Novi izazovi Kiber bezbednosti Informacionih Sistema – Mesto i uloga Sistema za detekciju i prevenciju Nove generacije (*Intrusion Prevention* System)

Zoran Živković, Milenko Ostojić, Nataša Simić, Društvo za Informacionu Bezbednost Srbije, Towers Net doo.

***Sadržaj* — U radu se daje osnovna klasifikacija Kiber (Cyber) napada na informacione sisteme, kao i najvažnije osobine napada u poslednjih nekoliko godina. Data je klasifikacija IPS-a (*Intrusion Prevention System*) na osnovu načina funkcionisanja, kao i klasifikacija metoda detekcije IPS-a. Date su osnovne tehničke karafkteristike koje treba da zadovolji IPS nove generacije.**

***Ključne reči* — Intrusion Prevention, Cyber attack.**

I. UVOD

INTERNET danas ima izuzetno veliku ulogu u globalnoj ekonomiji. Ovo je pre svega zbog činjenice da je postao univerzalni komunikacioni medijum za prenos informacija.

Sa druge strane svedoci smo vrlo brzog razvoja javnih informacionih sistema, koji nude veći broj usluga informacionog društva putem Interneta širokom krugu korisnika. U tom smislu narastanje pretnji informacione bezbednosti postaje vrlo aktuelno.

Pitanjem informacione bezbenosti, na nivou EU se bavi organizacija ENISA, koja skuplja i koncentriše sve informacije vezane za bezbednosne incidente na Internetu sa sistemom nacionalnih organizacija CERT (*Computer Emergency Response Team*), koje prikupjaju informacije na nacionalnom nivou i distribuiraju ih ostalim nacionalnim organizacijama, a takođe se informacije dostavlju i organizaciji ENISA. Pored ovih organizacija, problemima Informacione bezbednosti bavi se i niz kompanija koje nude proizvode iz ove oblasti, a koji publikuju svoje izveštaje najčešće na godišnjem nivou.

Ovako dobijeni podaci se koriste za formiranje odgovarajućih strategija i postupaka Informacione bezbednosti na nacionalnom nivou, kao i na nivou svakog od poslovnih subjekata, sa ciljem da se na vreme preduprede sve maliciozne aktivnosti, koje bi mogle da nanesu štetu poslovanju, kao i šteta koje mogu nastati na nacionalnom nivou.

U ovom radu će biti reči o nekim malicioznim bezbednosnim rizicima u praksi, pre svega o teškim napadima na integritet informacionog sistema koji koristi Internet kao komunikaciono sredstvo, kao i mogućnostima za detekciju i onemogućavanje savremenih napada na IS. Efikasna odbrana i stvaranje uslova za neprekidan i pouzdan rad danas je nezamislivo bez savremenih sistema za detekciju i prevenciju napada od Kiber napada (*Intrusion prevention system - IPS, Intrusion detection System - IDS*).

mr. Zoran Živković, dipl.ing.: z.zivkovic@towersnet.rs.
dr.Milenko Ostojić,dipl.ing.: m.ostojic@towersnet.rs,
mr. Nataša Simić. Dipl.ing. e-mail: n.simic@towersnet.rs.

II. VIDOVI NAPADA NA IS

U nastavku će biti dat kraći pregled savremenih zlonamernih (malicioznih) aktivnosti nad informacionim sistemima koji su dominantni u poslednjih nekoliko godina, koje dovode do degradacije funkcionisanja i bezbednosti sadržaja pohranjenjih u informacionim sistemima.

Kompjuterski virusi

Crv (Worms) je program kreiran da se samostalno kreće i prebacuje sa računara na računar. Tipičan crv je dizajniran tako da može da otrkrije druge kompjutere u okruženju sa specifičnim osobinama koje mu omogućuju da uspešno napadne sledeći računar i instalira se samostalno na isti. Nakon toga crv skenira neposredno okruženje novoosvojenog domaćina i ciklus se ponavlja dokle god ima novih računara pogodnih za osvajanje.

Trojanski konj je drugi tip štetnog softvera. Kao i crv, Trojanac je dizajniran da se prebacuje sa sistema na sistem. Za razliku od crva, Trojanac zahteva intervenciju čoveka da bi se prebacivao sa sistema na sistem.

