HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Sustav za prevenciju neovlaštenog pristupa

**CCERT-PUBDOC-2004-08-86**

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

**CARNet CERT**, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

**LS&S**, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

Glavna zadaća IT profesionalaca i stručnjaka za računalnu sigurnost jest zaštita organizacijske imovine od zlonamjernih napadača koji na bilo koji način ugrožavaju povjerljivost, integritet i raspoloživost informacijskih sustava. U provođenju tih zadataka otežavajuće su okolnosti svakako sve kompleksniji informacijski sustavi te sve veće područje zaštite o kojem je potrebno voditi računa. Sve veći broj mobilnih korisnika, udaljenih podružnica te bežičnih računalnih mreža problemi su koji dodatno otežavaju zaštitu informacijskih sustava.

Za potpunu zaštitu računalne mreže od neovlaštenog pristupa i brojnih malicioznih programa više nisu dovoljne pojedinačne sigurnosne kontrole kao što su antivirusna zaštita, vatrozidi (eng. *firewall*) ili sustavi za detekciju neovlaštenog pristupa (eng. *Intrusion Detection System*, *IDS*), s obzirom da nude ograničenu razinu zaštite, a svaka ima i određenih nedostataka. U današnje vrijeme kada se poslovanje u sve većoj mjeri bazira na informacijskim tehnologijama i pratećim servisima potrebno je osigurati znatno višu razinu zaštite i to na više razina.

Jedno od mogućih rješenja je sustav za prevenciju neovlaštenog pristupa (eng. *Intrusion Prevention System*, *IPS*) koji je detaljnije opisan u nastavku dokumenta. IPS tehnologija omogućuje zaštitu na višoj razini, a sastoji se od kombinacije postojećih sigurnosnih tehnologija. U dokumentu su ukratko opisane osnovne karakteristike i načini rada IPS sustava, prednosti i nedostaci njihove primjene u praksi te općenite sigurnosne tehnologije na kojima cijela ideja počiva.

# 2. Sigurnosne tehnologije

Različiti sigurnosni proizvodi i tehnologije koje na različitim razinama nude sigurnosnu zaštitu informacijskih sustava svakodnevno se pojavljuju na tržištu. U ovom dijelu dokumenta opisane su neke osnovne tehnologije koje su već duže vremena prisutne na tržištu, zajedno sa svojim prednostima i nedostatcima kako bi se omogućio bolji uvod u, kasnije opisan, sustav za prevenciju neovlaštenog pristupa.

## 2.1. Antivirusna zaštita

Antivirusna zaštita svakako je jedan je od najvažnijih aspekata zaštite informacijskih sustava danas. U modernom poslovnom okruženju, gdje se koriste različiti Internet servisi poput elektroničke pošte, World Wide Web-a i sl., a lokalne računalne mreže imaju izravnu vezu na Internet, antivirusna zaštita je servis koji se nikako ne smije zanemariti. Brojni maliciozni programi kao što su virusi, crvi, trojanski konji i sl., svakodnevna su prijetnja informacijskim sustavima, a antivirusna zaštita prva je linija obrane u tom smislu.

Antivirusnu zaštitu preporučljivo je implementirati na dvije razine; na lokalnoj razini (na klijentskim računalima) te na razini servisa (na mail poslužiteljima). Ovakva zaštita realizira se u obliku odgovarajućih programskih alata koji na temelju definiranih potpisa provode detekciju i filtriranje zlonamjernih programa. Također je preporučljivo da se na različitim razinama koriste programski alati različitih proizvođača kako bi se osigurala pouzdana detekcija u onim slučajevima kada jedan od programa zakaže.

Treba napomenuti da pouzdanost i kvaliteta antivirusnih programa ponajviše ovisi o ažurnosti baze s potpisima na temelju koje se provodi detekcija. Samim time jasna je i potreba za redovitim održavanjem i nadogradnjom AV programa kako bi se osigurala pouzdana zaštita u svakom trenutku. Antivirusna zaštita iako predstavlja vrlo važnu kariku u cijelom sustavu zaštite, sama po sebi nije dovoljna za uspostavu cjelovitog sustava sigurnosti.

