafic observate. În plus, acesta oferă datele necesare interpretării evenimentului şi înțelegerii amenințării la adresa utilizatorilor. Poate include informații precum:

- *Scopul* : set de prefixe de rețele atacate, informații de corelație spațială sau temporală asupra atacurilor
- *Severitatea* : rata de trafic de atac din volumul total de trafic
- *Impactul*: efectul atacului asupra echipamentelor de rețea, serviciilor şi utilizatorilor
- *Informații* de contact persoane care au autoritatea şi responsabilitatea pentru adresarea acestui gen de evenimente

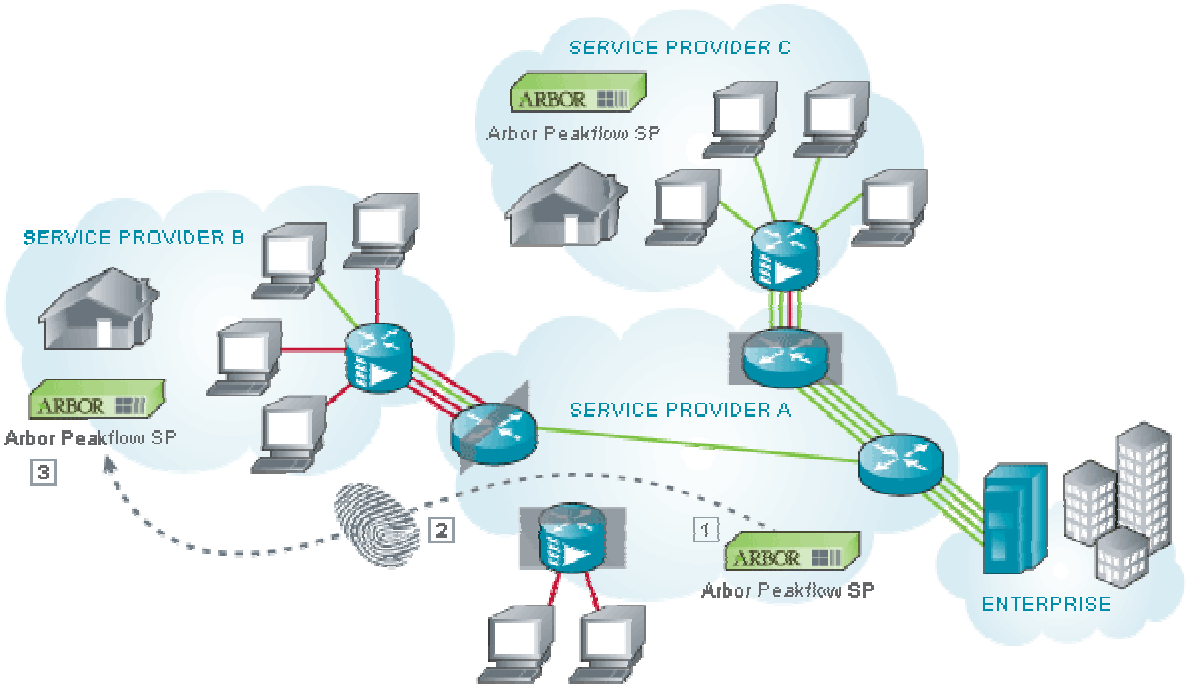


Figura 3.23 - Arhitectura de monitorizare globala Arbor/ATLAS [FSA11]

3.5.4 Studii de caz

3.5.4.1 Monitorizarea amenințărilor pe baza datelor CAIDA

Un eveniment major identificat de CAIDA (utilizând o soluție de monitorizare de tip Network Telescope) a fost propagarea viermelui Conficker. Apărut în Noiembrie 2008, acesta a avut o propagare foarte rapidă, precum şi o serie de transformări într-o perioadă de câteva luni. Versiunea inițială, Conficker A, a început pe 21/11/2008 infectând stațiile prin exploatarea vulnerabilității MS08-067 a Microsoft Windows [MS11-01]. CAIDA a observat trafic de la stațiile infectate cu Conficker utilizând UCSD Network Telescope şi documentat comportamentul în [Cai08].

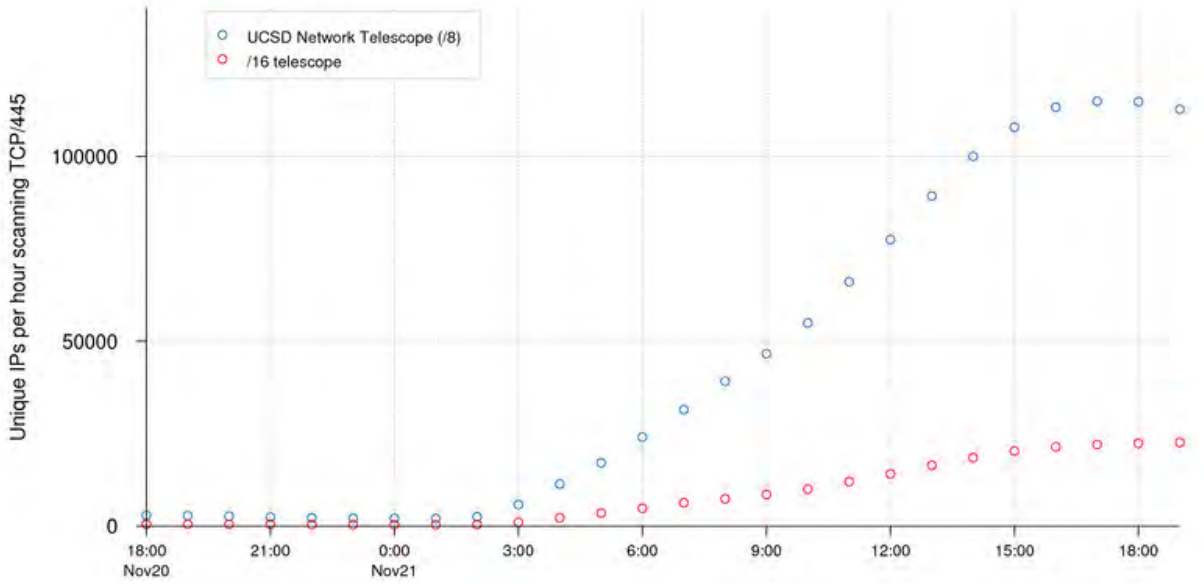


Figura 3.24 - Evoluția inițială a numărului de IP scanează port TCP/445 - Sursa [Cai08].

Trendul din această perioadă inițială indică prezență unui vierme care afectează infrastructura globală a Internetlui, putându-se estima şi rata de infectare la nivel global. În cazul de față, rata de infectare la nivelul Internetlui (calculata pe baza [PPN05-01]) este de $\beta = 18 = 114911 * 8/(14 * 3600)$ stații pe secundă, unde 114911 este valoarea maximă atinsă a numărului de adrese IP ce scanează spațiul telescopului de clasă A (/8) (între ora 17 şi 18), iar 14 reprezintă numărul aproximativ de ore în care trendul de creştere este uniform.

Propagarea Conficker B a fost observată începând cu data de 29/12/2008, şi a introdus tehnici suplimentare pentru răspândire. Conficker A şi B au utilizat un algoritm de generare pseudo-aleatoare de nume de domenii, şi încărcau cod nou de pe un webserver când era identificat la respectivul nume de domeniu [Por09].

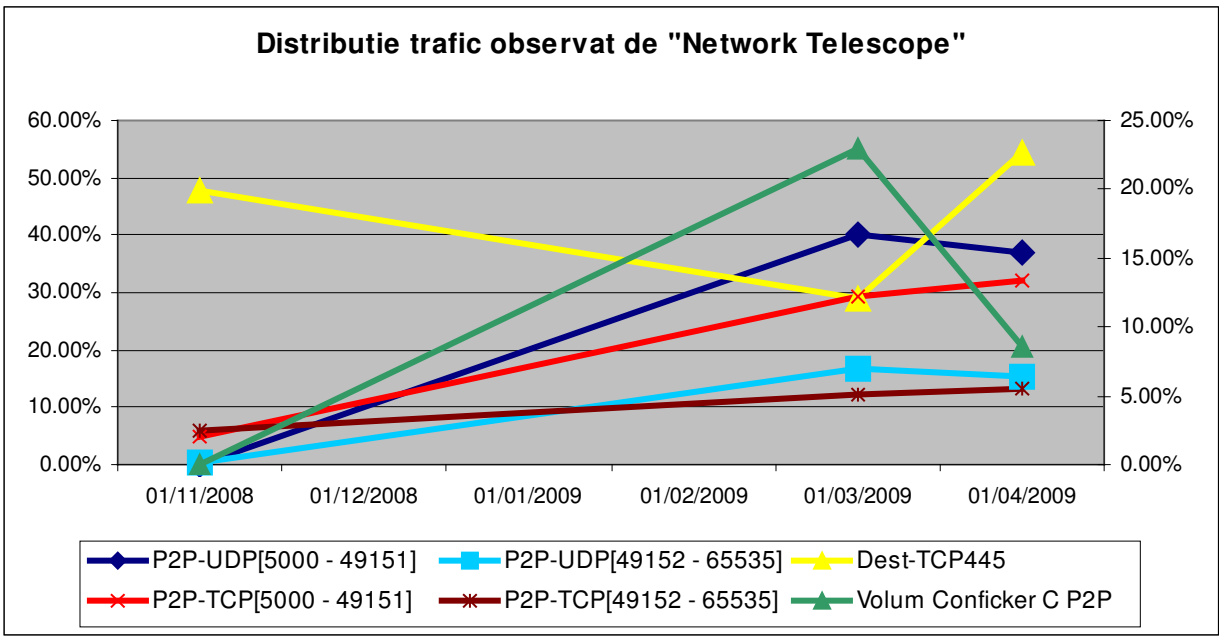


Figura 3.25 – Distribuție trafic observat de „Network Telescope"

Pentru a exemplifica modul de utilizare a informațiilor colectate de telescop pentru analiza evoluției viermelui, se va utiliza un eşantion de date bazat pe traficul recepționat de telescop de durata unui interval de 1 oră din zilele de 21/11/2008 (începutul propagării Conficker A), 18/03/2009 (după Conficker C) şi 25/04/2009 (după Conficker E). Perioada aleasă este ilustrativă pentru înțelegerea caracteristicilor de propagare ale versiunii Conficker C (versiunea P2P) lansată pe 05/03/2009. După cum se poate observa aproape 25% din traficul recepționat pe 18/03 de telescop a fost de tip Conficker C ce a utilizat pentru propagare porturi TCP/UDP peste 5000. Numărul de pachete TCP cu portul destinație 445 este în scădere, ceea ce sugerează că Conficker C nu scanează vulnerabilitatea MS08-067. Pe 25/04 se observă o scădere a volumului de trafic Conficker C la 8% din traficul recepționat de telescop ceea ce indică o scădere a populației, însă distribuția pe porturi menținându-se în acelaşi trend, ceea ce indică acelaşi gen de activitate. Volumul de pachete TCP 445 este în creştere ceea ce sugerează că celelalte versiuni Conficker sondează din nou vulnerabilitatea MS08-067.

3.5.4.2 Monitorizarea amenințărilor pe baza datelor DShield (ISC)

Pentru a ilustra utilitatea unei astfel de soluții în procesul de monitorizare de tip intelligence se va analiza evoluția numărului de scanări pentru portul TCP 445 pe o durată reprezentativă din activitatea viermelui Conficker [Aco09].

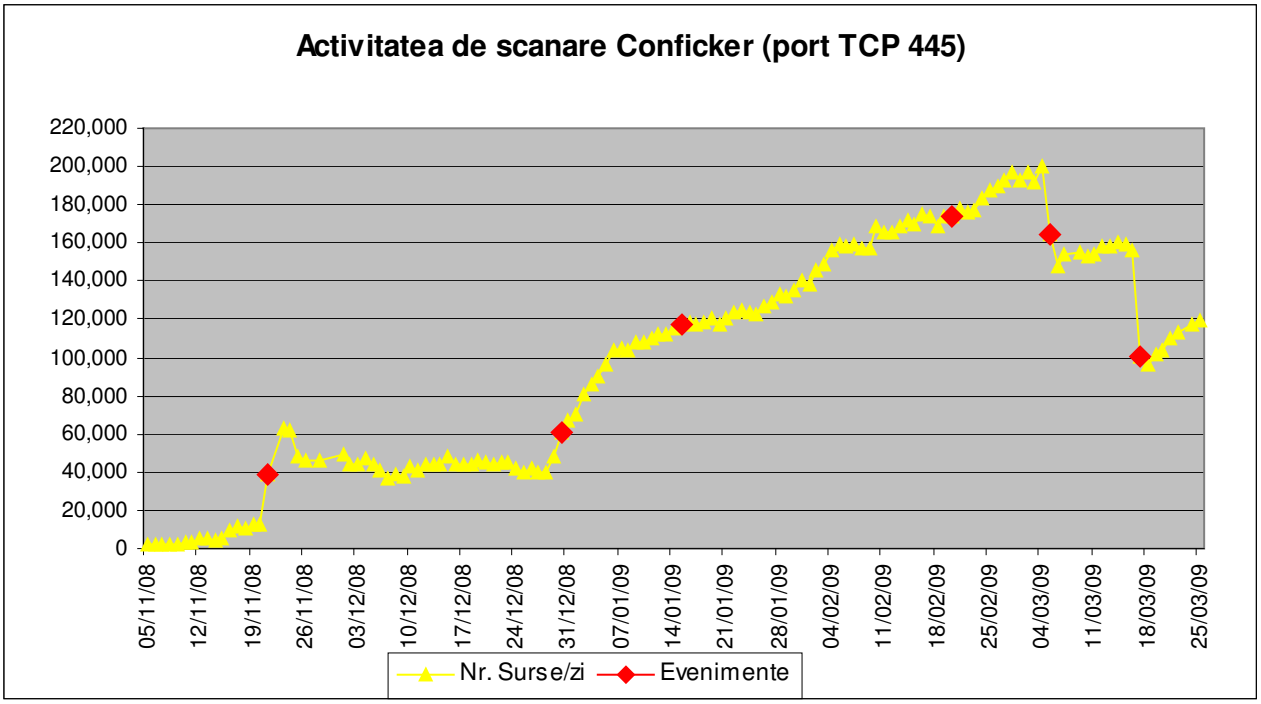


Figura 3.29 – Activitatea de scanare pentru port TCP 445 11/2008 – 03/2009 (sursa [ISC--])

În ciuda limitărilor care afectează acuratețea datelor în cazul (CAIDA şi DShield), unele (menționate în secțiunea 3.5.1), precum şi accesului limitat la datele colectate (în cazul ATLAS şi CAIDA), analiza trendului este în măsură să ofere rezultate foarte utile mai ales prin prisma monitorizării contextului general extern global şi identificării schimbărilor ca apar în spațiul amenințărilor.

Data	Eveniment	Stare observată
21/11/2008	Începutul propagării viermelui Conficker A ce scanează uniform întreg spaţiul Internet exploatând vulnerabilitatea MS08-067 Microsoft Windows accesibilă via port TCP/445	Creşte imediată a numărului de scanări. Majoritatea infecţiilor se finalizează în primele zile. După câteva zile scade cu 25% în principal datorită măsurilor de răspuns ale organizaţiilor. Un număr mare de PC (în mare parte sisteme personale continuă) să fie infectate
29/12/2008	Începe propagarea Conficker B. Acesta incorporează algoritmul de hashing MD6 hashing pentru a securiza comunicaţia staţiile infectate şi punctele de întâlnire . Scopul urmărit a fost de a împiedica botnet-urile rivale de a prelua controlul asupra staţiilor infectate	Creşterea a numărului de scanări datorat unui nou vector de propagare (USB) . Trendul de creştere se menţine în contextual unei reacţii minime datorate sărbătorilor de Anul Nou, precum şi al faptului că maşinile preponderent afectate sunt cele personale.
15/01/2009	Microsoft oferă un program de dezinfecţie pentru versiunile iniţiale	Oferă o stabilizare a numărului de scanări. Faptul că volumul se menţine ridicat indică gradul încă ridicat de lipsă de interes al utilizatorilor finali în ceea ce priveşte problemele de securitate.
20/02/2009	Se lansează Conficker C	Volumul de scanare îşi menţine acelaşi trend deoarece populaţia Conficker A,B existentă , cât şi cea vulnerabilă îşi menţin caracteristicile, iar Conficker C nu utilizează scanare TCP/445.
05/03/2009	Conficker C începe să preia controlul asupra staţiilor PC infectate cu Conficker B şi B++. Conficker C organizează staţiile infectate în reţele P2P şi întrerupe scanarea aleatoare asupra portului TCP/445	Se observă o scădere accentuată în volumul de scanare datorată faptului ca versiunea C nu utilizează scanarea TCP445. Scanarea nu a revenit la nivelul lui 11/2008 deoarece există încă o populaţie mare Conficker A
17/03/2009	Începe migrarea PC infectate către Conficker D	Se observă o scădere justificată prin migrarea unor sisteme cu versiunea A, direct către D

Tabel 3.2 – Momente de referință în evoluția viermelui Conficker în perioada 11/2008-03/2009

Motto: *Modul cum abordezi o problemă este mai important decât problema în sine.*
- Voltaire

CAPITOLUL 4

ARHITECTURA DE MONITORIZARE A SECURITĂȚII

O arhitectură generică de monitorizare a securității are următoarele componente: surse de evenimente cu relevanță pentru procesul de monitorizare (sisteme IDS de rețea, rutere, sisteme de verificare a integrității fişierelor, etc.), colectoare de evenimente, baza de date cu mesaje de securitate, module de analiză şi aplicații pentru suportul răspunsului la incidentele de securitate identificate [PPN08]. Problema cea mai des întâlnită în implementarea unei arhitecturi o reprezintă integrarea componentelor enumerate anterior, în contextul asigurării integrității, disponibilității şi securității datelor, şi a canalelor de comunicație între componente. Pentru o aplicabilitate extinsă se va considera că infrastructura ce se doreşte a fi monitorizată aparține unei organizații diferită de cea ce oferă serviciile de monitorizare - cazul tipic pentru serviciile externalizate cum ar fi Managed Security Servicies [Cou02]. Pentru simplificare, se va utiliza termenul de „infrastructura clientului" pentru a desemna „infrastructura clientului ce se doreşte a fi monitorizată".

4.1 Evaluarea stării de securitate a infrastructurii IT a clientului

Eficacitatea componentei de monitorizare este strâns legată de modul de operare ale celorlalte componente ale programul de management al securității organizației clientului. De aceea, înainte de a începe implementarea arhitecturii de monitorizare, este necesar a se evalua [PPN07-01]:

- Identificarea claselor de amenințare şi stabilirea zonelor de monitorizare
- Politica de securitate în termeni de drepturi de acces, operații permise, etc.
- Starea generală de securitate a infrastructurii clientului. În acest mod se poate determina dacă o cale de atac poate conduce efectiv la o intruziune pe sistemele clientului, precum şi nivelul critic asociat încercării de intruziunii.

4.1.1 Inventarul tehnic şi organizațional

Evaluarea nivelului de securitate poate fi împărțită în următoarele componente [PPIN08-01]:

- Stabilirea stării de vulnerabilitate a infrastructurii clientului. Colectarea acestor date se poate efectua utilizând tehnici precum [PNN10]:
  - ♦ Black Box (cutie închisă) – Asemenea unui proces PenTest (testarea penetrării), se scanează infrastructura clientului pentru a obține informații

despre: topologie, porturi deschise, aplicații, vulnerabilități, sisteme de operare. Este o opțiune folosită pe scară largă deoarece informațiile se obțin foarte rapid.

- ♦ White Box (cutie deschisă) – În acest caz clientul va oferi informații legate de inventarul hardware, topologia infrastructurii sale, aplicații, etc. Se recomandă a fi utilizată în cazul în care se doreşte generarea căilor de intruziune precum şi când infrastructura foarte complexă şi utilizează controale care previn scanarea.

- Importanța pentru procesele organizației clientului a fiecărei componente din infrastructura IT a acestuia. Deoarece această componentă prezintă un grad ridicat de subiectivism, pentru a determina cât mai obiectiv impactul asupra clientului pe care-l poate avea o intruziune, se recomandă ca analiza să se efectueze utilizând o metodă standard pentru clasificarea şi taxonomia atacurilor de genul celei prezentate în secțiunea 1.5.5 (o versiune simplă) sau 2.4.5 (dacă se doreşte o versiune mai complexă).

Datele obținute la acest pas se vor salva în baza de cunoştințe (modulul Înregistrare Configurație Client).

4.1.2 Stabilirea modelelor de amenințare şi a zonelor de monitorizare

Un modelul de amenințare este o expresie a aşteptărilor referitoare la natura atacatorului şi la caracteristicile potențialelor victime. Atacatorii pot fi grupați în următoarele clase [Bej04]:

- Atacatori externi care lansează intruziuni din Internet
- Atacatori externi care lansează intruziuni din segmente wireless
- Atacatori interni care lansează intruziuni dintr-un LAN
- Atacatori interni care lansează intruziuni din segmente wireless.

Abilitatea de a observa victimele pentru diferite tipuri de atac determină şi amplasarea platformelor de monitorizare (senzori). Figura 4.1 arată un exemplu de rețea ale cărei componente pot fi regăsite în organizații mici şi mijlocii, având patru zone de monitorizare. Zonele de monitorizare sunt locațiile în care traficul are anumite nivele de privilegiu, stabilite pe baza unui nivel de încredere definit de inginerul de securitate. Aceste trăsături sunt determinate de un dispozitiv de control al accesului, care segmentează traficul în zone diferite. În cazul exemplului de față, dispozitivul de control al accesului este un firewall, care împarte organizația în patru zone distincte: perimetrul, zona demilitarizată (DMZ), zona wireless şi intranet.

Perimetrul cuprinde zona dintre interfața externă a firewall-ului şi ruter-ul de conectare la Internet. Această zonă a reprezentat în mod tradițional locul de amplasare al senzorilor, deoarece oferă cea mai bună vizibilitate asupra amenințărilor externe din Internet. Perimetrul este de asemenea considerat zona cu cel mai scăzut nivel de încredere, deoarece organizația are control limitat asupra stațiilor care inițiază conexiuni către acesta.

Organizațiile care amplasează senzori în perimetru au posibilitatea să colecteze informații despre amenințări. Activitatea de scanare şi încercările de intruziune eşuate la nivelul firewall-ului pot constitui indicatori pentru viitoare atacuri.

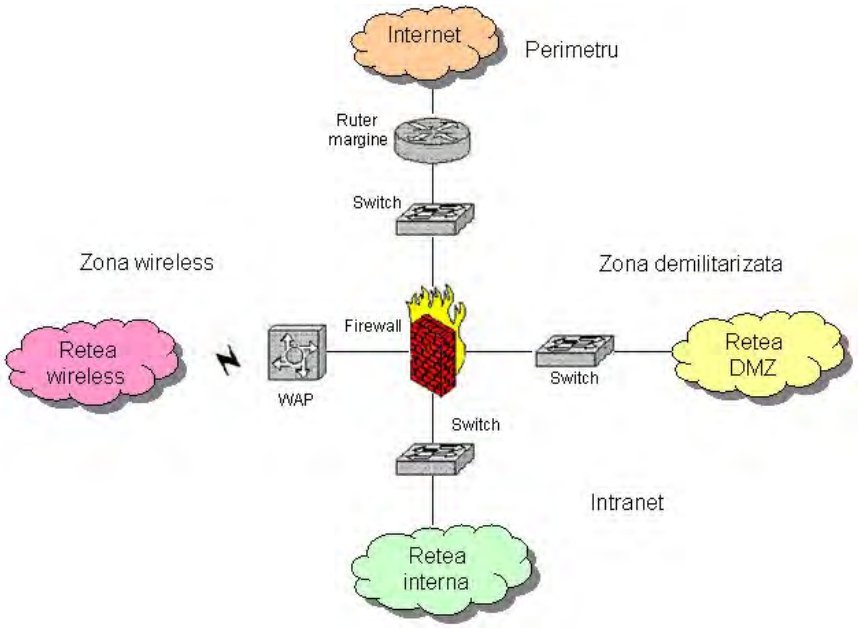


Figura 4.1 - Zone de monitorizare

Zona demilitarizată cuprinde stațiile conectate la switch-ul DMZ. Senzorii plasați în această zonă vor urmări în mare măsură descoperirea atacurilor împotriva serviciilor uzuale din DMZ (e-mail, web, DNS, FTP, etc), precum şi atacuri inițiate din DMZ către alte zone. Produsele de detecție pe baza traficului de rețea oferă un grad de eficiență ridicat în monitorizarea stațiilor DMZ, datorită nivelului scăzut de trafic de zgomot şi politicii de securitate relativ simple care guvernează activitatea DMZ. Principala problemă a senzorilor din DMZ o constituie manipularea traficului criptat. Senzorii generici nu pot inspecta conținutul traficului de web ce utilizează criptare SSL, dar există anumite tehnici specializate pentru a oferi vizibilitate la nivel rețea cum ar fi: senzorii cu chei ”escrow”, dispozitive de accelerare a SSL şi proxy reverse web.

DMZ reprezintă o rețea cu nivel de încredere mediu, deoarece stațiile sunt sub controlul direct al organizației, dar sunt expuse utilizatorilor din Internet. O bună administrare va limita conectivitatea stațiilor din DMZ către celelalte segmente, în special intranet.

Zona wireless cuprinde toate stațiile cu conectivitate wireless. Stațiile din această zonă au nivel de încredere scăzut, ca şi cele din Internet, deoarece oricine aflat în raza de acces a punctului de acces wireless (WAP) se poate conecta în mod teoretic la segmentul wireless. Atacatorii externi din această zonă pot fi grupați în două categorii:

- Utilizatori de servicii fără plată, neautorizați (datorită unei configurări neadecvate)
- Potențiali spioni care doresc acces la informații confidențiale.

Metodele şi tehnicile de detecție disponibile pentru această sunt: Airdefense RogueWatch, Airdefense Guard, Snort-Wireless, WIDZ [Pfl11]. Strategiile curente vizează detecția atacurilor din această zonă către intranet. Multe organizații au soluții ineficiente pentru protecția clienților din această zonă. În ceea ce priveşte amenințările externe din Internet, stațiile din zona wireless adesea sunt tratate la fel ca şi cele din Intranet.

Intranet-ul cuprinde toate stațiile conectate la switch-ul intern şi este delimitat de interfața internă a firewall-ului. Stațiile din această zonă au nivelul de încredere cel mai ridicat. Utilizatorii din Internet nu trebuie să acceseze direct aceste sisteme, decât după ce au fost autentificați utilizând un mecanism VPN. Se recomandă monitorizarea în special pe bază de HIDS, deoarece intruziunile împotriva stațiilor intranet sunt cel mai adesea lansate din interior. NIDS sunt mai puțin eficiente în această zonă deoarece atacatorii interni nu scanează sisteme vulnerabile, nu caută să exploateze victima, nu copiază informația confidențială prin rețea către stații externe, ci pot accesa informația folosind un cont şi parolă validă şi o pot copia pe un mediu extern.

Metodele de detecție bazate pe NIDS vizează în special atacurile lansate din exterior. În cazul în care este necesară monitorizarea intranetului la nivel rețea, se recomandă următoarele abordări pentru a adresa limitări datorate complexității intranetului şi a volumului ridicat de trafic al acestuia:

- Datorită segmentării rețelelor interne şi a faptului că în majoritatea cazurilor stațiile de aceeaşi importanță sunt grupate în acelaşi segment, senzorii se pot plasa în aceste subrețele.
- Amplasarea de agenți de colectare pe stațiile critice, care vor transmite traficul către un senzor centralizat.

4.1.3 Considerații specifice zonelor de monitorizare wireless

Conceptual se pot implementa următoarele tipuri de monitorizare:

- Monitorizarea ca participant la rețea în care senzorul este plasat între WAP şi firewall. O astfel de instalare va monitoriza activitatea din şi spre zona wireless, dar nu şi în zona wireless.
- Monitorizarea ca participant în zona wireless în care senzorul este echipat cu interfață wireless. În cazul în care senzorul este participant în rețeaua wireless, acesta se asociază unui WAP şi obține o adresă de IP de la acesta. Traficul de monitorizare observat va fi asemănător unui client conectat la o rețea Eternet clasică.
- Monitorizarea ca observator în zona wireless poate fi realizată cu dispozitive specializate sau utilizând un kernel Linux Knoppix [Kno02]. În acest mod senzorul poate accesa şi frame-urile de management care sunt invizibile majorității participanților în rețeaua wireless. Ca observator se pot depista atacurile de tip disociere.
- Monitorizarea la nivelul WAP. Majoritatea punctelor de acces bazate pe kernel Linux, sau BSD oferă posibilitatea accesului la traficul din rețeaua wireless [Sam02]. WAP comerciale actuale oferă posibilitatea de a copia local traficul care-l operează prin instalarea de IDS (Snort), sistemul de fişiere fiind accesat via NFS de către o stație de colectare centrală.

4.1.4 Baza de date cu vulnerabilități

Această componentă conține informații despre breşe de securitate şi combinații de situații care ar putea avea impact asupra securității în general, sau ar putea fi exploatate de un atacator pentru a realiza o intruziune. Formatul bazei de date va trebui sa includă următoarele tipuri de vulnerabilități [Tho05]:

- *Vulnerabilități structurale* – acestea sunt vulnerabilități interne ale unei aplicații cum ar fi: condiții de concurență (race conditions), buffer overflow, erori de format de şir de caractere, etc. Această parte a bazei de date este cel mai uşor de implementat, şi actualizat. Majoritatea acestor procese pot fi automatizate având în vedere că informația este accesibilă prin intermediul subscrierii la anumite liste publice de poştă, sau direct de pe anumite site-uri web unde se găsesc vulnerabilități [CVE--]. În cazul utilizării mai multor surse, este necesară validarea şi corelarea acestora de către o echipă abilitată în acest sens.
- *Vulnerabilități funcționale* – acestea depind în principal de mediul operațional (configurații, condițiile operaționale, utilizatori, etc.). De exemplu, o partiție montată via NFS se consideră a fi vulnerabilitate funcțională în contextul în care atacatorul poate accesa un cont sau sistem care îi permite montarea sistemului de fişiere. De aceea, se poate presupune că există un număr mare de astfel de vulnerabilități în sisteme, dar pot fi considerate ca inactive atât timp cât cel puțin o condiție necesară nu este satisfăcută. Definirea, reprezentarea şi actualizarea bazei de date reprezintă o sarcină destul de dificilă pentru această categorie de vulnerabilități, şi necesită conlucrarea unor echipe din mai multe domenii (aplicații, sisteme de operare, rețea, baze de date, etc.).
- *Vulnerabilități topologice* – includ vulnerabilități datorate protocoalelor de comunicație în rețea (de exemplu: sniffing, spoofing, hijacking, etc). Pentru a putea fi introduse în baza de date, aceste vulnerabilități trebuie să ofere suport pentru modelarea topologiei.

