Upotreba sistema za otkrivanje i sprečavanje neovlaštenih pristupa u centrima podataka

Srđan Nogo
Elektrotehnički fakultet, Univerzitet u Istočnom Sarajevu
Istočno Sarajevo, BiH
srdjan.nogo@gmail.com

Sažetak— ***Centri podataka izloženi su raznim metodama ugrožavanja bezbjednosti koji postaju sve teži za otkrivanje i umanjivanje njihovog pojavljivanja. Napadi i zlonamjerne aktivnosti mutiraju u skladu sa razvojem IT usluga i tehnologije. U savremenim javno-privatnim organizacijama, IT infrastruktura i aplikacije postaju ključne komponente u poslovnim procesima ili elektronskim javnim uslugama. Blokiranje ili kompromitovanje IT usluga može izazvati ekonomsku štetu ili narušiti ugled, što je za jednu organizaciju neprihvatljivo. U ovome radu detaljno ćemo opisati pristup "dubinske odbrane" koja ima za cilj da obezbjedi slojevito, distribuirano i raznovrsno bezbijednosno rješenje primjenom više bezbijednosnih tehnologija sa različitim mogućnostima inspekcije i kontrole na različitim mjestima u mreži.***

Ključne riječi-Intrusion Detection and Prevention System-IDPS ; ***SQL injection***; ***Iframe tags***; ***(key words)***

I. UVOD

U proteklih nekoliko godina, kada analiziramo zaštite centara podataka primjećene su sigurnosne prijetnje koje se po svojim karakteristikima mijenjaju u sve manjim i manjim vremenskim periodima. Najsavremeniji vektori prijetnji su sve sofisticiraniji i uglavnom kao ciljnu grupu imaju napad na aplikativni nivo koji kao krajnji cilj imaju neovlašten pristup podacima. Sve je više zlonamjernih web softvera koje koriste tehnike poput *SQL injection, iFrame injection, Javascripts* kao i mnogobrojni kompromitovani reklamni slogani koji nas ometaju u optimalnom korištenju web prostora.

II. VRSTE NAPADA

A. Tehnika ubrizgavanja

Pojam ubrizgavanja (eng.injection) podrazumjeva nešto što je insertovano od strane treće strane u Web sajt organizacije koja pruža web usluge. Najčešći primjer ubrizgavanja jeste "*SQL injection*", što predstavlja ubrizgavanje u samu bazu podataka koja služi kao resurs podataka samoj aplikaciji. Kao što je opšte poznato SQL je jezik koji se najčešće koristi za programiranje i pristup bazi podataka i samim time ova vrsta napada je najčešća od strane zlonamjernih korisnika. Ova vrsta napada najčešće je omogućena od strane nemarnih developera koji nisu primjenili minimalne tehničko bezbjedonosne korake prilikom razvoja web sajta. Ovim gore navedenim pristupom oni vrlo lako rizikuju mogućnost da ostave zadnja vrata (*eng.Backdoors*) otvorena da zlonamjerni korisnik može da kroz njih infiltrira nasumične podatke u samu bazu podataka, [1]. Vrlo često se dešava najgori scenario kod ove vrste napada da se pojedine baze podataka isisaju kroz (eng. Backdoors) zajedno sa svim povjerljivim podacima koji se nalaze u bazi podataka, [2]. Vendor koji pruža web usluge čuvanja pojedinih specijalizovanih podataka u svojim bazama podataka dolazi u situaciju da izgubi povjerenje klijenata jer pojedini povjerljivi podaci mogu biti predmet zloupotrebe od strane trećih lica.