## 2.2. Vatrozid

Vatrozid je sustav (softverski ili hardverski) čija je osnovna uloga filtriranje dolaznog i odlaznog mrežnog prometa organizacije. Svoju osnovnu zadaću vatrozid obavlja putem sigurnosnih pravila koja definiraju koji je promet dopušten, a koji zabranjen u skladu sa sigurnosnom politikom organizacije.

Jedan od nedostataka vatozidne zaštite je taj što se nakon definicije pravila filtriranja ona više ne mijenjaju, ili se moraju mijenjati ručno. U slučaju napada može proći dugi vremenski period dok se

napad ne detektira i dok se pravila vatrozida ručno ne prilagode novoj situaciji s ciljem sprječavanja neovlaštenih aktivnosti. Situaciju dodatno pogoršava i činjenica da vatrozidi ne omogućuju kontrolu internog mrežnog prometa, odnosno detekciju napada sa interne računalne mreže. Vatrozidi se najčešće postavljaju između javnog Interneta i lokalne računalne mreže te kao takvi pružaju zaštitu samo od prijetnji s Interneta, dok za napade iznutra ne nude adekvatnu zaštitu.

## 2.3. Sustav za detekciju neovlaštenog pristupa

Sustavi za detekciju neovlaštenih aktivnosti su uređaji koji se koriste za detekciju pokušaja napada na sustav. Na temelju baze sa definiranim pravilima program prati aktivnosti na sustavu te detektira i prijavljuje sve događaje koji nisu u skladu s definiranim pravilima. Međutim, bitan nedostatak IDS sustava su lažna upozorenja (eng. *false alarm*) koja mogu umanjiti vrijednost ovakvog uređaja ukoliko je isti pogrešno podešen. Dva su osnovna tipa grešaka koji se javljaju kod IDS sustava (ali i kod drugih uređaja slične namjene):

- ***False positives*** – situacija u kojoj IDS sustav prijavi legitiman mrežni promet kao pokušaj napada. Ovo je vrlo čest slučaj ukoliko se IDS sustav postavi na mrežu bez dodatnih podešavanja koja će sustav prilagoditi okruženju u kojem se koristi.
- ***False negative*** – slučaj kada IDS sustav neovlaštenu aktivnost ne detektira, odnosno kada je prepozna kao legitiman mrežni promet. Kod IDS sustava koji napade detektiraju na temelju baze sa potpisima (engl. *signature based* IDS sustavi), broj lažnih negativnih upozorenja najčešće ovisi o ažurnosti baze sa potpisima na temelju koje se provodi detekcija.

Nakon velikog broja lažnih upozorenja administratori ih najčešće počnu ignorirati nakon čega se znatno umanjuje vrijednost cijelog sustava s obzirom da postoji velika vjerojatnost da će pravi napadi proći nezabilježeno. Ono čemu se teži prilikom implementacije IDS sustava je identifikacija što je moguće više napada te da se broj lažnih upozorenja smanji na prihvatljivu razinu.

Razlikuju se dva osnovna tipa sustava za detekciju neovlaštenog pristupa:

- sustav za detekciju neovlaštenog pristupa pojedinačnim računalima(eng. *host-based IDS*),
- sustav za detekciju neovlaštenog pristupa na računalnoj mreži (eng. *network IDS*).