Trojanski konj je dobio ime jer liči na nešto bezopasno. Može da bude ugrađen u kompjuterski program kao da je igrica, čuvar ekrana ili neki drugi program. Ali jednom aktiviran Trojanac će napraviti štetu za koju je dizajniran. Može to da bude skeniranje okolne mreže u cilju pronalaženja nove žrtve, skeniranje sistema u cilju pronalaženja važnih podataka ili instalacija drugog malicioznog softvera.

Napadi zagušenja bafera. To je specifična vrsta napada gde je napad dizajniran tako da izvršavanjem instrukcija napadača zbuni napadnuti računarski sistem. Napadački program uspostavlja komunikacionu sesiju sa specifičnim komponentama za napadnuti sistem i šalje specijalno napravljene poruke na isti. Takve poruke namerno šalju veliku količinu podataka u ulazni bafer napadnutog sistema. Tako velika količina podataka u programima osetljivim na ovu vrstu napada može da dovede do izvršavanja napadačkih instrukcija umesto izvornih. Te nove instrukcije obično sadrže kod kojim se otvara napadnuti sistem i dozvoljava delimično ili potpuno preuzimanje kontrole nad napadnutim računarskim

sistemom. Ova vrsta napada je komplikovana za razvoj i pretpostavlja detaljno znanje o internoj arhitekturi ciljnog sistema (hardver i softver) kao i detaljno znanje o programu ili servisu koji se napadaju. Crvi, trojanci, virusi i drugi maliciozni softveri veoma često koriste ovu vrstu napada radi ubacivanja u novi sistem žrtve.

Špijunski softver, Pecanje, Butmreže

Špijunski softver (*Spyware*) je izraz dodeljen širokoj grupi tehnika koje se koriste da na skriven način dobiju informacije sa računara. Špijunski softver najčešće uzima oblik računarskog koda koji je instaliran na računar korisinka bez njegovog znanja i pristanka, koji sakuplja određene informacije i šalje ih nekom centralnom izvoru. Špijunski softver može takođe izmeniti ponašanje korisnikovog računara.

Phising. Igra reči sa reči fishing (pecanje) - phishing napad je napad na korisnike računara u pokušaju da ih prevari da učine radnju koja je predviđena da ih ošteti. Ta šteta može, na primer, imati oblik finansijske prevare ili instalacije malvera ili špijunskog softvera na njihov računar.

Botnet mreže. Botnet mreža je skup računara žrtava okupljenih u botnet vojsku, snažan računarski resurs koji čeka instrukcije od svog vlasnika. Autori Botneta su obično finansijski motivisani.

SYN poplave i napadi zagušenja usluge

SYN poplava je napad na ciljani sistem, konkretno napad na ključne projektne karakteristike TCP/IP mrežnog protokola.

U SYN poplavi, napadač šalje hiljade SYN paketa ciljanom sistemu. SYN paket je obično poruka poslata sa drugog računara koji želi da ustanovi mrežnu konekciju sa metom. Nakon prijema SYN, ciljani sistem odgovara sa SYN/ACK, u tom trenutku počinje komunikacija.

Napad za odbijanje usluge (*Denial of Service – DoS Attacks*) je napad na ciljani sistem pri čemu je cilj napada da delimično ili potpuno onesposobe ciljani sistem. Svrha DoS napada jeste da predstavi ciljani sistem beskorisnim za legitimne namene. Radi efikasnije prikrivenosti napada napadači koriste razne tehnike za izbegavanje detekcije kao što je šifrovanje kao i druga rešenja za izbegavanja detekcije (*Encryption and other detection evasion*). U malver ekonomiji, autori malvera smatraju da su njihovi proizvodi uspešni ukoliko su u stanju da izbegnu detekciju.

Napadi nultog dana

Napad nultog dana je ime novih napada na prethodno nepoznatoj ranjivosti napadnutog sistema, ili potpuno nova vrsta napada na postojeće slabosti napadnutog sistema.
Izraz *nulti dan* potiče od broja dana upozorenja od vremena kada je ranjivost objavljena i kada je zloupotrebljena. Drugim rečima, ovo su ranjivosti za koje ne postoje zakrpe.

