Sisteme de detecție a intruziunilor

Drd. ing. Sorin SOVIANY[1], Dr. ing. Sorin PUŞCOCI[1],
Drd. ing. Gheorghiță PESCARU[1], Drd. ing. Radu DRAGOMIR[1]

Cuvinte cheie: *detecția intruziunilor,notificare, politică de detecție.*

Rezumat: *Sistemele de detecție a intruziunilor sunt soluții de securitate care constau în componente hardware şi software destinate asigurării protecției unor sisteme informatice şi rețele vulnerabile. În foarte multe cazuri, capabilitățile de detecție a intruziunilor sunt asociate şi cu elemente care asigură prevenirea evenimentelor cu caracter intruziv. Astfel de sisteme prezintă avantaje şi dezavantaje, de aceea soluțiile practice de implementare trebuie să țină cont de cerințele aplicațiilor şi sistemelor care ar trebui protejate.*

Keywords: *intrusion detection, notification, detection policy*

Abstract: *The Intrusion Detection Systems are security solutions consisting in hardware and software components that are designed to supprt the protection for vulnerable information systems and networks. The intrusions detection capabilities are very often associated with elements enablinf the intrusive events prevention. These systems have a lot of advantages and drawbacks, and therefore the practical implementation solutions should consider the requirements of the applications and systems that should be protected.*

1. Introducere

Securitatea sistemelor informatice şi de comunicații a devenit, în prezent, o problemă extrem de importantă, de care trebuie să țină cont atât producătorii de echipamente, cât şi dezvoltatorii de aplicații şi integratorii de sistem, precum şi administratorii de rețea. Desigur, integritatea sistemelor informatice şi de comunicații, precum şi cerințele de protejare a confidențialității datelor, pot fi abordate printr-o multitudine de tehnici şi metode. În prezent, metodele de autentificare bazate de tehnologii biometrice devin din ce în ce mai folosite.

Pe de altă parte, soluțiile actuale de securitate se bazează pe utilizarea de componente hardware şi pe dezvoltarea de soluții software capabile să detecteze elemente suspecte de a fi considerate intriziuni, acțiuni nepermise şi consecințe ale acestora. Foarte des, însă, detecția evenimentelor cu caracter intruziv în cadrul unui sistem informatic conectat în rețea nu este suficientă. În principiu, după cum se va arăta în continuare, detecția intruziunilor se bazează pe tipuri de comportament sau pe pattern-uri („semnături" ale enitităților malițioase) care s-au manifestat după ce hackerii au început deja să interacționeze cu sistemele atacate. Foarte importantă s-ar dovedi şi capabilitatea de prevenire a intruziunilor. Aceasta ar asigura un nivel de securitate mai ridicat, deoarece ar bloca orice interacțiune dintre o entitate malițioasă şi sistemul informatic care se doreşte a fi protejat. Desigur, în cazul sistemelor IDS (Intrusion Detection Systems) care implementează şi funcții de prevenire a intruziunilor, problema care se pune este în ce măsură o

[1] Institutul Național de Studii şi Cercetări pentru Comunicații – INSCC.

astfel de capabilitate nu poate conduce la o blocare a funcționării serviciilor utile ale sistemului, afectând aplicațiile practice ale utilizatorilor finali. De aceea, problema implementării unor mecanisme eficiente de detecție/prevenire a intruziunilor este foarte importantă. Pentru abordarea eficientă a acesteia, se impune cunoaşterea potențialului pe care soluțiile tipice de detecție şi prevenire a intruziunilor îl prezintă.

2. Detecția intruziunilor

Detecția intruziunilor este procesul de monitorizare a evenimentelor apărute la nivelul unui sistem de calcul sau al unei rețele, precum şi de analizare a acestora pentru a căuta semne de *intruziuni*, definite ca încercări de realizare a unor acțiuni neautorizate de penetrare, prin ocolirea mecanismelor de securitate ale unui sistem de calcul şi/sau rețele. Intruziunile sunt cauzate de oricare dintre următoarele situații: atacatori care accesează sistemul din Internet, utilizatori autorizați ai sistemului care încearcă să obțină privilegii suplimentare pentru care nu au permisiuni, sau utilizatori autorizați care folosesc în mod inadecvat privilegiile care le sunt alocate. **Sistemele de detecție a intruziunilor** (IDS, Intrusion Detection Systems) sunt produse software sau hardware care asigură procesul de monitorizare şi analiză a intruziunilor.