Također, IDS sustavi mogu se razlikovati i prema načinu rada, odnosno tehnikama detekcije neovlaštenog pristupa. U tom smislu razlikujemo:

- sustav koji vrši detekciju neovlaštenog pristupa na temelju anomalija protokola (eng. *protocol anomaly detection*),
- sustav koji vrši detekciju neovlaštenog pristupa na temelju potpisa (eng. *signatures detection*),
- sustav koji vrši detekciju neovlaštenog pristupa na temelju *backdoor* programa (eng. *backdoor detection*),
- sustav koji vrši detekciju neovlaštenog pristupa na temelju anomalija mrežnog prometa (eng. *port scanning*, *network scanning*),

Neki od IDS sustava posjeduju i određenu mogućnost prevencije napada pomoću ugrađenih mehanizma za prekidanje TCP konekcija. Ovakvi mehanizmi najčešće zahtijevaju posebno povezivanje i komunikaciju s vatrozidom, mrežnim usmjerivačem ili nekim drugim uređajem koji je u mogućnosti blokirati mrežni promet. Kod takvih rješenja, IDS sustavi određenih proizvođača najčešće omogućuju povezivanje samo sa određenim tipovima vatrozida, što korisnika obvezuje da koristi opremu koju je moguće međusobno uskladiti.

Kod implementacije mrežnih IDS sustava također je potrebno posebnu pažnju posvetiti rasporedu senzora (IDS senzori su agenti koji prate promet na računalnoj mreži) na računalnoj mreži na kojoj se želi pratiti promet. Pravilan razmještaj senzora, ključan je ukoliko se želi omogućiti kvalitetan nadzor sustava te pouzdana detekcija neovlaštenih aktivnosti.

# 3. Sustav za prevenciju neovlaštenog pristupa

Koncept sustava za prevenciju neovlaštenog pristupa često se poistovjećuje sa upravo opisanim sustavima za detekciju neovlaštenog pristupa. No, između ovih dvaju tehnologija postoje određene razlike koje će biti opisane u ovom dijelu dokumenta.

Obzirom da svaka od sigurnosnih tehnologija posjeduje određene prednosti i nedostatke, ono što može omogućiti višu razinu sigurnosti informacijskih sustava općenito, jest međusobna integracija i kombinacija svojstava nekoliko različitih tehnologija koje na različite načine mogu identificirati različite vrste napada te reagirati u skladu s njima.

Potrebno je naglasiti da IPS sustavi nisu revolucija u području sigurnosti informacijskih sustava, već samo integracija postojećih sigurnosnih tehnologija u jedan cjeloviti sustav. IPS sustavi namijenjeni su isključivo prevenciji poznatih napada. Nove napade potrebno je prethodno identificirati i analizirati te na temelju toga kreirati odgovarajuće potpise koji će se dodati u bazu IPS sustava kako bi se omogućila njihova detekcija. Zahtjevi koji se stavljaju pred IPS sustave obuhvaćaju poznate i nepoznate prijetnje informacijskim sustavima. IPS mora blokirati maliciozne akcije korištenjem višestrukih algoritama koji uključuju potpise poznatih napada. Nije dovoljno samo koristiti jednostavne potpise koje u praksi koriste antivirusni programski alati ili IDS sustavi, već je potrebno otići korak dalje i podržavati algoritme koji će omogućiti detekciju na temelju definiranih sigurnosnih politika te anomalija u sustavu. Ono što se očekuje od sustava za prevenciju neovlaštenog pristupa jest ne samo detektirati i izvijestiti o neovlaštenom pristupu, već izvršiti automatizirani odgovor kojim će se spriječiti daljnji tijek napada. Sprječavanje detektiranih napada najčešće se provodi prekidanjem malicioznih konekcija sa onih adresa sa kojih su primijećene maliciozne aktivnosti.

Neke od funkcionalnosti IPS sustava navedene su u nastavku:

- identifikacija neautoriziranog prometa na temelju potpisa,
- identifikacija neautoriziranog prometa na temelju detektiranih anomalija protokola,
- ukidanje ili smanjenje kvalitete usluga na temelju loše usklađenosti,
- evidencija i/ili upozorenje administratorima u realnom vremenu,
- omogućavanje forenzičnih podataka prema detektiranim anomalnim paketima.