Napadi nultog dana su značajni zato što su IPS uređaji na bazi potpisa (na bazi eksploita) generalno nesposobni da se odbrane od njih. Ipak, IPS koji takođe koriste detekciju na bazi anomalije i pravila na bazi ranjivosti (nasuprot potpisima na bazi eksploita) mogu efikasno zaštititi od napada nultog dana.

Napredene istrajne pretnje

Trenutno postoji mnogo buke i dezinformacija o naprednim istrajnim pretnjama (APT). Istina, ne postoji nikakvo magično rešenje ili jedan jedini uređaj za odbranu od APT-a. Danas je nemoguće efikasno odbraniti. Mrežni IPS je strateška komponenta strategije dubinske odbrane koja može pomoći da dobijete prednost u ovoj borbi [2].

Šta je APT?. Napredna istrajna pretnja je informacioni rat, kojim komanduju sofisticirani protivnici, namerni da kontrolišu informacione sisteme i sakupe informacije o licima, organizacijama i državama. Neke od APT pretnji su navedene u nastavku.

Brutal-force attack. Ovo je vrsta napada koja za cilj ima razbijanje lozinki za pristup sistemu. Napad se izvodi od strane zlonamernog korisnika ili softvera na računar ili operativni sistem da bi se došlo do tajne lozinke ili simetričnog ključa za enkripciju. Najčešće se vrši pogađanjem lozinke ili ključa dok se ne otkrije tačna lozinka ili ključ.

SQL injection. Predstavlja napad na bilo koju vrstu baze podataka, uključujući i Oracle baze podataka. Ovaj vid napada se često zanemaruje u diskusijama o problemima SQL baza podataka, a važi i za sve druge baze podataka, kao i činjenica da SQL injection nije samo web problem.

Cross-site scripting (XSS). Predstavlja tip ranjivosti računarske mreže i tipično se javljaju u veb aplikacijama, pri čemu napadač ubacuje client-side skript u veb strane koje su pregledali drugi korisnici. XSS ranjivosti mogu se koristiti od strane napadača, radi zaobilaženja kontrole pristupa određene politikom sajta. XSS napadi čine oko 80% napada koji su izvršeni na veb sajtovima, dokumentovano od strane Symantec-a, od 2007. godine pa nadalje. Uticaj ovog napada može biti u rasponu od male smetnje do ozbiljnog bezbednosnog rizika, u zavisnosti od osetljivosti podataka sa kojima se rukuje na ranjivom sajtu i prirode umanjenja bezbednosti koje je implementirano na sajtu vlasniku podataka.

Root.kit napadi. Ovaj vid softvera se infiltrira u ciljani sistem. Dizajniran je tako da skriva sebe u okviru ostalih resursa (direktorijuma, fajlova, procesa ili registara), sa ciljem da ne bude otkriven. Pri tome svoje delovanje zadržava u računarskom sistemu sve vreme.

III. NAJVAŽNIJE OSOBENOSTI NAPADA U PROTEKLIH NEKOLIKO GODINA

U 2011. - 2012. godini su se između ostalih izdvojila tri osnovna tipa pretnji: krađa podataka, ciljani posvećeni napadi na odabrane ciljeve i mogućnost kupovine paketa za organizovanje napada na standardne nebranjene platforme.

U 2012./2013. Znatno se menja standarni IT ambijent:

- Pojava i nagli porast broja novih platformi.
- Sve veća prihvaćenost filozofije Cloud Computing-a i novih rizika koji stim u vezi nastaju.
- Masovna prodaja pametnih telefona i pratećih aplikacija.
- Sve veći broj dinamički - geografski nezavisnih korisnika (*BYOD*).

- Neodređena i promenljiva priroda krajnje tačke korisničnog uređaja.
- Tradicionalno fizički i geografski homogen korporativni svet transformiše se u svet bez jasno vidljivih granica.

Najrasprostranjenija pretnja je bila *BlackHole* i predstavljala je oko 80% pretnji, kojima se vrši redirekcija adresa sajtova, ponajviše legitimnih hakovanih sajtova.