B. IFrame ubrizgavanje

Iframe ubrizgavanje predstavlja ubrizgavane jednog ili više Iokvir oznake (*eng.Iframe tags*) u sami sadržaj stranice. Kod ove vrste napada koji kompromituje sistem korisnika koristi se metoda da *IFrame* učini zlonamjernu akciju. Navešćemo jedan primjer ovoga napada a to je da se bez odobrenja korisnika izvrši *download* jednog ili više izvršnih fajlova koji sadrži viruse ili crve. Djelimično ovaj problem je riješen upotrebom najnovijih verzija internet pretraživača koji posjeduju sigurnosne mehanizme odbrane od ovoga napada. Ti mehanizmi impliciraju se tako da se korisniku ponudi opcija da li želi da instalira specijalizovani softver na svoj računar sa zabranom automatske instalacije izvršnih fajlova bez odobrenja korisnika. Ako imamo u vidu stanje u praksi da većina običnih korisnika ne vrše redovno ažuriranje svog korisničkog okruženja na internet pretraživačima koji imaju malo stariji datum izlaska u web okruženje imamo ozbiljan problem kada je u pitanju ova vrsta napada. Razlog je vrlo jednostavan internet pretraživači ranijih godina bilu su mnogo povjerljiviji kada su u pitanju ove vrste ponuda instalacije novih softvera za krajnje korisnike a koji su se automatski preuzimali sa web sadržaja.

C. Elementi bezbjednosti

U predhodnom paragrafu naveli smo dva scenarija, tradicionalni elementi za bezbjednost uređaja zaštitni zidovi *(eng. Firewalls*) nisu dovoljni da zaštite imovinu i usluge provajdera ili organizacije.

Potrebno je da se obezbjede sofisticiraniji elementi zaštite sistema koji bi trebalo da obuhvataju pregled nivoa 4-7 protokola sa posebnim fokusom na nivo aplikacije. Ovaj pristup može se obezbjediti principom primjene tkz. "Dubinske odbrane" što je danas opšti trend. Pristup "Dubinska odbrana" ima za cilj da obezbjedi slojevito, distribuirano i raznovrsno bezbijednosno rješenje primjenom više bezbijednosnih tehnologija sa različitim mogućnostima inspekcije, kontrole i na različitim mjestima u mreži. Ovakvu vrstu odbrane može da obezbjedi samo sistematičan pristup koji se naziva ***Intrusion Detection and Prevention System-IDPS.***

Na osnovu gore navedenog, IDPS sistemi predstavljaju važnu bezbjedonosnu komponentu koju treba integrisati sa tradicionalnim bezbjedonosnim uređajima (zaštitnim zidovima, aplikacijskim proksijima itd.). Provajderi i organizacija može imati koristi od uvođenja senzorske mreže, a koje se tiču razvijanja svijesti o prijetnjama, mogućnosti otkrivanja i sprečavanja kao i mogućnost monitoringa napada.

III. TEHNIKE OTKRIVANJA NEOVLAŠTENOG PRISTUPA

Termin „*otkrivanja neovlašćenog pristupa"* identifikuje proces monitoringa događaja i obrasce za saobraćaj u mreži i analizira da li se pokazuju znakovi mogućih bezbjednosnih incidenata. Incidenti predstavljaju narušavanje bezbjednosti ili neposredne prijetnje kršenju bezbjednosne politike računara, prihvatljive politike korišćenja ili standardne prakse bezbjednosti. Postoje mogućnosti automatizovanja procesa zaštite kroz korištenje softvera ili uređaja koji se naziva opštim imenom Sistem otkrivanja neovlašćenog pristupa (*eng. Intrusion Detection System*)- IDS. Ovakav sistem IDS omogućava *on line* zaštitu u realnom vremenu dijelova sistema u kojima se nalaze senzori i omogućava da se identifikuju i zaustave akcije čiji cilj je kršenje ili ugrožavanje računarskog sistema uređaja ili mrežne infrastrukture. IDS je u stanju da primijeni niz tehnika za identifikovanje anomalija i mogućih prijetnji na nivou mreže, na nivou aplikacija i ako je potrebno blokira prijetnje koje smatra opasnim i istovremeno umanji broj lažnih uzbuna, [4].

Kod tehnike IDS otkrivanja neovlaštenog pristupa odnosno "anomalija" imamo glavne tehnike i to:

Anomalije protokola, senzori analiziraju tok i identifikuju svaku anomaliju na protokolima koji se obično koriste u IP mrežama, u skladu sa definicijama koje su propisane standardom, poput (*eng. Request for comment*)- RFC koju izdaje (*eng. Internet Engineering Task Force*)- IETF za otvorene protokole.