Jednostavnije rečeno, sustav za prevenciju neovlaštenih aktivnosti automatski će pokušati i blokirati detektirane maliciozne aktivnosti, za razliku od IDS sustava koji će takvu akciju samo prijaviti administratoru sustava na kojemu je poduzimanje odgovarajućih preventivnih mjera.

Slično kao i IDS tako se i IPS sustavi dijele na dva osnovna tipa:

- sustav za prevenciju neovlaštenog pristupa pojedinačnim računalima (eng. *host-based IPS*),
- sustav za prevenciju neovlaštenog pristupa na računalnoj mreži (eng. *network IPS*).

## 3.1. Host-based IPS sustavi

*Host-based IPS* (*HIPS*) sustavi su programski alati za prevenciju neovlaštenog pristupa koji omogućuju zaštitu od malicioznih aktivnosti na razini pojedinačnih računala. Okosnicu HIPS sustava čine agenti koji su instalirani na klijentskim računalima i koji u suradnji sa operacijskim sustavom nadgledaju aktivnosti na sustavu na kojem su instalirani. Nakon detekcije potencijalno zlonamjernih radnji, zlonamjerni proces automatski se blokira kako bi se spriječilo njegovo daljnje izvršavanje.

Metode zaštite koje se pri tom koriste najčešće su povezane sa detekcijom napada temeljenih na pravilima pristupa. Svaki proizvođač HIPS sustava nudi predefiniranu listu pravila kojima se definiraju legitimne i nelegitimne aktivnosti na sustavu i na temelju kojih je moguće uočiti potencijalne nepravilnosti u ponašanju samog operacijskog sustava ili aplikacija koje se na njemu pokreću. Nakon što je detektirana aktivnost koja odstupa od sigurnosne politike definirane pravilima programa, zlonamjerni proces se u istom trenutku zaustavlja kako bi se spriječili eventualni problemi.

Osim upravo opisanog pristupa, HIPS sustavi vrlo često koriste i metode nadgledanja sustava gdje agenti kontinuirano prate promjene u važnijim komponentama sustava kao što su npr. *registry* te važnije sistemske datoteke i servisi. Sve aktivnosti koje na bilo koji način ukazuju na neovlaštene modifikacije nad takvim komponentama u istom se trenutku blokiraju.

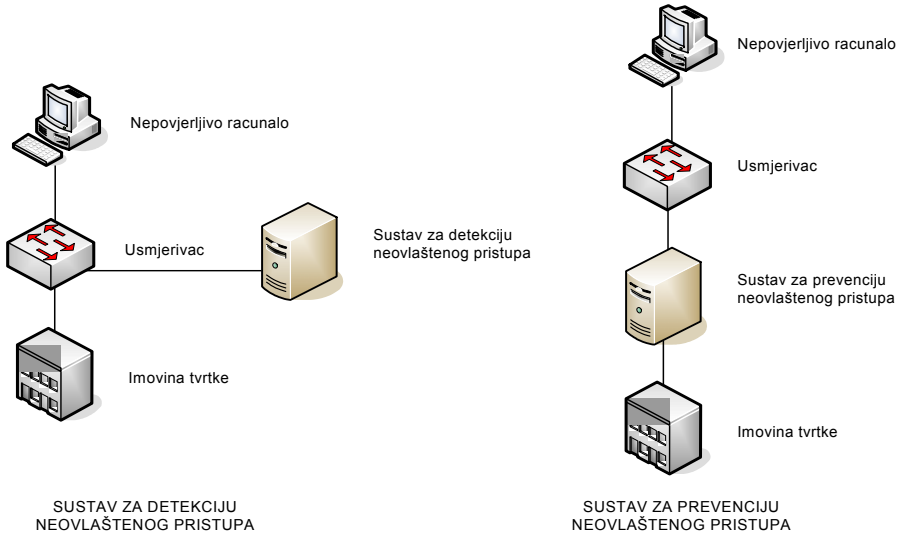
Treća metoda je hibridni pristup koji objedinjuje kombinaciju navedenih metoda s ciljem detekcije i prevencije neovlaštenog pristupa.