Takođe prema izveštaju ENIS-e za 2013 godinu [4], registruju se efekti pet osnovnih kategorija incidenata: Prirodni fenomeni, Ljudske greške, Maliciozni napadi, Sistemske greške i Kvarovi kao posledica delovanja treće strane. Pokazuje se da u poslednje tri godine, učešće malicioznih aktivnosti prouzrokuje sve veće vreme zastoja u raspoloživosti IS, gde se za 2013 godinu, zastoji prouzrokovani malicioznim aktivnostima približavaju vrednosti 50% ukupnog zastoja. Iz ovoga direktno sledi značaj borbe protiv maliciozih aktivnosti na mreži, koje tako prouzrokuju i proporcionalni nivo štete po IS.

U Izveštaju CISCO 2015 [5], stoji da je oko 1%, malicioznih aktivnosti i direktno korišćeno za napade na IS. *BlackHole*, ostaje daleko najeksploatisanija maliciozna pretnja. Takođe, u značajnoj meri (oko 34%) smanjenja je registrovano u Java aplikacijama, što značajno podiže nivo pouzdanosti jezika. Uočava se nagli porast *Spam* softvera, tokom 2014 godine i to za oko 240% u periodu Januar-Novembar 2014.

Očigledna je potreba da se korporativni, a i svi drugi važni sistemi zaštite od mogućih napada ili pretnji, što je i osnovna funkcija ***TND* sistema za detekciju i prevenciju kiber napada.**

IV. VRSTE IPS SISTEMA

Postoji više vrsta IPS sistema, koji obezbeđuju detekciju i prevenciju od napada na informacione sisteme. Obzirom na princip rada IPS-a, mogu se svrstati u tri tipa sistema za detekciju i prevenciju od Kiber napada [1]:

Serverski tip. Kod serverskog tipa zaštite IPS je instaliran na branjenom resursu. Sam program zaštite se izvršava na istoj mašini na kojoj se realizuju svi procesi servera. Na ovaj način se značajno koriste resursi servera, kako procesorski tako i memorijski i to može biti i do 40% resursa servera. Takođe u okviru IPS programa, nalaze se i sve potrebne baze podataka za realizaciju odluke. Baza podataka se periodično osvežava. Ovaj tip je IPS-a je potencijalno veoma brz, pod uslovom da na vreme detektuje napad vrlo brzo i reaguje na isti bilo slanjem izveštaja bilo odbrambenom reakcijom. Takav tip odbrane je vidljiv napadaču te je moguće napasti sam IPS, bilo blokadom rada bilo napadom na njegove interne baze podataka. Relativno kašnjenje u osvežavanju baze poznatih malicioznih kodova kao i jednostavni algoritmi za prepoznavanje novih vrsta napada čine ovaj tip IPS osetljivim na potpuno nove napade kao i na DDOS napade.

Gateway tip. Kod Gateway tipa zaštite, između servera klijenta i Interneta se postavlja *gateway* sistem koji filtrira i kontroliše saobraćaj. Ova vrsta IPS sistema je tradicionalna i prilično je zastupljena kod najvećih proizvođača opreme i rešenja. S obzirom da zahteva svakodnevno nadziranje, podešavanje i kontrolu pretpostavlja neprekidan angažman profesionalnog osoblja. U velikim i složenim dinamičnim sistemima, sa različitim IT servisima mora se svakodnevno simhronizovati rad svih korisnika sistema. Prilikom filtriranja dolazi do usporavanja jer se skeniranje vrši na samom linku. Ovaj vid zaštite pati od nekoliko nedostataka. Pre svega, usporava se protok paketa na linku. Stvara se vendor zavisnost od isporučioca *gateway* uređaja, koji su obično i isporučioci mrežne opreme. Potrebno je investirati u opremu od odgovarajućeg proizvođača, šro je poseban trošak. Potrebno je administrirati i održavati opremu *gateway*-a (potreba za administratorom sistema, obuka, svakodnevno nadgledanje, podešavanje i slično…). Svakodnevno se vrši daljinsko ažuriranje baze podataka malicioznih programa. Takođe, omogućen je daljinski pristup od strane vendora ili integratora, što potencijalno može povećati nivo pretnji.