Otkrivanje zasnovano na potpisu, sistem je u mogućnosti da primijeni analizu zasnovanu na potpisu u dobro definisanim aplikativnim okruženjima koja se odnose na tu vrstu potpisa npr. određeni potpis se može odnositi samo na (*eng.Domain Name System*)- DNS saobraćaj ali ne i na druge vrste saobraćaja. Sistem ukoliko je propisno konfigurisan, može vezati različite potpise za različite tokove saobraćaja koji pojedinačno gledano ne predstavljaju napade ali njihova kombinacija može biti otkrivena kao mogući neovlašteni pristup.

Otkrivanje preko „zadnjih vrata" *(eng. backdoor*), sistem može otkriti prisustvo „*backdoors*" na sistemima analizom interakcije unutrašnjeg i vanjskog sistema, upotrebom analize interaktivnog saobraćaja između klijenata i servera na standardnim i nestandardnim portovima.

Analiza saobraćaja, senzori mogu uočiti anomalije u mrežnom saobraćaju koje nisu u vezi sa određenom vrstom napada na aplikaciju npr. skeniranjem mreže ili porta.

„Zamke" na mreži (*eng. network honeypots*), Sistem može da obezbjedi konfiguraciju zamke koja bi oponašala tražene usluge koristeći mrežni mehanizam skeniranja i eventualno identifikovala izvor napada.

Zaštita Syn-Flood, Sistem štiti od (*eng.Denial of Service*)- DoS napada koristeći mehanizam za detekciju *Syn-Flood,* najčešće sesije u kojima se dešavaju „poplave" sesija koje nisu u stanju da izvrše trostruko rukovanje (*eng. 3-Way handshake*).

Otkrivanje „Spoofing-a", Sistem je u stanju da otkrije saobraćaj izmanipulisanim IP-om. Najčešće, ovaj tip napada je napravljen kako bi obmanuo sistem zamjenom IP-a koji nije dozvoljen sa dozvoljenim IP-om.

IV. SMJERNICE ZA PRIMJENU IDPS-A

Postoje tri osnovna parametra na koje trebamo da obratimo posebnu pažnju prilikom primjene mrežnog IDS-a ili IPS-a i to :

- bezbjednost
- prevencija
- učinak

A. Parametar bezbjednost

Administratori zaduženi za bezbjednost najčešće primjenjuju IDS ili IPS u sljedećim slučajevima:

- U svakom hostu u mreži kako bi zaštitili hostove za koje se zna da su osjetljivi na poznate napade u cilju identifikacije napada.

  Ovo posebno treba da se odnosi na nove hostove koji se naknadno dodaju u mrežu i hostove koji su podložni napadima prema predhodnim monitorinzima mreže.

- U svakoj unutrašnjoj tački mreže kako bi se zaštitili vanjski perimetri mreže.

- Na tačkama mrežnog perimetra u kojima dolazi do zagušenja kako bi se obezbjedila metoda za otkrivanje ili prevenciju mrežnih napada zasnovana na potpisu ili anomaliji, uz klasične kontrole zasnovane na politici koje provode drugi uređaji za bezbjednost mreže.
- U blizini svake tačke tj. sredstva koje je od posebnog značaja za organizaciju.

B. Režim prevencije ili otkrivanja

Prilikom upotrebe IPS senzora, neophodno je da administrator za bezbjednost i osobe zadužene za njeno planiranje odrede za cilj režim otkrivanja ili prevencije. Administratori za bezbjednost mogu konfigurisati potpise kako bi dobili agresivniju reakciju (blokiranje hostova ili odbacivanje paketa), kao i druge potpise kako bi upozorili ili prikupili sumnjive aktivnosti.