4.1.5 Politica de securitate

După stabilirea inventarului infrastructurii client, se vor evalua aspectele politicii de securitate care influențează generarea de evenimente, procesele de raportare şi reacție la intruziuni, pentru a fi păstrate în baza de cunoştințe.

Aspecte precum autorizarea, procedurile de testare şi auditare vor oferi informații legate de tipul de comportament pe care senzorii îl vor putea detecta. Evenimentele generate (cum ar fi: accesul de nivel administrator, scanare porturi, etc.) vor fi evaluate în contextul politicii de securitate. Cele găsite ca neconforme cu criteriile politicii de securitate vor fi analizate ca parte posibilă a unei încercări de intruziune [PN08].

4.1.6 Evaluarea nivelului de securitate a clientului

Ultima componentă a bazei de cunoştințe o reprezintă evaluarea detaliată a nivelului de securitate a infrastructurii clientului. Această evaluare conține [OSS05]:

- Vulnerabilitățile la care sunt expuse sistemele identificate (la pas 4.1.1) conform bazei de vulnerabilități (4.1.4) şi a cerințelor definite în politica de securitate (4.1.5)
- Impactul relativ pentru fiecare vulnerabilitate la care există expunere
- Căile de atac ce conduc la activarea vulnerabilităților inactive.

Acest nivel de evaluare va trebui regenerat de fiecare dată când sunt modificări în rândul vulnerabilităților (de exemplu: o nouă vulnerabilitate este identificată), sau al sistemelor client monitorizate (de exemplu: un server web este instalat pe un client deja monitorizat, sau clientul introduce un nou sistem în infrastructura sa).

4.1.7 Considerații asupra administrării senzorilor dispuşi în perimetrul clientului

Managementul senzorilor utilizează una sau mai multe strategii, fiecare având caracteristici de securitate, utilitate şi eficiență specifice. Serviciile necesare arhitecturii de monitorizare determină adesea opțiunile de acces la distanță. Cele mai populare metode de acces la senzori sunt [Bej04]:

- Accesul senzorului prin consolă reprezintă cea mai sigură modalitate de management a senzorului. Deşi accesul strict prin consolă limitează capacitatea atacatorului de a lansa atacuri împotriva senzorului, acesta nu este imun totuşi la compromitere. Atâta timp cât activitatea malițioasă este vizibilă senzorului, atacatorul are o modalitate de a influența modul de operare al senzorului. Cele mai distructive modalități de atacare a senzorilor presupun exploatarea unor vulnerabilități ale software-ului care colectează date prin interfața de monitorizare. Un exemplu în acest sens îl reprezintă vulnerabilitățile unor aplicații majore utilizate în sistemele IDS de rețea cum ar fi tcpdump [CER--].
- Acces la distanță în bandă presupune administrarea senzorului prin utilizarea infrastructurii de rețea a organizației (senzorul şi stația de management, utilizează aceeaşi infrastructură utilizată de ceilalți utilizatori pentru trafic de e-mail, web, etc). Atât accesul la date cât şi administrarea se face utilizând VPN. Dezavantajul acestui tip de acces îl reprezintă fragilitatea – configurări greşite ale SSH, serviciilor VPN (IPSec), sau unele aspecte ale stivei de rețea pot duce la izolarea senzorului.
- Acces la distanță în afară de bandă presupune administrarea senzorilor utilizând canale de comunicație separate de cele utilizate pentru transferul traficului utilizator. Ca opțiuni în acest sens ar fi echiparea senzorului cu o interfață dedicată şi utilizarea de linii dedicate pentru conectarea cu site-ul unde este dispus senzorul. Unii administratori consideră că Internetul este destul de fiabil, dar există posibilitatea de blocare al senzorilor, care ar necesita o repornire la rece. Pentru aceasta, senzorii se conectează la surse de alimentare controlate prin rețea.

4.2 Componentele Arhitecturii de Monitorizare a Securității

Definiție: *Arhitectura de monitorizare a securității* este un termen generic pentru o colecție de sisteme al cărei scop este de a furniza servicii de detecție şi răspuns la incidentele de securitate care au loc în organizația respectivă.

Pe baza acestei definiții se pot distinge următoarele operații efectuate de arhitectura de monitorizare: generarea, colectarea, stocarea, analiza evenimente de securitate şi răspunsul la incidentele de securitate.

Utilizând terminologie similară celei definite în CIDF şi IDMEF [RFC-4765], sistemele care alcătuiesc arhitectura de monitorizare a securității se clasifică în funcție de operațiile efectuate după cum urmează:

- Sisteme **E** - generează evenimente de securitate
- Sisteme **C** - colectează evenimente de la sistemele E
- Sisteme **D** - stochează baza de date cu evenimente
- Sisteme **A** - realizează analize şi corelații de evenimente

- Sisteme **K** - responsabile cu managementul cunoştinţelor despre vulnerabilităţi, semnături de intruziuni, configuraţia platformelor protejate, precum şi alte informaţii utile analistului de securitate
- Sisteme **R** - răspund la incidente, sau suportă personalul de securitate în procesul de răspuns la incidente.

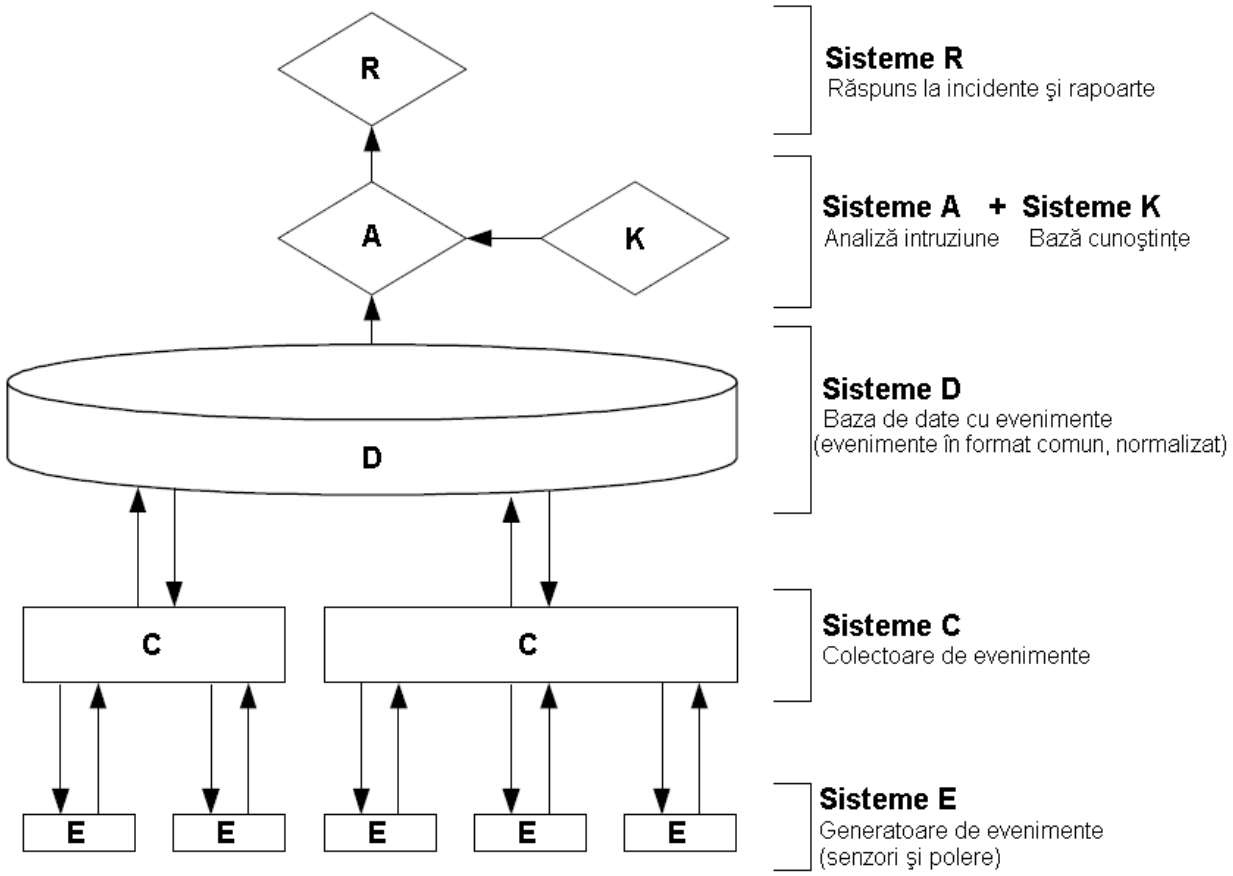


Figura 4.2 - Componentele arhitectura de monitorizare a securităţii şi relaţiile între acestea

4.2.1 Sisteme E

În funcţie de modul de creare a evenimentelor, sistemele de tip E se împart în două categorii [Els08]:

- Generatoare bazate pe evenimente (senzori). Evenimentele de securitate sunt create ca urmare a unei operaţii specifice executate de sistemul de operare, de aplicaţie sau a unei activităţi detectate în reţea.
- Generatoare bazate pe stare (pollers). Evenimentele sunt generate ca urmare a unui interogări externe cum ar fi: cerere ping, verificare a integrităţii datelor, verificarea stării unui daemon, etc.

Senzorul este un agent autonom ce rulează într-un mediu potenţial ostil, şi care are următoarele caracteristici [Spa00]: rulează permanent, este configurabil şi adaptabil, este scalabil, tolerant la defecţiune, rezistent la atacuri, necesită resurse limitate, asigură o degradare treptată a serviciului, şi permite o reconfigurare dinamică.

Exemple de senzorii utilizați în implementarea soluțiilor de monitorizare sunt [PPN07-01]:

- NIDS, HIDS
- Sisteme de filtrare (la nivel de rețea, aplicație sau utilizator) cum ar fi: sisteme firewall, rutere cu liste de control al accesului (ACLs), switch-uri ce implementează filtrare pe adrese de tip MAC, servere de autentificare (RADIUS).
- Honeypots,
- Snifere de rețea, etc.

Polerele generează un eveniment atunci când detectează o anumită stare pe un sistem terț. Un exemplu de polere îl reprezintă sistemele de management în rețea. În contextul monitorizării securității, polerele vor verifica starea serviciilor (pentru a detecta situații de tip DoS) şi integritatea datelor (de exemplu conținutul unei pagini web). Principala limitare a acestui tip de sistem E o reprezintă performanța. În cazul în care polerul este configurat să interogheze multe stații țintă la intervale scurte de timp, consumul de resurse (CPU, bandă de rețea) poate afecta operarea polerului.

4.2.2 Sisteme C şi D

Sistemele de tip C au rolul de a colecta evenimentele generate de sistemele E şi de a le translata într-un format standard ce permite o procesare consistentă la nivelul întregului spațiu monitorizat. Principalele riscuri arhitecturale ale sistemelor C le reprezintă disponibilitatea şi scalabilitatea, însă aceste riscuri se pot adresa utilizând soluții tipice serverelor pentru rezolvarea unor astfel de probleme cum ar fi: folosirea unor soluții de tip cluster, HA (High Availability - de disponibilitate ridicată), şi LB (Load Balanced – de distribuire a încărcăturii) [OSS05].

În momentul de față nu este definit un standard legat de formatarea datelor colectate, acest subiect fiind încă o problemă nerezolvată în rândul comunității de securitate.

Sistemele de tip D sunt baze de date şi reprezintă componentele cu cel mai înalt grad de standardizare din arhitectura de monitorizare a securității. MySQL este adesea opțiunea pentru implementările bazate pe surse deschise (cum ar fi OSSIM), iar Oracle sau MS SQL pentru implementări comerciale, sau foarte complexe (cum ar fi Counterpane). Aceste sisteme realizează totodată şi normalizarea evenimentelor – identificarea şi combinarea evenimentelor duplicate generate de aceeaşi sursă sau provenind de la surse distincte [PPN08].

Dintre problemele ce trebuie avute în vedere la implementarea acestei componente într-o arhitectură de monitorizare a securității se amintesc: disponibilitatea, integritatea şi confidențialitatea bazelor de date (acestea fiind aspecte tipice legate de bazele de date), precum şi performanța bazelor de date. Pentru ca arhitectura de monitorizare a securității să răspundă eficace la încercările de intruziune, evenimentele vor trebui stocate, procesate şi analizate cât mai rapid.

4.2.3 Sisteme A şi K

Sistemele K (în general baze de date) conțin informații şi cunoştințe despre: politica de securitate, infrastructura monitorizată, vulnerabilități, scenarii de intruziune şi indicatori

de securitate la nivel global.

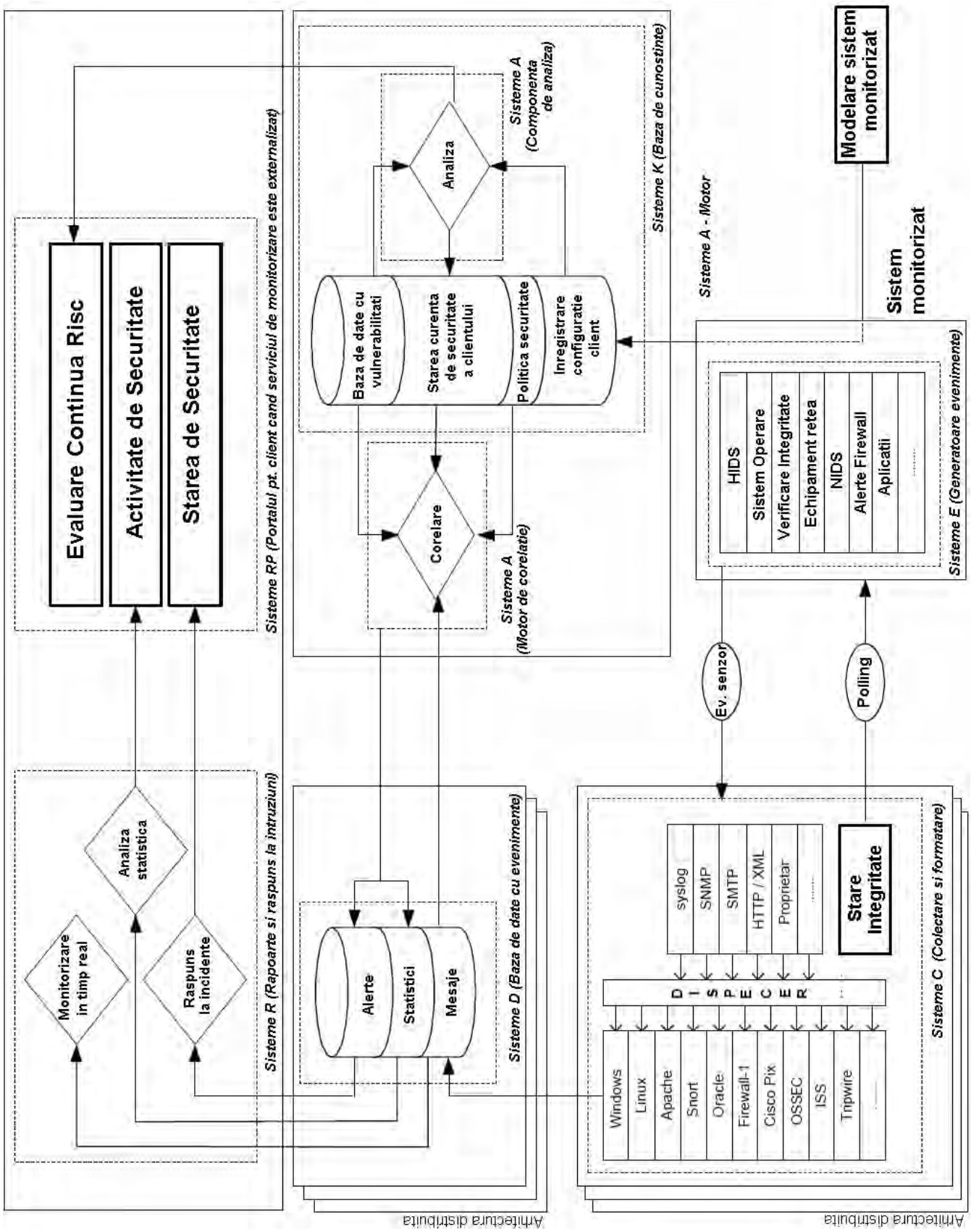


Figura 4.3 - Arhitectură generică de monitorizare a securității [Gan08][OSS05][Cou03]

Sistemele A au rolul de a analiza evenimentele stocate în sistemele de tip D în contextul cunoştinţelor oferite de sistemele K, cu scopul de a genera mesaje de alertă cu un grad cât mai mare de acurateţe.

Noile tehnologii şi aplicaţii în Internet, precum şi modificări în spaţiul vulnerabilităţilor, ameninţărilor şi al managementului de risc, necesită o revizuire constantă a sistemelor A . Aceasta a determinat ca implementările comerciale actuale ale acestor componente să fie proprietare (cum ar fi Socrates folosit de BT Counterpane [Cou02]), iar cele din surse deschise, deşi destul de diverse, să fie limitate la stadiul de verificare a conceptului. [PPN09]

Totodată, operarea acestor sisteme necesită o activitate umană intensă (analişti de securitate), care să adreseze limitările proceselor de analiză curente în situaţii conflictuale (datorate unor scenarii de atac incorecte), contradictorii (când unii senzori au fost corupţi şi oferă evenimente fabricate), sau cu grad de nedeterminare ridicat (în cazul unor încercări de intruziune în desfăşurare, sau reuşite, care au evitat mecanismul de detecţie) [PPN08].

Funcţiile oferite de aceste sistemele de tip A vor constitui pentru o lungă durată de timp obiectul celor mai multe preocupări de cercetare din aria monitorizării securităţii, cum ar fi: modelarea şi reprezentarea matematică a noilor ameninţări, algoritmi de corelaţie, îmbunătăţirea ratei de alerte false, procesarea distribuită a alertelor, etc. Capitolul următor va prezenta şi evalua un model matematic care ar putea fi folosit pentru a adresa limitări curente din această zonă.

4.2.4 Sisteme R

În cazul în care se doreşte implementarea unui răspuns automat la intruziune trebuie să se ia în considerare aspecte de ordin legislativ, contractual (de exemplu: în cazul în care un furnizor de servicii detectează un atac venind de la un client) cât şi strategia de impunere a respectării politicii de securitate (de exemplu: o staţie care rulează procese importante pentru organizaţie, şi care a fost contaminată de un vierme, se pune în carantină automat, chiar cu riscul privării utilizatorilor de serviciul respectiv) [NIST SP 800-61].

Acest gen de constrângeri au determinat ca în cele mai multe cazuri sistemele R să aibă un rol preponderent de suport al echipei de securitate care răspunde la incidente cum ar fi: oferind documentaţie despre modul de adresare a incidentului, rapoarte care să asiste echipa care răspunde la incident (oferind informaţii despre impactul intruziunii asupra organizaţiei, progresul de restaurare a serviciilor sau de dezinfectare a staţiilor [OSS05]), acţiune asupra sistemelor proprii afectate (de exemplu: punerea în carantină automată a staţiilor afectate de un atac pe bază de vierme în desfăşurare) [Zou03].

4.3 Consideraţii asupra performanţelor şi limitărilor în generarea evenimentelor

Sistemele E se vor configura astfel încât să genereze maximum posibil de date. Aceste date pot fi trimise în timp real către sistemele C sau pot fi păstrate local pentru a fi conectate la un moment ulterior de către sistemele C (acest caz fiind similar probelor

RMON). Atunci când generarea unui volum mare de date va crea probleme de performanță (de exemplu: colectarea fişierelor access_log pentru un centru de hosting web larg) se poate opta pentru filtrarea informației la nivelul sistemelor sursă de tip E, după efectuarea în prealabil unei evaluări [Bej04].

Din punct de vedere teoretic se doreşte un volum maxim de date de la senzori a fi prezentate sistemelor colectoare. Însă acest punct de vedere are limitări în ceea ce priveşte performanța. Dacă o astfel de abordare poate fi implementată în mod rezonabil pentru sistemele IDS, în cazul evenimentelor de securitate generate de sisteme de operare precum şi de alte aplicații sau echipamente din rețea, soluția devine ineficientă în practică (de exemplu, colectarea fişierelor log de acces la fiecare pagină web pentru o companie care oferă servicii webhosting)[Lar06].

Devine astfel necesar în cele mai multe cazuri prefiltrarea informației la nivelul sursei. Un astfel de filtru poate reduce semnificativ volumul de date colectate. Totuşi aplicarea unui filtru înainte de generarea de evenimente înseamnă că o primă calificare este efectuată, aceasta fiind determinată de următorii factori [Voo07]:

- Specificații structurale – este cazul în care unele evenimente nu vor fi generate după cum interesează componentele (hardware, sistem de operare, aplicație) care nu sunt prezente în sistemul monitorizat. Acest tip de filtru este de obicei aplicabil echipamentelor de tip IDS, firewall sau de flitrare.
- Prefiltrări pe baza politicii de securitate – este cazul filtrelor stabilite pentru a nu genera evenimente care sunt conforme politicii de securitate. De exemplu, scanările de porturi inițiate de echipamentele proprii de securitate pentru verificarea vulnerabilităților.

Aceste filtre pot reduce în mod semnificativ resursele necesitate de colectori, însă au două mari limitări: dificultatea menținerii filtrelor într-o arhitectură distribuită, în acest sens sunt necesare proceduri riguroase pentru controlul modificărilor pentru a asigura că filtrele sunt într-adevăr conforme cu politica de securitate, cât şi proceduri care să asigure că schimbările în politica de securitate şi arhitectura sistemelor sunt reflectate în aceste filtre. În plus, cum multe din aceste prefiltrări sunt necesare la nivelul aplicație, varietatea aplicațiilor va determina o complexitate crescută în ceea ce priveşte managementul acestor fişiere de configurare [Cis11].

Un alt aspect este lipsa de reprezentare cât mai precisă a realității (statisticile vor fi mult mai puțin fiabile iar unele investigații post-incident vor fi lipsite de anumite informații ceea ce va limita înțelegerea a ceea ce s-a întâmplat.

4.4 Colectarea evenimentelor

Principalele operații efectuate de colectori sunt: recepția de mesaje primare (evenimente) prin diferite protocoale şi identificarea tipului de sursă pentru formatare. Odată ce evenimentul este formatat va fi stocat în baza de date a evenimentelor. Aspectele legate de performanță şi disponibilitate necesită proiectarea unei arhitecturi scalabile care permite o distribuție a colectorilor şi bazelor de date în rețea.

Colectarea de date din surse eterogene implică implementarea de două tipuri de agenți la nivel de protocol şi aplicație. Primul nivel colectează informații de la sistemele E, cel din urmă translatează informația într-un format standard pentru stocare. Cele două module sunt conectate printr-un dispecer. O astfel de arhitectură permite

implementarea de sisteme HA (high availability) şi LB (low-balancing) la orice nivel al arhitecturii.

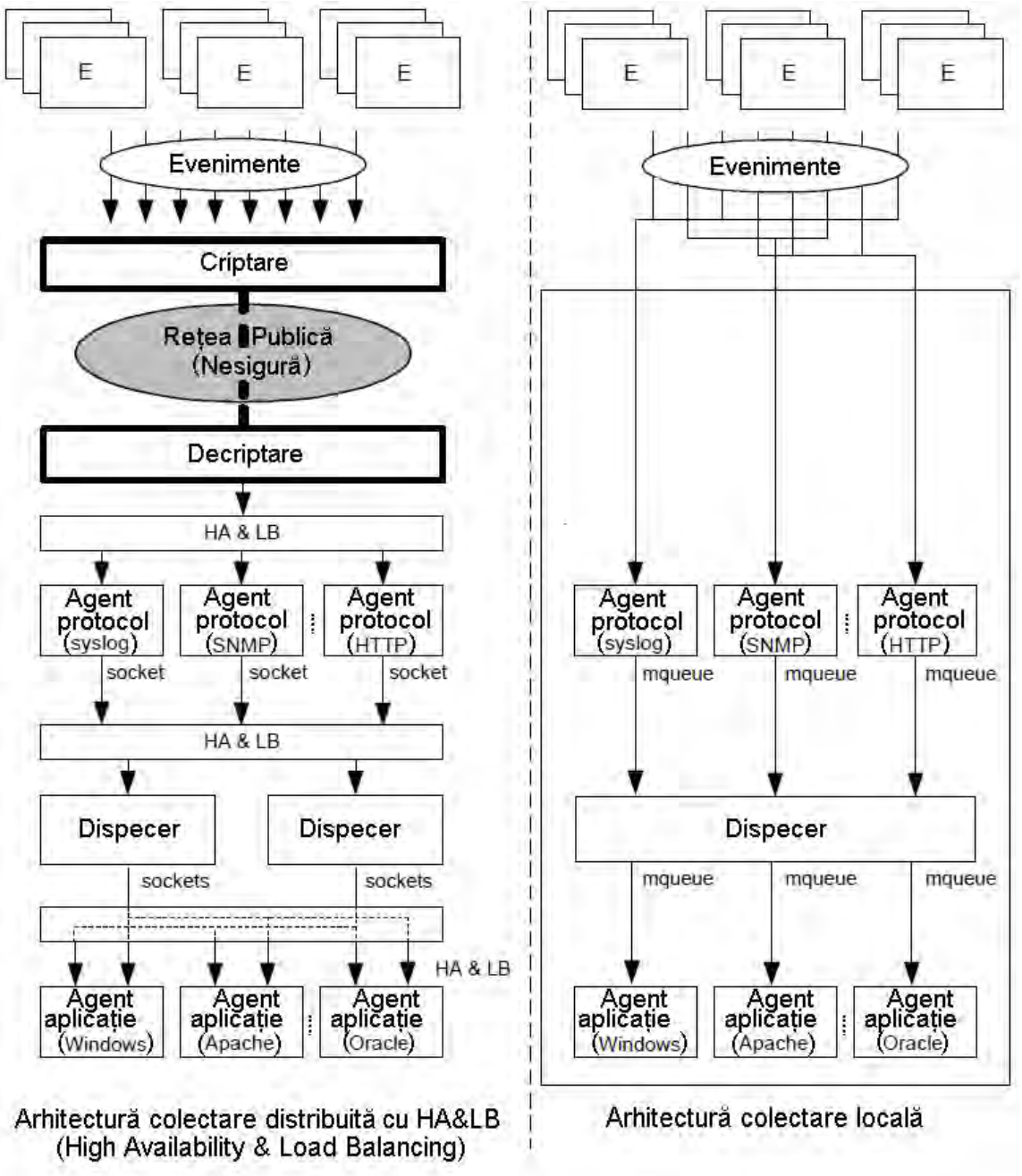


Figura 4.4 - Exemple de arhitecturi HA, LB bazate pe detaliile oferite mai jos.

4.4.1. Agenții de tip protocol

Agenții de tip protocol sunt proiectați să recepționeze informații de la diferite protocoale de nivel transport sau aplicație cum ar fi: Syslog, SNMP, SMTP, HTTP, etc. Aceştia acționează ca aplicații server, iar obiectivul lor este de a asculta conexiunile de intrare

către sistemele E şi de a furniza datele colectate către dispecer [Ngu02].

Simplicitatea unor astfel de agenți face ca implementarea şi menținea să fie uşor de efectuat. Formatul datelor de stocare este în general de tip fişier utilizând ca metodă de transfer către dispecer “named pipes”, “sockets” sau “shared memory” pentru a asigura o performanță mai bună.

Datorită simplicității acestor aplicații şi a faptului că nu necesită partajare de date, se pot implementa cu uşurință grupuri de agenți pentru sistemele foarte mari. Cel mai important aspect de securitate care trebuie avut în vedere este asigurarea integrității datelor colectate de agenți, în mod special dacă aceste date sunt transferate printr-o rețea partajată sau nesigură. Actualmente există o multitudine de protocoale pentru colectarea informațiilor care rulează având ca suport nivelul UDP. În acest sens este necesar încapsularea datelor printr-un tunel securizat pentru a avea siguranța integrității datelor pe durata transportului. [OSS--]

Pentru a menține un nivel de performanță ridicat precum şi operarea eficientă a HA şi LB se recomandă ca operațiile de criptare şi decriptare să se efectueze pe un echipament dedicat la fiecare capăt al comunicației.

4.4.2 Dispecerul

Dispecerul are rolul de a determina tipul sursă al evenimentului de intrare şi de a distribui mesajul original către agentul aplicație corespunzător. Odată ce identificatorul specific pentru fiecare tip de sursă este determinat, implementarea este relativ simplă.

Operațiile autonome efectuate de dispecer sunt [Ngu02]:

- Ascultă canalul de intrare pentru agenții protocol (socket, named pipes, massage queue)
- Execută o operație pattern matching utilizând o bază de date de şabloane, care pentru o performanță sporită poate fi preîncărcate în memorie. Deoarece generatorii de evenimente pot utiliza formate de mesaje diferite în funcție de protocolul de transmisie, formatul înregistrărilor din baza de date va avea următoarele câmpuri: tip sistem E, protocol transmisie, pattern
- Transmite mesajul original către un agent de aplicație specific sistemului E.

4.4.3 Agenții aplicație

Agenții aplicație sunt specifici fiecărei entități (sistem E, protocol de transmisie) şi efectuează formatarea de mesaje la un model generic de mesaje al bazei de date [Alk08]

Operațiile efectuate de agenții aplicație sunt [Mic09]:

- Ascultă canalul de intrare de la dispecer
- Procesează mesajul original generând înregistrarea generică de mesaj
- Transmite mesajul formatat către sistemele D.