Tows Net Defender pristup. Pristup je jedinstven po tome što za razliku od konvencionalnog serverskog pristupa, TND pristup koristi virtuelni uređaj (*Towers Net Server*), kome se šalju svi logovi posebnom tunelskom kodiranom vezom, a instalirani agentski program na serveru vrši analizu saobraćaja, detekciju i po potrebi izvršava komandu blokiranja, ako se utvrdi da je došlo do pokušaja napada na sistem. Pri tome, minimalno se usporava rad servera, čak i kada detektuje-blokira napad. TND IPS je nevidljiv za napadače čime se obezbeđuje njegova izuzetna elastičnost i otpornost na sve pokušaje ometanja ili blockade. Ukupna cena posedovanja TND je veoma optimizovana, prestaje potreba za administriranjem i obukom lokalnog kadra, kao i dodatnim troškovima s'tim u vezi. Važna je i karakteristika potpune vendorske neutralnosti servisa.

V. KARAKTERISTIKE IPS-A NOVE GENERACIJE

IPS sistemi nove generacije, obezbeđuju neke bitne karakteristikue, olakšavajući primenu, na način da se radi pametnije- ne napornije, u svrhu dinamičke odbrane.

Automatizovana procena uticaja. Nije neuobičajeno za IPS uređaje da kreiraju stotine bezbednosnih događaja dnevno. Kada uzmete u obzir da jedno tradicionalno preduzeće može imati desetine IPS uređaja ili više, provera hiljada bezbednosnih događaja svakog dana doslovno je nemoguća i može realno proizvesti beskoristan IPS, zato što će on biti ignorisan. TND kao IPS Sledeće generacije, s druge strane, povezuje pretnje i informacije sa krajnje tačke kako bi smanjio operativne bezbednosne događaje za 95 procenata i više. Jednom detektovan napad na bilo kojem od servera u mreži biće prosleđen automatski svim ostalim i na taj način potpuno redukovati sve potencijalne buduće događaje koje bi taj napad izazvao na celoj mreži.

Automatsko fino podešavanje. Svaka mreža je različita. Prilagodite vašu IPS politiku detekcija sa pravilima važnim za vašu organizaciju. Ako je politika detekcije suviše mala, IPS neće nuditi adekvatnu zaštitu. A ako je prevelika, može previše opteretiti IPS i izazvati smanjen protok mreže i povećano kašnjenje. TND kao IPS Sledeće generacije može pasivno odrediti profil vaše mreže i automatski preporučiti koja pravila omogućiti a koja

isključiti u intervalu koji odredi korisnik (na primer, nedeljno ili mesečno).

Praćenje identiteta korisnika. Kakva je korist od neke IP adrese za uređaj krajnjeg korisnika u odnosu na bezbednosni događaj ili događaj usklađenosti ako ne znamo ko je napadnut ili ko krši IT politiku firme? Umesto detaljnog pregledanja evidencija DHCP i Aktivnog direktorijuma da bi se ručno uparili korisnici sa IP adresama, TND kao IPS Sledeće generacije će obezbediti da se identifikuje IP adresa i korisnika odakle je napad došao. Vreme koje je potrebno da se poveže korisnik sa bezbednosnim događajem može biti smanjeno sa jednog sata na manje od jedne sekunde.

VI. METODE DETEKCIJE NAPADA

Postoji više metodologija detekcije pretnji. Obično se više vrsta detekcije kombinuju u cilju postizanja preciznije i detekcije šireg dijapazona pokrivanja anomalija. Glavne metodologije su sledeće [1]:

Sugnature-based, metoda bazira na poređenju poznatih pretnji, čije su karakteristike dobro poznate, da utvdi incident na posmatranom događaju. Ovo je vrlo efikasan pristup za detekciju poznatih pretnji, ali neefikasan u detekciji nepoznatih pretnji ili složenijih varijanti poznatih pretnji. Ovaj vid detekcije ne uspeva da prati i otkrije incidente u slučajevima kompleksnih događaja u mreži.

Anomaly-based detection, bazira svoju funkcionalnost na komparaciji posmatrane aktivnosti sa uobičajenim aktivnostima na mreži, u cilju otkrivanja anomalije. Metod formira profil tipičnih aktivnosti tokom vremena. IPS potom komparira karakteristike konkretne aktivnosti sa formiranim pragom odlučivanja, formiranim na bazi formiranih tipičnih profila. Ovaj vid detekcije je veoma efikasan kada se radi o predhodno nepoznatim pretnjama.