2.1. Caracterizare generală a sistemelor de detecție a intruziunilor

Un **sistem de detecție a intruziunilor (IDS)** reprezintă, în esență, o soluție de securitate ad-hoc care urmăreşte protejarea sistemelor de calcul vulnerabile. Sarcinile majore ale unui sistem de detecție a intruziunilor (IDS) sunt acelea de a colecta date de la un sistem, de a analiza aceste date pentru a descoperi evenimente relevante de securitate şi de a prezenta rezultatele analizei către administratorul de sistem. Mecanisme de răspuns mai mult sau mai puțin automatizate pot fi construite, de asemenea, în cadrul unui astfel de sistem.

Figura 1 ilustrează schema de principiu a unui sistem IDS (sistem de detecție a intruziunilor generic). Sunt evidențiate componentele generice ale unui sistem de detecție a intruziunilor. Cele 3 blocuri generice, cel de colectare de date, blocul de detecție şi cel de răspuns includ, la rândul lor, module funcționale care asigură realizarea acțiunilor specifice ale unui sistem de detecție a intruziunilor. De notat ar fi şi lanțul de interacțiuni dintre respectivele module funcționale, şi care susține îndeplinirea activităților pe care trebuie să le realizeze sistemul de detecție a intruziunilor, indiferent de tipul de politică de detecție care este implementat, de tipul de politică de răspuns.

Sistemul țintă are mecanisme pentru a colecta variate tipuri de date, cum ar fi cele referitoare la traficul de rețea, evenimente la nivelul sistemului de operare sau la nivelul aplicației.

Blocul funcțional *GENERATOR DE EVENIMENTE* ține evidența informațiilor colectate şi poate achiziționa date el însuşi. Unele activități de pre-procesare pot fi efectuate de această componentă (cum ar fi aceea de a transforma datele într-un format comun şi de a realiza o anumită filtrare a datelor). Adesea, componenta *STOCARE DATE DE MONITORIZARE* este utilizată pentru a arhiva date înainte ca acestea să fie trimise la „motorul de analiză". Acest modul de stocare mai poate fi utilizat şi pentru investigarea alarmelor.

Blocul funcțional *MOTOR DE ANALIZĂ* implementează algoritmul de detecție. O metodă simplă de detecție este aceea de a utiliza scripturi de potrivire a şirurilor de text care sunt unice pentru diferite tipuri de intruziuni (care au „semnături" specifice). Alte tipuri de tehnici de recunoaştere de pattern-uri pot fi, de asemenea, utilizate. Această

abordare este similară celei pe care o folosesc multe dintre soluțiile anti-virus actuale, necesitând o bază de date cu „semnături” ale tuturor evenimentelor malițioase cunoscute care se doresc a fi detectate. Pot fi impuse praguri de alarmă pentru anumite tipuri de evenimente. Semnăturile pot fi pentru un eveniment sau pentru o secvență de evenimente. Mai pot fi utilizate sisteme expert pentru implementarea unor forme avansate de detecție a semnăturilor. Toate aceste metode au în comun faptul că ele sunt pre-programate să detecteze evenimente considerate implicit intruzive.