4.4.4 Conlucrarea dispecerilor şi a agenților de aplicație

Din considerente de scalabilitate şi disponibilitate unele implementări vor necesita operații redundante pentru executarea funcțiilor de dispecer şi agent aplicație [Alk08].

De exemplu un dispecer va efectua următoarea operație pentru identificarea unei alerte de tip Snort:

```
if($line =~ /.*snort: \[\d+:\d+:\d+\] .*) {
       send_to_snort_2.9_syslog_agent($line)
}
```

Aplicația agent va efectua următoarea operație:

```
if($line =~ /.*\[\d+:\d+:\d+\] (.*) \[Classification: (.*)\]
             \[Priority:.*\]: \{(.*)\} (.*) -> (.*)/) {
       # completează câmpurile mesaj formatat per 4.5.2
       $msgtype = “Snort 2.9 - Alert”;
       $proto = getprotobyname($3);
       $src = $4;
       $dst = $5;
       $intrusion_type = $intrusion_type[SnortIntrusionType($2)];
       $info = $1;
}
```

În cazul unei platforme centralizate, operațiile pot fi combinate după cum urmează:

```
if($line =~ /.*snort: \[\d+:\d+:\d+\] (.*)
          \[Classification: (.*)\] \[Priority:.*\]:
             \{(.*)\} (.*) -> (.*)/) {
       $msgtype = $msgtype[1];
       $proto = getprotobyname($3);
       $src = $4;
       $dst = $5;
       $intrusion_type = $intrusion_type[SnortIntrusionType($2)];
       $info = $1;
}
```

În unele cazuri se poate combina funcționalitatea dispecerilor şi agenților de aplicație pentru simplificare şi o performanță sporită.

4.5. Formatarea de date şi stocarea

Pentru a asigura o procesare consistentă şi interpretarea de către fiecare componentă a arhitecturii de monitorizare, atât evenimentele colectate cât şi informațiile despre sisteme vor fi formatate într-o manieră standard [PPN08].

4.5.1 Structura de date stație (host)

Necesitatea de standardizare a structurii de date pentru stație este determinată de [OSS05]:

- Senzorii pot transmite informațiile despre stații în format IP sau FQDN (Fully Qualified Domain Name)
- Un sistem fizic poate avea mai multe adrese IP
- Un sistem fizic poate avea mai multe FQDN utilizând tehnici de virtualizare a stației
- Sistemele HA şi LB pot raporta o singură adresă IP sau FQDN pentru mai multe sisteme fizice.

Astfel identificarea unei stații pe baza adresei IP sau FQDN nu este fiabilă. Mai mult, datorită unor considerente de performanță, rezoluțiile DNS inverse nu pot fi executate pentru fiecare IP/ FQDN identificate în fişierele log. Arhitectura propune crearea unui identificator independent de IP/ FQDN numit token de stație.

Pentru o mai bună căutare şi actualizare a structurilor de date de stație se recomandă ca acestea să fie stocate într-o structură de tip “hash table” (şi nu arbori sau liste).

Tabelul hash va fi creat în memorie la pornirea sistemului şi actualizat de fiecare dată când este identificată o nouă adresă IP/ FQDN.

4.5.2 Structura de date pentru mesaj

Manipularea evenimentelor generate de tipuri diferite de echipament, precum şi transmiterea acestora utilizând protocoale multiple, impune necesitatea unui format standard.

Standardul IDMEF [RFC4765] elaborat în acest sens prezintă totuşi unele limitări în termen de performanță datorat consumului mare de resurse şi volumului mesajului XML în procesul de corelație. Totuşi, o translatare separată a procesului trebuie implementată dacă se doreşte conformare cu standardul IDMEF.

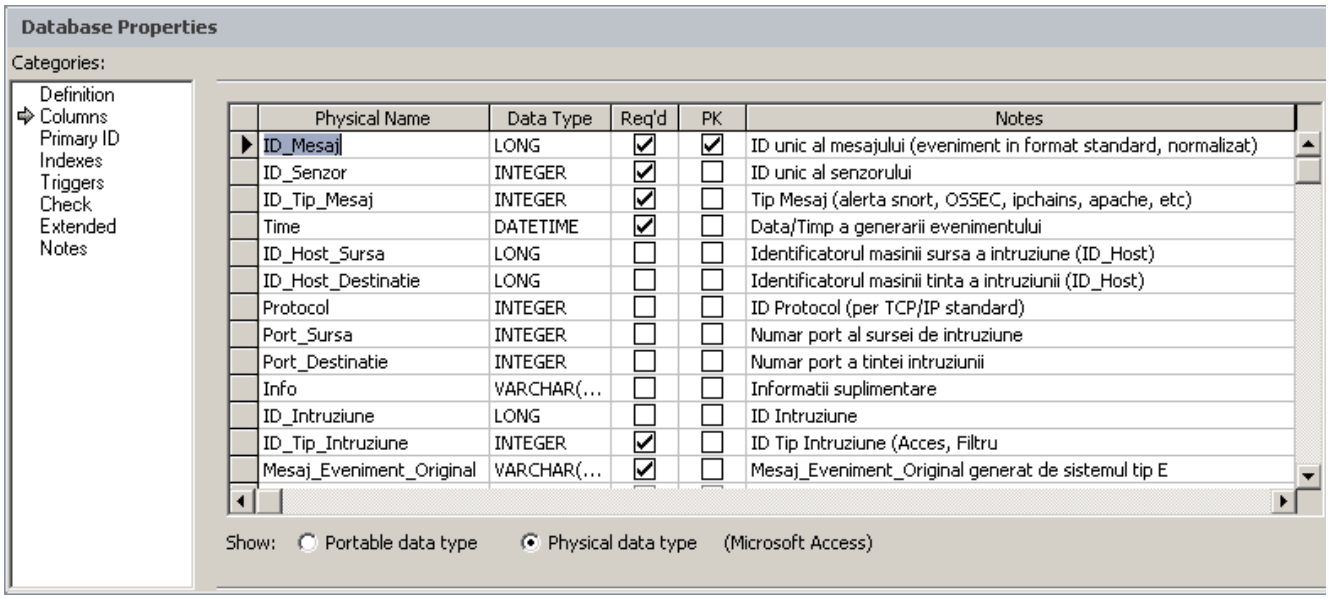


Figura 4.5 - Structura mesajului formatat

În crearea mesajelor cu format comun sunt implicate şi alte structuri de date. Relațiile între aceste structuri sunt prezentate în figura 4.6.

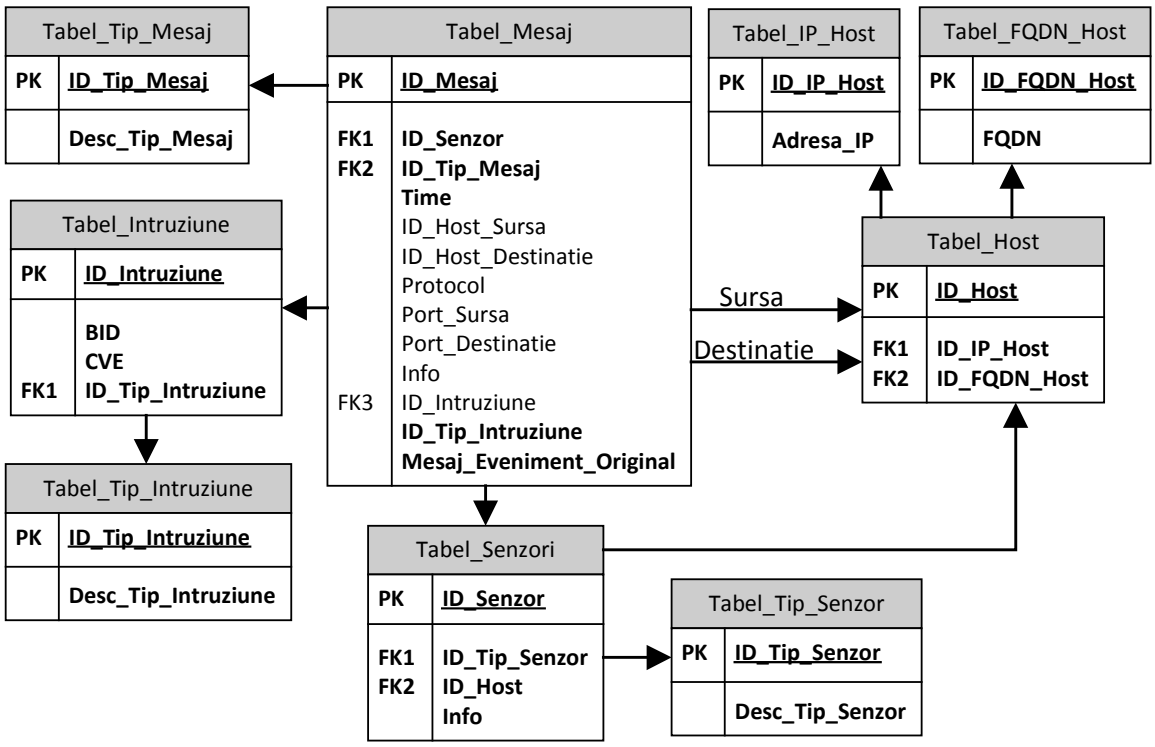


Figura 4.6 - Structurile de date în mesajul de format generic

Tabelele implicate în construirea unui mesaj de format generic sunt următoarele:

- Tabelul cu stații (host table) descris anterior
- Tabelul cu senzori – acesta are rolul de a identifica fiecare senzor din sistemul monitorizat. Fiecărui senzor îi este atribuit un ID unic şi un tip. Alte date opționale pot fi token-ul de stație şi o descriere a senzorului.
- Tabelul tipului de senzor – acesta are rolul de a oferii detalii pentru fiecare tip de senzori
- Tabelul tipului de mesaj – acesta conține descrierea pentru fiecare identificator de tip de mesaj
- Tabel cu intruziuni – acesta oferă identificarea pe baza unor referințe multiple a genului de atac. De exemplu, BID (for BugTraq), CVE ID (for CVE) [CVE--].
- Tabel tip intruziune – acesta defineşte clasele de familii de intruziuni majore cum ar fi: filtrare, scanare, finger printing, acces, etc.

4.6. Analiza datelor

Operațiile principale efectuate pentru generarea alertelor sunt: corelația, analiza structurală, analiza funcțională şi analiza comportamentului.

Corelația este o operație de sine stătătoare pe baza căreia se creează contexte care vor oferi suportul unei analize ulterioare, pentru a verifica dacă aceasta prezintă caracteristicile unei încercări de intruziune [PPN06-04].

- Analiza structurală este în esență un proces avansat de tip “pattern matching” utilizat pentru a determina dacă evenimentele dintr-un anumit context conduc către o cale de intruziune cunoscută, referiți adesea şi ca arbori de atac [Mau05].

- Analiza funcțională va oferi informații despre expunerea sistemului țintă la încercarea de intruziune detectată.
- Analiza de comportament va integra elemente din politica de securitate pentru a determina dacă încercarea de intruziune este de fapt o acțiune permisă.

Obiectivul acestor operații este de a genera alerte care nu doar verifică calea structurală de intruziune (de exemplu: scan, finger printing, exploatări, backdoors, etc.), dar care iau în considerare şi politica de securitate definită, precum şi importanța sistemelor țintă [Cla09].

4.6.1 Corelația

Corelația se defineşte ca fiind o relație cauzală, complementară, paralelă, sau reciprocă, ce vizează o corespondență structurală, funcțională sau calitativă între două entități comparabile. [PPN06-04]

În cazul arhitecturii de monitorizare a securității, corelația are rolul de a valida evenimentele de securitate colectate, cât şi de a ajuta în procesul de identificare a originii, magnitudinii şi impactului unei intruziuni, prin efectuarea analizei secvențelor de evenimente şi generarea de alerte simple, sintetizate şi precise. Pentru aceasta este necesar a se efectua următoarele operații [PPN06-04]:

- *Identificarea duplicatelor* - constă în identificarea evenimentelor duplicate şi etichetarea acestora pentru eficientizarea procesării, simplificând analiza efectuată de aplicații sau personal.
- *Pattern matching secvențial* - reprezintă operația de bază a modului de corelare şi constă în identificarea unei secvențe de mesaje care ar fi caracteristică unei încercări de intruziune. Această operație permite identificarea intruziunilor în curs de desfăşurare, precum şi scenariilor de intruziune complexe.
- *Pattern matching temporal* - utilizat în principal pentru managementul contextului, precum şi identificarea proceselor de intruziune distribuite sau care se desfăşoară pe o durată extinsă.
- *Analiza expunerii sistemului şi a severității* - oferă informații despre vulnerabilitățile sistemului țintă pentru detectarea încercărilor de intruziune. Spre exemplu, arhitectura de monitorizare a securității nu va genera alarme în legătură cu scenarii de intruziune bazate pe vulnerabilități la care sistemul țintă nu este expus. Un alt element important îl constituie severitatea intruziunii şi anume impactul general asupra sistemului monitorizat. Aceasta ajuta la o mai bună stabilire a priorităților în cazul în care trebuie să se răspundă simultan la mai multe incidente.
- *Verificarea conformării cu politica de securitate* - reprezintă un filtru bazat pe comportament pentru eliminarea evenimentelor specifice în cazul în care acestea sunt conforme cu criteriile politicilor de securitate (log-in administrator, autorizare, restricții).

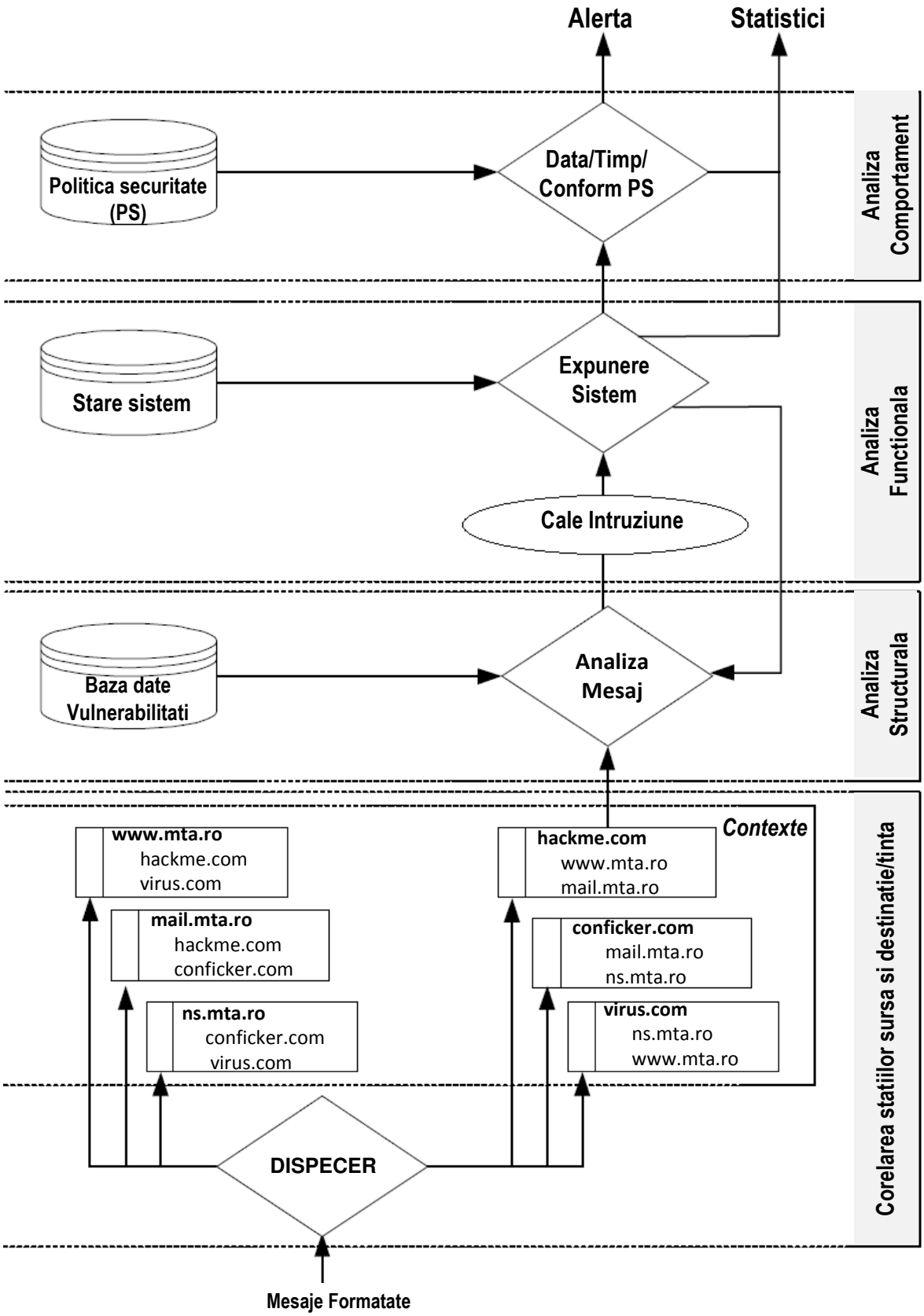


Figura 4.7 - Principalele operații de analiză

4.6.1.1 Contexte de corelație

Pentru o identificare mai eficientă a evenimentelor care aparțin aceluiaşi scenariu de intruziune, se utilizează tehnica corelării pe bază de context. Această tehnică are la bază o structură specifică denumită *context*, iar toate operațiile de corelare sunt efectuate pe baza acestor structuri. Implementările care utilizează această tehnică de corelare vor avea şi o rată de alarme false mai scăzută [PPN06-04].

Definiție: un *context* este o structură de date în care elementele membru satisfac un criteriu dat. De exemplu, contextul de tip destinație pentru stația A va conține toate stațiile X_1, X_2, .. X_n pentru care există evenimente, unde X_i i=1,n este sursă iar A este destinație.

Astfel oricare mesaj stocat în baza de date cu mesaje va face parte din unul sau mai multe contexte. Operațiile de corelare se vor efectua în paralel, astfel încât să ruleze simultan pentru fiecare context. Se pot implementa următoarele tipuri de management al contextului [Pie08]:

- *Contexte independente şi distincte* - fiecare context va conține mesaje specifice fiecărui criteriu. O astfel de arhitectură va fi numită *şir de contexte*.
- *Contexte ierarhice* - se definesc contextele de nivel superior care se potrivesc unui număr limitat de criterii, apoi se creează sub-contextele pe baza diferitelor criterii, rezultând astfel un *arbore de contexte*.

In practică datorită cerințelor de performanță şi funcționalitate se va evalua eficiența fiecăreia dintre cele două abordări. În multe cazuri se va utiliza o arhitectură mixtă, care îmbină cele două abordări.

4.6.1.2 Definirea contextului

Criteriul de definire al contextului trebuie făcut în conformitate cu evenimentele de securitate la care arhitectura de monitorizare va trebui să răspundă (operații de scanare distribuită, finger printing, volum mare de încercări de exploatare, încercări de tip “brut force”, spamming, etc.). O arhitectură funcțională a contextelor este prezentată în figura 4.9.

Un prim criteriu este combinația ID stație atacată, ID stație atacatoare [Gre99].

- *Sursa* - prin definirea sursei drept criteriu de creare a contextelor, se vor putea detecta sondări de tip ping, sistemele intermediare folosite de atacatori sau compromise de viermi
- *Destinație* - contextele create pe criteriul destinație vor oferi informații despre scanări (fie ele distribuite normal sau desfăşurate pe o durată extinsă) şi vor permite observarea încercărilor de intruziune precum şi a celor reuşite.

Se vor defini două şiruri de contexte, unul cu context (potrivire) pe sursă, iar celălalt cu context pe destinație. Fiecare context al fiecărui şir va fi apoi considerat drept context rădăcină pentru arborii de context. Criteriile pentru potrivire către ramurile cele mai mici ar fi:

- Token ID destinație (pentru contextele create prin potrivirea ID-ului sursă) sau
- Token ID sursă (pentru contextele create prin potrivirea ID-urilor destinație).

Pe durata procesării datelor, protocoalele şi porturile sistemelor destinație vor forma

criteriul nivelului următor al ramurilor de context. Aceasta se va efectua pentru izolarea operațiilor singulare de scanare dintr-un şir masiv repetat de încercări de compromitere a sistemului printr-o aplicație specifică. În plus, aceasta permite şi identificarea diferiților paşi ai intruziunii.

Unul din scenariile de intruziune des întâlnite este scanarea porturilor urmată de identificarea versiunii pentru porturile deschise (fingerprinting), după care este lansată exploatarea asupra sistemelor ce se presupun a fi vulnerabile [Nma--].

Pentru a identifica tipul de mesaj stocat, ce permite totodată efectuarea unei analize cât mai precise a mesajelor, se efectuează generarea unui context de nivel următor pe baza ID-ului tipului de intruziune. Un exemplu de definire a ID_tip_intruziune este prezentat în tabelul 4.8.

ID_Tip_Intruziune	Desc_Tip_Intruziune
0 / Necunoscut	Intruziune necunoscuta
Secțiunea 1xx – Identificare	**Identificare tinta**
100 / Filtrare	Pachete filtrate de firewalls, ACLs, etc.
110 / Scanare de Baza	Scanare de porturi
120 / Fingerprinting	Identificare tinta
Secțiunea 2xx – Exploatare	**Grup de incercari intruziune**
200 / Exploatare	Lansare exploatare
Secțiunea 3xx – Denial of Service (DOS)	**Atacuri DOS cu succes**
300 / Denial of Service	Atac DOS patial
310 / Denial of Service	Atac DOS global
Sectiunea 4xx – Evitare Securitate	**Incercari de evitare a politicii de securitate**
400 / Spoofing	IP / MAC spoofing
410 / Continut	Evitare filtare de continut
420 / Privilegii	Incercari elevare privilegiu
Secțiunea 5xx – Compromitere Sistem	**Incercari de compromitere a sistemului tinta**
510 / Accesare Cont	Succes accesare cont
520 / Eroare Acces Date	Incercari de acces la date private
530 / Integritate	Compromitere integritate sistem

Figura 4.8 - ID tip intruziune

Ultima ramură a contextelor conține ID-ul specific de intruziune (caracterizarea fiecărui mesaj). La acest nivel se realizează la o dimensionare atomică a fiecărui mesaj. Acest câmp face referință la tabelul de intruziune şi va fi responsabil pentru legătura între motorul de corelare şi informația de stare a sistemului stocat în baza de cunoştințe.

4.6.1.3 Organizarea contextelor

Deoarece fiecare operație de corelare este efectuată în mod exclusiv pe contexte, structura acestora reprezintă una dintre cele mai importante aspecte ale arhitecturii de monitorizare.

Arhitectura funcțională este descrisă în paragraful precedent şi este constituită dintr-un şir de arbori de contexte. Fiecare arbore conține patru nivele de ramuri după cum este prezentat în figura 4.9.

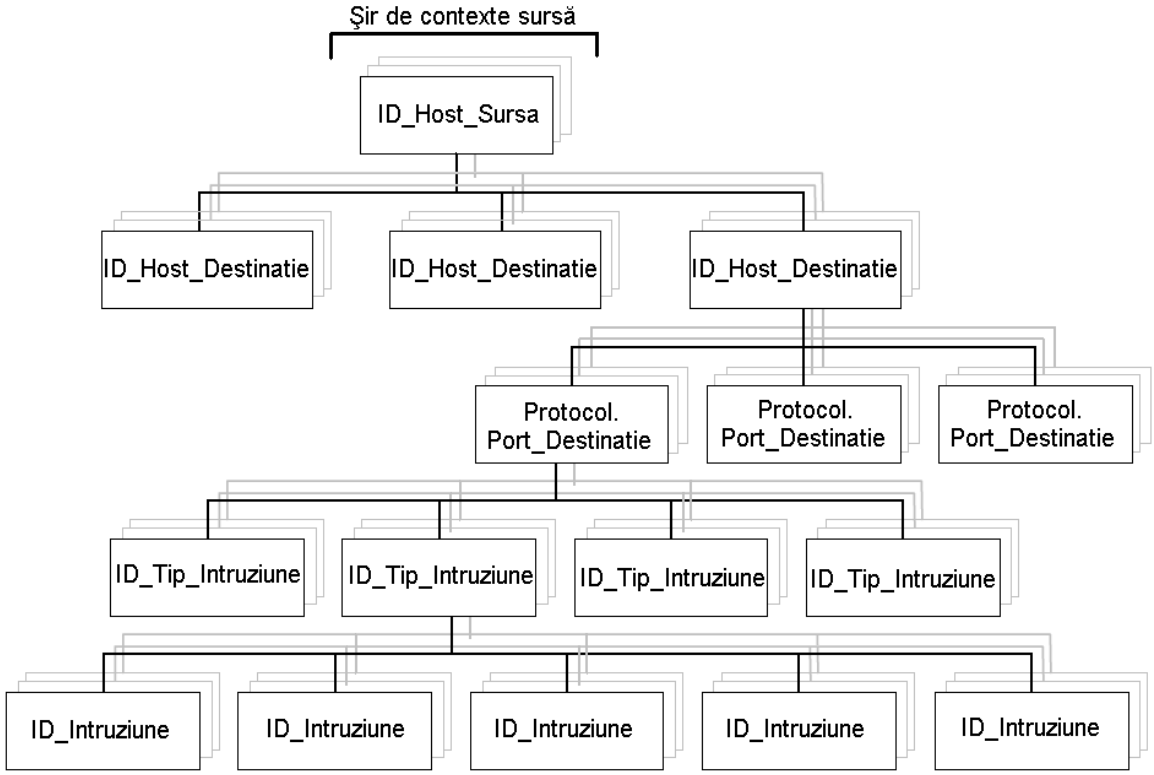


Figura 4.9 - Arhitectura funcțională a contextelor

4.6.1.4 Structuri de date pentru contexte

Pentru o funcționare corespunzătoare a arhitecturii definite anterior va fi necesară implementarea unei structuri care va asigura accesul la informații şi stocarea corespunzătoare. Figura 4.10 descrie o schemă de implementare a contextului utilizând notații specifice Perl.

Exemplu de implementare defineşte următoarele câmpuri:

- Timp_start şi timp_stop - aceste câmpuri se vor găsi în fiecare ramură a structurii de context şi oferă informații despre timpul de generare al primului şi respectiv ultimului mesaj asociat acelui subarbore
- Numărul de mesaje duplicate (no_duplicate). Mesajele duplicate conțin aceleaşi informații cu excepția câmpului de timp.

Celelalte câmpuri se regăsesc în structurile de date asociate mesajului de tip generic şi care au fost prezentate în figura 4.6.

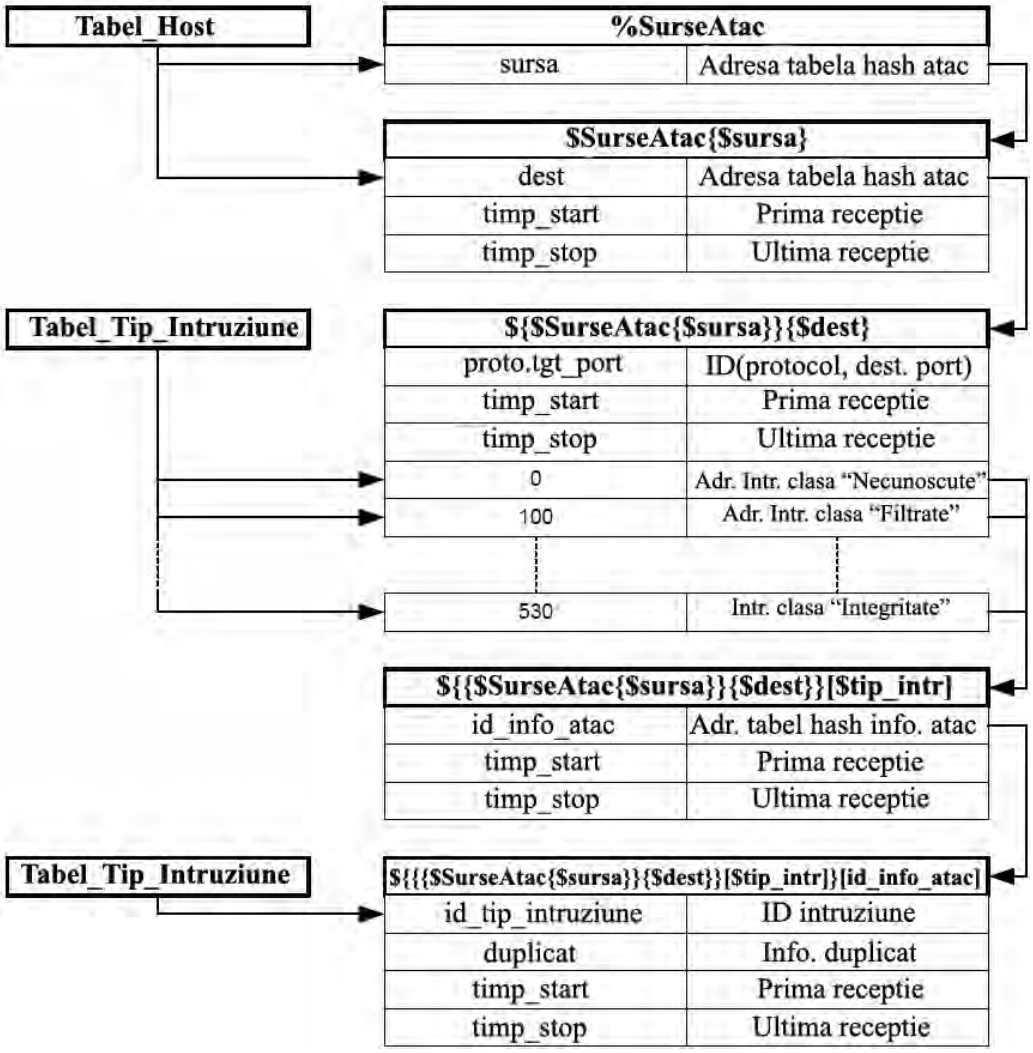


Figura 4.10 - Scheme de implementare a contextelor [Gan08]

4.6.1.5 Starea contextelor

O altă importantă caracteristică a contextului o reprezintă starea acestuia.

