COLEGIUL TEHNIC „VICTOR UNGUREANU”
CÂMPIA TURZII

PROIECT

PENTRU OBŢINEREA CERTIFICATULUI DE CALIFICARE
PROFESIONALĂ NIVEL 4

TEHNICIAN OPERATOR TEHNICĂ DE CALCUL

ABSOLVENT:
POP I.F. ANCA-PATRICIA

COORDONATOR:
prof. ARION LOREDANA

2019 – 2020

Prevenirea și combaterea atacurilor informatice

CONȚINUT

ARGUMENT

Guvernele, armata şi economia mondială nu mai pot funcţiona fără ajutorul computerului. Computerele care tranzacţionează această creştere uriaşă de informaţii comunică între ele prin Internet sau prin alte numeroase reţele militare sau financiare.

Fiind un bun foarte important, informația trebuie protejată deoarece rămâne utilă atâta timp cât este validă, nealterată și adevărată. Fără un sistem de securitate implementat și funcțional, sistemele informatice, de telecomunicații și datele prelucrate, stocate sau transportate de acestea pot fi oricând supuse unor atacuri informatice. Unele atacuri sunt pasive - informațiile sunt monitorizate sau copiate, iar alte atacuri sunt active - fluxul de informații este modificat cu intenţia de a corupe sau distruge datele sau chiar sistemul sau rețeaua în sine. Sistemele informatice și de telecomunicații, rețelele formate de acestea și informațiile pe care le dețin sunt vulnerabile la numeroase tipuri de atacuri dacă nu sunt apărate de un plan de securitate informatică eficient.

Criminalitatea informatică reprezintă un fenomen al zilelor noastre, reflectat în mod frecvent în mass-media. Un studiu indică chiar că teama de atacuri informatice depăşeşte în intensitate pe cea faţă de furturi sau fraude obişnuite.

Cu mulţi ani în urmă au existat voci care avertizau că, într-o bună zi computerul va preface toate formele de delincventă. Se pare că a existat o mare doză de adevăr în aceste previziuni şi, mai mult, acestea au rămas valabile şi în ziua de azi.

Dacă luăm în considerare statisticile din ultimii cincisprezece ani, se poate susţine cu tărie că infracţiunea asistată de calculator nu poate fi socotită deloc inofensivă şi că fenomenul este într-o continuă creştere.

Încă din momentul în care răspândirea prelucrării automate a datelor a devenit o certitudine, s-a prevăzut că delictul cel mai frecvent care va fi întâlnit în statisticile privind criminalitatea va deveni criminalitatea prin computer. Cu toate acestea, abia în penultimul deceniu al secolului trecut s-au pus la punct primele legi importante pentru combaterea fenomenului.

« Modul cum culegi, administrezi şi foloseşti informația fac din tine un câştigător sau un înfrânt în viață », subliniază Bill Gates rolul actual al sistemelor de calcul în viaţa noastră, a tuturor.

I. INFRACȚIUNI INFORMATICE

Prin infracţiune informatică în **sens larg** se înţelege:

«*orice infracţiune în care un calculator sau o reţea de calculatoare este obiectul unei infracţiuni, sau în care un calculator sau o reţea de calculatoarea este instrumentul sau mediul de înfăptuire a unei infracţiuni.*»

Prin infracţiune informatică în **sens restrâns** se înţelege:

«*orice infracţiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor.* »

Conţinutul noţiunii de faptă penală de natură informatică este deosebit de variat, fiind abordat din diferite perspective în cadrul lucrărilor de specialitate. Astfel, în raportul Comitetului European pentru probleme criminale, infracţiunile informatice sunt sistematizate în următoarele categorii:

- infracţiunea de fraudă informatică;
- infracţiunea de fals în informatică;
- infracţiunea de prejudiciere a datelor sau programelor informatice;
- infracţiunea de sabotaj informatic;
- infracţiunea de acces neautorizat la un calculator;
- infracţiunea de interceptare neautorizată;
- infracţiunea de reproducere neautorizată a unui program informatic protejat de lege;
- infracţiunea de reproducere neautorizată a unei topografii;
- infracţiunea de alterare fără drept a datelor sau programelor informatice;
- infracţiunea de spionaj informatic;
- infracţiunea de utilizare neautorizată a unui calculator;
- infracţiunea de utilizare neautorizată a unui program informatic protejat de lege.

Manualul Naţiunilor Unite pentru prevenirea şi controlul infracţionalităţii informatice sintetizează următoarele categorii de infracţiuni:

- fraude prin manipularea calculatoarelor electronice;
- fraude prin falsificarea de documente;
- alterarea sau modificarea datelor sau a programelor pentru calculator;
- accesul neautorizat la sisteme şi servicii informatice;
- reproducerea neautorizată a programelor pentru calculator protejate de lege.