U praksi se pokazalo da je najefikasnija upotreba senzora u režimu prevencije kada je to tehnički izvodljivo. Tehničke mogućnosti automatizovanja sprečavanja napada u ovome režimu još je jedan razlog za upotrebu ove tehnologije. Ova tehnologija zahtijeva dodatne ljudske resurse (inžinjer sati) kada je u pitanju konfiguracija i stalno tuniranje postavljenog sistema za prevenciju napada u cilju optimalnog setovanja istog. Ovaj režim zahtijeva da senzori budu pravilno podešeni kako bi se postigao visok stepen preciznosti potreban za omogućavanje preventivnih aktivnosti.

Kod režima otkrivanja sistemi imaju mogućnost slanja signala uzbuna administratorima kao i mogućnost stalnog snimanja sumnjivih aktivnosti na mreži. Režim otkrivanja primjenjuje se u dva slučaja, prvi ako se organizaciona mreža suoči sa previše lažnih uzbuna da bi se podesila senzibilnost sistema i to se naziva- Monitoring kritičnih sistema. Drugi gdje je moguće poboljšanje senzitivnosti senzora da bi otkrili što je moguće više sumnjivih i zlonamjernih aktivnosti- Monitoring na segmentima mreže. Ovim drugim pristupom povećava se rizik od povećanja broja lažnih uzbuna. Stoga, administratori često primjenjuju kombinaciju sa drugim senzorom koji funkcioniše u režimu prevencije a podešen je da ima veoma nisku stopu lažnih uzbuna, ovakvim pristupom dobijamo izbalansirani primarni senzor u režimu otkrivanja.

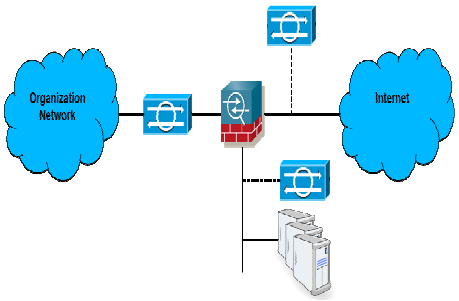
C. Uticaj učinka

Potreba određenih akcija administratora nad sistemom pružiće odgovarajući učinak u mrežnom okruženju u kojem će optimalno funkcionisati. Kada govorimo o učinku tri su osnovna kriterija ili pitanja koja administratori mogu i trebaju da koriste prilikom primjene IPS ili IDS senzora i to:

- *Konekcije u sekundi*, analiza stope broja sesija na aplikaciji može biti ključna za izbjegavanje potencijalnih „uskih grla“.
- *Kašnjenje i ometanje*, to je mogućnost zaobilaženja senzora kod rada aplikacija u realnom vremenu ukoliko je to u skladu sa minimalnim zahtjevima koji su propisani bezbednosnom politikom. Primjer aplikacije koja je osjetljiva na kašnjenje i ometanje je HD video konferencija.
- *Produktivnost,* saobraćajni obrasci i svojstva koji se u velikoj mjeri razlikuju u pogledu stope prenosa paketa i veličine paketa, obično podrazumijevaju potrebu za administratorskom intervencijom koji će izabrati senzor sa većim učinkom da bi se izbjegla uska grla u samom funkcionisanju.

D. Smjernice za implementaciju mrežnog IPS-a

Edge Internet je dio provajdera ili mrežne infrastrukture organizacije koji obezbjeđuje povezivanje na Internet. Edge internet je mrežna infrastruktura direktno povezana na internet i naročito je izložena velikom broju vanjskih prijetnji, tako da sveobuhvatne bezbjednosne mjere treba da budu implementirane do tog trenutka, uključujući i otkrivanje neovlašćenih pristupa i njihovo sprečavanje. Generalno, osnovna kontrola podrazumijeva odvajanje manje pouzdane mreže od interne mreže organizacije ili provajdera u različite domene bezbjednosti. U ovome navedenom slučaju, manje pouzdana mreža je internet mreža ili mreža poslovnih partnera. Sistem zaštitnog zida (ili u ovom slučaju, granica mrežne bezbjednosti) obično je kombinacija bezbijednosnih kontrola na mreži kao što je prikazano na “Sl.1”. Mrežni IDS ili IPS je zajednička komponenta unutar sistema zaštitnog zida koja kontroliše pristup između domena i provodi željenu politiku pristupa.