Se definesc următoarele trei tipuri de stare [Mul09]:

- *Activă* - contextul se potriveşte unui criteriu specific (de exemplu cel bazat pe timp), care poate fi caracteristic unui proces de intruziune în curs de desfăşurare. În mod uzual astfel de context va fi folosit pentru procesarea unui volum mare de date odată cu sosirea unui nou mesaj, iar analiza acestuia, efectuată de motorul de corelare, va trebui efectuată cu cea mai ridicată prioritate posibilă.
- *Inactiv* - un astfel de context fie nu îndeplineşte criteriul "activ" sau nu a recepționat codul specific de închidere. Aceasta înseamnă că nu este supus analizei de către motorul de corelare, dar va putea fi reactivat de următorul mesaj care se potriveşte criteriului de context.
- *Închis* - în această stare contextul este încheiat. Orice nou mesaj care potriveşte contextual va crea un nou context.

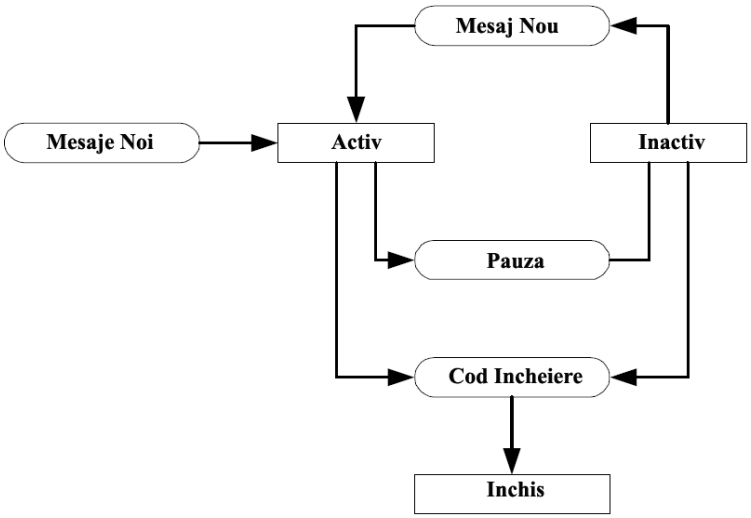


Figura 4.11 - Diagrama stărilor contextului

4.6.2 Analiza structurală

Analiza structurală constă într-un set de operații efectuate pe fiecare context de către module independente, şi are scopul de a identifica încercările de intruziune în curs de desfăşurare, de management al stării de context şi a condițiilor de încheiere a contextelor. Fiecare modul este activat de un mesaj specific şi realizează analiza utilizând o semantică standard [Hou95].

Analiza structurală se bazează pe un set de operatori, iar modulele de analiză generează rezultatele pe baza operațiilor logice între condițiile autonome şi câmpuri din contexte.

Activarea modulelor de analiză se poate efectua după [Dou93]:

- *Mesaje* - anumite condiții de câmp trebuie îndeplinite pentru activarea modulului de analiză. Un antet conținând condițiile de câmp ce trebuie îndeplinite este apoi generat pentru fiecare modul de analiză. Considerând structura modulului de analiză, antetul va fi un set de operații logice de tip SAU, ai cărei membri vor fi condiții de câmp ce necesită cel mai mic număr de resurse pentru a fi evaluate.
- *Timp* - antetul modulului de analiză poate conține informații de timp pentru a determina evaluarea corelației. Aceasta este în principal utilizată pentru închiderea contextelor şi detectarea intruziunilor desfăşurate pe o durată mare de timp cum ar fi scanări de porturi încetinite şi atacuri de tip “brut force”.

4.6.3 Analiza funcțională

Se efectuează pentru evaluarea expunerii sistemului la intruziune şi a impactului general al unei astfel de intruziuni asupra sistemului monitorizat

Odată ce analiza structurală oferă informații despre încercarea de intruziune în curs de desfăşurare, se face o cerere către secțiunea din sistemul K cu “Starea curentă de securitate a clientului”. Această cerere conține ID-ul intruziunii şi token-ul stație al sistemului țintă. Răspunsul va conține următoarele informații:

- Severitatea - o valoare dintr-o scară arbitrară cum ar fi: info, warning, minor, major, critical, etc.

- Cod de încheiere - dacă contextual urmează să fie închis (de exemplu ținta nu este afectată de încercarea de intruziune)
- Mesaj - un mesaj nou formatat care va fi adăugat la contextual actual, în acest fel putându-se activa module de analiză suplimentară.

4.6.4 Analiza de comportament

Determină dacă încercarea este conformă politicii de securitate. Acest gen de analiză se va utiliza pentru managementul accesului la conturi, dar poate fi implementată şi în cazul auditărilor scanărilor de porturi. Într-o astfel de situație un cod de încheiere este trimis către context. În mod tehnic, această analiză se va efectua în mod similar celei structurale - prin intermediul unor module specifice a căror structură este încărcată din secțiunea „Politici de securitate" a sistemului K.

4.7 Raportarea şi răspunsul la incidente

Pentru arhitectura de monitorizare a securității prezentată în figura 4.3 se regăsesc două interfețe utilizator: *consola arhitecturii de monitorizare* (disponibilă furnizorului de servicii) şi *portalul pentru client* (cu informații specifice despre activitatea şi starea infrastructurii clientului monitorizat).

4.7.1 Consola arhitecturii de monitorizare

Consola arhitecturii de monitorizare (sisteme R) este destinată analizei interne, accesului la datele neformatate din diferite sisteme ale arhitecturii cum ar fi: K şi D. Consola are în principal trei clase de interfețe:

- *Interfață de monitorizare în timp real* - oferă acces direct la datele din mesajele stocate pe sistemele stocate D. Aceasta permite funcții generice de filtrare de tipul "grep" pentru izolarea anumitor mesaje şi este utilizată pentru analiza în detaliu a unor evenimente specifice şi a răspunsului la acele evenimente.
- *Interfața de răspuns la incidente* - este motorul intern folosit pentru generarea şi actualizarea înregistrărilor incident şi a procedurilor de răspuns descrise mai jos. Interfața oferă informații detaliate de alertă precum şi date de depanare. Aceasta este o interfață de complexitate ridicată deoarece trebuie să adreseze aspecte de performanță operațională, ergonomicitate, filtrare avansată, identificare şi căutare. Una din cerințele de bază este în a asigura suport pentru un răspuns eficace şi eficient la intruziuni.
- *Interfața pentru analiză statistică* - oferă acces la datele sursă ale activității de securitate pe termen scurt cât şi evoluția pe termen mai lung. Aceste date vor fi utilizate în special pentru reprezentări grafice.

4.7.2 Portalul pentru client

Portalul clientului oferă date formatate despre activitatea de securitate. Acesta este proiectat pentru a oferii rapoarte pe mai multe nivele destinate atât inginerilor de securitate cât şi managementului din organizația clientului. Portalul este alcătuit din trei porțiuni:

- *Interfața de evaluare continuă a riscului* - oferă informații despre nivelul curent de securitate al sistemelor şi versiunilor de software monitorizate (nivelul general

de securitate, caracteristicile şi nivelul critic al vulnerabilităților, scenarii de intruziune şi detalii de configurare şi patching).

- *Activitatea de securitate* - prezintă rapoarte de evoluție pe termen mediu şi lung legate de tipuri de intruziune, frecvențe, surse, consecințe asupra sistemelor monitorizate. Activitățile pe termen scurt pot fi folosite în suportul identificării surselor recurente de atac sau a serviciilor urmărite cu precădere de atacator, pentru a elabora sau reevalua controalele de securitate asociate acestor aspecte.
- *Starea de securitate* - permite accesul la incidentele în curs de desfăşurare, sistemele atacate şi a căilor de intruziune activate de atacatori. Interfața oferă informații despre procedurile de răspuns şi escaladare disponibile la momentul respectiv pentru contracararea atacului.

4.7.3 Procedurile de răspuns şi escaladare

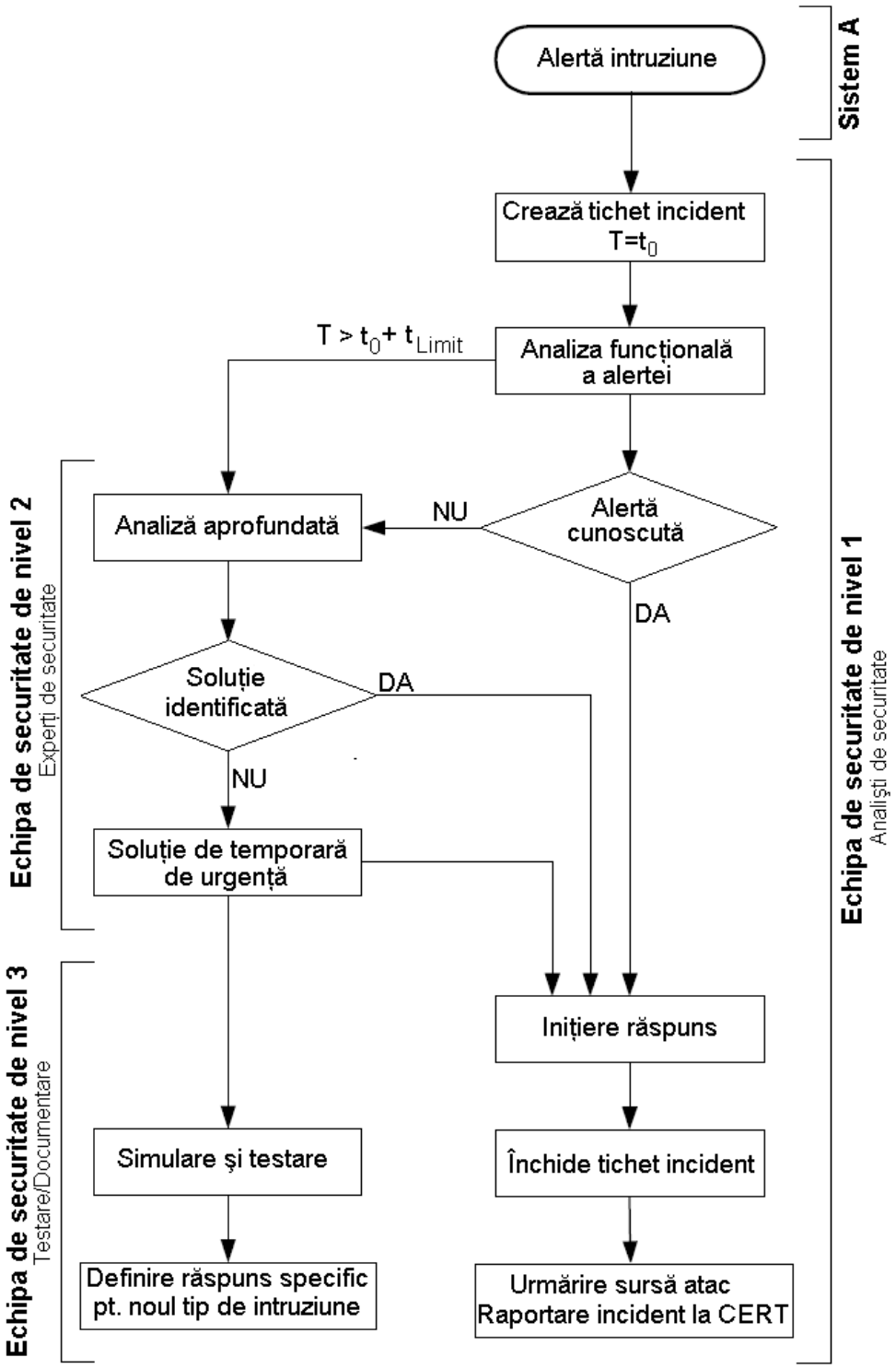
Răspunsul la un atac reprezintă setul de proceduri şi măsuri organizatorice care trebuie aplicate de echipele de răspuns la incident. Răspunsul poate varia de la o monitorizare pasivă pentru a colecta informații suplimentare până la oprirea în sistem de urgență a sistemului monitorizat şi raportarea incidentului către CERT. [Cer--]. Scenariile de răspuns şi procedurile din documentație vor fi validate şi vor fi securizate, în principal în termeni de integritate.

Nivelele de escaladare (raportarea şi solicitarea implicării nivelului imediat următor) trebuie definite pentru a asigura o reacție rapidă şi eficace, în paralel cu utilizarea corespunzătoare a resurselor umane disponibile. Un alt aspect ce trebuie menționat este întârzierea (timpul T_{Limit}, figura 4.12) după care procedura de răspuns trebuie inițiată în conformitate cu nivelul de severitate a atacului.

Odată ce această întârziere este consumată, escaladarea către nivelul următor - raportarea şi implicarea managementului - se va produce în mod automat.

Procedura de escaladare este prezentată în Figura 4.12 şi defineşte trei nivele de escaladare după cum urmează:

- Nivelul 1 - personalul tehnic de nivel mediu, care este capabil să înțeleagă şi să interpreteze evenimentele generate de sistemele A, precum şi aplicarea procedurii de răspuns. Agenții raportează incidentele către nivelul 2 în cazul în care evenimentul observat este unul necunoscut, reacția predefinită este nedocumentată, sau timpul limită T_{Limit} (timpul alocat pentru rezolvarea incidentului la nivel1) este depăşit.
- Nivelul 2 - personalul tehnic de nivel expert. Aceşti experți sunt responsabili pentru analiza evenimentelor de intruziune noi. Prioritatea acestora este de a stabili nivelul de severitate a intruziunii, şi a oferi o soluție de moment pentru agenții de la nivel 1, precum şi de a continua cercetarea şi identificarea unei soluții permanente post incident.
- Nivelul 3 - ar trebui să fie un laborator în care pachetele suspecte, operațiile efectuate de sisteme, vor fi reproduse pentru a determina natura noului tip de intruziune şi de a oferi o procedură de răspuns complet elaborată. Laboratorul va fi responsabil cu contactarea furnizorilor sistemelor de operare, aplicațiilor, hardware-ului, pentru proiectarea patch-ului.



Figira 4.12 - Procedura de escaladare

4.8 Riscuri şi amenințări la adresa arhitecturii de monitorizare

Pentru a creşte gradul de complexitate al atacului, atacatorul va căuta să-şi mențină gradul de anonimat, să evite detecția sau, în cel mai bun caz, să pară normal. În caz că nu reuşeşte, atacatorul va căuta să degradeze sau să stopeze colectarea de evidențe,

fapt care va complica investigațiile de după incident. Practica a arătat că atacatorii exploatează în esență consecințele unui management deficitar şi lipsa de experiență.

4.8.1 Menținerea gradului de anonimat

Indiferent de faza de compromitere a victimei, atacatorul va căuta întotdeauna să-şi păstreze gradul de anonimat. Atacatorii caută să rupă orice legătură ce se poate stabili între stația de la care au lansat comenzile şi victimele atacurilor. Modalitățile prin care atacatorul îşi poate menține un grad ridicat de anonimat sunt [PPN06-02]:

- *Lansarea atacurilor de pe stații deja compromise*, pentru care nu există o afiliere directă cu atacatorul. Atacurile complexe realizează fiecare etapă de compromitere utilizând diferite adrese IP sursă, singurul numitor comun în acest caz fiind adresa IP destinație. Apărarea are două metode la dispoziție pentru a rezolva ecuația anonimatului:
  - conlucrarea cu administratorii maşinilor folosite în atacul asupra victimei finale
  - penetrarea maşinii de pe care s-a generat atacul (reverse hacking), dar care nu se recomandă deoarece penetrarea altor sisteme este ilegală conform multor legislații, chiar dacă se face în scopul de autoapărare.
- *Atacuri prin utilizarea de adresă sursă modificată* (spoofing). Deşi multe implementări TCP/IP prezintă o predictibilitate în ceea ce priveşte alocarea numerelor de secvență lipsa unor atacuri, care să utilizeze această caracteristică a determinat experții în domeniu să concluzioneze atacurile de tip Mitnick - cu adresă IP modificată şi determinarea numerelor de secvență TCP are probabilitate scăzută. Atacurile frecvente care folosesc adrese spoofed sunt cele de tip DoS, în care nu se încheie negocierea completă pentru stabilirea sesiunii. În ultimii ani s-a observat că atacatorii au folosit din ce în ce mai puțin adrese sursă IP modificate. O motivație ar fi faptul că din ce în ce mai mulți utilizatori utilizează conexiuni broadband, ceea ce face ca atacatorii să aibă o bază mult mai mare de victime [Ver11].
- *Atacuri dintr-un alt bloc de rețea*. Atacatorii elevați, familiarizați cu BGP (border gateway protocol) pot încerca publicarea propriilor rute pe durata atacurilor, beneficiind de filtrarea necorespunzătoare a ruterelor la nivelul furnizorului de servicii.
- *Atacuri declanşate de pe o stație de încredere pentru victimă*. În general, această tehnică exploatează încrederea acordată unei alte stații sau grup de stații.
- *Atacuri dintr-un bloc de rețea familiar*. Atacurile declanşate de pe o stație din acelaşi oraş sau aceeaşi țară pot scăpa neobservate utilizatorilor şi analiştilor.
- *Atacul asupra clientului şi nu a serverului*. Această tehnică se bazează pe faptul că conexiunile către exterior sunt mult mai puțin verificate decât conexiunile către interior. Atacarea clientului presupune oferirea unui serviciu malițios şi aşteptarea clienților vulnerabili (potențialele victime să se conecteze la servere).
- *Utilizarea de intermediari publici*. Această tehnică este utilizată după ce una din metodele anterioare a compromis victima, în special pentru comunicarea între atacatori şi victimă. Actualmente, majoritatea atacatorilor preferă să controleze victimele prin intermediul canalelor IRC sau rețele P2P.

4.8.2 Evitarea detecției

Tehnicile prin care atacatorul caută sa-şi păstreze anonimatul sunt relativ simple, în marea majoritate bazându-se pe o altă stație care să conducă defensiva către piste false. Aceste tehnici nu-l fac pe atacator invizibil, ci doar mai greu de depistat [Mat11]. Dintre cele mai semnificative tehnici se amintesc:

- *Coordonarea în timp a atacului*. Pentru atacator timpul poate fi un aliat foarte bun. Sondarea victimei la intervale suficient de mari poate fi confuză şi trece neobservată. Apărarea ar trebui să gândească acest tip de problemă în acelaşi fel ca şi tehnicile de păstrare a anonimatului: orientarea către victimă.
- *Distribuirea atacurilor în întreg spațiul de adrese IP*. Distribuția temporală a traficului de atac, este adesea însoțită şi de o distribuție spațială în Internet. Tehnicile distribuite au devenit populare odată cu atacurile DDoS.
- *Utilizarea criptării*. Atacatorul poate folosi criptarea pe durata diferitelor faze ale compromiterii, dar în limitele stabilite de victimă (pe durata recunoaşterii, exploatării atacatorul este limitat la metodele de criptare oferite de stația țintă). Această tehnică devine din ce în ce mai interesantă pentru atacatori, deoarece un număr din ce în ce mai mare de servicii oferă criptare. Exemple de servicii care utilizează mecanisme de criptare şi care ar putea fi compromise de atacatori ar putea fi: HTTPS, secure pop (port 995), SMTP peste TLS, open SSH, etc.

4.8.3 Generarea de trafic normal

Dacă activitatea atacatorului se înscrie în caracteristicile utilizatorului legitim, descoperirea incidentului este dificil de realizat. Două tipuri de atacatori sunt extrem de dificil de detectat: utilizatorii interni şi impersonarea unui utilizator legitim (atacatorul care a reuşit să obțină un cont şi o parolă care îi permite accesul la informația care o doreşte). O metodă eficientă de combatere a impersonării o reprezintă utilizarea autentificării pe bază de doi factori: parolă şi token. Comportarea normală a atacatorului este necesară mai ales în cazul penetrării site-urilor monitorizate de sisteme IDS bazate pe anomalii. Cu cât comportamentul atacatorului este în limitele utilizatorului normal, probabilitatea de a genera o alertă este scăzută [Gu07].

4.8.4 Degradarea sau stoparea procesului de monitorizare

Reprezintă o altă modalitate de a exploata produse (atacarea senzorilor sau dispozitivelor de colectare şi ştergerea informațiilor de jurnalizare), persoane (activități de diversiune pentru a distrage atenția personalului ce efectuează analiza) sau procese (separarea fizică a analistului de consolă) în scopul perturbării operațiilor arhitecturii de monitorizare.

Diversiunile pot urmări atât intoxicarea cu trafic prefabricat, cât şi crearea unui volum mare de alerte. Atacurile de volum sunt cel mai adesea cauzate de alegerea ineficientă a semnăturilor IDS, şi generează probleme datorită timpului şi efortului necesar investigării tuturor alertelor.

Atacurile asupra senzorilor se desfăşoară în două etape. În prima se urmăreşte identificarea adreselor IP care efectuează monitorizarea traficului, iar apoi se declanşează atacul propriu-zis.

Una din puținele posibilități pe care atacatorul le are să detecteze senzorii îl reprezintă exploatarea serviciului DNS. Presupunând că atacatorul are vizibilitate sau controlul asupra serviciului DNS pentru un anumit bloc de rețea, acesta poate trimite pachete de sondare în care adresa IP sursa este asociată cu serverul DNS respectiv. Dacă senzorul este configurat să rezolve adresele IP din pachetele recepționate, va transmite cereri către serverul DNS care sunt interceptate de atacator. Metode mai eficiente pentru detecția sistemelor ce funcționează în regim de monitorizare sunt bazate pe protocolul ARP [San01], şi presupun accesul la segmentul LAN în care senzorul este plasat.

Atacurile asupra senzorului pot fi de tip: [CVE--]

- DoS - vizează resursele senzorului cum ar fi CPU, memoria, disc, bandă
- Exploatări de vulnerabilități în aplicațiile de monitorizare rulate pe senzori

Atacurile îndreptate asupra procesului urmăresc atât culegerea de informații despre personal şi echipamente utilizând mijloace specifice ingineriei sociale, cât şi perturbarea activității în locația unde se desfăşoară monitorizarea (Centrul Operațional de Securitate) prin mijloace specifice de diversiune cum ar fi de exemplu alarme de incendiu, amenințări cu bombe, etc. Soluția pentru astfel de situații o reprezintă o politică riguroasă de revizuire a alertelor. Un politică de monitorizare solidă se bazează pe principiul răspunderii analistului pentru tratarea fiecărei alerte generate.

4.8.5 Probleme organizaționale

În ciuda tuturor atacuri de natură tehnică amintite anterior, problema majoră în operarea unei arhitecturi de monitorizare gravitează în jurul personalului şi proceselor. Verificarea şi motivarea personalului, pregătirea profesională continuă sunt aspecte pe care managementul trebuie să le considere pentru a asigura succesul operațional al arhitecturii de monitorizare.

Motto*: Toate adevărurile sunt uşor de înţeles odată ce au fost descoperite.*
Problema este să fie descoperite.
- Galileo Galilei

CAPITOLUL 5

MONITORIZAREA SECURITĂȚII ÎN CONDIȚII DE INCERTITUDINE

Prin activitățile care le desfăşoară în etapele premergătoare, cât şi pe durata unei intruziuni, atacatorii pot folosi tactici specifice confruntărilor din spațiul militar pentru inducerea în eroare a sistemelor de detecție având ca rezultat date de monitorizare incerte, şi confuze. O serie de acțiuni pe care atacatorul le poate întreprinde pentru a diminua calitatea datelor de monitorizare au fost prezentate în secțiunea 4.8, şi este de aşteptat o diversificare şi rafinare pe viitor a acestor tactici (diversiune, dezinformare, camuflaj, etc.) [Mat11].

În plus, transpunerea a tot mai multor activități umane în spațiul virtual, conjugată cu dinamica schimbărilor de ordin tehnologic, va determina o complexitate crescută a arhitecturilor IT şi a proceselor de management asociate acestora. Conform principiului incompatibilității dintre precizie şi complexitate, care se manifestă puternic la sistemele umanoide [Zad86], este de aşteptat ca, în ceea ce priveşte managementul securității, această complexitate să se traducă prin disponibilitatea unei mase mari de date şi informații, dar care va avea un conținut din ce în ce mai ridicat de imperfecțiune.

Capitolul de față îşi propune realizarea unui experiment de monitorizare securității pe bază de evenimente generate de surse (IDS) ce nu prezintă confidență deplină asupra celor raportate. Metodologia utilizată în acest sens cuprinde următoarele elemente: cercetarea cauzelor de imperfecțiune a datelor, identificarea unor modele matematice ce pot adresa date imperfecte, construirea modelului experimental şi a aplicației de experimentare, realizarea experimentului şi interpretarea rezultatelor obținute, concluzii şi direcții ulterioare de experimentare.

5.1 Categorii de imperfecțiune a datelor

Imperfecțiunea datelor, trebuie încorporată în sistemele ce încearcă să ofere o modelare cât mai corectă a realității. Acest lucru este însă greu de realizat prin utilizarea soluțiilor actuale oferite de sistemele de management a informațiilor. Un motiv major ar putea fi găsit în dificultatea înțelegerii diferitelor aspecte ale imperfecțiunii şi a reprezentării cunoştințelor imperfecte.

Datele se consideră perfecte atunci când sunt precise şi sigure. Principalele cauze ale imperfecțiunii sunt [Sme96]:

- *Imprecizia* – acoperă aspectele legate de conținutul datelor cum ar fi: proprietatea, raportarea la lumea externă, neglijența, etc.
- *Inconsistența* – acoperă aspectele legate de contradicții, incoerență, etc.
- *Incertitudinea* – este determinată de lipsa datelor şi unele aspecte legate de imprecizie

Pe baza clasificării lui Smet [Sme96], a imperfecțiunii informațiilor, se identifică următoarele aspecte ale imperfecțiunii datelor în sfera monitorizării securității:

Cauza	Clasa	Caracteristica	Descriere	Exemplu
Imprecizie	Date neafectate de erori	Ambigue	Poate avea mai multe interpretări	Alarme generice ale sistemelor IDS (ce nu izolează cauza)
		Incomplete	Anumite părți din date lipsesc	Documentarea incompletă a unui incident anterior
		Deficiente	Anumite parți de date esențiale procesării lipsesc	Sisteme introduse incomplet în baza de cunoştințe
	Date afectate de erori	Invalide	Neconformitate cu realitatea	Alerte IDS false (false positives)
		Incorecte	Date incorecte sau greşite	Trafic injectat de atacator
		Fără sens	Date ce nu respectă specificațiile protocoalelor	Trafic de atac la implementările de protocol
		Distorsionate	Greşit dar nu departe de adevăr	Rapoarte de stare ce iau în calcul date incorecte
		Bazate pe premise incorecte	Datorate unei erori sistematice	Reguli de detecție incorecte
Inconsistență	Date	Incoerente	Concluzii diferite pe baza datelor	Un sistem de detecție generează alerte, în timp ce altul, având acelaşi câmp de vizibilitate, nu indică probleme.
		Inconsistente	Incoerență cu conotație temporală	Monitor care la anumite intervale regulate nu raportează starea.
		Conflictuale	Incompatibilitate între date	Cazul procesul de analiză a evenimentelor în care entități de date par imposibil de a coexista.
Incertitudine	Date	Obiectivă	Legată de realitate şi de date	Posibilitatea unui atac asupra organizației
	Agent	Subiectivă	Opinia agentului expert legată de validitatea datelor determinată pe baza informațiilor existente	În evaluarea unei intruziuni în curs de desfăşurare, agentul (analist de securitate sau aplicație) poate considera datele prezentate ca probabile, îndoielnice, posibile, nefiabile, or nerelevante.

Tabelul 5.1 – Categorii de imperfecțiuni a datelor procesul de monitorizare a securității

Teoriile tradiționale de tratare a informațiilor imperfecte (cum ar fi teoria clasică a probabilităților), au limitări în ceea ce priveşte adresarea cazurilor complexe, cum ar fi de exemplu cele cu un grad ridicat de informație vagă, nesigură, imprecisă, ambiguă şi

conflictuală, iar multitudinea de preocupări în zona modelării imperfecțiunii (teoria posibilităților bazate pe seturi fuzzy, teoria evidențelor, teoria probabilităților imprecise, etc.) reflectă recunoaşterea asupra dimensiunilor multiple ale imperfecțiunii.

Având în vedere modul de generare a evenimentelor de securitate de către sistemele de detecție a intruziunilor (pe baza unor evidențe sau indicatori observați în traficul de date, fişierele de jurnalizare, starea sistemului, etc.), precum şi parametrul utilizat pentru evaluarea calității alertelor generate (rata de alarme false, sau nivelul de încredere în alerta generată), se alege teoria evidențelor pentru modelarea imperfecțiunii datelor ce vor fi evaluate în cadrul experimentului.

În contextul teoriei evidențelor, rezolvarea unei probleme de *fuziune* (combinare a informațiilor de alertă având ca scop o estimare cât mai bună a stării de securitate a entității monitorizate) presupune [Sma04]:

- Definirea clară a cadrului de discernământ
- Alegerea corespunzătoare a modelului
- Selectarea setului corespunzător pe care vor fi definite funcțiile de încredere
- Alegerea unei reguli eficiente de combinare a funcțiilor de încredere
- Stabilirea criteriului adoptat pentru luarea deciziei
- In cazul unei fuziuni dinamice (în care cadrul sau modelul se schimbă în timp) se stabilesc condițiile în care se face schimbarea şi detaliile de tranziție.

În următoarele două paragrafe vor fi prezentate modele matematice reprezentative pentru teoria evidențelor, precum şi etapele rezolvării problemei de fuziune.

5.2 Teoria Dempster-Shafer (TDS)

Unul dintre modelele matematice ce permite lucrul în condiții incerte este cunoscut sub numele de teoria raționamentului bazat pe evidență (sau teoria Dempster-Shafer - TDS)[Sha76]. Premisa teoriei a constituit-o faptul că ignoranța unui agent față de o afirmație nu trebuie să determine împărțirea în mod egal a probabilității între valoarea de adevăr şi cea de fals, aşa cum se asumă în raționamentul probabilistic clasic. Mai mult, în cazul în care există posibilitatea câtorva alternative singulare mutual exclusive (singletons), iar agentul poate stabili probabilitățile doar pentru câteva dintre acestea, conform raționamentului probabilistic clasic, probabilitățile rămase trebuie distribuite într-o anumită manieră între celelalte alternative.