II. NECESITATEA SECURIZĂRII INFORMAŢIEI

Securitatea informaţiei reprezintă un lucru extrem de important pentru fiecare computer conectat la Internet, sau aflat într-o reţea de tip intranet, extranet şi chiar o reţea locală. Mai mult, chiar şi pentru un PC stand-alone securitatea informaţiei poate fi o problemă serioasă, atunci când acesta conţine informaţii personale, secrete, cu anumite grade de confidenţialitate.

Securitatea informaţiei protejează informaţia de o paletă largă de pericole legate de asigurarea continuă a activităţilor, de minimizarea pagubelor şi de maximizarea recuperării investiţiilor şi a oportunităţilor de afaceri.

Indiferent dacă calculatorul se află într-un birou la serviciu sau pe un pupitru de acasă, asigurarea securităţii informaţiei se poate pune cu aceeaşi acuitate.

Evident, în cazul în care avem de-a face cu o reţea de calculatoare asigurarea securităţii reprezintă o problemă deosebit de serioasă şi, totodată, cu mult mai dificilă.

Orice conectare obişnuită la Internet nu este întotdeauna lipsită de riscuri. Conexiunea propriu zisă, absolut inocentă la prima vedere, ar putea fi însoţită prin partaj fraudulos de către un parazit sau un program spion, care are un rol foarte bine definit: de a fura o parte din informaţiile manipulate, desigur, parte din ele cu caracter strict confidenţial pentru proprietar.

Studiile arată că în medie 90% din breşele de securitate identificate nu sunt datorate problemelor tehnologice ci instalării şi configurării necorespunzătoare sau datorită nerespectării unor proceduri de utilizare şi administrare a sistemului de calcul. În multe cazuri, aceste proceduri nici nu există. Securitatea trebuie să fie o caracteristică intrinsecă a sistemului. Un sistem sigur este unul bine proiectat, implementat, utilizat şi administrat.

În lumea specialiştilor IT se obişnuieşte să se spună că un PC este complet protejat de un produs firewall şi de un program antivirus. Există produse informatice care pot asigura o protecţie foarte bună pentru grupurile mici sau pentru PC-urile individuale. De exemplu, firewall-uri precum ZoneAlarm (www.zonelabs.com) sau BlackICE Defender (www.netice.com), sunt foarte la modă astăzi, iar produsele antivirus sunt foarte multe şi foarte eficace.

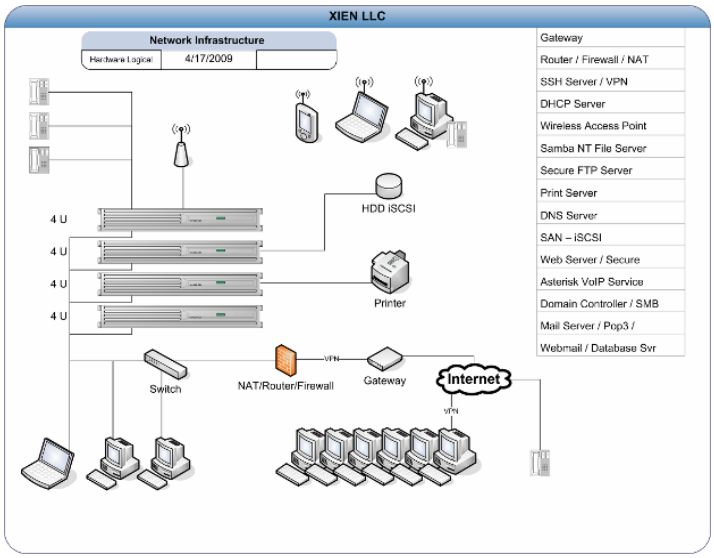
Tranziţia către o societate informaţională implică nevoia de informaţii credibile, iar progresul tehnologic are implicaţii de ordin exponenţial asupra evoluţiei. Din acest punct de vedere necesitatea securizării informaţiei păstrate şi procesate prin intermediul calculatoarelor decurge pur şi simplu din necesitatea de conectare şi de comunicare, iar globalizarea şi Internetul au schimbat complet faţa lumii.

III. SECURITATEA INFORMAŢIEI

III.1. SECURITY BY DESIGN

Conceptul de „**security by design**” este foarte bun atunci când posibilităţile de implementare sunt justificate. De multe ori totuşi acest concept impune unele restricţii care limitează foarte mult utilizarea sa în arii diferite, metoda fiind folosită în zone speciale, foarte specializate (zone cu statut de importanţă majoră, ca de exemplu reţelele de calculatoare care controlează traficul aerian, laboratoare de cercetare, etc.), zone în care accesul prin definiţie este foarte restrictiv.

Acest concept aplicat la „nivel software” generează un principiu de funcţionare al aplicaţiei cu restricţii foarte clare şi puternice – care de multe ori din pricina acestor limitări devine în scurt timp inutil.