Stateful protocol analysis, metoda bazira na predeterminisanim profilima prihvatljivih protokolarnih aktivnosti u svakoj fazi aktivnosti protokola, sa posmatranim događajem u cilju identifikacije devjacije. Stateful analiza pruža mnoge efikasne mogućnosti za detekciju, a koje nisu prisutne u predhodne dve metode.
Towers Net Defender u svom funkcionisanju koristi sve tri metode detekcije pretnji.

VII. TND IPS Sledeće generacije ili načini smanjenja ukupne cene posedovanja

Koje su prednosti TND-a, kao IPS-a sledede generacije, objasnidemo opisom deset načina kako da se smanji ukupna cena posedovanja (TCO) IPS-a. Kada procenjujemo cenu nekog mrežnog IPS-a, ne samo da je važno proceniti troškove nabavke i naknade godišnjeg održavanja, već i cenu puštanja u rad i održavanja IPS-a, baze podataka, kao i licenciranja – što često predstavlja vedi deo ukupne cene posedovanja (TCO) tokom trogodišnjeg ili petogodišnjeg perioda. Takođe, jako je važno prepoznati elemente vendor zavisnosti i šta to znači sa aspekta očekivanog srednjeg vremena života hardvera koji čini sastavni deo IPS-a ili mogudnost redovne i efikasne nadogradnje softvera u sklopu IPS-a. IPS Sledede generacije nudi bolju zaštitu mreže u realnom vremenu, zaštitu aplikacija, kontroliše ponašanje korisnika i rastereduje sistem i korisnika automatizacijom ključnih IPS funkcija. Ovakvo podizanje nivoa mogudnosti IPS-a pruža neuporedivo veći uvid, smanjujući oslanjanje na druge IT timove i omogućuje potpunu automatizaciju ključnih IPS funkcije koje tradicionalni IPS jednostavno ne može. TND kao IPS Sledede generacije ima brojne prednosti nad tradicionalnim IPS-a i to:

- Jača zaštita mreže,
- Vrhunske performanse,
- Neprekidna automatizovana mogućnost nadogradnje,
- Neprekidna dostupnost,
- Veoma jednostavnija primena i tekude održavanje,
- Niža ukupna cena posedovanja.

Ukupna cena posedovanja (TCO – *Total Cost of Ownership*) sadrži sve troškove vezane za nabavku, puštanje u rad, održavanje i rad sistema – u ovom slučaju, mrežnog IPS-a. Preko snažne automatizacije i kompleta naprednih funkcija TND, kao IPS Sledede generacije, značajno smanjuje i TCO – u mnogim slučajevima povraćaj svih troškova IPS –a u veoma kratkom roku putem drastičnih smanjenja u operativnim troškovima.

Deset načina za smanjenje TCO kupovinom TND kao IPS Sledeće generacije:

1. **Smanjite smetnje uz pomod procene uticaja**. Poređenjem pretnji i informacija krajnje tačke u realnom vremenu TND može smanjiti količinu operativnih bezbednosnih događaja za 95 procenata ili više. Na primer, zašto istraživati *Conflicker* događaj koji ošteduje samo *Windows* matične računare kada pokušava napad na *Linux* računar?
2. **Izbegnite nagađanje uz pomoć automatizovanog finog podešavanja IPS-a**. TND zna koji program radi na vašoj mreži i može da primeni IPS pravila koja će da uključi i isključi, što za rezultat ima povećanu zaštitu, optimizovan rad IPS senzora. Nakon uvođenja u rad IPS će brzo prepoznati sve korisne i prijateljske programe na mreži koje će isključiti iz neprekidne provere i skeniranja. Kao rezultat toga imamo veoma optimizovane izveštaje kako urgentne tako i redovne mesečne što stvara velike uštede jer administratorima ne oduzima dragoceno vreme.
3. **Povežite korisnike na bezbednosne događaje i događaje usklađenosti**. Šta vredi da znamo da je 192.168.4.12 pod napadom ako ne znamo koga da kontaktiramo? TND trenutno javlja podatke za kontakt korisnicima koji se bave bezbednosnim događajima i događajima usklađenosti, eliminišudi potrebu da manuelno pretražuju kroz evidencije Aktivnog direktorijuma, LDAP-a i DHCP-a. Ako je IPS urađen na tradicionalni način,

napad može biti završen i pre nego što znate gde treba da gledate!