Definiție: $\Theta = \{\theta_1, \ldots, \theta_n\}$ se numeşte cadru de discernământ al problemei de fuziune, unde θ_i cu $i = 1, \ldots, n$ reprezintă setul de ipoteze.

Modelul Shafer ($M^0(\Theta)$) presupune că θ_i ($i = 1, \ldots, n$) sunt precis identificate astfel încât să asigure exclusivitatea şi exhaustivitatea ipotezelor. Dacă Θ este deschis (condiția de exhaustivitate nu este îndeplinită), se poate adaugă un element θ_{n+1} de închidere astfel încât să se lucreze cu un cadru închis $\{\theta_1, \ldots, \theta_n, \theta_{n+1}\}$. Astfel, fără a pierde din generalitate, se va considera că $\Theta = \{\theta_1, \ldots, \theta_n\}$ formează un cadru de discernământ închis.

În TDS inițială, subseturile sunt construite ca propoziții, unde propozițiile de interes au

forma:

$P_\theta(A) \triangleq$ Valoarea de adevăr a lui θ este într-un subset A din Θ.

Având în vedere izomorfismul între $P_\theta(A)$ şi A, pentru simplicitate şi consistență cu terminologia adoptată în alte teorii curente, se va utiliza o reprezentare bazată pe mulțimi în definițiile ce vor urma.

Definiție: Se numeşte *setul de putere* (power set) $2^\Theta \triangleq (\Theta, \cup)$ mulțimea alcătuită din toate submulțimile lui Θ creată pe baza următoarelor reguli:

- $\varnothing, \theta_1, \ldots, \theta_n \in 2^\Theta$.
- Dacă $A, B \in 2^\Theta$, atunci $A \cup B \in 2^\Theta$.
- 2^Θ nu conține nici un alt element cu excepția celor obținute utilizând primele doua reguli.

Pentru $\Theta = \{\theta_1, \theta_2, \theta_3\}$, se obține

$2^\Theta = \{\varnothing, \{\theta_1\}, \{\theta_2\}, \{\theta_3\}, \{\theta_1 \cup \theta_2\}, \{\theta_2 \cup \theta_3\}, \{\theta_1 \cup \theta_3\}, \{\theta_1 \cup \theta_2 \cup \theta_3\}\}$, având cardinalitatea $|2^\Theta| = 8$

Definiție: Se numeşte *masa de încredere de bază* (numită simplu şi *funcția de masă*), funcția $m(.): 2^\Theta \to [0,1]$ asociată unui corp de evidență B după cum urmează:

$$m(\varnothing) = 0 \qquad \text{şi} \qquad \sum_{A \in 2^\Theta} m(A) = 1 \tag{1}$$

valoarea $m(A)$ este denumită masa generalizată de încredere de bază a lui A.

Definiție: A este un *element focal* al spațiului de fuziune 2^Θ dacă $m(A) > 0$.

Definiție: Se definesc funcțiile *încredere* (credibilitate) şi cea de *plauzibilitate* pentru $A \subseteq \Theta$ după cum urmează:

$$\mathrm{Bel}(A) = \sum_{\substack{B \subseteq A \\ B \in 2^\Theta}} m(B) \qquad \mathrm{Pl}(A) = \sum_{\substack{B \cap A \neq \varnothing \\ B \in 2^\Theta}} m(B) \tag{2}$$

Bel(A) reprezintă masa totală de informații care implică existența lui A, iar Pl(A) este masa totală de informații consistentă cu A.

5.2.1 Regula de combinare DS

Fuziunea a două surse independente cu mase $m_1(.), m2(.)$ şi având aceeaşi fiabilitate se efectuează pe baza formulei următoare:

$$m(\varnothing) = 0 \quad \text{şi} \quad \text{pentru } \forall A \in 2^\Theta \setminus \{\varnothing\},\ m_{DS}(A) = \frac{1}{1 - k_{12}} \sum_{\substack{X, Y \in 2^\Theta \\ X \cap Y = A}} m_1(X) * m_2(Y), \tag{3}$$

unde $k_{12} = \sum_{\substack{X,Y \in 2^{\Theta} \\ X \cap Y = \varnothing}} m_1(X) * m_2(Y)$ reprezintă gradul total de conflict (4)

Efectul factorului de normalizare $1 - k_{12}$ din (3) constă în eliminarea componentelor de informație conflictuale între cele două surse combinate.

Regula DS realizează o combinare de tip conjunctiv, este asociativă şi comutativă, putând fi astfel aplicabilă pentru N>2 surse. De asemenea, în cazul când elementele focale sunt doar singletons (ipoteze singulare din Θ), regula devine una consistentă cu una de tip Bayes în care $\mathrm{m}(.) \equiv \mathrm{P}(.)$.

Regula prezintă limitări în situații cu conflict ridicat (valoarea lui k_{12} mare), iar când $k_{12} = 1$, masa combinată $m(.)$ nu este definită, iar cele două surse de evidență sunt în contradicție totală. Soluțiile curente constau în aplicarea unor tehnici de selectare ad-hoc a unor valori prag asupra acceptării (sau respingerii) rezultatelor de fuziune, sau aplicarea unei tehnici de tip „actualizare" asupra surselor. Departe de a adresa riscul prezentat de limitările menționate anterior, aceste soluții transferă riscul în alte zone cum ar fi: modul de selectare a valorii de prag, modul de executare a actualizării în absența unor date statistice, etc.

O serie de eforturi au fost depuse în zona identificării de noi reguli de combinare bazate pe modelul Shafer care să adreseze limitările regulii de combinare. [Dub86] [Yag87] [Ina91]

Cum monitorizarea securității mediilor complexe generează uneori date impredictibile, se recomandă o utilizare circumspectă a regulii de combinare DS.

Pentru exemplificarea modului de operare a acestei reguli de combinare, se consideră un cadru de discernământ $\Theta = \{\theta_1, \theta_2\}$ unde θ_1 este ipoteza de trafic de atac, iar θ_2 este ipoteza de trafic legitim, iar $m_1(.), m2(.)$ sunt funcțiile de masă asociate unor sisteme IDS independente ale căror valori sunt exemplificate mai jos:

$$m_1(\theta_1) = 0.1 \quad m_1(\theta_2) = 0.2 \quad m_1(\theta_1 \cup \theta_2) = 0.7$$
$$m_2(\theta_1) = 0.3 \quad m_2(\theta_2) = 0.2 \quad m_2(\theta_1 \cup \theta_2) = 0.5$$

$$k_{12} = m_1(\theta_1)m_2(\theta_2) + m_1(\theta_2)m_2(\theta_1)$$
$$k_{12} = 0.1 \cdot 0.2 + 0.2 \cdot 0.3 = 0.02 + 0.06 = 0.08$$

$$m(\theta_1) = [m_1(\theta_1)m_2(\theta_1) + m_1(\theta_1)m_2(\theta_1 \cup \theta_2) + m_2(\theta_1)m_1(\theta_1 \cup \theta_2)]/(1 - k_{12}) = 0.29/0.92 \approx 0.316$$
$$m(\theta_2) = [m_1(\theta_2)m_2(\theta_2) + m_1(\theta_2)m_2(\theta_1 \cup \theta_2) + m_2(\theta_2)m_1(\theta_1 \cup \theta_2)]/(1 - k_{12}) = 0.28/0.92 \approx 0.304$$
$$m(\theta_1 \cup \theta_2) = m_1(\theta_1 \cup \theta_2)m_2(\theta_1 \cup \theta_2)/(1 - k_{12}) = 0.35/0.92 \approx 0.380$$

Figura 5.2 - Exemplu combinare DS

În cazul combinării informațiilor provenind de la surse cu fiabilitate diferită, este necesară actualizarea prealabilă a maselor, prin alocarea procentului corespunzător de nefiabilitate către ignoranță. Considerând o sursă nefiabilă având funcția de masă $m(.)$, şi un indice de fiabilitate $\alpha \in [0,1]$ unde $\alpha = 0$ reprezintă sursă total nefiabilă (sau ignorantă), iar $\alpha = 1$ sursă total fiabilă, actualizarea valorilor funcției de masă se va efectua pe baza următoarelor formule:

$$\begin{cases} m(A) \\ m(\Theta) \end{cases} \rightarrow \begin{cases} m'(A) = \alpha \cdot m(A) & \forall A \neq \Theta \\ m'(\Theta) = (1-\alpha) + \alpha \cdot m(\Theta) \end{cases} \quad (5)$$

Figura 5.3 - Formulele de ajustare a maselor pe baza fiabilității senzorului

Această ajustare necesită însă un proces adecvat de estimare a factorului de fiabilitate a fiecărei surse, bazat pe experimente statistice validate.

5.3 Teoria Dezert-Smarandache (TDSm)

Pentru a adresa situațiile în care este necesară combinarea informațiilor provenind de la surse imprecise, nesigure, şi aflate în conflict, Jean Dezert şi Florin Smarandache au extins teoria TDS prin relaxarea condiției de exclusivitate mutuală a elementelor cadrului de discernământ, punând bazele unei noi teorii care le poartă numele (TDSm).

Spre deosebire de TDS, TDSm permite combinarea formală a informațiilor provenite de la orice tip de surse independente, reprezentată în pe baza funcțiilor de încredere. TDSm şi-a arătat deja utilitatea în rezolvarea unor probleme complexe de fuziune în mod special atunci când conflictul între surse este ridicat, sau rafinamentul spațiului de discernământ Θ, este dificil de realizat datorită naturii vagi, imprecise a elementelor din Θ [Sma04].

Definiție: Se numeşte *set hiper-putere* (hyper-power set) $D^{\Theta} \triangleq (\Theta, \cup, \cap)$ structura alcătuită din toate submulțimile lui $\Theta = \{\theta_1, \ldots, \theta_n\}$ utilizând operatorii $\cup$ şi $\cap$ după cum urmează:

- $\varnothing, \theta_1, \ldots, \theta_n \in D^{\Theta}$
- Dacă $A, B \in D^{\Theta}$, atunci $A \cap B \in D^{\Theta}$ şi $A \cup B \in D^{\Theta}$
- D^{Θ} nu conține nici un alt element cu excepția ce lor obținute utilizând regulile 1 şi 2.

Cardinalitatea seturilor de hiper putere urmează şirul de numere Dedekind. Când $\Theta = \{\theta_1, \theta_2, \theta_3\}$, se obține $D^{\Theta} = \{\alpha_0, \alpha_1, \ldots, \alpha_{18}\}$ cu cardinalitatea $| D^{\Theta} | = 19$ [Sma04].

$$\begin{aligned}
&\alpha_0 = \varnothing \\
&\alpha_1 = \theta_1 \cap \theta_2 \cap \theta_3 && \alpha_{10} = \theta_2 \\
&\alpha_2 = \theta_1 \cap \theta_2 && \alpha_{11} = \theta_3 \\
&\alpha_3 = \theta_1 \cap \theta_3 && \alpha_{12} = (\theta_1 \cap \theta_2) \cup \theta_3 \\
&\alpha_4 = \theta_2 \cap \theta_3 && \alpha_{13} = (\theta_1 \cap \theta_3) \cup \theta_2 \\
&\alpha_5 = (\theta_1 \cup \theta_2) \cap \theta_3 && \alpha_{14} = (\theta_2 \cap \theta_3) \cup \theta_1 \\
&\alpha_6 = (\theta_1 \cup \theta_3) \cap \theta_2 && \alpha_{15} = \theta_1 \cup \theta_2 \\
&\alpha_7 = (\theta_2 \cup \theta_3) \cap \theta_1 && \alpha_{16} = \theta_1 \cup \theta_3 \\
&\alpha_8 = (\theta_1 \cap \theta_2) \cup (\theta_1 \cap \theta_3) \cup (\theta_2 \cap \theta_3) && \alpha_{17} = \theta_2 \cup \theta_3 \\
&\alpha_9 = \theta_1 && \alpha_{18} = \theta_1 \cup \theta_2 \cup \theta_3
\end{aligned}$$

Figura 5.4 – Setul de hiper-putere pentru un spațiu de discernământ cu $| \Theta | = 3$

Pentru Modelul Shafer ($M^0(\Theta)$), setul de hiper putere se reduce la setul de putere clasic ($D^\Theta \equiv 2^\Theta$)

$\mid \Theta \mid = n$	$\mid 2^\Theta \mid = 2^n$	$\mid D^\Theta \mid$
2	4	5
3	8	19
4	16	167
5	32	7580

Tabelul 5.2 - Cardinalitatea setului de putere şi a celui de hiper-putere

5.3.1 Funcțiile generalizate de încredere

Definiție: Pentru un cadru general Θ, se defineşte funcția de masa $m(.): G^\Theta \to [0,1]$ asociată unui corp de evidență B dat ca fiind:

$$m(\varnothing) = 0 \quad \text{şi} \quad \sum_{A \in G^\Theta} m(A) = 1 \tag{6}$$

Definiție: Se definesc *funcțiile încredere* (credibilitate) şi cea de *plauzibilitate* pentru $A \subseteq \Theta$ în mod similar TDS şi anume:

$$\mathrm{Bel}(A) = \sum_{\substack{B \subseteq A \\ B \in G^\Theta}} m(B) \qquad \mathrm{Pl}(A) = \sum_{\substack{B \cap A \neq \varnothing \\ B \in G^\Theta}} m(B) \tag{7}$$

G^Θ este o notație generică pentru un set pe care funcția de masă este definită (G^Θ poate fi 2^Θ sau D^Θ în funcție de modelul ales pentru Θ). Aceste definiții sunt compatibile cu definițiile funcțiilor clasice de încredere ale TDS când $G^\Theta = 2^\Theta$ pentru problemele de fuziune unde modelul Shafer $M^0(\Theta)$ este utilizabil [Sma09].

Pe parcursul capitolului, se vor utiliza diagramele Venn pentru reprezentarea grafică a relațiilor logice posibile între elementele lui G^Θ. O exemplificare a utilizării acestora este efectuată în figura 5.5.

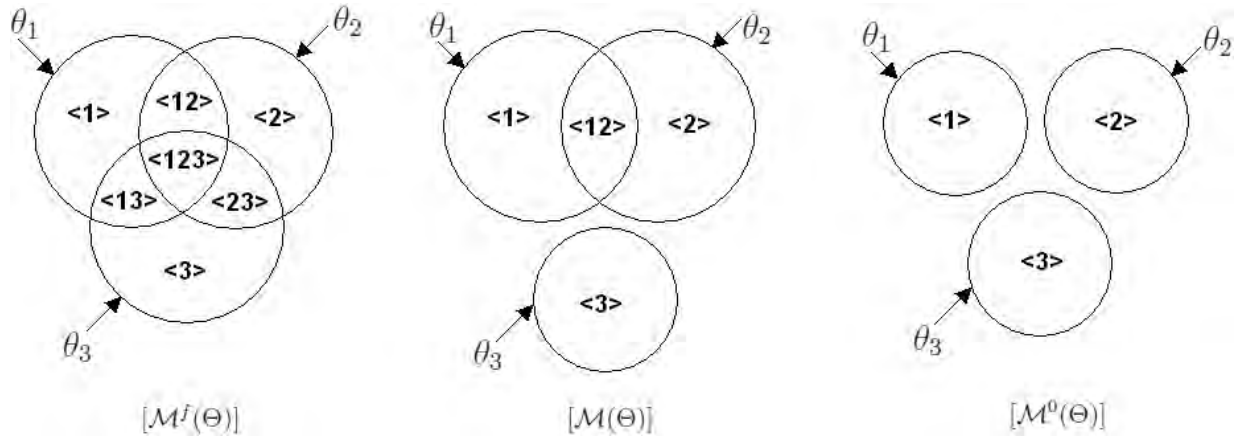


Figura 5.5 - Diagramele Venn pentru modelele

DSm liber ($M^f(\Theta)$), DSm hibrid ($M(\Theta)$), şi Shafer ($M^0(\Theta)$) cu $\mid \Theta \mid = 3$

5.3.2 Modele DSm

În funcție de natura (discretă sau continuă, precisă sau vagă, absolută sau relativă, etc) conceptelor implicate în procesul de fuziune, se stabileşte granularitatea modelului utilizat pentru cadrul de fuziune după cum urmează [Sma06]:

- *Modelul DSm liber* ($M^f(\Theta)$) - impune o singură condiție asupra elementelor θ_i, $i = 1,\ldots,n$ ale cadrului de discernământ Θ, şi anume cea de exhaustivitate (cadrul de discernământ închis). Elementele cadrului sunt vagi şi se pot suprapune. Este util în manipularea conceptelor continue, având o interpretare relativă (în care rafinamentul total este indisponibil)
- *Modelul DSm hibrid* ($M(\Theta)$)) – presupune introducerea unor constrângeri de integritate în $M^f(\Theta)$. Unele elemente ale cadrului pot fi exclusive sau inexistente în cazul anumitor fuziunii datelor pentru anumite aplicații.
- *Modelul Shafer* (($M^0(\Theta)$)) – este un caz special de $M(\Theta)$ în care toate elementele exhaustive ale cadrului sunt cunoscute a fi exclusive

5.3.3 Regula de combinare clasică DSm

Dacă modelul liber $M^f(\Theta)$ este adecvat problemei de fuziune ce trebuie adresate, regula clasică de combinare $m_{M^f(\Theta)} \equiv m(.) \triangleq [m_1 \oplus m_2](.)$ a două surse independente de evidență B_1 şi B_2 pe acelaşi cadru Θ având funcțiile masă $m_1(.)$ şi $m_2(.)$ corespunde consensului conjunctiv al surselor şi este dat de formula:

$$\forall C \in D^\Theta, \qquad m_{M^f(\Theta)}(C) \equiv m(C) = \sum_{\substack{A,B \in D^\Theta \\ A \cap B = C}} m_1(A) m_2(B) \tag{8}$$

```
Data: n experts ex: ex[1] ... ex[n], ex[i].focal, ex[i].bba
Result: Fusion of ex by conjunctive rule: conj
extmp ← ex[1];
for e = 2 to n do
    comb ← ∅;
    foreach foc1 in extmp.focal do
        foreach foc2 in ex[e].focal do
            tmp ← extmp.focal(foc1) ∩ ex[e].focal(foc2);
            comb.focal ← tmp;
            comb.bba ← extmp.bba(foc1) × ex[e].bba(foc2);
    Concatenate same focal in comb;
    extmp ← comb;
conj ← extmp;
```

Figura 5.6 - Algoritm implementare regulă combinare clasică DSm

Datorită numărului mare de elemente în D^Θ când cardinalitatea lui Θ creşte (vezi tabelul 5.2), regula clasică de combinare va necesita foarte multe resurse computaționale şi de memorie. Totuşi în cazul multor aplicații practice, cardinalitatea *nucleelor* $K_1(m_1)$ şi $K_2(m_2)$ (seturile de elemente focale $A \neq \varnothing \in D^\Theta$ unde $m_1(A) > 0$ sau $m_2(A) > 0$) este mult mai mică decât cea a lui D^Θ, putându-se astfel realiza unele

optimizări de implementare a regulii de combinare clasică DSm [Sma04].

Regula de combinare este foarte uşor de implementat. Pentru ilustrare se oferă algoritmul utilizat în implementarea toolkit-ului de funcții DSm realizat de A. Martin care operează pe un set redus (D_r^Θ) al lui D^Θ care conține numai nucleele ce trebuie combinate [Mar11].

5.3.4 Regula de combinare DSm hibridă (DSmH)

Când $M^f(\Theta)$ nu este conform cu natura problemei de fuziune considerate şi necesită luarea în considerare a unor constrângeri de integritate cunoscute, se va opera cu un model DSm hibrid construit corespunzător $M(\Theta) \neq M^f(\Theta)$.

Definiție: Se defineşte *mulțimea vidă extinsă* $\varnothing \triangleq \{\varnothing_M, \varnothing\}$ care include $\varnothing_M$ (mulțimea tuturor elementelor D^Θ care au fost forțate a fi vide prin aplicarea constrângerilor asupra modelului M) şi $\varnothing$ mulțimea vidă clasică.

Definiție: Se numeşte *funcția caracteristică de existență* $\phi(A)$ a unui set A, funcția definită după cum urmează:

$$\phi(A) = 1 \text{ dacă } A \notin \varnothing \text{ şi } \phi(A) = 0 \text{ dacă } A \in \varnothing \tag{9}$$

Având ca punct de plecare regula Dubois & Prade [Dub86], se defineşte pe modelul DSm hibrid ales $M(\Theta)$ cu $k \geq 2$ surse de informație independente regula de combinare DSm hibridă (DSmH) pentru $A \in D^\Theta$ ca fiind:

$$m_{DSmH}(A) = m_{M(\Theta)}(A) \triangleq \phi(A)[S_1(A) + S_2(A) + S_3(A)] \tag{10}$$

unde $S_1(A) \equiv m_{M^f(\theta)}(A)$, $S_2(A)$, $S_3(A)$ sunt definite astfel:

$$S_1(A) \triangleq \sum_{\substack{X_1, X_2, \ldots, X_k \in D^\Theta \\ X_1 \cap X_2 \cap \ldots \cap X_k = A}} \prod_{i=1}^{k} m_i(X_i) \tag{11}$$

$$S_2(A) \triangleq \sum_{\substack{X_1, X_2, \ldots, X_k \in \varnothing \\ [U=A] \vee [(U \in \varnothing) \wedge (A = I_t)]}} \prod_{i=1}^{k} m_i(X_i) \tag{12}$$

$$S_3(A) \triangleq \sum_{\substack{X_1, X_2, \ldots, X_k \in D^\Theta \\ X_1 \cup X_2 \cup \ldots \cup X_k = A \\ X_1 \cap X_2 \cap \ldots \cap X_k \in \varnothing}} \prod_{i=1}^{k} m_i(X_i) \tag{13}$$

cu $U \triangleq u(X_1) \cup u(X_2) \cup \ldots \cup u(X_k)$ unde $u(X)$ este reuniunea tuturor θ_i care compun X, iar $I_t = \theta_1 \cup \theta_2 \cup \ldots \cup \theta_n$ este ignoranța totală.

$S_1(A)$ corespunde regulii de combinare clasică DSm pentru k surse independente bazate pe modelul liber $M^f(\Theta)$;

$S_2(A)$ reprezintă masa tuturor seturilor relativ sau absolut vide care este transferată către ignoranța relativă sau totală asociată cu o constrângere de tip non-existență

$S_3(A)$ transferă suma seturilor relative vide direct într-o formă canonică disjunctivă de seturi nevide.

Regula de combinare pentru DSm hibrid generalizează regula de combinare clasică DSm şi nu este echivalentă regulii DS. Poate fi utilizată pentru orice model (modelul liber, modelul Shafer, sau orice model hibrid) atunci când manipulează funcții de încredere generalizate precise. O extensie a acestei reguli pentru combinarea de funcții de încredere generalizate imprecise este disponibilă în [Sma04].

Date intrare: (X_1, X_2), $S_1[]$, $S_2[]$, $S_3[]$

S_1: $A = (X_1 \cap X_2)$
if (A) este constrângere
then go to S_3
else $S_1(A) = S_1(A) + m_1(X_1)m_2(X_2)$

S_3: $A = (X_1 \cup X_2)$
if (A) este constrângere
then go to S_2
else $S_3(A) = S_3(A) + m_1(X_1)m_2(X_2)$

S_2: $A = (u(X_1) \cup u(X_2))$
if (A) este constrângere
then $I_t = I_t + m_1(X_1)m_2(X_2)$
else $S_2(A) = S_2(A) + m_1(X_1)m_2(X_2)$

Figura 5.7 - Algoritm de aplicare a regulii de combinare DSmH asupra unei perechi (X_1, X_2)

5.3.5 Regula de redistribuire proporțională a conflictului

Scopul regulii de redistribuție proporțională a conflictelor este de a transfera (total sau parțial) masele de conflict către seturi nevide implicate în conflict în mod proporțional cu masele asociate acestora de către surse după cum urmează:

- Calculează regula conjunctivă a maselor de încredere :

$$m_{12}(X) = \sum_{\substack{X_1, X_2 \in G^\Theta \\ X_1 \cap X_2 = X}} m_1(X_1)m_2(X_2) \quad (14)$$

- Calculează toate masele în conflict:

$k_{12} = \sum_{\substack{X_1, X_2 \in G^\Theta \\ X \cap X_2 = \varnothing}} m_1(X_1)m_2(X_2)$, unde $m_1(X_1)m_2(X_2)$ este masa de conflict parțial (15)

- Redistribuie masele în conflict (totale sau parțiale) către seturile nevide implicate în conflict în mod proporțional cu masele asociate de surse şi în conformitate cu toate constrângerile de integritate.

Multiplele posibilități de redistribuție a maselor în conflict, a dus la crearea unei serii de reguli de distribuție a conflictului (cunoscute sub numele de PCR1.. PCR6). Aceste reguli operează pentru orice grad de conflict, orice model, şi situații de fuziune statică sau dinamică.

În continuare este prezentată regula PCR5, considerată a fi cea mai eficientă regulă de combinare disponibilă în acest moment. Formula PCR5 pentru $s = 2$ surse este [Sma06]

$$m_{PCR5}(\varnothing) = 0 \text{ şi } \forall X \in G^{\Theta} \setminus \{\varnothing\}$$

$$m_{PCR5}(X) = m_{12}(X) + \sum_{\substack{Y \in G^{\Theta} \setminus \{X\} \\ X \cap Y = \varnothing}} \left[\frac{m_1(X)^2 m_2(Y)}{m_1(X) + m_2(Y)} + \frac{m_2(X)^2 m_1(Y)}{m_2(X) + m_1(Y)} \right] \quad (16)$$

5.3.6 Exemplu utilizare a regulilor de combinare

Pentru un spațiu de discernământ format din 2 elemente (A,B), un model Shafer şi două surse de masă $m_1(.)$, respectiv $m_2(.)$ cu valorile de masă date în liniile corespunzătoarele din tabelul de mai jos, se calculează $m_{12}(.)$ pe baza formulei (8) (valorile rezultat în ultima linie a tabelului). Acestea reprezintă totodată şi valorile pentru regula DSmH:

	A	B	$A \cup B$
$m_1(.)$	0.6	0.3	0.1
$m_2(.)$	0.2	0.3	0.5
$m_{12}(.)$	=0.6*0.2+0.6*0.5+0.2*0.1 0.44	=0.3*03+0.3*0.5+03*0.1 0.27	=0.1*0.5 0.05

Tabelul 5.3 – Exemplu combinare pe baza regulii DSm/DSmH

Masa de conflict $k_{12} = 0.24 = m_1(A)m_2(B) + m_1(B)m_2(A) = 0.24$ iar A şi B sunt singurele elemente focale implicate în conflict, aşa că ele vor primi o parte din masele conflictuale. PCR5 redistribuie masa de conflict 0.18 către A şi B proporțional cu masele $m_1(A)$, respectiv $m_2(B)$, iar masa de conflict 0.06 către A şi B proporțional cu masele $m_2(A)$, respectiv $m_1(B)$.

$$x_1/0.6 = y_1/0.3 = (x_1 + y_1)/(0.6 + 0.3) = 0.18/0.9 = 0.2 \rightarrow \begin{cases} x_1 = 0.6 \cdot 0.2 = 0.12 \\ y_1 = 0.3 \cdot 0.2 = 0.06 \end{cases}$$

$$x_2/0.2 = y_2/0.3 = (x_2 + y_2)/(0.2 + 0.3) = 0.06/0.5 = 0.12 \rightarrow \begin{cases} x_2 = 0.2 \cdot 0.12 = 0.024 \\ y_2 = 0.3 \cdot 0.12 = 0.036 \end{cases}$$

Valorile pentru regula PCR5 sunt calculate după cum urmează :

$$m_{PCR5}(A) = 0.44 + 0.12 + 0.024 = 0.584$$
$$m_{PCR5}(B) = 0.27 + 0.06 + 0.036 = 0.366$$
$$m_{PCR5}(A \cup B) = 0.05 + 0 = 0.05$$

Valorile pentru regula DS sunt calculate pe baza formulelor (3), (4) şi se obțin următoarele rezultate:

$$m_{DS}(A) = \frac{0.44}{1-0.24} \approx 0.579 \quad m_{DS}(B) = \frac{0.27}{1-0.24} \approx 0.355 \quad m_{DS}(A \cup B) = \frac{0.05}{1-0.24} \approx 0.066$$

Centralizând rezultatele în tabelul de mai jos, se observă că ignoranța totală $m_{DS}(A \cup B)$ obține prin redistribuire masă adițională, deşi nu ar trebui să primească nimic din masa conflictuală (conform ipotezei PCR5). Regula PCR5 este mai exactă decât cea DS

	A	B	$A \cup B$
m_{DS}	0.579	0.355	0.066
m_{DSmH}	0.440	0.270	0.290
m_{PCR5}	0.584	0.366	0.050

Tabelul 5.4 – Rezultatele combinării pe baza regulilor DS, DSmH şi PCR5

5.3.7 Transformarea pignistică

Managementului informației este un proces cu două niveluri: *credal* (cel de combinare a evidențelor), şi *picnistic* (cel de luare a deciziei). Când este necesară luarea unei decizii, trebuie construită o funcție de probabilitate pe baza funcțiilor de încredere ce descriu starea *credal* [Sme88].

TDSm urmează această abordare şi oferă câteva opțiuni pentru alegerea funcției de probabilitate ce se doreşte a fi utilizată pentru luarea deciziei în condiții de incertitudine.

O modalitate simplă de construire a funcției de probabilitate are la bază transformarea pignistică clasică definită în cadrul TDS [Sha76]:

$$BetP\{A\} = \sum_{X \in 2^{\Theta}} \frac{|X \cap A|}{|X|} m(X) \qquad (17)$$

unde $|A|$ reprezintă cardinalitatea lui A (şi convenția ca $|\varnothing| / |\varnothing| = 1$ pentru a extinde definiția şi pentru $BetP\{\varnothing\}$).

Definiție: Se defineşte *cardinalitatea DSm* ($C_M(A)$) pentru $\forall A \in D^{\Theta}$ ca fiind numărul de părți ale lui A în diagrama Venn corespunzătoare modelului M ales şi luând în considerare setul de constrângeri şi toate intersecțiile posibile.