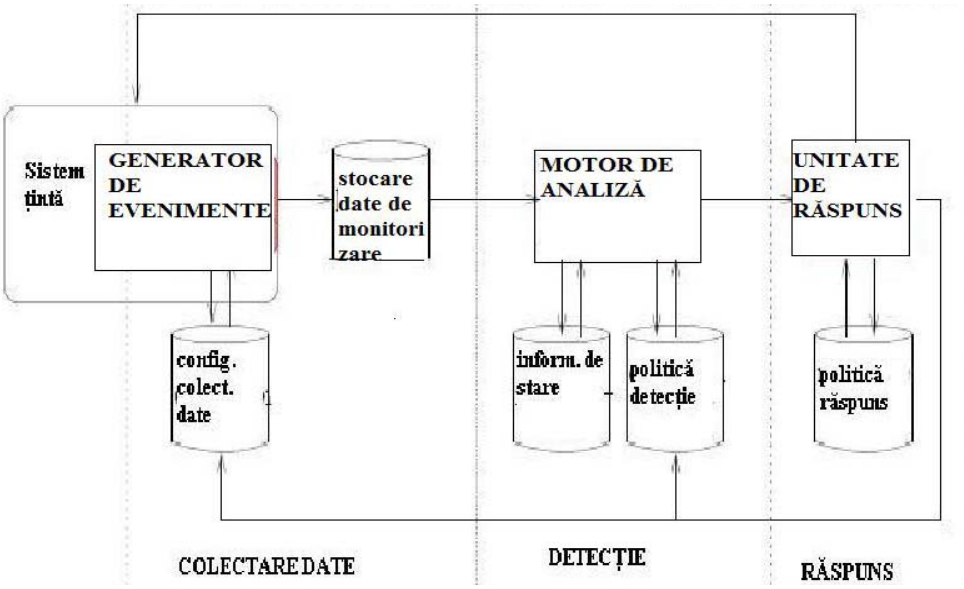

Fig. 1. Schema-bloc de principiu a unui sistem de detecție a intruziunilor.

Un alt mod de a efectua detecția este acela care se bazează pe sesizarea distincției între comportament „normal” şi, respectiv, „anormal” în cadrul sistemului țintă. Metoda constă în crearea de profile de comportament pentru programe sau utilizatori ai sistemului şi clasificarea ca posibil intruzive a acelora care deviază de la profilele stabilite. Acest lucru se poate realiza folosind statistici simple sau metode „inteligente”, cum ar fi cele bazate pe rețele neurale, tehnici de modelare şi simulare, tehnici de extragere de date relevante. În orice caz, motorul de analiză poate combina mai multe metode de detecție pentru a realiza o determinare mai completă a intruziunilor.

Componenta *POLITICĂ DE DETECȚIE* conține informații pre-programate despre modul de detectare a intruziunilor. Practic, aici sunt stocate semnăturile intruziunilor şi pragurile de alarmă. Informațiile de configurare pentru detectarea anomaliilor, ca şi regulile referitoare la informațiile care trebuie transmise la unitatea de răspuns, sunt, de asemenea, stocate la acest nivel. Baza de date cu informații de stare (*state information*) conține informații dinamice folosite pentru detecție. Acestea pot fi informații de stare despre semnăturile intruziunilor parțial completate şi despre comportamentul curent al sistemului.

Informațiile despre evenimente care sunt categorisite drept intruzive sau anormale de către motorul de analiză sunt trimise la *UNITATEA DE RĂSPUNS*. În baza regulilor pre-programate din baza de date *POLITICĂ DE RĂSPUNS*, se decide modul de răspuns la diferite evenimente. Decizia

poate fi afectată de parametri şi caracteristici cum ar fi probabilitatea de confirmare a evenimentului sau potențialul impact al acestuia. Într-un sistem distribuit, unitatea de răspuns poate primi intrări de la mai multe motoare de analiză şi, de asemenea, poate corela alarmele. Posibilele acțiuni de răspuns sunt acelea de notificare a administratorului, de reconfigurare automată a sistemului țintă pentru blocarea acțiunilor autorului intruziunii, sau de implementare a unor mecanisme specifice care să susțină răspuns manual (al utilizatorului). O altă opțiune de răspuns ar fi aceea de a permite sistemului IDS să modifice configurația pentru colectarea datelor sau politica de detecție pentru a permite colectarea mai multor informații despre un eveniment în desfăşurare.