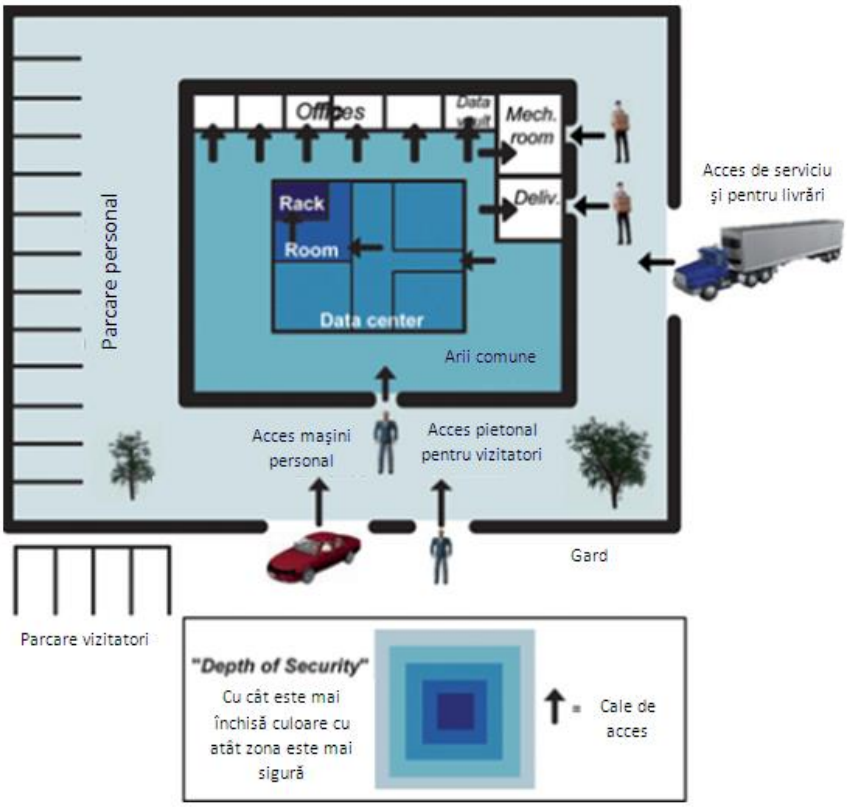


III.2. IN-DEPTH SECURITY

„In-depth security” sau „defence in depth” este un principiu bazat pe mai multe „straturi” de securitate în vederea protejării sistemului sau reţelei din care face parte.

Trebuie să se înţeleagă că nu contează cât de bun este fiecare „strat” – privit singular, există cineva mai deştept, cu resurse materiale şi temporale suficiente cât să treacă de acesta. Acesta este motivul pentru care practicile uzuale de securitate sugerează existenţa mai multor nivele de securitate sau pe scurt „in-depth security”.

Folosirea de nivele (layers) diferite de protecţie, de la diferiţi producători oferă o protecţie substanţial mai bună.



III.3. FIREWALL

Definiție

O definiție a unui sistem de protecție tip Firewall ar putea fi: un sistem capabil sa implementeze politici de securitate pentru controlul accesului, in vederea restricționării comunicațiilor la pe perimetrul dintre doua rețele. Traficul din interior şi spre exterior este filtrat, restricţionat, blocând eventualele transmisii nenecesare.

Cum funcționează?

De fapt, un firewall, lucrează îndeaproape cu un program de routare, examinează fiecare pachet de date din reţea (fie cea locală sau cea exterioară) ce va trece prin serverul gateway pentru a determina dacă va fi trimis mai departe spre destinaţie. Un firewall include de asemenea sau lucrează împreună cu un server proxy care face cereri de pachete în numele staţiilor de lucru ale utilizatorilor. În cele mai întâlnite cazuri aceste programe de protecţie sunt instalate pe calculatoare ce îndeplinesc numai această funcţie şi sunt instalate în faţa routerelor.

Astfel, un firewall este folosit pentru două scopuri:

- pentru a păstra în afara reţelei utilizatorii rău intenţionaţi (viruşi, viermi cybernetici, hackeri, crackeri)
- pentru a păstra utilizatorii locali (angajaţii, clienţii) în reţea

Politica firewall-ului

Prin politica de securitate se înțelege un ansamblu de reguli (condiții si acțiuni) specificate, care trebuie aplicate pentru atingerea obiectivelor de securitate cerute.

Înainte de a construi un firewall trebuie hotărâtă politica sa, pentru a şti care va fi funcţia sa şi în ce fel se va implementa această funcţie.