Pe baza conceptului de cardinalitate DSm enunțat, se defineşte *transformarea pignistică generalizată* ca fiind:

$$\forall A \in D^{\Theta}, \qquad BetP\{A\} = \sum_{X \in D^{\Theta}} \frac{C_M(X \cap A)}{C_M(X)} m(X) \qquad (18)$$

unde $C_M(X)$ reprezintă cardinalul DSm al propoziției X pentru modelul DSm M al problemei considerate [Sma06].

$A \in D^\Theta$	$\mathcal{C}_\mathcal{M}(A)$
$\alpha_0 \triangleq \emptyset$	0
$\alpha_1 \triangleq \theta_1 \cap \theta_2$	1
$\alpha_2 \triangleq \theta_3$	1
$\alpha_3 \triangleq \theta_1$	2
$\alpha_4 \triangleq \theta_2$	2
$\alpha_5 \triangleq \theta_1 \cup \theta_2$	3
$\alpha_6 \triangleq \theta_1 \cup \theta_3$	3
$\alpha_7 \triangleq \theta_2 \cup \theta_3$	3
$\alpha_8 \triangleq \theta_1 \cup \theta_2 \cup \theta_3$	4

Figura 5.8 Cardinalitate DSm $C_M(A)$ pentru modelul hibrid $M(\Theta)$ din Figura 5.5

5.4 Experiment de monitorizare a securității utilizând TDSm şi TDS

Obiectivul acestei secțiuni este de a verifica aplicabilitatea TDSm pentru monitorizarea securității. Pentru simplificare se consideră cazul unui detector IDS care generează alerte şi care vor fi combinate pe baza TDS sau TDSm.

5.4.1 Modelarea detecției de intruziuni utilizând teoria DSm

Se alege cadrul de discernământ $\Theta = \{\theta_1, \theta_2, \theta_3\}$ unde ipotezele sunt definite după cum urmează:

- θ_1 - activitate legitimă
- θ_2 - activitate suspectă
- θ_3 - situație de intruziune

Pentru reprezentarea problemei se utilizează modelul DSm hibrid $M(\Theta)$ descris pe baza diagramei Venn din figura 5.9.

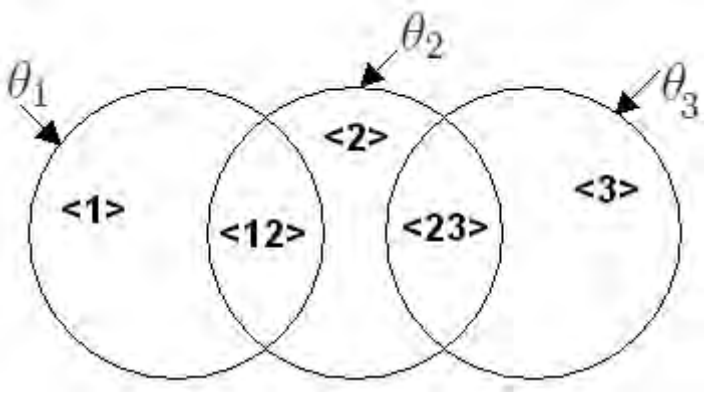


Figura 5.9 – Diagrama Venn pentru problema de detecție a intruziunii

Se utilizează <xy> pentru a desemna $\theta_x \cap \theta_y$, unde $x < y$ şi $x, y \in \{1,2,3\}$.

Setul de constrângeri (elemente D^Θ care sunt imposibil de obținut) pentru acest model este: $\{\theta_1 \cap \theta_3$, $(\theta_1 \cup \theta_2) \cap \theta_3$, $(\theta_2 \cup \theta_3) \cap \theta_1$, $(\theta_1 \cap \theta_3) \cup \theta_2$, $(\theta_1 \cap \theta_2) \cup (\theta_1 \cap \theta_3) \cup (\theta_2 \cap \theta_3)$, $\theta_1 \cap \theta_2 \cap \theta_3\}$.

Se consideră că sistemul IDS are un factor de încredere de 80% în alertele generate. Astfel funcția de masă de încredere pentru fiecare alertă va fi $m(.): G^\Theta \to [0,1]$ $m(\varnothing) = 0$ $m(A) = 0.8$ unde $A \in \Theta$ şi reprezintă rezultatul generat de sistemul IDS, iar $m(I_t) = 0.2$ reprezintă masa asociată ignoranței totale).

Pentru combinarea maselor se vor utiliza regulile DSmH şi PCR5. De asemenea, se vor evalua rezultatele obținute pe baza acestor reguli cu rezultatul aplicării regulii DS pe un modelul $M^0(\Theta)$ corespunzător cu $|\Theta| = 3$.

Decizia se va lua pe bază transformării pignistice generalizate (18)

5.4.2 Descrierea experimentului

Se va considera trafic de atac (corespunzător lui θ_3) acela identificat de regulile IDS al căror câmp de prioritate este mai mică decât prioritatea 4. Alertele generate de reguli având altă prioritate se vor considera suspecte (şi corespund lui θ_2). Dacă nici o alertă nu este generată, se va considera că activitatea vizibilă sistemului IDS este legitimă (ipoteza θ_1).

Se utilizează `hping` (versiunea 2) [Hpi--] pentru a genera trafic de atac de tip SYN Flood şi `ping` pentru a genera trafic ce va fi identificat ca suspect de sistemul IDS (Snort 2.9.1)[Sno--].

Traficul de atac va fi generat de la adresa `192.168.254.4`, iar ținta are adresa `192.168.254.101`.

Regulile IDS pentru detecția traficului de atac şi suspect generat sunt :

```
.............
alert tcp any any -> any any (msg:"Successful Test DOS "; flow: stateless;
flags:S,12; threshold: type threshold, track by_src, count 300, seconds 15;
classtype:successful-dos; sid:10002;)
alert tcp any any -> any any (msg:"My Syn Flood Scenario "; flow: stateless;
flags:S,12; threshold: type threshold, track by_src, count 30, seconds 5;
classtype:attempted-dos; sid:10008;)
...........
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING Windows"; itype:8;
content:"abcdefghijklmnop"; depth:16; reference:arachnids,169; classtype:misc-
activity; sid:382; rev:7;)
.............
```

Figura 5.10 – Reguli de detecție folosite pentru experiment

Prioritățile claselor de intruziune sunt definite în fişierul

```
$SNORT_HOME/etc/classification.config
```

```
...........
config classification: misc-activity,Misc activity,4
config classification: successful-dos,Denial of Service,2
config classification: attempted-dos,Attempted Denial of Service,3
...........
```

Figura 5.11 – Prioritățile regulilor de detecție folosite pentru experiment

Pe o durată de 10 minute eşantionată în intervale a câte 6 secunde fiecare, se creează următorul tip de trafic:

- Pentru primele 5 minute (eşantioanele 1-50) se generează cu o probabilitate de 70% trafic normal, 15% trafic suspect, şi 15% trafic de atac
- Primele ultimele 5 minute (eşantioanele 51-100) se generează cu o probabilitate de 70% trafic de atac, 15% trafic suspect, şi 15% trafic normal

```
...........
.
09/08-20:40:36.195766  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity]
[Priority: 4] {ICMP} 192.168.254.4 -> 192.168.254.101
09/08-20:40:38.589998  [**] [1:10008:0] My Syn Flood Scenario [**] [Classification:
Attempted Denial of Service] [Priority: 3] {TCP} 192.168.254.4:3507 -> 192.168.254.101:8084
09/08-20:40:40.650505  [**] [1:10008:0] My Syn Flood Scenario [**] [Classification:
Attempted Denial of Service] [Priority: 3] {TCP} 192.168.254.4:3537 -> 192.168.254.101:8084
09/08-20:40:42.708614  [**] [1:10008:0] My Syn Flood Scenario [**] [Classification:
Attempted Denial of Service] [Priority: 3] {TCP} 192.168.254.4:3567 -> 192.168.254.101:8084
09/08-20:40:43.597842  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity]
[Priority: 4] {ICMP} 192.168.254.4 -> 192.168.254.101
09/08-20:40:44.722941  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity]
[Priority: 4] {ICMP} 192.168.254.4 -> 192.168.254.101
.........
```

Figura 5.12 – Eşantion de trafic de testare

Pe baza definiției funcției de masă (definită în paragraful precedent), se vor genera valorile funcției pentru fiecare eşantion după cum urmează:

- Dacă nu există nici o alertă în eşantion, atunci $A = \theta_1$ (trafic legitim)
- Dacă pentru alertele din eşantionul de timp `min(Priority)< 4` atunci $A = \theta_3$ (trafic de atac), altfel $A = \theta_2$ (trafic suspect)

Combinarea datelor se efectuează după cum urmează:

```
Date: m[100] - set de 100 înregistrări cu valorile de masă
      Model_DSmH, Model_Shafer

Rezultat: Rezultate combinare
Valoare_start= m[random(100)]

Masa_SistemDS[0]= Valoare_start
Masa_SistemDSmH[0]= Valoare_start
Masa_SistemPCR5[0]= Valoare_start

         #(alege aleator o valoare din setul de înregistări

for I=1 to 100 do
   Masa_SistemDS[I]:= Combinare_DS(Masa_SistemDS[I-1], m[I])
      Masa_SistemDSmH[I]= Combinare_DSmH(Masa_SistemDSmH[I-1], m[I])
      Masa_SistemPCR5[I]= Combinare_PCR5(Masa_SistemPCR5[I-1], m[I])
done
```

Figura 5.12 – Algoritm de combinare a evenimentelor IDS

Pentru implementarea aplicației de combinare utilizată în acest test, s-au utilizat rutine Matlab din biblioteca de funcții DST şi DSmT realizată de Arnaud Martin [Mar11], precum şi rutine create de Pascal Djiknavorian şi disponibile în [Sma06][Sma09].

Probabilitățile se vor calcula pe baza transformatei generale pignistice. Pentru detalii de implementare a acestor funcții, se poate consulta codul sursă disponibil pe CD-ul ataşat lucrării.

Rezultatele obținute sunt prezentate în figurile 5.13, 5.14 şi 5.15.

5.4.3 Interpretarea rezultatelor obținute

Analizând rezultatele fuziunii se pot face următoarele observații:

- Toate *combinările detectează schimbarea trendului* (care se produce la iterația #54) în ceea ce priveşte starea generală de securitate, de la preponderent sigură în prima parte a intervalului, la cea de atac în partea a doua. DSmH şi PCR5 indică cu o probabilitate de 80% o stare de atac începând cu iterația #55, în timp ce combinația DS determină această schimbare cu o probabilitate de peste 80% abia la iterația #57.
- DSmH şi PCR5 *identifică* evenimentele de atac care au loc pe fond de trafic legitim, precum şi evenimentele normale pe durata secțiunii de atac.
- PCR5 efectuează o *redistribuție mai bună a conflictului* (a se vedea $m(\theta_1)$ pentru iterațiile din intervalul [15,21].)
- Rezultatele DSmH cât şi PCR5 *nu mai sunt cele aşteptate* atunci când aproape toată masa (peste 98%) se acumulează în $\theta_1 \cap \theta_2$ sau $\theta_2 \cap \theta_3$ (a se vedea spre exemplu iterația #41 pentru PCR5 şi #37 pentru DSmH). În acest caz probabilitățile pignistice vor indica cu aceeaşi tărie atât situație de trafic normal cât şi suspect. O soluție pentru a adresa astfel de situații este de a limita cantitatea de masă care se poate asocia la orice moment de timp unei entități a diagramei Venn. O *recomandare* în acest sens este ca orice masă în exces de 0.98 pentru un element să se realoce către ignoranța totală I(t) [Dji10].

Pe baza acestor observații se poate concluziona aplicabilitatea teoriei DSm pentru monitorizarea securității în cazul testat. O serie validări utilizând diferite clase de alarme, şi combinări de surse eterogene (IDS de rețea şi de stație) sunt necesare pentru a creşte gradul de confidență în aplicabilitatea teoriei. Pentru o implementare de succes în sisteme reale, este necesară rescrierea rutinelor de combinare şi de luare a deciziei utilizând un limbaj ce permite o rulare mai rapidă (cum ar fi C++).

Considerând limitările existente în ceea ce priveşte adresarea alarmelor false generate de sistemele IDS, precum şi previziunile legate de creşterea continuă a imperfecțiunii datelor de securitate, se anticipează ca identificarea şi utilizarea modelelor matematice ce adresează mai eficient datele imperfecte să constituie o preocupare importantă şi în domeniul managementului securității IT.

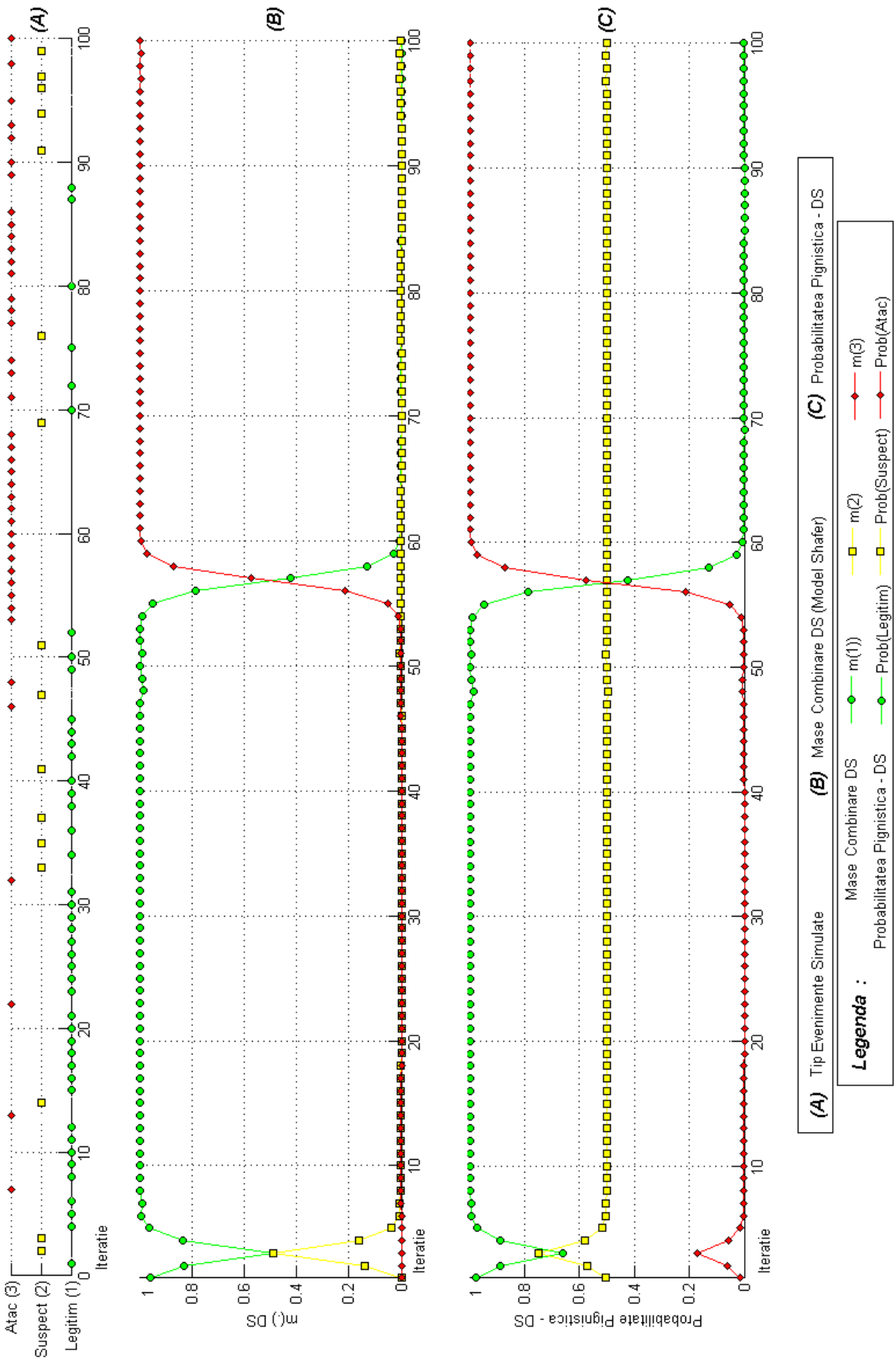


Figura 5.13 – Rezultatele combinării datelor de trafic utilizând modelul DS (Shafer)

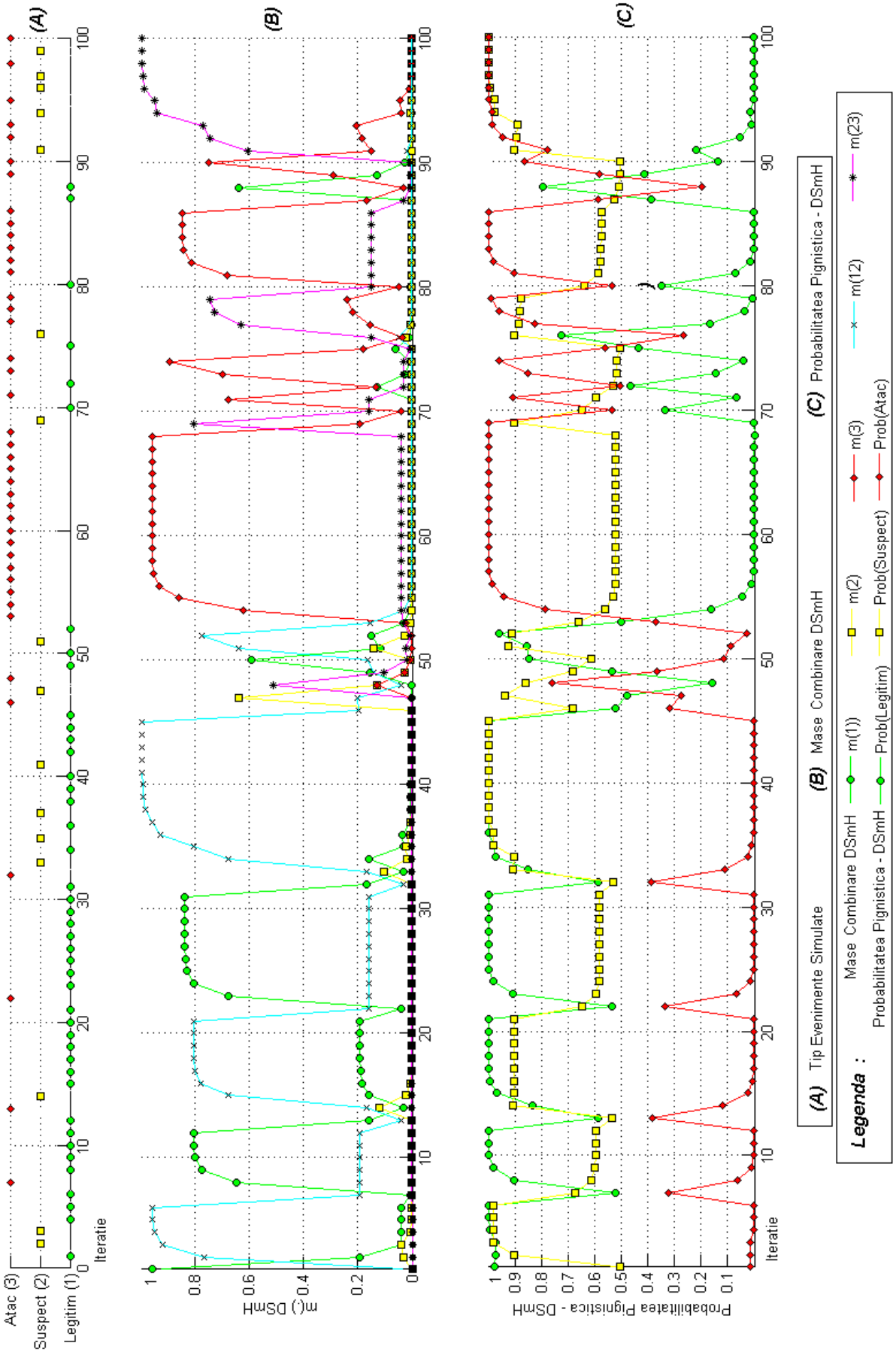


Figura 5.14 – Rezultatele fuziunii datelor de trafic utilizând regula de combinare DSmH

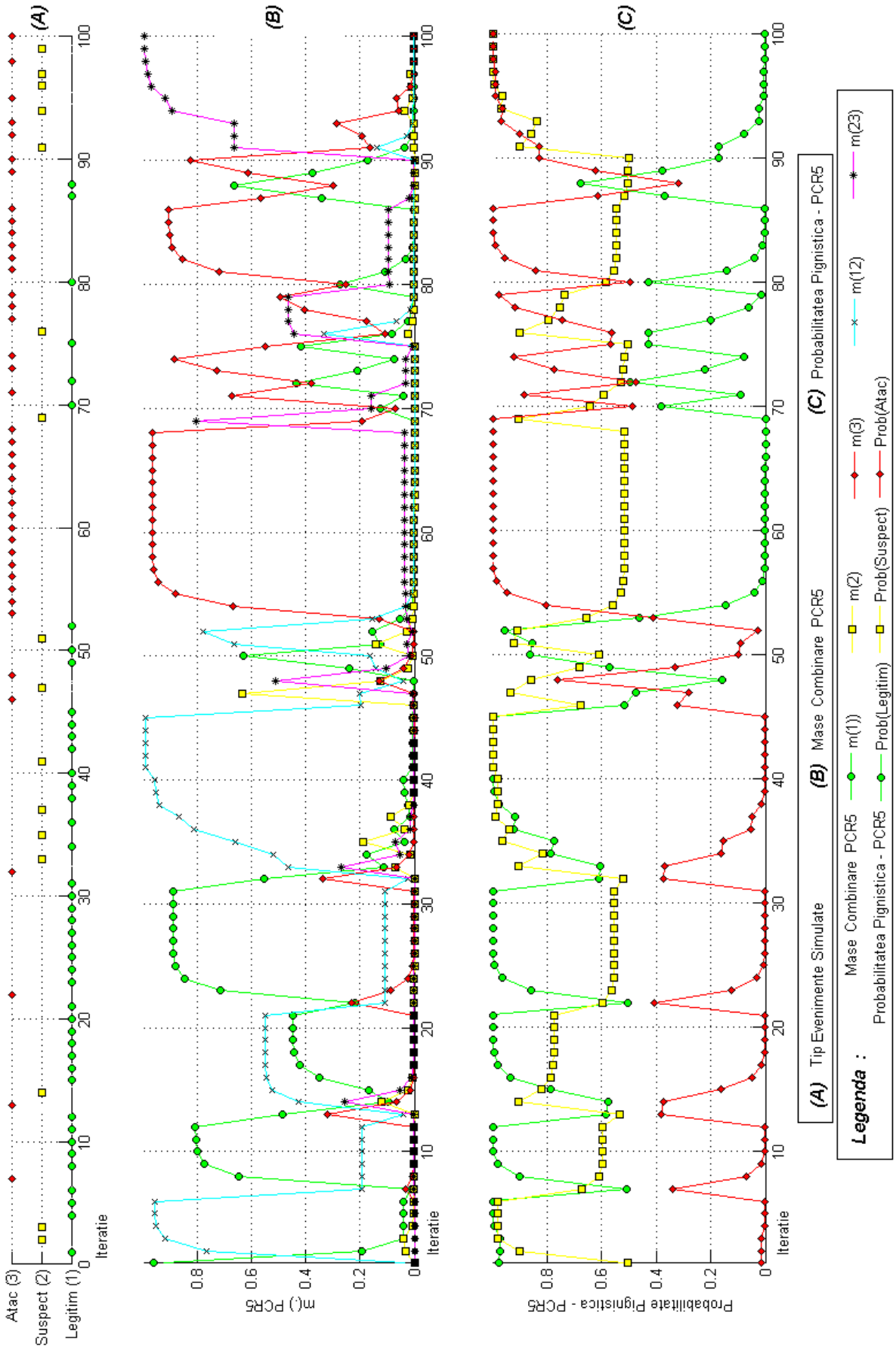


Figura 5.15 – Rezultatele fuziunii datelor de trafic utilizând regula de combinare PCR5

Motto*: Un punct, care ieri era nevăzut, este ţinta atinsă azi şi va fi punctul de plecare mâine!*
- Macanlay

CAPITOLUL 6

CONTRIBUŢII ŞI REZULTATE ŞTIINŢIFICE OBŢINUTE

Plecând de la abordarea *direcţiilor de cercetare* propuse în secţiunea introductivă, în perioada de pregătire şi de elaborare a tezei de doctorat s-au obţinut o serie de *rezultate ştiinţifice* şi s-au propus *contribuţii originale*, care au fost prezentate în detaliu în conţinutul tezei.

Ca metodologie de lucru s-a avut în vedere obţinerea de rezultate ştiinţifice şi de contribuţii originale care să se regăsească în cadrul fiecărui capitol al tezei. Este şi motivul pentru care se vor prezenta în continuare, sintetizat, pe capitole, rezultatele ştiinţifice şi contribuţiile originale propuse. Astfel, în:

Capitolul 1:

- *Elaborarea unui studiu asupra vulnerabilităţilor spaţiul virtual*. Complexitatea şi dinamica din spaţiul virtual constituie premisele existenţei unui volum în creştere şi diversificat de vulnerabilităţi. Vulnerabilităţile pot fi datorate *configuraţiei, politicii de securitate, utilizatorilor şi tehnologiei*. Vulnerabilităţile tehnologice sunt datorate deficienţelor structurale de securitate la nivelul suitei de protocoale de comunicaţie TCP/IP sau a implementărilor acestora, deficienţelor de securitate în aplicaţii, sistemele de operare sau ale echipamentelor de reţea. O bună înţelegere a spectrului vulnerabilităţilor e în măsură să contribuie la definirea şi implementarea unor strategii de securitate care să ofere rezultatele aşteptate. [PPN06-01]
- *Definirea unui cadru pentru detecţia intruziunilor şi a procesului de monitorizare asociat acestuia*. Pentru a detecta intruziunile, trebuie înţelese acţiunile necesare pentru compromiterea unei ţinte. În acest sens se prezintă un cadru cu fazele tipice prin care un atacator poate prelua controlul asupra unei victime, şi se evaluează oportunităţile de monitorizare corespunzătoare fiecărei faze. [PPN08]
- *Extinderea unui model de clasificare a atacurilor în Internet*. Odată cu progresele făcute în securizarea tehnologiilor şi infrastructurii Internetului, s-a observat o complexitate sporită în elaborarea şi managementul intruziunii din partea atacatorilor. În acest context este necesară utilizarea unor formalisme pentru caracterizarea atacurilor, astfel încât să se obţină o descriere completă şi consistentă a acestora. Extinderea efectuată a vizat adăugarea de atribute

necesare din perspectiva monitorizării securității care să ofere un management post incident mai eficient.

- *Construcția unor scheme pentru atacuri tipice pe bază de mesaje de poştă*. Având la bază principiul arborilor de atac, schemele prezintă succesiunea de paşi urmați atât de atacator cât şi de victimă pentru ca atacurile să se încheie cu succes. Schemele sunt utile pentru o înțelegere adecvată a căilor de atac, dar şi pentru a identifica modul în care tehnologiile disponibile la ora actuală pot fi utilizate pentru a reduce vulnerabilitatea la diferitele clase de atacuri. [PPN06-01]
- *Elaborarea unei analize comparative a tehnicilor de scanare utilizate în propagarea viermilor.* Obiectivul atacurilor pe bază de viermi este de a asigura infectarea a cât mai multor stații, iar detecția propagării să fie întârziată. Un rol important în acest sens îl are strategia de scanare (de identificare a potențialelor victime), identificarea factorilor care influențează performanțele de propagare putând ajuta la elaborarea unei defensive eficiente. Pe baza analizei s-a identificat necesitatea ca sistemele defensive să urmărească prevenirea atacatorului de la identificarea adreselor IP ale unui număr mare de stații vulnerabile, sau obținerea unor informații legate de adresele alocate, care determină reducerea spațiului de scanare. [PPN05-01]

Capitolul 2:

- *Construirea unui cadru de definire şi implementare a monitorizării securității centrat în jurul organizației şi a activităților sale.* Monitorizarea securității la nivelul organizației se defineşte ca fiind procesul de menținere în mod constant a atenției asupra securității informaționale, vulnerabilităților şi amenințărilor, cu scopul de a oferi suport deciziilor legate de managementul riscului la adresa organizației. Obiectivul este de a realiza monitorizarea în mod constant a securității rețelelor şi sistemelor informaționale ale organizației şi de a răspunde prin acceptarea, evitarea, transferul sau adresarea riscurilor atunci când sunt schimbări. [PPN08]
- *Elaborarea unui cadru pentru definirea de metrici de securitate*. Asemenea oricărui alt proces, managementul efectiv al securității nu poate avea loc dacă aceasta nu este măsurată. Pornind de la modelul CVSS (Common Vulnerability Scoring System) s-a elaborat un cadru pentru definirea de metrici de securitate în organizație. Această contribuție (publicată în [PPN06-05]) a constituit un punct de referință pentru comunitatea ştiințifică internațională, fiind printre primele cercetări efectuate în zona metricilor de securitate.
- *Definirea şi evaluarea unui cadru pentru partajarea informațiilor de intruziune la nivel* global. Multe organizații au implementat programe de răspuns la incidente de securitate, însă continuă să trateze atacurile ca evenimente singulare fără a colecta informații despre ele. Colectarea unor astfel de informații ar oferi posibilitatea de a analiza evoluția în timp a amenințărilor la adresa organizației, precum şi oportunitatea identificării unor riscuri structurale care să poată fi evaluate şi în procesul de analiză a riscului. VerIS (Verizon Incident Sharing) Framework permite colectarea şi analiza într-o manieră consistentă a informațiilor despre atacuri, astfel încât organizațiile să aibă o mai bună înțelegere asupra a ceea ce s-a întâmplat, precum şi a impactului, analiza

comparativă cu starea de securitate a altor organizații similare (din aceeaşi industrie, regiune geografică, sau de aceeaşi dimensiune).