2.2. Mecanisme tipice de detecție a intruziunilor

Deoarece sistemele informatice au devenit din ce în ce mai complexe (în scopul de a rula aplicații diverse), sistemele de *detecție a intruziunilor* au fost încorporate inițial ca elemente componente ale sistemelor de operare, deci nu ca aplicații separate. În principiu, majoritatea sistemelor IDS încearcă să detecteze evenimente suspecte de a fi considerate intruziuni neautorizate, pe care apoi să le semnaleze prin alerte către administratorii de sistem. De asemenea, tehnologiile de răspuns automat la evenimente de tip intruziune sunt în plină evoluție. Primele sisteme de detecție a intruziunilor vizau sisteme de calcul de sine stătătoare şi cu un singur procesor; detecția consta în procesarea post-facto a înregistrărilor de evidență a evenimentelor consemnate în sistem. Sistemele de calcul actuale constau adesea în noduri de procesare multiple care rulează sisteme de operare diferite, adesea interconectate în rețea sau ca sisteme distribuite. Intruziunile pot implica mai mulți hackeri executând acțiuni de penetrare. Totuşi, prezența mai multor entități schimbă doar complexitatea, nu şi esența problemei. Oricum, creşterea în complexitate este substanțială.

Detecția intruziunilor implică determinarea faptului că o anumită entitate (denumită *intrus*) a încercat să obțină, sau, mai rău chiar, a reuşit un acces neautorizat la sistem. Nici una dintre metodele actuale de detecție automată nu identifică un intrus înainte ca acesta să inițieze interacțiunea cu sistemul. Desigur, administratorii de sistem pot aplica măsuri de rutină pentru prevenirea intruziunilor. Acestea pot include solicitarea de a se furniza parole înainte ca utilizatorii să poată obține orice fel de acces la sistem, remedierea vulnerabilităților cunoscute pe care un potențial intrus ar putea încerca să le exploateze în scopul obținerii de acces neautorizat, blocarea anumitor tipuri de acces la rețea sau limitarea accesului fizic. Sistemele de detecție a intruziunilor sunt utilizate în plus față de asemenea măsuri preventive.

Intruşii pot fi clasificați în două categorii. *Intruşii externi* nu au nici un fel de acces autorizat la sistemele pe care le atacă. *Atacatorii interni* au un anumit nivel de autorizare, dar ei urmăresc să obțină, în mod fraudulos, capabilități suplimentare.

În ceea ce priveşte abordările pentru mecanismele de detecție a intruziunilor, trebuie notat faptul că în prezent metodele de detecție se încadrează în două categorii de bază: *detectarea anomaliilor* şi *detectarea utilizării inadecvate („misuse").* Prima abordare (*detecția anomaliilor*) se bazează pe definirea şi caracterizarea comportamentului dinamic şi a stării corecte a sistemului, precum şi pe detectarea schimbărilor (abaterilor) de la acestea. A doua abordare (*misuse detection*) impune caracterizarea modurilor cunoscute de penetrare a unui sistem. Fiecare dintre acestea poate fi descris, de regulă, printr-un pattern. Metoda urmăreşte descoperirea

unor pattern-uri cunoscute explicite. Un astfel de pattern poate fi un şir fix de caractere, de exemplu o semnătură specifică a unui virus. Alternativ, pattern-ul poate descrie un set sau secvență suspectă de acțiuni.

Noua generație de sisteme de detecție a intruziunilor ia în considerare aspectele majore de rețea. În acest caz, provocările sunt următoarele:

– gestionarea unor volume considerabile de date, care se transmit şi se procesează în rețele extinse;

– creşterea acoperirii (sistemul IDS trebuie să fie capabil să recunoască cât mai multe tipuri de comportament sugestiv pentru intruziuni);

– reducerea frecvenței alarmelor false (comportamente benigne raportate în mod eronat ca intruziuni);

– detectarea intruziunilor în desfăşurare, şi

– reacția în timp real pentru a alerta în legătură cu o intruziune sau pentru a limita daunele potențiale.