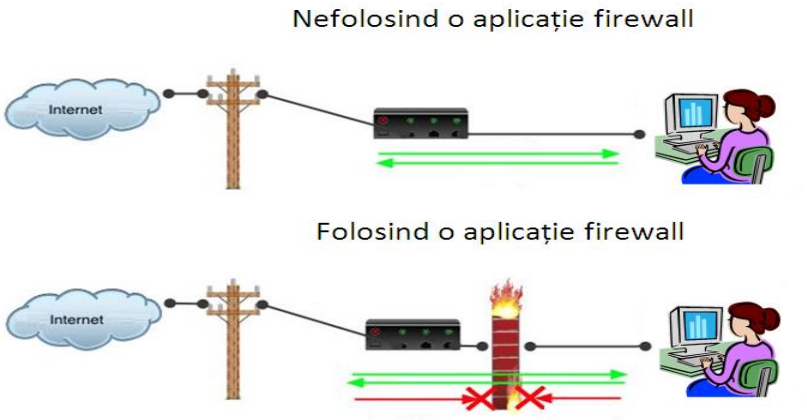
Politica firewall-ului se poate alege urmând câţiva paşi simpli:

- se alege ce servicii va deservi firewall-ul
- se desemnează grupuri de utilizatori care vor fi protejaţi
- se defineşte ce fel de protecţie are nevoie fiecare grup de utilizatori
- pentru serviciul fiecărui grup se descrie cum acesta va fi protejat
- se scrie o declaraţie prin care oricare alte forme de acces sunt o ilegalitate

Politica va deveni tot mai complicată cu timpul, dar deocamdată este bine să fie simplă şi la obiect.

Această politică poate însemna:

- protejarea resurselor reţelei de restul utilizatorilor din alte reţele similare – Internetul - sunt identificaţi posibilii "musafiri" nepoftiţi, atacurile lor asupra PC-ului sau reţelei locale putând fi oprite.
- controlul resurselor pe care le vor accesa utilizatorii locali.



Clasificare

Firewall-urile pot fi clasificate după:

- Layerul (stratul) din stiva de reţea la care operează
- Modul de implementare

În funcţie de layerul din stiva TCP/IP (sau OSI) la care operează, firewall-urile pot fi:

- Layer 2 (MAC) şi 3 (datagram): packet filtering.

- Layer 4 (transport): tot packet filtering, dar se poate diferenţia între protocoalele de transport şi există opţiunea de "stateful firewall", în care sistemul ştie în orice moment care sunt principalele caracteristici ale următorului pachet aşteptat, evitând astfel o întreagă clasă de atacuri
- Layer 5 (application): application level firewall (există mai multe denumiri). În general se comportă ca un server proxy pentru diferite protocoale, analizând şi luând decizii pe baza cunoştinţelor despre aplicaţii şi a conţinutului conexiunilor. De exemplu, un server SMTP cu antivirus poate fi considerat application firewall pentru email.

Deşi nu este o distincţie prea corectă, firewall-urile se pot împărţi în două mari categorii, în funcţie de modul de implementare:

- dedicate, în care dispozitivul care rulează software-ul de filtrare este dedicat acestei operaţiuni şi este practic "inserat" în reţea (de obicei chiar după router). Are avantajul unei securităţi sporite.
- combinate cu alte facilităţi de networking. De exemplu, routerul poate servi şi pe post de firewall, iar în cazul reţelelor mici acelaşi calculator poate juca în acelaţi timp rolul de firewall, router, file/print server, etc.

Ce "poate" şi ce "nu poate" să facă un firewall?

Un firewall **poate** să:

- monitorizeze căile de pătrundere în reţeaua privată, permiţând în felul acesta o mai bună monitorizare a traficului şi deci o mai uşoară detectare a încercărilor de infiltrare;
- blocheze la un moment dat traficul în şi dinspre Internet;
- selecteze accesul în spaţiul privat pe baza informaţiilor conţinute în pachete.
- permită sau interzică accesul la reţeaua publică, de pe anumite staţii specificate;
- şi nu în cele din urmă, poate izola spaţiul privat de cel public şi realiza interfaţa între cele două.

De asemeni, o aplicaţie firewall **nu poate**:

- interzice importul/exportul de informaţii dăunătoare vehiculate ca urmare a acţiunii răutăcioase a unor utilizatori aparţinând spaţiului privat (ex: căsuţa poştală şi ataşamentele);
- interzice scurgerea de informaţii de pe alte căi care ocolesc firewall-ul (acces prin dial-up ce nu trece prin router);

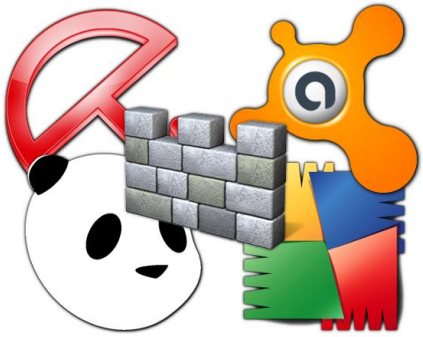
- apăra reţeaua privată de utilizatorii ce folosesc sisteme fizice mobile de introducere a datelor în rețea (USB Stick, dischetă, CD, etc.)
- preveni manifestarea erorilor de proiectare ale aplicaţiilor ce realizează diverse servicii, precum şi punctele slabe ce decurg din exploatarea acestor greşeli.