HIPS sustavi organizacijama pružaju dodatnu razinu zaštite u smislu da osim poznatih, omogućuju detekciju i onih najnovijih napada za koje pravila još nisu definirana. Ovakav pristup posebno je pogodan kod detekcije i blokiranja tzv. *zero day* napada koji se baziraju na iskorištavanju najnovijih sigurnosnih propusta prije nego što su objavljene odgovarajuće sigurnosne zakrpe. Ono što je također važno je to da će HIPS sustav blokirati sve aktivnosti za koje se smatra da odstupaju od legitimnog ponašanja definiranog postavkama programa. Iako ovakav koncept može rezultirati i velikim brojem

lažnih upozorenja ovakav pristup vrlo je efikasan upravo kod detekcije novih napada za koje još nisu dostupni odgovarajući potpisi ili sigurnosne zakrpe.

## 3.2. Network IPS sustavi

*Network IPS* (*NIPS*) sustav je bilo koji programski alat ili sklopovlje koje ima mogućnost detektiranja i sprječavanja poznatih napada na temelju analize mrežnog prometa. Mrežna arhitektura NIDS i NIPS sustava prikazana je na slici 1 kako bi se izvršila usporedba ovih dvaju sustava.




**Slika 1:** Mrežna arhitektura NIDS i NIPS sustava

Ukoliko se klasična arhitektura NIPS sustava usporedi s klasičnom arhitekturom NIDS sustava može se uočiti da su NIDS sustavi više orijentirani prema nadgledanju mrežnog prometa dok su NIPS sustavi postavljeni tako da im se omogućuje blokiranje konekcija ukoliko se smatra da su iste malicioznog karaktera (tzv. (eng. *in-line* arhitektura).

NIPS pristup zaustavljanju neželjenog mrežnog prometa sastoji se od odbacivanja neželjenih paketa iz mrežnih konekcija koje su prepoznate kao maliciozne. Ovaj pristup omogućuje da korisnici koji pokušaju izvesti neovlašten pristup sustavu budu spriječeni u tome, ali da im se pritom ne onemogući pristup ostalim dijelovima sustavima ukoliko se radi o legitimnim konekcijama.

NIPS sustavi tipično se sastoje od dva mrežna sučelja: internog i eksternog. Kada se paket pojavi na bilo kojem od ovih sučelja, on prolazi kroz detekciju kao kod klasičnog NIDS sustava. Maliciozni paketi se blokiraju, a legitimni su propušteni kroz drugo sučelje prema ciljnoj adresi. Samim time može se zaključiti da se NIPS sustavi mogu najbolje opisati kao kombinacija vatrozida i mrežnih IDS (NIDS) sustava kako bi se u jednom uređaju objedinile ove dvije tehnologije.

## 3.3. Prednosti i nedostaci

Kao što sve sigurnosne tehnologije imaju određene prednosti i nedostatke, niti sustav za prevenciju neovlaštenog pristupa nije imun na takva svojstva.

Neke od prednosti HIPS sustava su:

- zaštita od tzv. *zero day* napada na sustav,
- smanjeni troškovi održavanja samog sustava,
- sprečavanje izvršenja napada na sloju jezgre operacijskog sustava (*engl kernela*),
- smanjene obveze zaposlenika odgovornih za sigurnost (npr. *patch management*),
- može biti implementiran i unutar vlastito razvijenih aplikacija.

Nedostaci ovog sustava su slijedeći:

- troškovi implementacije jer sustav zahtjeva agenta za svaku radnu stanicu i poslužitelja,
- period implementacije je dug,
- nakon implementacije potrebno je podešavanje sustava kako bi bio funkcionalan,

- ukoliko je krivo podešen, sustav može izazvati probleme u radu aplikacija,
- svaka nova aplikacija mora biti testirana u interakciji s HIPS sustavom prije uvođenja,
- ne identificiraju napade po imenu i ne čiste infekcije.