Detecția anomaliilor. Mecanismul de detecție a anomaliilor trebuie să fie capabil să distingă între comportament normal şi anomalie. Detecția anomaliilor se poate realiza static sau dinamic. Un detector *static* de anomalii se bazează pe presupunerea că există o parte a sistemului monitorizat care rămâne constantă. Detectoarele statice vizează, de regulă, componentele software ale sistemului, bazându-se pe presupunerea implicită că aspectele hardware nu necesită verificare. Despre detectoarele statice de anomalii se spune că verifică pentru *integritatea datelor*.

Detectoarele *dinamice* de anomalii trebuie să includă o definiție a comportamentului. Aici intervine noțiunea de *eveniment*. Comportamentul sistemului este definit ca o secvență (eventual parțial ordonată) de evenimente distincte.

Detectoarele statice de anomalii definesc unul sau mai multe şiruri binare statice pentru a specifica starea dorită a sistemului. Se arhivează o reprezentare a acestei stări, uneori comprimată. Periodic, detectorul static de anomalii compară reprezentarea arhivată a stării cu o reprezentare similară calculată pe baza stării curente. Orice diferență semnalează o eroare cauzată de probleme hardware sau de o intruziune.

Detectoarele dinamice de anomalii necesită realizarea distincției între activitatea normală şi cea anormală. De obicei, se creează un *profil de bază* pentru a caracteriza comportamentul normal, acceptabil. După inițializarea profilului de bază, detecția intruziunilor poate începe. Principial, detectoarele dinamice sunt similare cu cele statice în faptul că ele monitorizează comportamentul prin compararea caracterizării curente a comportării cu o caracterizare inițială a comportamentului anticipat (profilul de bază). De aici apare, însă, diferența. Pe măsură ce sistemul de detecție a intruziunilor îşi execută acțiunile specifice, el „observă" evenimente care sunt legate de entitatea sau de procesele asociate cu entitatea vizată. Construieşte în mod incremental un *profil curent* (posibil incomplet). Deoarece este uzual să existe o variație largă în comportamentul acceptabil al sistemului, deviația de la profilul de bază este adesea măsurat în termeni statistici. Comportamentul normal este deosebit de cel anormal pe baza unor criterii stabilite empiric sau a unor măsuri standard ale abaterilor. Principala dificultate în cazul sistemelor dinamice de detecție a anomaliilor este aceea că ele trebuie să construiască profile de bază suficient de precise şi să recunoască comportamente deviante care să fie în conflict cu profilul.

Detecția utilizării inadecvate (necorespunzătoare) prin analiza pattern-urilor sau a „semnăturilor" intruziunilor („misuse detection"). Este o tehnică care vizează detectarea intruşilor care încearcă să penetreze un sistem folosind anumite tehnici cunoscute. Principiul de bază al

acestei metode este acela că se caută tipuri cunoscute de intruziuni indiferent de comportamentul normal al utilizatorului.

În acest context, se foloseşte termenul de *scenariu de intruziune* pentru o descriere a unui tip bine cunoscut de intruziune; acesta poate fi specificat ca o secvență (parțială) de acțiuni care conduc la realizarea unei intruziuni, cu excepția situației în care o intervenție externă opreşte completarea respectivei secvențe de acțiuni. Un sistem de detecție a intruziunilor bazat pe această metodă, în mod tipic, va evalua continuu activitatea curentă a sistemului pentru a determina scenarii de intruziune, încercând astfel să detecteze un scenariu în progres. Modelul sau descrierea scenariului intruziunii va determina, substanțial, cât de eficientă va putea fi monitorizarea. Activitatea curentă a sistemului, aşa cum este ea „văzută" de către sistemul de detecție a intruziunilor, poate fi relevată prin observații în timp real din utilizarea sistemului de detecție a intruziunilor, sau poate fi stabilită din înregistrări ale activităților, efectuate automat de către sistemul de operare.