Limitări

- fiabilitate redusă, din cauza implementării centralizate a acestui sistem
- posibila gâtuire (en. bottleneck) a traficului
- necesită suport pentru asigurarea imunității sale la diverse categorii de atacuri (ex. atacul prin fragmentare IP, viruși/viermi);

III.4. ANTIVIRUS

Definiție



Antivirusul este un program pe care-l instalăm pe calculatorul personal pentru a-l proteja de infectarea cu malware. Termenul „malware“ este un termen generic, care desemnează orice tip de program software dăunător bunei funcționări a calculatorului, cum ar fi virușii, viermii, caii troieni sau programele de monitorizare spyware.

Problema este că antivirusul nu mai poate ține pasul cu ritmul atacatorilor cibernetici, aceștia dezvoltând și lansând constant noi tipuri de malware. Există atât de multe versiuni noi de malware lansate zilnic încât nici un program antivirus nu poate detecta și nu poate oferi protecție pentru toate. Acesta este motivul pentru care este important să înțelegem că, deși antivirusul ajută la protecția calculatorului personal, el nu poate detecta și stopa toate tipurile de malware. Aceştia ocupa resursele PC-ului (procesorul şi memoria RAM) ducând astfel la încetinirea pornirii sistemului de operare şi a programelor legitime ce pornesc o dată cu el. Pe lângă pagubele provocate, aceştia reușesc să se ascundă prin atașarea de cod unor fișiere de sistem iar la rularea acestora este executat inevitabil şi virusul putând să infecteze şi alte fișiere. Un virus poate infecta un alt PC exclusiv prin mutarea unor fișiere infectate de pe un alt PC prin diferite moduri (transfer pe CD-compact disc, transfer pe rețea, stick de memorie, website-uri etc). Unii oameni folosesc termenul generic de virus pentru a se referi la orice program maliţios şi nu fac deosebiri. Termenul corect pentru orice program maliţios este malware.

Un virus (informatic) este un program (software) ce se autocopiază şi infectează un PC fără permisiunea userului (utilizatorului). În cele mai multe cazuri acestea produc pagube precum ștergerea de fișiere, împiedicarea rulării programelor antivirus şi a programelor legitime instalate şi sunt şi cazuri de formatare de partiții ale hard disk-ului.

Cum funcţionează un antivirus?

În general sunt două moduri în care un antivirus identifică un program malware: detecție pe bază de semnături și detecția bazată pe comportament.

a) Detecția bazata pe semnături

Detecția pe bază de semnătură funcționează similar sistemului imunitar al omului. El scanează calculatorul pentru caracteristici sau semnături ale programelor cu funcționare dăunătoare cunoscute. Aceasta o face prin referirea la un dicționar de programe malware cunoscute: dacă ceva din calculator se potrivește cu unul din tiparele conținute în dicționar, antivirusul încearcă să-l neutralizeze. Asemeni sistemului imunitar uman, abordarea bazată pe dicționar necesită actualizări, cum sunt vaccinurile pentru gripă, ca să poată asigura protecția necesară față de noi versiuni de malware.

Antivirusul poate oferi protecție față de ceea ce poate recunoaște ca fiind periculos. Problema este că răufăcătorii dezvoltă noi versiuni de malware într-un ritm atât de rapid încât furnizorii de soluții antivirus nu reușesc să țină pasul cu ei. Ca o consecință, indiferent cât de recent actualizat este programul antivirus, va exista întotdeauna o variantă de malware care poate ocoli protecția oferită de antivirus. Deși este o componentă importantă a securității, antivirusul nu poate detecta și stopa toate atacurile.

b) Detecție bazată pe comportament

Cu mecanismul de detecție bazat pe comportament antivirusul nu încercă să detecteze un program malware cunoscut ci monitorizează comportamentul în funcționare a programelor software instalate pe calculator. Atunci când un program are o funcționare suspectă, cum ar fi încercarea de accesare a fișierelor protejate sau modificarea altui program, antivirusul detectează comportamentul suspect și ne alertează asupra acestuia.

Această abordare oferă protecție față de cele mai noi tipuri de malware care nu sunt încă incluse în niciun dicționar. Problema acestei abordări, este că poate genera atenționări false. Ca utilizatori ai calculatorului am putea fi nesiguri pe ce să permitem sau nu și, în timp, să devenim neutri față de toate aceste atenționări. Am putea fi tentaţi să dăm clic pe „Acceptă“ la toate notificările, lăsând astfel calculatorul vulnerabil la atacuri și infectare. În plus, în momentul când comportamentul suspect este semnalat, programul malware cel mai probabil că este deja instalat și se execută pe calculatorul nostru și nu avem de unde ști ce a făcut până când a fost detectat de către antivirus. Indiferent de modul cum funcționează programul antivirus pe care-l folosim, acesta nu ne poate proteja mereu față de orice tip de malware.