Kod NIPS sustava također je bitno spomenuti prednosti i nedostatke. Prednosti su:

- onemogućava širenje crva bez zaustavljanja legitimnog mrežnog prometa,
- štiti od novih napada prije izdavanja koda za eksploataciju,
- smanjuje troškove rješavanja incidenata,

a uočeni nedostaci su:

- troškovi uvođenja sustava,
- predstavljanju *single point of failure*,
- funkcionalnost mu ovisi o nadogradnji sustava.

## 3.4. Zahtjevi za funkcionalnost sustava

Kako bi sustav za prevenciju neovlaštenog pristupa zaista bio efikasan, potrebno je zadovoljiti određene zahtjeve koji će osigurati potpunu funkcionalnost sustava.

Prvi zahtjev prilikom implementacije IPS sustava jest da on bude *in-line* (**Error! Reference source not found.**), jer jedino na taj način može operativno nuditi dobru zaštitu te blokirati sav sumnjiv promet. IPS sustav mora konstantno biti pouzdan i dostupan. Ovaj zahtjev je izuzetno bitan, jer u slučaju da je sustav prestao funkcionirati, omogućen je bilo kakav neovlašteni pristup. Zbog toga je izuzetno bitno obratiti pažnju na učestalost prekida rada sustava (eng. *failure rate*) te koje su posljedice takvog događaja. Poželjno je da IPS sustav, ukoliko i dođe do problema u radu, kompletno ne blokira sav mrežni promet (eng. *fail closed*) kako se ne bi onemogućile legitimne konekcije. Time se dolazi i do slijedećeg zahtjeva, a to je dinamika sustava. Prethodno spomenuto rušenje sustava, gdje će sav mrežni promet biti blokiran ima i drugu krajnost, a to je kompletno otvoren mrežni promet (eng. *fail open*). Optimalna kombinacija je svakako ona u kojoj IPS sustav neće predstavljati *single point of failure* u slučaju bilo kakvih nepredviđenih situacija.

Svakako je poželjno da djelovanje IPS sustava ne utječe na propusnost računalne mreže tj. da je utjecaj minimalan. U tom smislu IPS sustav mora zadovoljiti zahtjev da se mrežni paketi obrađuju dovoljno brzo, odnosno da je vrijeme kašnjenja paketa što manje.

# 4. Zaključak

Iz opisanih karakteristika može se zaključiti da sustav za prevenciju neovlaštenog pristupa, nije novost u području sigurnosti, već predstavlja integraciju postojećih sigurnosnih tehnologija. Kombiniranjem svojstava različitih tehnologija iz područja računalne sigurnosti razvijeno je rješenje koje će osim detekcije neovlaštenih aktivnosti omogućiti i njihovu prevenciju.

Kao i svaka druga tehnologija, tako i IPS sustavi imaju svoje prednosti i nedostatke. Prilikom razmišljanja o implementaciji ove tehnologije potrebno je svakako sagledati koliko će proces implementacije utjecati na postojeće stanje sigurnosti unutar organizacije, na mrežnu arhitekturu, podršku korisnicima, itd. Prema dosadašnjim trendovima može se zaključiti da IPS sustavi svakako donose osvježenje u područje sigurnosti informacijskih sustava, no vrijeme će pokazati da li će samo upotpuniti paletu proizvoda na tržištu ili će izvršiti potpunu zamjenu određenih tehnologiju.

# 5. Reference

[1] Barkett, Mike: Intrusion Prevention Systems
http://techlibrary.networkcomputing.com/data/detail?id=1090517905_391&type=RES&src=hdl_aa (10.07.2004)

[2] Lindstrom, Pete: Instrusion Prevention Systems (IPS): Next Generation Firewalls
http://techlibrary.networkcomputing.com/detail/RES/1080065083_331.html (10.07.2004)

[3] Ahlm, Eric: Is Intrusion Prevention Changing Information Security?
http://wp.bitpipe.com/resource/org_1027678760_263/IntrusionPrevention_WhitePaper.pdf (17.07.2004)