Două categorii (generații) de sisteme de detecție a intruziunilor se bazează pe această metodă. Diferența dintre ele provine din modul în care acestea descriu sau modelează comportamentul inadecvat care este semnificativ pentru o intruziune. Prima generație de sisteme de detecție a intruziunilor bazate pe metoda „misuse detection" foloseşte reguli pentru a descrie aspectele care trebuie căutate în sistem în cursul procesului de detecție. Totuşi, un număr mare de reguli poate fi dificil de interpretat deoarece nu este obligatoriu ca acestea să poată fi grupate sau asociate într-un scenariu de intruziune. Pentru a depăşi aceste dificultăți, a doua generație de sisteme introduce reprezentări alternative ale scenariului. Acestea includ organizări ale regulilor bazate pe model şi reprezentări de tranziții de stare. Deoarece scenariile de intruziune pot fi specificate destul de clar, sistemele de detecție a intruziunilor pot urmări tentativele de intruziune față de scenariul de intruziune acțiune cu acțiune. Pe parcursul secvenței de acțiuni, sistemul de detecție a intruziunilor poate anticipa următorul pas al posibilei intruziuni. Caracterizările bazate pe model şi pe tranziții de stare permit anticiparea intruziunilor.

Sisteme bazate pe reguli. Sistemele expert detectează intruziuni prin codarea scenariilor de intruziune sub forma unui set de reguli. Aceste reguli reflectă secvența parțial ordonată de acțiuni care constituie scenariul intruziunii. Unele reguli pot fi aplicabile la mai mult de un scenariu de intruziune.

Starea sistemului este reprezentată într-o *bază de cunoştințe* constând într-o *bază de fapte* şi o *bază de reguli*. O *bază de fapte* este o colecție de aserțiuni care pot fi făcute pe baza datelor acumulate din înregistrări de evaluare sau direct din monitorizarea activității sistemului. *Baza de reguli* conține acele reguli care descriu scenarii de intruziuni cunoscute sau tehnici generice de atac.

Reprezentări ale scenariului de intruziune bazate pe stare. În reprezentările bazate pe stare, perechi atribut-valoare caracterizează stările sistemelor de interes. Acțiunile care contribuie la scenariile de intruziune sunt definite ca tranziții între stări. Fiecare acțiune schimbă valoarea atributului sau atributelor de interes. Scenariile de intruziune sunt definite în forma unor *diagrame de tranziții de stare*. Nodurile acestor diagrame reprezintă stările sistemului, iar arcele reprezintă acțiuni relevante pentru intruziune. Acțiunea reprezentată de un arc cauzează o tranziție între stări şi determină modul în care valorile atributelor stării precedente se modifică ca rezultat al tranziției.

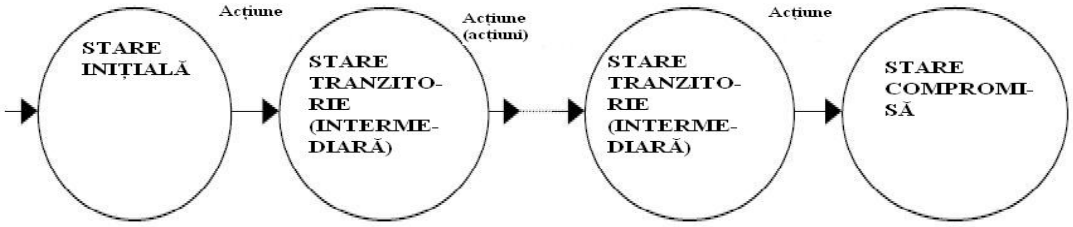

Fig. 2. Diagramă generică de tranziție de stare pentru un sistem afectat de intruziune.

Starea sistemului este funcție de toți utilizatorii, procesele şi datele prezente în sistem la un moment dat. O diagramă de tranziție de stare care defineşte un scenariu de intruziune constă într-o *stare inițială* (starea anterioară declanşării intruziunii) şi o *stare compromisă* (care este starea sistemului după ce intruziunea s-a realizat efectiv), aşa cum este ilustrat, de exemplu, în figura 2. Între cele 2 stări există un număr de *stări intermediare (tranzitorii)*. Acțiunile de interes sunt cele pe care le-ar efectua un intrus (atacator) pentru a aduce sistemul în starea compromisă. Acțiunile care nu implică un arc etichetat pornind de la o stare curentă (care poate fi starea inițială sau o stare intermediară) sunt ignorate în raport cu obiectivele scenariului specific de intruziune. Dacă s-a atins o stare finală (compromisă), înseamnă că a apărut o intruziune. O acțiune care cauzează tranziția la starea finală în diagramă indică o intruziune. În aceste condiții, un motor separat de decizie determină ce acțiune trebuie efectuată.