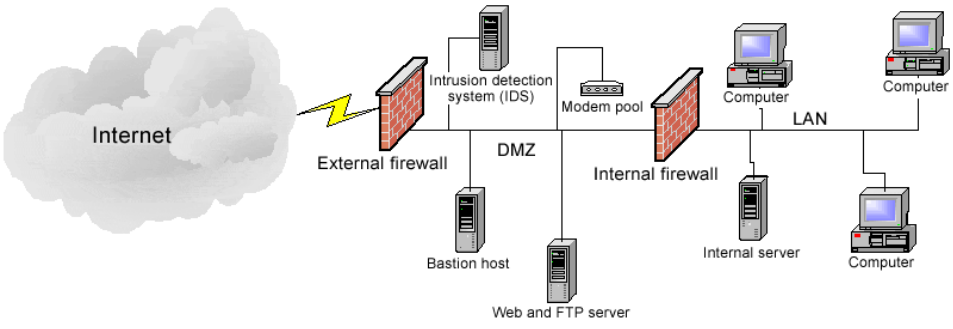
Eficienţa programelor antivirus poate fi redusă sau chiar anulată prin diverse moduri de atac, dintre care două sunt utilizate intens. Un virus de tip rootkit va înlocui fişierele sistemului de operare cu fişierele proprii „păcălind” astfel programul antivirus şi putând să-şi execute astfel propriul cod. Atacarea fişierelor AV presupune înlocuirea executabilelor programului antivirus sau alterarea dicţionarului de semnături.

III.5. ZONA DMZ

Definiție

DMZ este un termen folosit pentru identificarea unei zone dintr-o reţea în care politica de securitate este permisivă (demilitarizată). O Zonă Demilitarizată (DMZ) este o arhitectură conceptuală de reţea în care serverele cu acces public sunt plasate separat pe un segment izolat de reţea. Scopul DMZ este acela de a asigura că serverele accesibile publicului nu pot intra în contact cu alte segmente interne de reţea, în situaţia în care un server este compromis.

Un firewall este deosebit de relevant în implementarea DMZ, din moment ce acesta este responsabil de punerea în aplicare a politicilor adecvate pentru a proteja reţelele locale de DMZ, în timp ce este menţinută accesibilitatea în DMZ.



Datorită naturii extraordinare a implementării DMZ, nu este recomandat să încercăm această soluţie decât dacă deţinem cunoştinţe solide de networking. DMZ-ul nu este în general o necesitate, dar este agreat de administratorii de reţea preocupaţi de securitate.

Cum funcționează?

DMZ este configurată pe un router sau un firewall şi funcţionează după următorul principiu: dacă avem o reţea privată cu conexiune la Internet, vom dori ca sistemele să poată accesa serviciile (sau doar anumite servicii) existente în reţeaua globală dar nu şi invers. Comunicarea între calculatoare se face prin trimiterea de solicitări către anumite servere şi primirea unor răspunsuri.

În mod normal calculatoarele din reţea vor accesa servicii din Internet trimiţând solicitări şi primind răspunsuri la acestea. Pot exista şi cazuri când reţeaua deţine un server public, adică un server care răspunde solicitărilor primite din afară (website, mail, FTP, etc). Având în vedere că de această dată vom primi solicitări la care trebuie să răspundem, vom vrea să ne asigurăm că serverul este singurul care primeşte cereri din Internet, nu şi calculatoarele private întrucât ne-am asuma un risc de securitate.

III.6. MBSA

Este un program uşor de folosit, dezvoltat de Microsoft, care are ca scop, detectarea slăbiciunilor de securitate și detectarea actualizărilor lipsa ale securității pentru următoarele programe

- Client Version of Windows (Windows 7 inclusiv)
- Windows Server (Windows Server 2008 inclusiv)
- SQL Server
- Internet Server
- Microsoft Office

MSBA creează și stochează rapoarte individuale de securitate pentru fiecare calculator scanat. Aceste rapoarte sunt expuse în HTML și nu includ doar recomandări şi informații despre nivelul de securitate, dar și detalii despre testele eşuate și despre măsurile corective recomandate.

Chiar daca rețeaua este actualizata la zi MSBA poate raporta o multitudine de erori. Nu este necesar să rezolvăm fiecare problemă din aceste rapoarte. Anumite vulnerabilități

raportate prezintă un risc redus pentru anumite sisteme. Totuși chiar daca MSBA nu raportează nici o problemă asta nu înseamnă ca sistemul nu este perfect funcțional.

După ce instalam/actualizăm anumite programe este recomandat să rulam scanare MSBA ca să ne asiguram că pachetele de date descărcate au fost instalate corespunzător și că nu există probleme cu acestea.