- *Definirea unui model de monitorizare completă a securității*. Dacă inițial monitorizarea stării de securitate viza identificarea amenințărilor (detecția intruziunilor), conceptul a fost ulterior extins şi către alte zone din sfera securității IT cum ar fi: monitorizarea conformării cu politica de securitate, monitorizarea eficacității controalelor de securitate, monitorizarea vulnerabilităților controalelor, etc. O soluție de monitorizare completă, care va putea oferi informații de starea securității cât mai apropiate de realitate, va trebui să acopere toate elementele cu relevanță pentru procesul de securitate: amenințări, vulnerabilități, controale de securitate, resurse, risc şi agenți de amenințare [PNCN09]

Capitolul 3:

- *Sintetizarea şi elaborarea unei evaluări asupra tehnologiilor de culegere a datelor utilizate în procesul de monitorizare a securității.* Aceste tehnologii sunt responsabile pentru culegerea de date utilizate în procesul de monitorizare completă a securității, acoperind toate elementele cu relevanță pentru procesul de securitate şi anume: vulnerabilități, management patch-uri, evenimentele şi incidentele de securitate, detecția de software malițios, managementul configurațiilor, managementul rețelei, managementul inventarului de echipamente şi sisteme [PPN07-01].
- *Elaborarea unui studiu comparativ şi a unei caracterizări structurale a tehnologiilor de detecție a intruziunilor şi a implementărilor de sisteme IDS.* Tehnologiile au fost evaluate în funcție de tehnica sau principiul de detecție utilizat – monitorizare fişiere de jurnalizare, monitoare de integritate (fişier sau sistem), anomalii, semnături, hibride, capcană (honeypot), cât şi în funcție de resursa monitorizată şi amplasare.
- *Implementarea şi testarea tehnologiilor de detecție a intruziunilor.* Tehnologii reprezentative pentru detecția intruziunilor au fost testate şi evaluate pe durata cercetării pentru a stabili eficacitatea, gradul de interoperabilitate, suportul pentru direcții ulterioare de cercetare (cum ar fi validarea aplicabilității Teoriei Dezert-Smarandache pentru monitorizare în condiții de incertitudine a datelor prezentată în capitolul 5). Tehnologiile testate au fost Snort, Bro, SEC, OSSEC, Logwatch, Flister, Revealer, Vice, Tripwire, Afick.
- *Sintetizarea şi elaborarea unui studiu asupra tehnicilor de urmărire a atacurilor DDoS.* O strategie eficientă de construirea defensivei împotriva atacurilor DDoS combină o serie de tehnici pentru a acoperi următoarele aspecte: prevenirea, detecția, urmărirea pachetelor fluxurilor sau traficului agregat creat de DDoS şi suprimarea atacurilor. Clasele de tehnici de urmărire care au fost studiate includ marcarea pachetelor, controlul căii, şi jurnalizarea pachetelor. [PNB09]
- *Elaborarea unui studiu de caz pentru analiza spațiului de amenințări pe baza datelor publice oferite de sistemele de monitorizare globală în Internet.* Pe baza datelor de trafic observate de sistemele de monitorizare globală (CAIDA şi DShield/ISC) începând cu data de 28 Noiembrie 2008, se identifică apariția unui eveniment major în rețea, prezentând caracteristicile unei propagări epidemice de vierme (numit ulterior Conficker). Datele disponibile pentru următoarele luni indică schimbări în comportamentul viermelui pe măsură ce apar noi variante care înlocuie sau coexistă cu cele anterioare.

Capitolul 4:

- *Elaborarea unei arhitecturi generice de monitorizare a securității, precum şi a unui set de considerații pentru faza de implementare a arhitecturii.* O arhitectură generică de monitorizare a securității, stabilită pe baza modelelor OSSIM, Counterpane şi MCI Sentry, are următoarele componente: surse de evenimente cu relevanță pentru procesul de monitorizare, colectoare de evenimente, baza de date cu mesaje de securitate, module de analiză şi aplicații pentru suportul răspunsului la incidentele de securitate identificate. Se prezintă o serie de considerente ce trebuie avute atât în faza de proiectare cât şi cea de implementare: integrarea componentelor enumerate anterior, în contextul asigurării integrității, disponibilității şi securității datelor, şi a canalelor de comunicație între componente, precum şi amenințările la adresa arhitecturii [PPN08].
- *Elaborarea unui studiu asupra tehnicilor de corelație a datelor în procesul de monitorizare a securității*. Pe măsură ce scenariile de atac devin mai complexe, datele de monitorizare oferite de senzori devin obiectul unei analize mai profunde. Tehnicile sunt în general grupate în două categorii: abordări fără cunoştințe, care se regăsesc în cele mai multe implementări curente (console de monitorizare, sau instrumente de analiză a fişierelor jurnal), şi cea de-a doua categorie reprezentată de tehnicile bazate pe cunoştințe (furnizate de un expert, sau deduse pe baza unor tehnici de învățare). [PPN06-04]
- *Sintetizarea şi elaborarea unui studiu aspra riscurilor şi amenințărilor la adresa arhitecturii de monitorizare.* Pentru a creşte gradul de complexitate intruziunilor, atacatorul va căuta să-şi mențină un grad de anonimat, să evite detecția. În caz că nu reuşeşte, atacatorul va căuta să degradeze sau să stopeze colectarea de evidențe, fapt care va complica investigațiile de după incident. Concluziile indică faptul că majoritatea atacatorilor exploatează în esență consecințele unui management deficitar şi lipsa de experiență a administratorilor arhitecturii.

Capitolul 5:

- *Tratarea unor subiecte de noutate în literatura de specialitate din domeniul securității informaționale:* Odată cu creşterea complexității ecosistemului de securitate, procesul de monitorizare va avea la dispoziție mase mari de date şi informații, dar care vor fi caracterizate de un conținut din ce în ce mai ridicat de imperfecțiune. Tratarea cazurilor complexe de imperfecțiune a datelor pe baza teoriilor tradiționale (cum ar fi teoria clasică a probabilităților) este inadecvată. În acest sens s-au explorat modele matematice alternative cum ar Teoria Dezert-Smarandache (TDSm) a raționamentului plauzibil şi paradoxist care permite combinarea formală a oricărui fel de informații: certe, incerte, paradoxale. [NPP11]
- *Construirea unui model experimental de evaluare a aplicabilității TDSm în monitorizarea securității:* Una din problemele constante a tehnologiilor de detecție a intruziunilor este generarea de alarme false, care în multe cazuri influențează negativ procesul de analiză şi decizie. Pentru a verifica aplicabilitatea TDSm în această direcție, s-a construit un model experimental în care date de trafic legitim şi atac create în regim controlat sunt recepționate de un sistem IDS, care la rândul său generează alerte cu priorități diferite. Pe baza acestor alerte se creează evenimente asociate unui spațiu de discernământ,

care ulterior se combină pe baza a diferite reguli de fuziune (Shafer, PCR5, DSmH). Validarea a constant în verificarea concordanței între realitate (datele de trafic generate) şi rezultatele obținute în urma fuziunii, precum şi rapiditatea de detecție a schimbărilor care apar în mediu. [NPP11]

- *Construirea unui cadru de identificarea imperfecțiunii datelor din sfera monitorizării securității*. Pentru suportul evaluării aplicabilității TDSm în monitorizarea securității, s-a construit un cadru de identificare a imperfecțiunii datelor din sfera monitorizării securității plecând de la clasificarea imperfecțiunii informațiilor realizată de Smet. Pe baza acestui cadru pe vor putea identifica şi alte aspecte legate de monitorizarea securității pentru care se va dori testarea aplicabilității şi eficacității teoriei DSmT.

Rezultatele cercetării obținute pe durata pregătirii tezei de doctorat, şi prezentate în această lucrare, au fost publicate în peste 20 articole, studii sau cărți din care:

- 5 articole cotate şi indexate ISI
- 2 articole indexate IEEE Xplore
- 1 carte publicată la o editură cotată CNCSIS
- 1 articol cotat CNCSIS în reviste A,
- 1 articol cotat CNCSIS în reviste B+,
- 3 articole cotate CNCSIS în reviste B,
- 4 articole cotate în reviste C sau asimilate (cu ISSN / ISBN)

Lista detaliată a lucrărilor publicate care conțin rezultate ale cercetării proprii desfăşurate în domeniul monitorizării este prezentată în secțiunea „Publicații personale" din capitolul de Bibliografie.

De asemenea, rezultate obținute au constituit puncte de referință pentru comunitatea ştiințifică internațională. Dintre lucrările altor autori care valorifică rezultatele cercetării pe care am desfăşurat-o în sfera monitorizării securității se amintesc :

Lucrări de Doctorat

- Sebastian Sowa - *Information-Security-Business-Performance-Measurement und -Management im Kontext von Compliance und Unternehmungszielen*, PhD Thesis, Ruhr-Universität Bochum, Germany, 2009; http://www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/SowaSebastian/diss.pdf
- Demetrius M. Kyriazanou - *Ensuring Privacy in Personal Networks with Situational Awareness*, PhD Thesis, National Technical University, Athens, Greece, 2009; http://artemis.cslab.ntua.gr/Dienst/Repository/2.0/Body/artemis.ntua.ece/PD2009-0056/pdf

Lucrări de Master

- Vilhelm Verendel - *Some Problems In Quantified Security*, Thesis For The Degree Of Licentiate Of Engineering, Chalmers University Of Technology, Göteborg, Sweden 2010; http://www.cse.chalmers.se/~vive/QuantHypothesis/
- Scott E. Schimkowitsch - *Key Components of an Information Security Metrics Program Plan*, Master of Science, University of Oregon, USA, 2009; https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/9479/Schimkowitsch-2009.pdf?sequence=1
- Laerte Peotta de Mello - *Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de TI* - Master Thesis, Universidate de Brasilia, Brasilia, Brazil, 2008; http://repositorio.bce.unb.br/bitstream/10482/1628/1/2008_LaertePeottaDeMelo.pdf
- Pranitha Koya - *A Framework for Security Assurances of Student Applicant Data in Educational Institutions* - Masters of Science In Technology Project Management - Information Systems Security, University of Huston, USA, 2008; http://www.tech.uh.edu/cae-dc/documents/Pranitha_Koyai_2008%20(4).pdf

Articole publicate în jurnale de specialitate sau rapoarte ştiinţifice de referinţă

- T. Sree Ram Kumar, K. Alagarsamy - *A Stake Holder Based Model for Software Security Metrics*, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011, ISSN: 1694-0814; http://www.ijcsi.org/papers/IJCSI-8-2-444-448.pdf
- Clare E. Nelson - *Security Metrics: An Overview*, ISSA Journal, 2010; http://www.issa.org/images/upload/files/Nelson-Security%20Metrics-An%20Overview.pdf
- Catalin Boja, Mihai Doinea - *Security Assessment of Web Based Distributed Applications*, Informatica Economică vol. 14, no. 1/2010; http://revistaie.ase.ro/content/53/16%20Boja,%20Doinea.pdf
- US Department of Defence - Information Assurance Technology Analysis Center (IATAC) - *State-of-the-Art Report Measuring Cyber Security and Information Assurance*, 2009; https://www.mocana.com/pdfs/iatac-measuring_cyber_security_and_information_assurance.pdf
- Vilhelm Verendel - *Quantified security is a weak hypothesis: a critical survey of results and assumptions*, NSPW '09 Proceedings of the 2009 workshop on New security paradigms workshop, ACM New York, NY, USA, 2009 http://dl.acm.org/citation.cfm?id=1719030.1719036&coll=DL&dl=GUIDE&CFID=45924325&CFTOKEN=73201276
- Anoop Singhal, Xinming Ou - *Techniques for enterprise network security metrics*, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies CSIIRW 09, ACM Press, 2009 http://www.mendeley.com/research/ccd-neural-network-processors-for-pattern-recognition/
- Antonietta Stango, Neeli R. Prasad, Dimitris M. Kyriazanos - *A Threat Analysis Methodology for Security Evaluation and Enhancement Planning, Emerging Security Information, Systems and Technologies*, SECURWARE '09, 2009; http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?reload=true&arnumber=5210987
- Meiring De Villiers - *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, Hastings Communications and Entertainment Law Journal, Australia, 2008 http://www.law.unsw.edu.au/staff/devilliersm/docs/Reasonable_Foreseeability_In_Information_Security_Law_A_Forensic_Analysis.pdf
- Gordon Housworth - *Structured IT risk remediation: Integrating security metrics and Design Basis Threat to overcome scenario spinning and fear mongering*, ICG, 2007 http://spaces.icgpartners.com/index2.asp?page=4&category=6E687EFC376F4D04AD504AB7543722E6

Motto*: Totul se transformă, nimic nu se pierde!*
- Ovidius

CAPITOLUL 7

CONCLUZII FINALE ŞI ABORDĂRI VIITOARE

Elaborarea tezei de doctorat a reprezentat rodul unei cercetări desfăşurate pe durata a peste 10 ani în domeniul securității informatice, având ca scop integrarea multiplelor tehnologii din sfera securității, dezvoltarea de procese şi modele de securitate care să permită un răspuns adecvat la schimbările din plan tehnologic şi organizațional, identificarea limitărilor existente în sistemele şi procesele de securitate, şi evaluarea oportunităților oferite de noi cercetări pentru a îmbunătăți tehnologiile şi procesele utilizate în asigurarea securității operaționale a organizațiilor.

Internet-ul reprezintă cel mai amplu proiect creat vreodată de civilizația umană, societatea modernă informațională reprezentând deja o realitate. Început ca un proiect de cercetare în urmă cu patru decenii, Internet-ul devine pe zi ce trece o „oglindă" cât mai fidelă a societății umane, multe din relațiile sociale, economice, politice, culturale transpunându-se pe această infrastructură informațională [PPBC98]. În aceste circumstanțe, *securitatea informațională* a devenit una din componentele majore şi vitale pentru buna operare ale Internet-ului.

Securitatea este un proces dinamic care trebuie să răspundă eficient noilor vulnerabilități, amenințări, precum şi schimbărilor constante care au loc în mediul de operare. O abordare de succes va combina elemente de natură tehnologică, procesuală şi umană, prin utilizarea unui proces structurat ce integrează securitatea informației şi activitatea de management a riscurilor în ciclul de viață al dezvoltării sistemelor.

Progresul realizat în zona securizării tehnologiilor şi infrastructurii Internetului a avut ca rezultat o repoziționare a strategiilor utilizate de elementele spațiului de amenințare. Migrarea a tot mai multor aplicații pe web, inclusiv a celor disponibile pe telefoanele inteligente, precum şi disponibilitatea a tot mai multor informații despre utilizatori pe site-urile de socializare, a creat noi oportunități pentru atacatori, majoritatea vectorilor de atac folosiți în prezent vizând vulnerabilități în aceste zone.

În condițiile actuale, riscurile datorate vulnerabilităților de securitate aparțin în principal utilizatorilor, ele fiind un element auxiliar pentru cei ce le produc (furnizorii de hardware software, sau servicii IT). În mod uzual, odată ce o vulnerabilitate este identificată, producătorul oferă mai repede sau mai târziu un remediu, însă utilizatorul tehnologiei suportă toate costurile urmărilor unui atac. Acest model nu oferă motivație pentru producători în investiția de resurse pentru a securiza tehnologia încă din fazele de

proiectare, strategia producătorilor fiind în principal orientată spre funcționalitatea „vizibilă”, care asigură vânzarea produsului sau soluției. În acest context, este de aşteptat ca prezența unui număr mare, şi în continuă creştere de producători pe piața aplicațiilor, să determine un număr ridicat de vulnerabilități, şi implicit de riscuri pentru utilizatori şi organizații.

Mai mult, schimbările din mediul organizației sau cel social pot genera noi riscuri. Spre exemplu, noua lege în domeniul sănătății din SUA promovează ca modalitate de reducere a costurilor, utilizarea înregistrărilor medicale în format digital, şi efectuarea de tranzacții digitale între furnizorii de servicii medicale (doctori, farmacii, laboratoare, case de asigurări, angajatori, departamentele de sănătate publică ale statului). Această schimbare va constitui o oportunitate pentru atacatori, având în vedere numărul mare de elemente ale acestui ecosistem, precum şi faptul că multe oficii medicale nu au experiență în zona securității, sau utilizării într-un context securizat a tehnologiilor.

O soluție de adresare a acestor riscuri permanente într-o manieră proactivă, şi chiar anticipativă o reprezintă *monitorizarea securității*. Monitorizarea securității reprezintă procesul care permite identificarea schimbărilor din spațiul vulnerabilităților şi amenințărilor, precum şi menținerea unei vizibilități continue asupra eficacității politicii şi controalelor de securitate implementate.

Deşi conceptul de monitorizare a securității a fost lansat de ceva vreme, iar unele companii oferă soluții ce monitorizează unele componente precum intruziuni, vulnerabilități, conformitate cu anumite reglementări, existența unor abordări de monitorizare unitare şi globale a întreg spectrului de informații cu relevanță de securitate este încă în faze incipiente. Lucrarea de față abordează în premieră aspectele complexe din sfera monitorizării securității, oferind o perspectivă unitară şi globală asupra procesului, tehnologiilor, modului de implementare. Aceasta poate fi un ghid util pentru organizații în înțelegerea problematicii complexe de securitate actuală, precum şi în elaborarea unui program de monitorizare şi implementarea acestuia.

Conform simbolisticii taoiste Yin-Yang [Wik11], legate de împletirea inevitabilă a dualității existente în toate lucrurile din natură, este de anticipat că monitorizarea securității nu reprezintă soluția „perfectă” în adresarea problemelor de securitate ale organizației, aducând pe lângă beneficiile discutate şi unele riscuri cum ar fi cel de acces neautorizat, sau de utilizare abuzivă a datelor de monitorizare. Organizația va trebui să adreseze aceste riscuri prin măsuri tehnologice şi procedurale care să asigure: securitatea datelor de monitorizare colectate, controlul şi monitorizarea accesului la aceste date, anonimizarea acestora când sunt utilizate pentru cercetare sau partajate cu alte organizații, verificarea regulată a personalului care are acces la date, disciplină în execuția procesului.

În final, se prezintă în sinteză, problematica abordată în cadrul tezei:

- motivația şi definirea alegerii temei, precum şi a direcțiilor de cercetare ştiințifică;
- studiul vulnerabilităților în spațiul virtual
- definirea unui cadru pentru detecția intruziunilor şi a procesului de monitorizare asociat acestuia.
- studiul atacurilor asupra infrastructurii Internet-ului
- schematizarea atacurilor tipice pe bază de mesaje de poştă
- analiza comparativă a tehnicilor de scanare utilizate în propagarea viermilor

- elaborarea unui cadru pentru definirea de metrici de securitate.
- prezentarea cadrului pentru partajarea informațiilor de intruziune la nivel global.
- definirea unui model de monitorizare completă a securității.
- evaluarea tehnologiilor de culegere a datelor utilizate în procesul de monitorizare a securității.
- studiu comparativ asupra tehnologiilor de detecție a intruziunilor şi a implementărilor de sisteme IDS.
- abordări în monitorizarea spațiului de amenințări pe baza datelor publice oferite de sistemele de monitorizare globală în Internet.
- prezentarea unei arhitecturi generice de monitorizare a securități
- studiu asupra tehnicilor de corelație a datelor în procesul de monitorizare a securității.
- studiu asupra eforturilor de standardizare în vederea asigurării interoperabilității elementelor arhitecturii.
- construirea unui cadru de identificare a imperfecțiunii datelor din sfera monitorizării securității.
- studiul unor noi modele matematice pentru eficientizarea monitorizării securității, şi construirea unui model experimental de evaluare a aplicabilității TDSm în monitorizarea securității
- contribuții personale şi rezultate ştiințifice obținute în cadrul elaborării tezei.

Contribuțiile personale şi rezultatele obținute oferă satisfacția necesară şi creează premisele pentru continuarea şi dezvoltarea activității în această direcție, în special pentru optimizarea tehnologiilor şi proceselor de monitorizare a securității. Astfel, în cadrul unor proiecte de cercetare ştiințifică se află în diferite faze de studiu şi de cercetare următoarele teme:

- evaluarea riscurilor la adresa securității şi libertăților utilizatorilor ca urmare a tendinței de concentrare masivă a datelor personale, sau care permit determinarea de caracteristici personale (căutări pe Internet, activități în rețele sociale, înregistrări ale tranzacțiilor financiare, medicale, etc.)
- studiul caracteristicilor specifice de monitorizare a securității în medii de calcul virtuale (cloud computing)
- evaluarea extinderii procesului de monitorizare pentru a adresa probleme specifice scurgerilor accidentale sau sustragerilor de date
- studiul eficacității utilizării TDSm în combinarea datelor de alertă a intruziunilor provenind din mai multe surse eterogene (HIDS, NIDS)
- construirea de metrici pentru un program de prevenire a pierderilor de date

Rezultatele acestor cercetări vor fi comunicate în jurnale, sau conferințe de specialitate, iar contribuțiile personale şi rezultatele ştiințifice obținute, cât şi cele viitoare, vor face subiectul unei cărți referitoare la monitorizarea securității în Internet.

Teza a tratat problematica monitorizării securității rețelelor şi sistemelor conectate la Internet pe baza studierii unei bibliografii bogate, prin efectuarea de experimente practice, analize de date şi prin obținerea de contribuții personale şi de rezultate ştiințifice în domeniul securității informatice, domeniu de importanță capitală pentru asigurarea bunei funcționări a unei infrastructuri de bază a societății umane - Internetul.

BIBLIOGRAFIE

Publicații Personale

[NPP11] Sebastian Nicolăescu, Victor-Valeriu Patriciu, Iustin Priescu - *Using DSm Theory to Address Conflicts and Uncertainty in Security Monitoring Process*, International Journal of Information Security, ISSN 1615-5270 (trimisă spre publicare) (**Revistă indexată ISI**).

[PNN10] Iustin Priescu, Rodica Neagu, Sebastian Nicolăescu - *Research Results of a Network Security Perimeter for Romanian E-Commerce Companies* - UTM Megabyte Magazine, Vol 6, No. 2, pp. 2010, Bucharest, Romania, ISSN: 1841-7361 (revistă cotată B)

[PNCN09] Iustin Priescu, Magdalena Negruțiu, Marilena Ciobanaşu, Sebastian Nicolăescu - *Perspectives on Financial Data Security in Offshoring Environments, Proceedings of 2009*, International Conference on Economics, Business Management and Marketing, Singapore, pp. 117-122, ISBN 978-9-8108-3816-4. (**Articol indexat ISI, MSES**)

[PPN09] Iustin Priescu, Victor Valeriu Patriciu, Sebastian Nicolăescu - *The Viewpoint Of E-Commerce Security In The Digital Economy*, International Conference on Future Computer and Communication, ICFCC 2009, Kuala Lumpur, Malaysia, IEEE Computer Society, pp. 431-433, ISBN 978-0-7695-3591-3, ISSN 1089-7789. (**Articol indexat ISI, IEEE**)

[PNB09] Iustin Priescu, Sebastian Nicolăescu, Ion Bica - *Design Of Traceback Methods For Tracking DOS Attacks*, International Association of Computer Science and Information Technology - Spring Conference, 2009. IACSITSC '09., Singapore, IEEE Computer Society, pp. 117-121, ISBN 978-0-7695-3653-8, ISSN 1089-7789. (**Articol indexat ISI, IEEE)**

[BPN09] Ion Bica, Iustin Priescu, Sebastian Nicolăescu – *Managing Enterprise Information Security with ISO/IEC 2700x Standards Family*, The Ninth International Conference on Informatics in Economy – Education, Research and Business Technology, Academy of Economic Studies and Romanian Association for Infromatics in Economy Training Promotion (INFOREC), pag. 923-931, ISBN 978-606-505-172-2, Bucharest, 2009

[PPN08] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Security Monitoring of Company Networks*, MTA Review , Vol. XVIII, No. 1, pp. 43-50, ISSN 1843-3391 Cod CNCSIS 842 (Revistă cotată B), 2008

[PN08] Priescu Iustin, Sebastian Nicolăescu - *Managing Security Monitoring in Enterprise Networks*, Buletinul Universitatii Petrol-Gaze din Ploiesti, Seria Matematica-Informatica-Fizica, Vol. LX, No. 2/2008, pag. 53-58, ISSN 1224-4899, Ploiesti, Cod CNCSIS 37 (Revistă cotată B), 2008

[PPIN08-01] Iustin Priescu, Victor-Valeriu Patriciu, Răzvan Ionescu, Sebastian Nicolăescu - *Current Perspectives On Information Security Management Systems*, The 7th International Conference Communications 2008, Edition IEEE Communications International Conference, Organized by The Military Technical Academy, "Politehnica" University of Bucharest, Electronica 2000 Foundation, and The IEEE Romanian Section, Romania, ISBN 973-718-479-3, 2008

[PPIN08-02] Iustin Priescu, Victor-Valeriu Patriciu, Răzvan Ionescu, Sebastian Nicolăescu - *Define Effectiveness Measurement Of Controls In Information Security Management Systems*, The 7th International Conference Communications 2008, Edition IEEE Communications International Conference, Organized by The Military Technical Academy, "Politehnica" University of Bucharest, Electronica 2000 Foundation, and The IEEE Romanian Section, Romania, ISBN 973-718-479-3, 2008

[PPN07-01] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *The Current Perspectives On Security Monitoring In Enterprise Networks*, 8th International Conference on Informatics in Economy (ICIE 2007), May 17-18, 2007, Bucharest

[PN06] Iustin Priescu, Sebastian Nicolăescu - *Tendințe actuale în criminalitatea informatică*, Conferința Națională a Specialiştilor în Domeniul Prevenirii şi Combaterii Criminalității Informatice, Piteşti, 27-29 Noiembrie 2006

[PPN06-01] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *The Outlook Of E-Commerce Security In The Digital Economy*, The 2006 International Conference On Commerce, ASE, March 27-29, 2006, Bucharest

[PPN06-02] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Securitatea Poştei Electronice în Internet*, Editura Academiei Tehnice Militare, Bucuresti, 2006, ISBN 973-640-043-3 (Carte publicată în editutră recunoscută CNCSIS - cod 158)

[PPN06-03] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Operational Security Metrics for Large Networks*, International Journal Of Computers, Communications & Control, vol1, pp 349-354, ISSN 1841-9836, E-ISSN 1841-9844, 2006. Revistă cotată A, Cod CNCSIS 849. **(Articol indexat ISI)**

[PPN06-04] Iustin Priescu, Victor-Valeriu Patriciu, Sebastian Nicolăescu - *Data Correlation Techniques in Network Security Monitoring*, 5th RoEduNet International Conference, June 1-3, 2006, Sibiu, Romania, ISBN 978-973-739-277-0

[PPN06-05] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Security Metrics for Enterprise Information Systems*, JAQM (Journal of Applied Quantitative Methods), Issue 2, 2006, pp. 151-159, ISSN 1842-4562, Cod CNCSIS 700 (Revistă cotată B+)

[PPN05-01] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Internet Worms - Propagation Modeling and Analysis*, The 4th ROEDUNET International Conference: "Education/Training and Information/Communication Technologies - ROEDUNET '05, Târgu-Mureş, Romania, pp. 218-224, ISBN 973-7794-26-5 **(Articol indexat ISI)**

[PPN05-02] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Trace Back Flows Methods for Tracking DoS Attacks* - The 15th International Conference on Control Systems and Computer Science, May 25-27, 2005, Bucharest Romania.