2.3. Tipuri uzuale de sisteme IDS

Cele 3 tipuri comune de sisteme de detecție a intruziunilor sunt produsele IDS bazate pe rețea, sistemele bazate pe host şi sistemele bazate pe aplicație. Fiecare tip de produs poate oferi, opțional, capabilități de prevenire a intruziunilor.

IDS bazate pe rețea. Aceste sisteme IDS detectează atacuri prin capturarea şi analizarea pachetelor de date care circulă prin rețea. Interceptând datele dintr-un segment de rețea sau cele care trec printr-un switch, un IDS bazat pe rețea poate monitoriza traficul de rețea care ajunge la multiple hosturi conectate la respectivul segment de rețea.

IDS bazate pe host. Aceste sisteme IDS operează pe informații colectate din cadrul unui sistem de calcul individual. Această abordare permite să se determine exact ce procese şi conturi de utilizator sunt implicate într-un atac particular la sistemul de operare. Mai mult decât atât, spre deosebire de sistemele IDS bazate pe rețea, sistemele IDS bazate pe „gazdă" pot determina mult mai uşor rezultatul intenționat al unei tentative de atac, deoarece ele pot accesa şi monitoriza direct fişierele de date şi procesele de sistem care sunt de regulă vizate de către atacatori.

IDS bazate pe aplicație. Sistemele IDS bazate pe aplicație constituie un subset special de sisteme IDS bazate pe host care analizează evenimentele apărute în cadrul execuției unei aplicații software. Cele mai comune surse de informații utilizate de astfel de sisteme de detecție a intruziunilor sunt fişierele de evidență (log) a evenimentelor create implicit de aplicația respectivă.

Prevenirea intruziunilor. Sistemele actuale de detecție a intruziunilor oferă, adesea, şi capabilități de prevenire a intruziunilor. Acest lucru înseamnă că ele nu numai că pot detecta activități cu caracter

intruziv, dar pot încerca şi să le oprească, în mod ideal înainte ca respectivele acțiuni să atingă țintele vizate. Prevenirea intruziunilor este mult mai valoroasă decât detecția intruziunilor, deoarece procesul de detecție a intruziunilor doar „observă" evenimentele în desfăşurare, fără a încerca să le oprească. Din păcate, prevenirea intruziunilor poate cauza şi probleme operaționale nedorite, deoarece dacă detecția intruziunilor nu este precisă, mecanismul de prevenire poate bloca activități legitime incorect clasificate ca fiind malițioase.

2.4. Caracteristici ale soluțiilor IDS importante pentru aplicațiile practice

În cazul sistemelor suport pentru aplicații practice cu cerințe ridicate privind protecția datelor şi a altor tipuri de resurse implicate, o soluție IDS eficientă trebuie să prezinte următoarele caracteristici:

- să fie uşor de operat;
- să fie adaptabile prin setarea adecvată a diverşilor parametri specifici proceselor de detecție/prevenire a intruziunilor, pentru a nu stânjeni funcționarea normală a aplicației;
- să ruleze continuu;
- să fie tolerantă la defecte;
- să determine o încărcare minimală a sistemului;
- să determine precis devieri de la comportamentul normal;
- să fie bine adaptată pentru cerințele specifice ale sistemului protejat;
- să fie uşor de întreținut;
- să se bazeze pe implementări pentru care se asigură actualizări periodice ale semnăturilor;
- să fie capabilă să țină evidența evenimentelor, şi să stocheze datele respective într-o locație securizată, de asemenea să asigure trimiterea de mesaje de alertă către administratorii de securitate.