4. **Imajte jednu platformu za fizičke i virtuelne IPS**. TND kao jedna jedinstvena vendor nezavisna platforma, za razliku od klasičnih IPS sistema koji kombinuju skupi hardver i virtualni softver te imaju potrebu za dnevnim ažuriranjem i nadzorom IPS-a, eliminiše potrebu za dupliranjem izveštaja, upozorenja, kontrolnih tabli i odeljenja za tehničku podršku.

5. **Prilagodite IPS pravila za licencirane aplikacije i sisteme**. Sa TND sistemom nemate potrebu da trošite novac na zaštitne zidove *web* aplikacija (WAF) ili druge proizvode mrežne bezbednosti da urade posao umesto TND-a IPS-a Sledede generacije.

6. **Uklonite mrtve uglove mreže preko provere svih pristupnih logova.** Poboljšajte vaš bezbednosni status dešifrovanjem svih pristupnih logova tokom IPS provere.

7. **Smanjite površinu izloženu napadu uz pomod pravila za usklađenost i belih lista**. TND kao IPS Sledeće generacije vam može pomoći da oblikujete i sprovedete politike prihvatljivog korišdenja (AUP - *Accepted Usage Policies*). Iskoristite prednosti usklađenih pravila i belih lista kako biste smanjili površinu mreže izloženu napadu.

8. **Otkrijte unutrašnje pretnje koje vaš IPS može prevideti**. Perimetar standardnog IPS će prevideti svaku zloupotrebu koja je ručno uneta kroz glavni ulaz firme na mobilnom računarskom uređaju. Poboljšajte svoj status dubinske odbrane primenom Analize ponašanja mreže (NBA – Network Behaviour Analysis) kako biste postavili osnovne postavke normalnog mrežnog saobradaja i otkrili anomalije.

9. **Poboljšajte bezbednost kontrolisanjem širenja VM (VM - *virtual machine*).** Treba da znate kada se na mreži pojave nove VMware, Xen ili neke druge vituelne mašine (VM) i bez znanja ili odobrenja IT bezbednosnog tima. Proverite nove VM za usklađenost sa internim bezbednosnim politikama. Ovo će vam pomoći da imate kontrolu nad vašom VM infrastrukturom.

10. **Integrišite vaš IPS na postojeću bezbednosnu infrastrukturu.** Unapredite postojeće investicije u *Security Information and Event Management* (SIEM), upravljanje ranjivošdu, mrežnu forenziku, kontrolu pristupa mreži (NAC – *Network Access Control*) i u druge infrastrukturne komponente kako biste delili informacije, automatizovali sanaciju i ubrzali odgovor na incident.

VIII. TEHNIČKE KARAKTERISTIKE

SAVREMENIH IPS-A

Od svaremenog IPS-a nove generacije [3], očekuje se neprekidan monitoring, po principu : 24/7/365. Detekcija i prevencija od napada, branjenog resursa/blokiranje kiber napada, imunog na sve poznate maliciozne pretnje-napade kao i detekcija potencijalnih malicioznih napada i njihovo sprečavanje u delovanju [2].

Ovde treba napomenuti da se sa IPS-om, zajedno sa *Antivirus* programom i *Firewall* sistemom, stvaraju uslovi za potpunu odbranu informacionog sistema od malicioznih aktivnosti. Dakle IPS je pre svaga namenjen za teške napade na informacioni sistem, koje ne podržavaju ostale komponente zaštite IS.

IPS treba pravovremeno da generiše izveštaje, o svim događajima od značaja za prevenciju i sprečavanje napada. Takođe, obavezno je automatsko generisanje i slanje izveštaja o napadu, Sertifikat uspešne odbrane.

