Intrusion Prevention System – Sustav zaštite od neovlaštenih i malicioznih upada

IPS je mrežni uređaj za praćenje mrežnih ili sistemskih aktivnosti u svrhu otkrivanja malicioznih aktivnosti. Osnovna funkcija IPS-a je identifikacija malicioznih aktivnosti, izrada zapisa o njima, pokušaj njihova blokiranja te izvještavanje.

Zaštita od neovlaštenih upada je preventivna mjera mrežne sigurnosti, u svrhu otkrivanja potencijalnih prijetnji i brzog odgovora na njih. Učinkovit IPS sustav mora obavljati svoju zaštitnu funkciju, a u isto vrijeme omogućiti nesmetan rad ostalih servisa unutar organizacije, tj. mora osigurati kontinuitet poslovanja.

Mrežni sustavi evoluiraju i mogli bismo reći da tu ne postoje granice, što organizaciju izlaže mnogim sofisticiranim prijetnjama. Mnoge organizacije teško drže korak s tom evolucijom, sustavi su zastarjeli, nedostaju potrebne vještine, IT budget je prenizak i osviještenost korisnika nije na zadovoljavajućoj razini.

U redu, razumijemo da nešto trebamo poduzeti i nakon analize zaključujemo da želimo implementirati moderni IPS u našu mrežu. Analizirajmo funkcije koje efektivan i moderan IPS mora imati, kako bi kvalitetno obavljao svoj posao.

Sukladno najboljim praksama postoji niz elemenata na koje morate paziti kod nabave i konfiguracije IPS-a:

Skeniranje SSL prometa – Napadači u današnje vrijeme sve češće koriste SSL enkripciju prometa kako bi zamaskirali svoj napad. Vaš IPS mora biti u stanju dekriptirati, analizirati, te ponovno enkriptirati SSL promet.

Zaštita od DOS (Denial Of Service) napada – Veliki broj organizacija u današnje vrijeme posluje putem Interneta, cilj nekih napadača je usporiti ili spriječiti mogućnost istoga kroz DOS ili DDOS napade. Vaš IPS mora odbiti svaku vrstu napada bez obzira na vrstu.

Mogućnost normalizacije prometa – Cyber kriminalci vrlo dobro poznaju najnovije IPS tehnologije i cilj im je proći neopaženo kroz obranu. Oni rade punom parom kako bi razvili napade koji će izbjeći ili prevariti vaš IPS. Zato se IPS mora obraniti od naprednih tehnika napada kroz normalizaciju prometa i lakše otkrivanje pokušaja izbjegavanja.

Pružanje kvalitetnih informacija i izvještaja – Vaš IPS mora vam na jednostavan i razumljiv način prikazivati informacije koje želite vidjeti. Dodatno, isti bi trebao imati mogućnost izvoza podataka u svrhu čuvanja povijesti napada, skrivenih komunikacija, korištenja VPN-a, VOIP-a ili Internet aplikacija.

Skeniranje ukupnog prometa (svih portova i protokola, ulazni i izlazni promet) – IPS mora skenirati sav promet, ne samo neke odabrane portove i protokole, jer moderni napadi mogu utjecati na sve aplikacije koje su u vašoj mreži. Zašto je bitno skenirati izlazni promet? Zato što napadači mogu slati povjerljive informacije iz vaše mreže ili vaše zgrade (a to može činiti i vaš djelatnik).

Višestruke metode zaštite od napada - IPS sustavi su učinkoviti koliko je učinkovita njihova sposobnost blokiranja napada, uz redovito nadograđivanje novim informacijama radi zaštite od iskorištavanja slabosti aplikacija (*application vulnerability protection*), preljevanja spremnika (*buffer*

overflow), sumnjivog prometa i malicioznog koda.

Prikupljanje višestrukih informacija – IPS se može povezati s *Active Directorijem*, te u isto vrijeme pratiti promet i aplikacije koje se koriste u mreži, uključujući i informacije o tome tko ih koristi. To omogućuje administratorima da donesu kvalitetnije odluke na temelju zapisa.

Blokiranje komunikacija s kompromitiranim sustavima – IPS kroz analizu prometa mora moći otkriti neregularan promet i svako odstupanje od normalnog djelovanja te spriječiti širenje napada ili malicioznog softvera kroz blokiranje komunikacija s kompromitiranim sustavima.

Detekcija i blokiranje malicioznog koda (virusi, trojani, crvi) pri ulazu u mrežu – Logična stvar je da ne želite da maliciozni kod uđe u Vašu mrežu. Isti može vrlo lako biti skriven u prometu koji djeluje benigno, zato IPS, mora moći prepoznati isti i zaustaviti ga pri ulasku.

Smještaj IPS-a – Bitno je znati gdje smjestiti IPS u organizaciji. Definitivno vas isti mora štiti na granici s Internetom. Trebate li još dodatnih IPS-ova? To ovisi o Vama, Vašoj infrastrukturi i potrebama.

Nije pitanje hoćemo li ili nećemo koristiti IPS, već kako odabrati odgovarajući za našu organizaciju? Odabir ovisi o vama, ali ako slijedite gore navedene upute, nećete pogriješiti.

pet, 2013-08-30 10:01 - Darie Marić**Kategorije:** Sigurnost [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1316

Links
[1] https://sysportal.carnet.hr/taxonomy/term/30