3. Concluzii

Problemele de securitate care afectează sistemele informatice şi rețelele conectate la Internet impun utilizarea unor soluții care să aibă în vedere diferitele tipuri de incidente şi amenințări care pot afecta resursele de date necesare aplicațiilor, precum şi sistemele suport. Produsele antivirus, firewall, soluțiile VPN, produsele antispyware ş.a. sunt utilizate în mod curent pentru protejarea împotriva diferitelor tipuri de malware, împotriva interceptării datelor confidențiale transmise prin rețelele IP publice, precum şi pentru protejarea rețelelor interne organizaționale împotriva unor acțiuni externe ostile.

Sistemele de detecție/prevenire a intruziunilor asigură mecanisme pentru detectarea activităților suspecte de a fi considerate ca având caracter intruziv, şi care pot afecta integritatea datelor şi a aplicațiilor implementate. Detecția intruziunilor, ca atare, nu este însă suficientă pentru a limita consecințele intruziunilor diverşilor atacatori, din interiorul sau din exteriorul unei rețele organizaționale. Acest lucru se explică prin faptul că metodele actuale de detecție a intruziunilor sunt operaționale din momentul în care au fost deja inițiate interacțiuni între intruşi externi şi sistemele pe care aceştia le accesează în scopul obținerii neautorizate de informații confidențiale sau în scopul perturbării funcționării normale a serviciilor acestora. De aceea, soluțiile inovatoare de implementare a sistemelor de detecție a intruziunilor trebuie să includă şi componenta funcțională de prevenire a activităților cu caracter intruziv. Provocarea majoră, în acest caz, se referă la faptul că implementarea unui mecanism eficient de prevenire a intruziunilor poate afecta funcționalitatea normală a sistemului care trebuie protejat. Prin urmare, necesitatea implementării de soluții eficiente pentru detecția/prevenirea intruziunilor implică asigurarea

unor metode de detecție şi prevenire care să nu afecteze serviciile furnizate de sistem, dar şi să prevină consecințele actțiunilor frauduloase lansate de către intruşi din exteriorul rețelei organizaționale.

Bibliografie

1. **Gregg M., Kim D.** *Inside Network Security Assessment. Guarding Your IT Infrastructure*, TechRepublic, http://search.techrepublic.com.com/search/Network+Security+Assessment.html
2. **Grime R.** *Implementing Vulnerability Scanning in a Large Organisation*, SANS Institute, June 2003, http://www.sans.org/reading_room/whitepapers/casestudies/1103.php
3. **Jones A.**, **Sielken R.** *Computer System Intrusion Detection: A Survey*, White Paper, http://www.cs.virginia.edu/~jones/IDS-research/Documents/jones-sielken-survey-v11.pdf
4. **Lundin E.**, **Jonsson E.** *Survey of Intrusion Detection Research*, Technical Report nr. 02-04, 2002.
5. **Petersen R.** *Security Breaches: Notification, Treatment and Prevention*, EDUCAUSE review, July/August 2005, http://www.educause.edu/ir/library/pdf/erm05413.pdf
6. **Walters N**. *Into the Breach: Security Breaches and Identity Theft*, AARP Public Policy Institute, July 2006, http://assets.aarp.org/rgcenter/consume/dd142_security_breach.pdf
7. **Zdrnja B**. *Two Factor Authentication Evaluation Project*, White Paper, The University of Auckland, New Zealand, November 2005, http://www.auckland.ac.nz/security/images/2FAReportv1.pdf
8. *** *Recommended Practices on Notice of Security* Breach Involving Personal Information, Office of Privacy Protection, February 2007, http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf
9. *** *Next Generation Data Auditing for Data Breach Detection and Risk Mitigation*, TIZOR Mantra, 2007, http://hosteddocs.ittoolbox.com/Tizor021507b.pdf
10. *** *Using a Network Analyzer as a Security Tool*, Network Instruments, 2004, http://www.netinst.com/assets/pdf/SecurityWhitePaper.pdf