Savremeni IPS treba da omogući da se na osnovu realizovane prakse, vrši procena rizika, periodične procene rizika, slabosti sistema, sve na osnovu monitoringa IPS-a. Na osnovu ovakvih podataka, vrše se fina podešavanja na sistemu, minimizacija rizika i otklanjanje slabosti, kao i fino podešavanje sistema, prema stvarnim potrebama korisnika.

Savremeni IPS nove generacije treba da brani sistem od sledećih malicioznih pretnji:

- *SYN* poplave,
- *DoS/DDoS* napadi
- Napadi nultog dana (*Zero day attack*)
- Napredne istrajne pretne: *Brutal-force attack*;
- *SQL Injection*;
- *Cross-site scriprting* (XSS),
- Rootkit attacks.
-

Ciljne platforme na koje se primenjuje savremeni IPS su: web serveri, mail serveri, file serveri, PC serveri i svi serveri koji imaju pristup Internetu.

Operativni sistemi koje je potrebno podržati su:

- svi distribuirani od strane Linux-a
- besplatni BSD (sve verzije)
- otvoreni BSD (sve verzije)
- net BSD (sve verzije)
- Solaris 2.7, 2.8, 2.9, 10 i 11
- AIX 5.3, 6.1 i 7.1
- HP-UX 10, 11 i 11i
- Windows 7, 8, Vista, XP i 2000
- Windows Server 2012, 2008 i 2003
- MacOSX 10
- VMWare: VMWare ESX 3.0, 3.5, 4.0, 4.5, 5 i 5.5 uključujući i CIS provere.

VII. ZAKLJUČAK

Treba imati u vidu činjenicu da je potreba za zaštitom od kiber napada svakim danom sve veća, obzirom na svakodnevno narastanje bezbednosnih izazova, koji se dešavaju na Internetom povezanim informacionim komponentama.

Cena štete koja može nastati može biti višestruko veća od cene koja se ulaže u zaštitu. Ovo se pre svega odnosi na javne informacione sisteme, koji svoju uslugu daju velikom broju ravznorodnih korisnika. Takođe, vrednost pohranjene arhivske građe i dokumentacionog materijala može biti veoma velika, pa se njenim uništenjem ili oštećenjem mogu naneti nenadoknadivi gubici.

Uloga IPS-a u detekciji i prevenciji od kiber napada u tom smislu postaje nezaobilazna. Takođe, IPS sistemi se svakodnevno usvršavaju i postaju spremni za funkcionisanje u narastajućem rizicima opterećenom okruženju.

VIII. LITERATURA

[1] Guide ti Intrusion Detection and Prevention Systems, NIST, Special Publication 800-94.
[2] Zoran Živković, STANJE IB u SVETU I SRBIJI, GLOBALNI ASPEKT, Konferencija o Inf. Bezbednosti, Beograd, Juni 2013.
[3] Towers Net Defender - Technical Specification, July 2014.
[4] ENISA – ANNUAL INCIDENT RESPORTS 2013, September 2014.
[5] CISCO – 2015 ANNUAL SECURITY REPORT, Cisco.
[6] Gartner – 2014 ANNUAL SECURITY Prediction, Gartner
[7] Sophos – 2013 ANNUAL SECURITY REPORT, Sophos
[8] Zoran Zivković,DIBS, Novi bezbednosni izazovi –Kiber rat ili kiber mir. Infofest, Budva 2014
[9] Zoran Zivković,DIBS, Novi bezbednosni izazovi –Kiber rat ili kiber mir. Infofest, Budva 2014
[10]SlobodanR.Petrović,prof.dr.DIBS,Kiber moć u kontekstu nacionalne bezbednosti, Konferencija Informaciona Bezbednost Srbije 2013

Abstract

Abstract. The paper gives a basic classification of cyber attacks against information systems, as well as the most important characteristics of attacks in recent years. Classification of IPS (Intrusion Prevention System) based on the mode of operation, as well as detection methods are shown. In following, some key technical characteristics are presented to meet the characteristics of new generation IPS.

NEW CYBER SECURITY CHALENGES OF INFORMATION SYSTEMS – PLACE AND ROLE OF INTRUSION PREVENTION SYSTEMS

Zoran Živković, Mr, DIBS, Milenko Ostojić, Ph.D.E.E., Towers Net, Nataša Simić,Mr, Towers net