III.7. IDS INTRUSION DETECTION SYSTEM

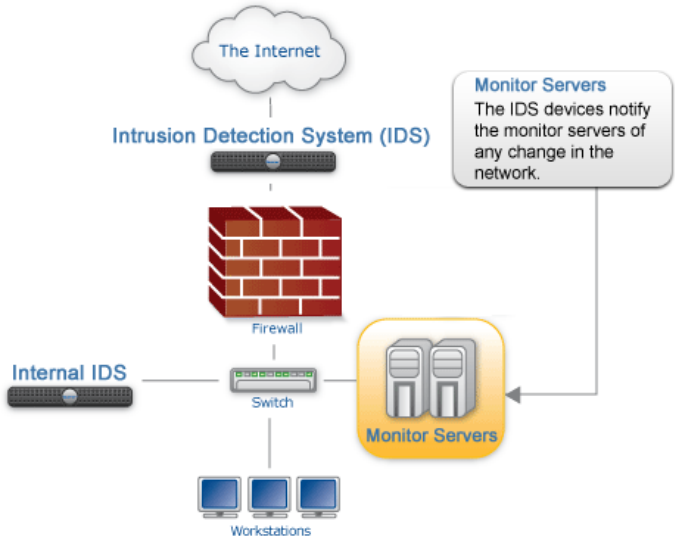
Definiție

Un sistem de detecţie al intruziunilor - IDS (Intrusion Detection System) reprezintă un echipament (sau o aplicație) care monitorizează activitățile rețelei şi/sau sistemului căutând activităţi maliţioase sau violări ale politicilor de securitate.

Detecția intruziunilor este procesul de monitorizare a evenimentelor care au loc într-un sistem sau o rețea de calculatoare şi analiza lor pentru a detecta posibile incidente care sunt amenințări iminente de violare a politicilor de securitate, a politicilor de utilizare acceptate sau a practicilor standard de securitate.

Prevenirea intruziunilor este procesul prin care se desfăşoară detecția intruziunilor şi încercarea de înlăturare a posibilelor incidente detectate. Sistemele de detecție şi prevenire ale intruziunilor - IDPS (Intrusion Detection-Prevention Systems) au ca scop principal identificarea posibilelor incidente, înregistrarea informațiilor despre ele, încercarea de înlăturare a incidentelor şi raportarea către administratorii de securitate.

În plus, organizaţiile pot folosi IDPS-urile şi pentru alte scopuri: identificarea problemelor legate de politicile de securitate, documentarea amenințărilor existente şi descurajarea indivizilor în a încălca politicile de securitate.



Tipuri de IDS-uri

Sistem de detecție al intruziunilor de tip network-based

Într-un sistem de detecție al intruziunilor de tip network-based - Network-based Intrusion Detection System (NIDS) - senzorii sunt localizați în puncte critice ale rețelei care este monitorizată, de cele mai multe ori la marginea rețelei sau in DMZ (demilitarized zone). Senzorii captează tot traficul din rețea şi analizează conținutul fiecărui pachet căutând urme de trafic maliţios.

Sistem de detecție al intruziunilor de tip host-based

Intr-un sistem de detecție al intruziunilor de tip host-based - Host-based Intrusion Detection System (HIDS) - senzorul constă, de obicei, într-un agent software care monitorizează toată activitatea ce se desfăşoară pe stația pe care este instalat, incluzând aici sistemul de fișiere, kernel-ul şi chiar aplicații în unele cazuri.

Funcționare

Sistemele de detecție ale intruziunilor folosesc cel puţin una dintre cele două tehnici de detecție: anomalii statice şi/sau semnături.

IDS bazat pe anomalii statice

- Un astfel de IDS stabileşte o valoare inițială de performanță bazată pe evaluări ale traficului normal din rețea. După efectuarea acestui pas inițial, IDS-ul va raporta traficul curent din rețea la valoarea inițială stabilită pentru a stabili dacă se încadrează în limitele normale. Daca traficul din rețea depășește limitele normale va fi generata o alarmă.

IDS bazat pe semnături

- Un astfel de IDS examinează traficul din rețea căutând modele de atac preconfigurate şi predeterminate cunoscute sub numele de semnături. Multe atacuri astăzi au semnături diferite. Pentru a putea face fața amenințărilor o colecţie de astfel de semnături trebuie actualizata in permanență.

III.8. IPS INTRUSION PREVENTION SYSTEM

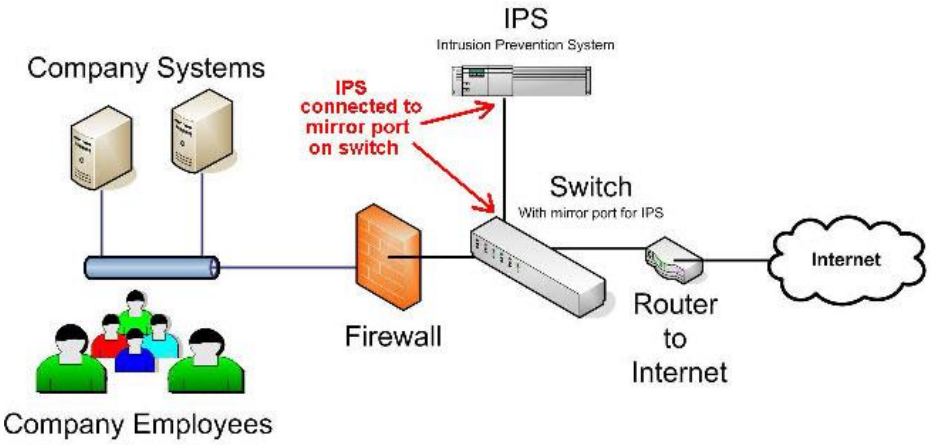
Definiție

Un Sistem de Prevenire al reprezintă un echipament de securitate al rețelei care monitorizează activitățile rețelei şi/sau sistemelor şi poate reacţiona, în timp real, să blocheze sau să prevină unele activităţi maliţioase.