[PPN05-03] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Internet Worms - Spreading of Active Worms using Random Scanning* – Conferința de Matematici Aplicate şi Industriale – CAIM 2005, Societatea Română de Matematică Aplicată şi Industrială - ROMAI, ROMAI Journal, Vol. 1, Nr. 1, pag. 141-150, ISSN 1841-5512, E-ISSN 2065-7714, (Revistă cotată B), 2005

[PPN04] Victor-Valeriu Patriciu, Iustin Priescu, Sebastian Nicolăescu - *Security Considerations about E-Mail Encryption Protocols*, International Conference on Computers and Communications (ICCC), May 27-29 2004, Oradea, Romania, pp. 315-319

Bibliografie generală

[Aco09] Byron Acohido - *The evolution of an extraordinary globe-spanning worm* - http://lastwatchdog.com/evolution-conficker-globe-spanning-worm/

[Afi--] Afick (Another File Integrity Checker) - http://afick.sourceforge.net/

[Alk08] Ghazi I. Alkhatib, David C. Rine - *IGI Global*, 2008

[Ame10] Suhair Hafez Amer, John A. Hamilton - *Intrusion Detection Systems (IDS) Taxonomy - A Short Review*, Jurnal of Software Technology, Vol 13, No 2, 2010. http://journal.thedacs.com/issue/54/163

[And80] James P. Anderson Co - Computer Security Threat Monitoring and Surveillance, Technical Report. 1980

[And95] D Anderson, T Frivold, A Valdes - *Next-generation intrusion-detection expert system (NIDES)*. Technical Report. Computer Science Laboratory, SRI, USA, May 1995

[Arb11-02] ATLAS – *Summary Report Global Attacks* - http://atlas.arbor.net/summary/attacks

[Arg--] Argus Project - An Architecture for Cooperating Intrusion Detection and Mitigation Applications, http://www.htc.honeywell.com/projects/argus/

[Bab06] Jacob Babbin et al - Security Log Management: Identifying Patterns in the Chaos, Syngress Publishing, 2006

[Bai09] Michael Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu, Manish Karir - *A Survey of Botnet Technology and Defenses*, Proceeding CATCH '09 Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security

[Bas01] Basel Committee on Banking Supervision, *Working Paper on the Regulatory Treatment of Operational Risk Bank for International Settlements*, Basel Committee, 2001 (http://www.bis.org/publ/bcbs_wp8.pdf)

[Bej04] R. Bejtlich - The Tao Of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley, 2004, ISBN 0321246772

[Ber05] S. Berinato, G. Campbell, D. Lefler, Security Metrics - *Influencing Senior Management*, CSO Executive Council 2005

[Bot11] *Bothunter Implementation* - http://www.bothunter.net/

[Bou01] Darren Bounds - *Packit - Network Injection and Capture* http://packit.sourceforge.net/

[Bro99] B. P. Brown - *Offshore Financial Services Handbook*, Second Edition, Gresman Books, 1999

[BS02] http://en.wikipedia.org/wiki/BS_7799

[Bue05] Axel Buecker, Hendrik H. Fulda, Dieter Riexinger, *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, IBM Redbooks, 2005

[Bug--] Bugtraq – SecurityFocus, www.securityfocus.com/

[But04] James Butler - *VICE - Catch the hookers!,* Black Hat, Las Vegas, July 2004. www.blackhat.com/presentations/bh-usa-04/bh-us-04-butler/bh-us-04-butler.pdf

[But05] Jamie Butler, Greg Hoglund - *Rootkits - Subverting the Windows Kernel*, Addison Wesley Professional, 2005. ISBN 0321294319

[Cai08] Conficker/Conflicker/Downadup as seen from the UCSD Network Telescope - http://www.caida.org/research/security/ms08-067/conficker.xml

[CBU--] US Homeland Security Department - CERT Cyber Security Bulletins - http://www.us-cert.gov/cas/bulletins/

[CCIMB-99-031] Common Criteria: *Part 1 - Introduction and general model*, Version 2.1 1999, http://www.radium.ncsc.mil/tpep/library/ccitse/ccitse.html

[CER--] CERT Advisories- http://www.cert.org

[Cert11] CERT, *CERT/CC Statistics 1988-2011*, CERT, 2011 (http://www.cert.org/stats/)

[Che03] Z. Chen, L. Gao, K. Kwiat -*Modeling the spread of active worms*, IEEE INFOCOM. 2003

[Chk--] *Chkrootkit* - http://www.chkrootkit.org/

[CIDF98-2] R. Feiertag, C. Kahn, P. Porras, D. Schnackenberg, S. Staniford-Chen, B. Tung - *A Common Intrusion Specification Language (CISL)* – 16/10/98 http://www.isi.edu/gost/cidf/drafts/language.txt

[CIDF98-3] C. Kahn, D. Bolinger, D. Schnackenberg - Communication in the Common Intrusion Detection Framework, v0.7, 8/98 http://www.isi.edu/gost/cidf/drafts/communication.txt

[CIDF98-4] B. Tung - CIDF APIs: Their Care and Feeding http://www.isi.edu/gost/cidf/drafts/api.txt

[CIDF98-5] C. Kahn, D. Bolinger, D. Schnackenberg - The Common Intrusion Detection Framework Architecture http://www.isi.edu/gost/cidf/drafts/architecture.txt

[Cis11] Cisco - *Cisco Security Information Event Management Deployment Guide* http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/sbaSIEM_deployG.pdf

[Cla09] Rodney Claude - *Investigative Tree Models*, SANS White paper, http://www.sans.org/reading_room/whitepapers/incident/investigative-tree-models_33183

[Cog06] Bryce Cogswell, Mark Russinovich – *RootkitRevealer*, http://technet.microsoft.com/en-us/sysinternals/bb897445

[Coh05] Fred Cohen - *The Use of Deception Techniques: Honeypots and Decoys*, Handbook of Information Security, Vol 3, 2005

[Con09] *Converged Network Digest* - http://www.convergedigest.com/packetsystems/packetsysarticle.asp?ID=26912

[Cou02] Counterpane - *Counterpane and Network Security Monitoring*, http://bt.counterpane.com/presentation2.pdf

[Cou05] Counterpane - *Managed Security Monitoring*, http://www.counterpane.com/msm.pdf

[Cup02] Frédéric Cuppens, Alexandre Miége - *Alert correlation in a cooperative intrusion detection framework*, Proceedings of the IEEE Symposium of Security and Privacy, 2002

[CVE--] MITRE Corporation, “Common Vulnerabilities and Exposures”, http://cve.mitre.org/

[Dan--] *MONITOR LOGS WITH LOGSURFER+* - http://www.dankalia.com/tutor/01005/0100501074.htm

[Deb92] H. Debar, M. Becker, D. Siboni - *A neural network component for an intrusion detection system*. Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy

[Den87] D. Denning - *An Intrusion-Detection Model* - IEEE Transactions on Software Engineering. 1987

[Dic08] John B. Dickson - *Black Box versus White Box:Different App Testing Strategies*, Denim Group White Paper, http://www.denimgroup.com/media/pdfs/BBvsWB_Minneapolis.pdf

[Dji10] Pascal Djiknavorian, P. Valin, D. Grenier - Approximation in DSm theory for fusing ESM reports, Information Fusion (FUSION), 13th Conference, 2010

[DoD09] DoD Information Assurance Technology Analysis Center (IATAC) – *Measuring Cyber*

Security and Information Assurance, State-of-the-Art Report (SOAR), May 8, 2009 https://www.mocana.com/pdfs/iatac-measuring_cyber_security_and_information_assurance.pdf

[DOE--] US Department of Energy CIRC - Cyber Incident Response - http://www.doecirc.energy.gov/

[Dou93] C. Dousson, P. Gaborit, M. Ghallab - *Situation recognition: Representation and Algorithms*. Proceedings of the 13th IJCAI, pp 166-172, August 1993

[Dow90] C. Dowel, Paul Ramstedt - *The computer watch data reduction tool.* Proceedings of the 13th National Computer Security Conference, 1990

[Du03] X. Du, M. Shayman, R.A. Skoog - Using Neural networks in distributed Management to identify Control and Management to identify Control and management plane poison messages. University of Maryland, US. Research supported by DARPA, 2003

[Dub86] D. Dubois, H. Prade - *On the unicity of Dempster rule of combination*, International Journal of Intelligent Systems, Vol 1, pp 133-142, 1986

[Duf00] N. Duffield, M. Grossglauser - *Trajectory Sampling for Direct Traffic Observation*. Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (ACM SIGCOMM'00). Stockholm, Sweden, pp 271–282. 2000 (http://portal.acm.org/citation.cfm?id=347555)

[Eey--] *Retina CS Management Products* - http://www.eeye.com/products/retina/retina-insight

[Els08] Constantine Elster, Danny Raz - Covering All Bases with a Short Blanket: A Dynamic Monitoring Resource Allocation Scheme, INFOCOM Workshops 2008, IEEE

[Fan93] J. Fan, K. Su - An Efficient Algorithm for Matching Multiple Patterns. ACM Magazine, 1993

[FCCC+96] S.Chen, S.Cheung, R.Crawford - *GrIDS: A graph based intrusion detection system for large networks*. Proceedings of the 19th National Information Systems Security Conference, 1996

[FIPS*] Lista publicatii FIPS - http://csrc.nist.gov/publications/PubsFIPS.html

[FSA11] *** - *Fingerprint Sharing Alliance*, http://www.arbornetworks.com/fingerprint-sharing-alliance.html

[Fse04-1] F-Secure - *Net-Worm:W32/Santy.A*, http://www.f-secure.com/v-descs/santy_a.shtml

[Fse04-2] F-Secure - *Net-Worm:W32/Sasser*, http://www.f-secure.com/v-descs/sasser.shtml

[Gan08] Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou, Francois Spies - *A global security architecture for intrusion detection on computer networks* – Computers & Security 27 (2008) pp 30–47

[Gar--] Gartner Security Study Reports - http://www.gartner.com

[Goo91] R.M. Goodman, H. Latin - *Automated knowledge acquisition from network management databases,* IFIP International Symposium on Integrated Network Management (ISINM'91), pp 541-549, 1991

[Gre11] Tim Greene - *The RSA Hack FAQ*, Network World, http://www.networkworld.com/news/2011/031811-rsa-hack-faq.html

[Gre99] John Green, David Marchette, Stephen Northcutt, Bill Ralph - *Analysis Techniques for Detecting Coordinated Attacks and Probes,* Proceedings of the Workshop on Intrusion Detection and Network Monitoring Santa Clara, California, USA, 1999

[Gu07] Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong, Wenke Lee - *BotHunter: Detecting Malware Infection Through IDS-Driven Dialog*, USENIX Security'07, 2007

[Han05] Hansman, S., Hunt R., *A taxonomy of network and computer attacks*, Computer and Security (2005)

[Har09] Mike Harwood - *CompTIA® Network+ Exam Cram, Third Edition*, Pearson

Certification, 2009

[Hät04] Antti Hätälä, Camillo Särs, Ronja Addams-Moring, Teemupekka Virtanen - *Event Data Exchange and Intrusion Alert Correlation in Heterogeneous Networks*, Proceedings of the 8th Colloquium for Information Systems Security Education West Point, NY, June 2004, pp 84-92

[HEB90] T. Heberlein, G. Dias, K. Levitt - *A network security monitor*. Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy

[Hin06] G. Hinson - *7 Myths About Security Metrics*, ISSA Journal, 2006

[HOC93] J. Hochberg, K. Jackson, C.Stallings - NADIR: An automated system for detecting network intrusion and misuse. Computers & Security, 12(3), 1993

[Hpi--] Hping2 Tool - http://www.hping.org/download.php

[IDWG02-02] B. Feinstein, G. Matthews, J. White - The Intrusion Detection Exchange Protocol (IDXP). 2002

[IDWG03] The TUNNEL Profile for Blocks Extensible Exchange Protocol (BEEP)

[IDWG05] H. Debar, D. Curry, B. Feinstein - Intrusion Detection Message Exchange Format

[Ilg95] K. Ilgun, R. Kemmerer, P. Porras - *State transition analysis: A rule-based intrusion detection approach.* IEEE Transactions on Software Engineering, March 1995

[Ina91] T. Inagaki - Interdependence between safety-control policy and multiple-sensor schemes via Dempster-Shafer theory, IEEE Trans. on reliability, Vol 40, no 2, pp 182-188, 1991

[Inn09] InnerWorkings - Offshoring Risks - How Will You Stay in Control? www.cio.com , 2009

[Ioa02] J. Ioannidis, S. Bellovin - *Implementing Pushback: Router Defence Against DDoS Attacks*. Proceedings of Network and Distributed System Security Symposium, San Diego 2002. http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/ioanni.pdf

[ISC--] Internet Strom Center – http://isc.sans.org

[ISO--] http://www.17799central.com/

[ISO05] ISO/IEC. Information Technology – Security Techniques, Code of Practice for Information Security Management (final draft), ISO, 2005

[Jac91] K. Jackson, D. DuBois, C. Stallings - *An expert system application for network intrusion detection*. Proceedings of the 14th National Computer Security Conference, 1991

[Jaq06] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty and Doubt, Addison Wesley, 2006

[Jon10] Robert Johnson; Mark Merkow - Security Policies and Implementation Issues, Jones & Bartlett Learning, 2010

[Jou97] Y. Frank Jou, F. Gong, C. Sargor - Architecture design of a scalable intrusion detection system for the emerging network infrastructure. 1997

[Kab98] Mitch Kabay - The Risks Digest, volume 19, issue 91 (http://catless.ncl.ac.uk/Risks/19.91.html)

[Kil03] Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek - *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*, Handbook - December 2003

[Kim94] Gene H. Kim, Eugene H. Spafford - *The design and implementation of tripwire: a file system integrity checker*, CCS '94 Proceedings of the 2nd ACM Conference on Computer and Communications Security ACM New York, NY, USA, 1994

[Kja05] M.Kjaerland - A taxonomy and comparison of compute securityincidents from the

commercial and government sectors. Computers and Security, 25:522–538, October 2005

[Ko96] Calvin Ko - Execution Monitoring of Security-critical Programs in a Distributed System: A Speciffication-based Approach. PhD thesis, Department of Computer Science, University of California at Davis, USA, 1996

[Kov05] Gerald L. Kovacich, Edward Halibozek, Security Metrics Management: How to Measure the Costs and Benefits of Security, Butterworth-Heinemann, 2005

[Krü01] C. Krügel, T. Toth, C. Kerer - *Decentralized Event Correlation for Intrusion Detection*, Proceedings of the 4th International Conference on Information Security and Cryptology, 2001

[Kum95] Sandeep Kumar - *Classification and Detection of Computer Intrusions*, PhD thesis, Purdue University, West Lafayette, Indiana, August 1995

[Lar06] Ulf Larson - *Aspects of Adapting Data Collection to Intrusion Detection*, Thesis For The Degree Of Licentiate Of Engineering, Chalmers University Of Technology, Sweden, 2006

[Lee99] Wenke Lee - A Data Mining Framework For Building Intrusion Detection Models. IEEE Symposium on Security and Privacy, May 1999

[Lef02] E. Lefevre, O. Colot, P. Vannoorenberghe - *Belief functions combination and conflict management*, Information Fusion Journal, Elsevier Publisher, Vol 3, No 2, pp 149-162, 2002

[Lig06] Jarred Adam Ligatti - *Policy Enforcement via Program Monitoring*, PhD Thesis, Princeton University, 2006

[Log--] *Logwatch* - http://sourceforge.net/projects/logwatch/

[Lou01] Daniel Lough - *A Taxonomy of Computer Attacks with Applications to Wireless Networks*, PhD thesis, Virginia Polytechnic Institute and State University, 2001

[Lun88] T. Lunt, R. Jagannathan, R. Lee - *IDES: The enhanced prototype, A real-time intrusion detection system.* Technical Report, SRI Project 4185-010, 1988

[Lun92] T. Lunt, A. Tamaru, F. Gilham - *A real-time intrusion-detection expert system (IDES).* Technical Report Project 6784 - SRI International, 1992

[Mah02] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, S. Shenker - *Controlling High Bandwidth Aggregates in the Network*. ACM SIGCOMM Computer Communication Review, Vol 32, Issue 3, July 2002. ACM Press, New York

[Man03] Kevin Mandia, Chris Prosise - *Incident Response and Computer Forensics*, 2nd ed. McGrawHill, 2003

[Mar11] Data Fusion Toolbox - http://bfas.iutlan.univ-rennes1.fr/wiki/index.php/Toolboxs

[Mat--] Mathworks: Matlab. http://www.mathworks.com/products/matlab/

[Mat11] A. Matrosov, et al - *Stuxnet Under the Microscope* http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

[Mau05] Sjouke Mauw, Martijn Oostdijk - *Foundations of Attack Trees*, in Proc. ICISC, 2005, pp.186-198. ACM

[Mcc01] Nils McCarthy - *Network Path Enumeration*. http://www.mainnerve.com/lft/

[McN07] Chris McNab - *Network Security Assessment*, Second Edition, O'Reilly Media, 2007

[Met--] *Metasploit Framework Penetration Testing Software* - http://metasploit.com/

[Mic09] Microsoft Patterns & Practices Team - *Microsoft Application Architecture Guide*, Microsoft Press, 2009

[Mir02] *Attacking DDoS at the Source* – Jelena Mirkovic, Gregory Prier, Peter Reiher – Technical Report, UCLA, 2002

[Mir04] Jelena Mirkovic; Sven Dietrich; David Dittrich; Peter Reiher - Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall, 2004

[Moo02-1] D. Moore, C. Shannon, J. Brown - *Code-Red: a case study on the spread and victims of an Internet Worm In Proc*. ACM/USENIX Internet Measurement Workshop, France, November, 2002

[Moo02-2] D. Moore - Network Telescopes: Observing Small or Distant Security Events. In 11th USENIX Security Symposium, 2002

[Moo03] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver - *Inside the Slammer Worm*. IEEE Magazine on Security and Privacy, 1(4):33-39, July 2003

[Moo04] D. Moore, C. Shannon, G. Voelker, S. Savage - *Network Telescopes: Technical Report*. Cooperative Association for Internet Data Analysis – CAIDA Technical Reports, 2004. (http://www.caida.org/outreach/papers/2004/tr-2004-04/tr-2004-04.pdf)

[Mor02] B. Morin, H. Debar, L. Me, M. Ducasse - *A Formal Data Model for IDS Alert Correlation*. Proceedings of the 5th Int'l Symposium on Recent Advances in Intrusion Detection (RAID'02), October 2002

[Mor02-1] C. Morrow - *Blackhole Routing with ICMP Backscatter*. In UUNet Technical Whitepaper, 2002

[Mor02-2] Y. Moreno, R. Pastor-Satorras, A. Vespignani - *Epidemic outbreaks in complex heterogeneous networks*, The European Physical Journal B, 26/2002, pp 521-529

[MS11-1] Microsoft - http://technet.microsoft.com/en-us/security/bulletin/ms11-057

[Mul09] Andreas Muller - *Event Correlation Engine*, Master Thesis, Switzerland, 2009

[Nass08] Nasscom BPO Newsline - The Indian BPO Sector Dealing with the Challenges, January 2008

[Nav02] Gonzalo Navarro, Mathieu Raffinot - *Practical on-line search algorithms for texts and biological sequences*. Cambridge University Press, 2002

[Naz03] J. Nazario - Defense and Detection Strategies against Internet Worms, Artech House, 2003

[Naz07-2] Jose Nazario - *Estonian DDoS Attacks – A summary to date* http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

[Naz07] J Nazario, et al. - *Future of Internet Worms* - http://www.crimelabs.net/docs/worms/worm.pdf

[Nes--] *Nessus Scanner Documentation* - http://www.tenable.com/products/nessus/documentation

[Ngu02] John V. Nguyen - *Designing ISP Architectures*, Prentice Hall, 2002 Agent Technologies and Web Engineering: Applications and Systems

[Nin02-01] Peng Ning, Yun Cui, Douglas S. Reeves - *Analysing Intensive Intrusion Alerts via Correlation*. Proceedings of Recent Advances in Intrusion Detection, 2002

[Nin02-02] Peng Ning, Yun Cui, D. Reeves - *Constructing attack scenarios through correlation of intrusion alerts*. Proceedings of the 9th ACM conference on Computer and Communications security, 2002

[Nin04] P. Ning, D. Xu, C. G. Healey, R. St. Amant - *Building Attack Scenarios through Integration of Complementary Alert Correlation Methods*. Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSSS'04). February 2004

[NIST*] *Lista publicatii NIST SP* - http://csrc.nist.gov/publications/PubsSPs.html

[Nma--] Nmap Network Scanning - http://nmap.org/book/toc.html

[Nor02] Stephen Northcutt, Judy Novak - *Network Intrusion Detection*, Third Edition, Sams, 2002

[Oik06] George Oikonomou, Peter Reiher, Max Robinson, Jelena Mirkovic: *A Framework for Collaborative DDoS Defense*, Proceedings of the Annual Computer Security Applications Conference (2006)

[Ore08] Angela Orebaugh, Becky Pinkard - Nmap in the Enterprise Your Guide to Network Scanning, Syngress, 2008

[Ort98] Rodolphe Ortalo - *A Flexible Method for Information System Security Policy Specification* - Proceedings of the 5th European Symposium on Research in Computer Security Springer-Verlag London, UK 1998, ISBN:3-540-65004-0

[Oss--] *OSSEC* - http://www.ossec.net/

[OSS05] OSSIM – *The Open Source SIEM*, http://alienvault.com/community/technical-documentation

[Osst--] OSSTMM - Open Source Security Testing Methodology Manual http://www.isecom.org/osstmm/

[Ou04] Xinming Ou, Sudhakar Govindavajhala, Andrew Appel - *Network Security Management with High-level Security Policies*, Technical Report, Princeton University, 2004

[OWA11] Open Web Application Security Project https://www.owasp.org/index.php/Top_10_2010-Main

[Par10] Ben Parr - *WikiLeaks Targeted in DDoS Attack as Latest Leak Hits the Web*, http://mashable.com/2010/11/28/wikileaks-ddos-attack/

[Pax99] V. Paxson - Bro: a system for detecting network intruders in real-time. Computer Networks No 31, 1999

[Pei04] Cyrus Peikari; Anton Chuvakin - *Security Warrior*, O'Reilly Media, 2004

[Per07] S. Persson - Managing Information Security with ISO/IEC 27001, 2005, atsec, www.atsec.com, 2007

[Pfl11] Charles P. Pfleeger, Shari Lawrence Pfleeger - Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach Prentice Hall, 2011

[Pie08] Roberto Pietro, Luigi V Mancini - Intrusion Detection Systems, Series: Advances in Information Security, Vol 38, 2008

[Por02] P.A. Porras, M.W. Fong, A. Valdes - *A Mission-Impact-based Approach to INFOSEC Alarm Correlation*. Supported by DARPA, SRI International Paper, 2002

[Por09] Phillip Porras, Hassen Saidi, Vinod Yegneswaran - *An Analysis of Conficker's Logic and Rendezvous Points*, http://mtc.sri.com/Conficker/

[Por98] P. Porras, A. Valdes - *Live traffic analysis of TCP/IP gateways*. Proceedings of the 1998 ISOC Symposium on Network and Distributed Systems Security

[Pri08] I. Priescu - *Electronic Commerce: From Paradigme to Implementation*", Editura UTM, Bucharest, 2008. ISBN 978-606-8002-20-7

[Pwc09] PwC - Financial services falling behind on data security, www.finextra.com, 2009

[Qin03] Xinzhou Qin, Wenke Leem - *Statistical Causality of INFOSEC Alert Data*. Proceedings of Recent Advances in Intrusion Detection, 2003

[RFC*] *Suita documente RFC* - http://tools.ietf.org/html/

[Ris05] Risto Vaarandi -*Tools and Techniques for Event Log Analysis*. PhD Thesis, Tallinn University of Technology, 2005

[Roe99] M. Roesch - *Snort - lightweight intrusion detection for networks*, 1999. Proceedings of LISA '99. 7-12 November 1999. USENIX http://portal.acm.org/citation.cfm?id=1039864

[Rut04] Joanna Rutkowska - Detecting Windows Server Compromises with Patchfinder 2

2004

[Rut05-1] Joanna Rutkowska - *Thoughts about Cross-View based Rootkit Detection*, June 2005. http://www.invisiblethings.org/papers/crossview_detection_thoughts.pdf

[Rut05-2] Joanna Rutkowska - *System Virginity Verifier: Defining the Roadmap for Malware Detection on Windows Systems*, 2005. http://www.invisiblethings.org/papers/hitb05_virginity_verifier.ppt

[San01] Daiji Sanai - Detection of Promiscuous Nodes Using ARP Packets. http://www.securityfriday.com/promiscuous_detection_01.pdf

[Sch07] H. Schauer, A. Fernandez-Toro - *ISO 27001:Interet de la mise en oeuvre d'un SMSI*, in Jurnees RSSI, Paris 2007

[Sch09] Mike Schiffman, Cisco CIAG, *A Complete Guide to the Common Vulnerability Scoring System (CVSS)*, Forum Incident Response and Security Teams (http://www.first.org/)

[Sec07] *SEC (simple event correlator)* - http://simple-evcorr.sourceforge.net/

[SEC--] SecuriTeam.com – Exploits Details

[Sec04] *** - *Patchfinder 2 - Windows Server Compromises Detector*, http://www.securiteam.com/tools/5FP0L00BPS.html

[Sec05] *** - *Klister - Windows Kernel Level Rootkit Detector*, http://www.securiteam.com/tools/5GP0315FFW.html

[Sec11] www.secnap.com/support/whitepapers/cyber-report-2010.html

[Sha76] G. Shafer - *A Mathematical Theory of Evidence*, Princeton Univ. Press, Princeton, NJ, 1976

[Sim10] Chris Simmons, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu - *AVOIDIT: A Cyber Attack Taxonomy*, IEEE Security and Privacy Magazine, 2010

[Sin10] Abhishek Singh - *Demystifying Denial-Of-Service Attacks, Part One.* http://www.symantec.com/connect/articles/demystifying-denial-service-attacks-part-one

[Sla--] *System Log Analysis and Profiling System 2* - http://www.openchannelsoftware.com/projects/SLAPS-2/

[Sma04] F. Smarandache, J. Dezert (Editors) - *Applications and Advances of DSmT for Information Fusion*, Am. Res. Press, Rehoboth, 2004 http://www.gallup.unm.edu/ smarandache/DSmT-book1.pdf

[Sma06] F. Smarandache, J. Dezert (Editors) - *Applications and Advances of DSmT for Information Fusion Vol 2*, American Research Press, Rehoboth, August 2006. http://www.gallup.unm.edu/ smarandache/DSmT-book2.pdf

[Sma09] F. Smarandache, J. Dezert (Editors) - *Applications and Advances of DSmT for Information Fusion Vol. 3*, American Research Press, Rehoboth, 2009. http://www.gallup.unm.edu/ smarandache/DSmT-book3.pdf

[Sma88] S. E. Smaha - *Haystack: An intrusion detection system*. Proceedings of the IEEE Fourth Aerospace Computer Security Applications Conference, 1988

[Sme88] Ph. Smets, E.H. Mamdani, D. Dubois, H. Prade (Editors) - *Non-Standard Logics for Automated Reasoning*, Academic Press, 1988

[Sme96] Philippe Smets - *Imperfect Information: Imprecision and Uncertainty*, In Uncertainty Management in Information Systems, pp 225-254, 1996

[Smi09] Craig Smith, Ashraf Matrawy, Stanley Chow, Bassem Abdelaziz - *Computer Worms: Architectures, Evasion Strategies, and Detection Mechanisms*, Journal of Information Assurance and Security 4 (2009), pp 69-83

[Sna92] S. Snapp, S. Smaha, D. Teal, T. Grance - *The DIDS (Distributed Intrusion Detection System) Prototype*, Proceedings of the Summer USENIX Conference, June 1992

USENIX Association

[Sno--] Snort – http://www.snort.org

[Sno01] A. Snoeren, Craig C. Partridge, L. Sanchez et al - *Hash Based IP Traceback*. Proceedings of ACM SIGCOMM'01, 2001. http://www.acm.org/sigs/sigcomm/sigcomm2001/p1-snoeren.pdf

[SOC09] www.facebook.com, www.twitter.com

[Sol05] Michael G. Solomon, Mike Chapple, *Information Security Illuminated*, Jones and Bartlett Publishers, 2005

[Son00] Dug Song - *Packet Fragmentation*. http://www.monkey.org/~dugsong/fragroute/

[SOX06] A Guide To The Sarbanes-Oxley Act - http://www.soxlaw.com/

[Spa00] Eugene H. Spafford, Diego Zamboni - *Intrusion detection using autonomous agents*, Computer Networks No 34, 2000

[SSE03] Systems Security Engineering-Capability Maturity Model Group, SSE-CMM – Model Description Document version 3.0, International Systems Security Engineering Association, 2003 (http://www.sse-cmm.org/docs/ssecmmv3final.pdf)

[Sta02] S. Staniford, V. Paxson, N. Weaver - *How to Own the Internet in your spare time*. 11th Usenix Security Symposium, San Francisco, August, 2002

[Ste00] R. Sterritt, A. H. Marshall, C. M. Shapcott, S. I. McClean - *Exploring dynamic Bayesian belief networks for intelligent fault management systems*. Proceedings of the IEEE International Conference Systems on Cybernetics, pp 3646-3652. Sept 2000

[Stj10] *Saint Jude IDS* - http://www.filetransit.com/view.php?id=97050

[Sto00] R. Stone - *CenterTrack, an IP Overlay Network for Tracking DoS Floods*. In USENIX Security Symposium, 2000 (http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/stone/stone.pdf)

[Sun08] Haibin Sun, John C. S. Lui, David K. Y. Yau - *Defending Against Low-Rate TCP Attacks: Dynamic Detection and Protection*, 12th IEEE International Conference on Network Protocols (ICNP'04), Berlin, Germany, 2008

[Swa--] *Simple Log Watcher* - http://sourceforge.net/projects/swatch/

[Sym--] Security Bulletins and Reports - http://www.symantec.com

[Sym03] Symantec – *W32.Blaster.Worm*, http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99

[Tem00] Steven J. Templeton, Karl Levitt - *A requires/provides model for computer attacks*. Proceedings of New Security Paradigms Workshop, pp 31-38. 2000

[Tho05] Herbert Thompson, Scott Chase - *The Software Vulnerability Guide*, Course Technology PTR, 2005

[Tjh11] Gina C. Tjhai - *Anomaly-Based Correlation Of Ids Alarms*, PhD Thesis, School of Computing and Mathematics Faculty of Science and Technology, University of Plymouth, UK

[Tri--] Open Source Tripwire – http://sourceforge.net/projects/tripwire/

[Tri10] *** - *Enforcing IT Change Management Policy*, Tripwire White Paper - http://www.tripwire.com/register/enforcing-it-change-management-policy

[USA95] U.S. Army Intelligence Center & FH - *Indicators In OOTW* http://www.fas.org/irp/doddir/army/miobc/shts4lbi.htm

[USAF96] US Air Force Computer Emergency Response Team - *Incident Categories*. 1996

[Val01] Alfonso Valdes, Keith Skinner - *Probabilistic alert correlation*. Proceedings of Recent Advances in Intrusion Detection, 2001

[Ver10] Verizon – VerIS – Verizon Enterprise Risk and Incident Sharing Metrics Framework, https://verisframework.wiki.zoho.com/

[Ver11] Verizon Business - *Data Breach Reports for 2008-2011*, www.verizonbusiness.com, 2011 http://www.verizonbusiness.com/Products/security/dbir/

[Voo07] James Voorhees - Distilling Data in a SIM: A Strategy for the Analysis of Events in the ArcSight ESM, SANS White Paper

[Wan05] Y. Wang, D. Beck, R. Roussev, C. Verbowski - *Detecting Stealth Software with Strider GhostBuster*. Microsoft Technical Report, Feb 2005

[Wea03] N. Weaver, V. Paxson, S. Staniford, R. Cunningham - *A Taxonomy of Computer Worms*, ACM Workshop on Rapid Malcode, Washington, DC, Oct 27, 2003

[Wik11] http://en.wikipedia.org/wiki/File:Yin_yang.svg

[Wir--] Wireshark Packet Analyzer (v.1.6.2) - http://www.wireshark.org/

[Wol05] Gullik Wold - Title of paper: Key factors in making Information Security Policies Effective, Master Thesis 2005

[Wot05] Brian Wotring, Host Integrity Monitoring Using Osiris and Samhain, Syngress Publishing, 2005

[Wri06] S. Wright - Measuring the Effectiveness of Security using ISO 27001, White Paper, 2006

[Xyp04] XYPRO Technology Corporation, *HP NonStop Server Security*, Digital Press, 2004

[Yag87] R. R. Yager - *On the Dempster-Shafer framework and new combination rules*, Information Sciences, Vol 41, pp 93-138, 1987

[Zad86] L. Zadeh - A Simple View of The Dempster-Shafer Theory of Evidence and Its Implication For The Rule Of Combination, AI Magazine 7, No2, pp 85-90, 1986

[Zou03] C.C. Zou, L. Gao, W. Gong, D. Towsley - *Monitoring and Early Warning for Internet Worms*. 10th ACM Symposium on Computer and Communication Security, Washington DC, 2003