Tehnologia prevenirii intruziunilor este văzută de către unii ca o extensie a tehnologiei de detecție a intruziunilor, deoarece un IPS trebuie să fie în același timp şi un foarte bun IDS pentru a asigura o rată scăzută de alarme false.

Un IPS este, în mod obişnuit, conceput pentru a opera complet invizibil în rețea. Produsele IPS nu au de obicei o adresa IP din rețeaua protejata dar pot răspunde în mod direct oricărui tip de trafic prin diverse metode (terminarea conexiunilor, renunţarea la pachete, generarea de alerte, etc.)

Deşi unele IPS-uri au abilitatea de a implementa reguli de firewall aceasta este de obicei o funcție adiţională şi nu una din funcțiile de bază ale produsului. Mai mult, tehnologia IPS oferă o mai bună monitorizare a operaţiilor unei rețele furnizând informaţii despre staţiile active, încercările de autentificare eşuate, conținut necorespunzător şi alte funcții ale nivelelor rețea și aplicație.



Tipuri de IPS-uri

Host-based

Un Sistem de Prevenire al Intruziunilor este de tip host-based (HIPS) atunci când aplicația de prevenire a intruziunilor se află pe adresa IP specifică sistemului protejat, de obicei o singură stație. HIPS complementează metodele antivirus tradiţionale bazate pe semnături deoarece nu necesită o actualizare continuă pentru a putea răspunde atacurilor. Deoarece codul dăunător trebuie să modifice sistemul sau alte componente software care se află instalate un HIPS va observa aceste modificări şi va încerca să prevină această acţiune sau să anunţe utilizatorul pentru permisiune.

Network-based

Un Sistem de Prevenire al Intruziunilor este de tip network-based (NIPS) atunci când aplicația/echipamentul de prevenire al intruziunilor se află la o altă adresă IP decât stația pe care o monitorizează. NIPS sunt platforme hardware/software care analizează, detectează şi raportează evenimente legate de securitatea unei rețele/segment de rețea de calculatoare.

IV. PORTALUL CRIMINALITATE-INFORMATICA.RO

Portalul **www.criminalitatea-informatica.ro** reprezintă canalul oficial al Asociației Române pentru Asigurarea Securității Informației pentru informarea în domeniul criminalității informatice.

Portalul este dezvoltat în cadrul proiectului de cercetare *Protejarea sistemelor informatice împotriva fenomenului de criminalitate informatică*, al cărui scop este dezvoltarea unei platforme de comunicare a informațiilor de interes major privind atacurile informatice de ultimă oră și mijloace de protecție împotriva acestora pentru a oferi publicului larg metode cât mai eficiente de prevenire și combatere a fenomenului de criminalitate informatică.

Criminalitatea-Informatica.ro prezintă ultimele noutăți în domeniul atacurilor on-line, vulnerabilităților aplicațiilor software sau investigării infracțiunilor informatice pentru prevenirea și combaterea fenomenului de criminalitate informatică. Portalul oferă informații legate de

- manifestările științifice (conferințe, sesiuni de comunicări științifice, seminarii științifice, workshop-uri etc.) ce au loc în România în domeniul criminalității informatice;
- cărți, manuale universitare, tratate și reviste științifice în domeniu;
- aplicații folosite în investigarea adreselor IP, a domeniilor sau a e-mail-urilor.

În cadrul *Forumului* se pot primi sfaturi și soluții pentru problemele legate de criminalitatea informatică de la utilizatorii ce au trecut prin aceeași experiență.

Portalul conține informații clasificate în următoarele categorii:

- Alerte de securitate;
- Legislație;
- Vulnerabilități informatice;
- Infracțiuni informatice;
- Tipuri de atacuri informatice;
- Tehnici de investigare;
- Prevenire și combatere;
- Securizarea sistemelor informatice;
- Știri de ultimă oră.

Portalul constituie o platformă de comunicare între specialiștii din domeniul investigării criminalității informatice și utilizatorii interesați să-și îmbunătățească sau să-și actualizeze cunoștințele în domeniu.

BIBLIOGRAFIE

1. Dabija George, ***Securitatea sistemelor de calcul şi a reţelelor de calculatoare,*** material elaborat în cadrul proiectului *Învăţământul profesional şi tehnic în domeniul TIC,* proiect cofinanţat din Fondul Social European în cadrul POS DRU 2007-2013, 2009
2. Petre Rău, ***Infracţionalitatea pe calculator***, Bucureşti, 2001
3. Pagini WEB:
   - http://www.criminalitatea-informatica.ro/
   - http://www.riti-internews.ro/
   - www.mygarage.ro
   - www.board.ro.tanoth.gameforge.com