Slika1: Primjer mrežnog IPS-a

Uobičajeno je i najpreporučljivije instalirati IPS senzore mreže na strani aktivne komponente zaštitnog zida koja je pouzdanija ali moguće je da to nije i najoptimalnije rješenje za sve organizacije. Drugi pristup je da koristimo mrežnu identifikaciju ili IPS analizu na nepoznatom (vanjskom) segmentu primjene mreže za praćenje saobraćaja "u divljini" ili otkrivanje i sprečavanje napada i pokušaja prije nego što oni pogode glavne komponente za filtriranje zaštitnog zida.

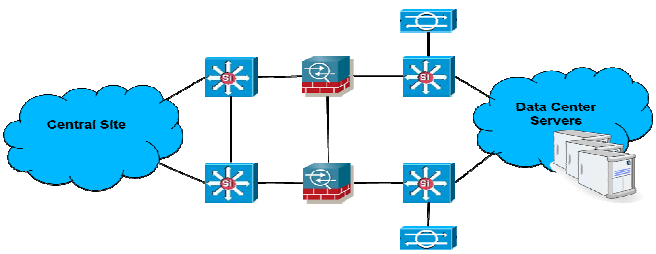
Ovakav monitoring je koristan za otkrivanje novih oblika napada, novih trendova u napadima i sirovih podataka koji mogu biti u vezi sa drugim senzorima. Ovaj senzor je obično vrlo osjetljiv i podešen da smanji šum i najosnovnije lažne uzbune, [4].

Generalno, IPS monitoring mreže koristi se na pouzdanom (unutrašnjem) segmentu mreže za otkrivanje napada koji bi mogli proći sa nepouzdane na pouzdanu stranu. IPS monitoring može se koristiti da se spriječe sumnjivi ili zlonamjerani mrežni saobraćaj da napusti intranet mrežu. Senzor ili senzori koji se primjenjuje na ovaj način obično je konfigurisan da radi u modu prevencije i setovan je za prihvatljivo niske stope lažnih uzbuna. Postoje i slučajevi u kojima su senzori postavljeni na pouzdanim i na nepouzdanim segmentima mreže korišćenjem tehnike korelacije. Senzori uzajamno povezuju događaje kako bi mogli da ukažu koji napadi su prošli kroz druge bezbijednosne komponente na mreži između dva senzora.

E. Centri podataka i framework IDPS-a

Centri podataka izloženi su raznim metodama ugrožavanja bezbjednosti koji postaju sve teži za otkrivanje i umanjivanje njihovog pojavljivanja. Napadi i zlonamjerne aktivnosti mutiraju u skladu sa razvojem IT usluga i tehnologije. U savremenim javno-privatnim organizacijama IT infrastruktura i aplikacije postaju ključne komponente u poslovnim procesima ili elektronskim javnim uslugama. Blokiranje ili kompromitovanje IT usluga može izazvati ekonomsku štetu ili narušiti ugled, što je za jednu organizaciju neprihvatljivo. U centrima podataka potrebno je primjeniti pristup "dubinske odbrane" koja ima za cilj da obezbjedi slojevito, distribuirano i raznovrsno bezbijednosno rješenje primjenom više bezbijednosnih tehnologija sa različitim mogućnostima inspekcije i kontrole na različitim mjestima u mreži. [6].

Većinu ključnih aplikacija i podataka nekog provajdera ili organizacije čuvaju se u bazama podataka koje se nalaze u Centrima podataka "Sl.2". Po osnovnim načelima informatičkih principa centar podataka okrenut je ka unutrašnjosti i nalazi se u unutrašnjem dijelu Intraneta, a većina njegovih klijenata je na internoj mreži organizacije. Izuzetak pravilu bili bi centri podataka provajdera koji se eksterno obraćaju klijentima koji mogu biti potrošači ili preduzeća. U oba slučaja centar podataka izlaže se eksternim opasnostima ali se mora sačuvati i od realne opasnosti a to su napadi iznutra.



Slika 2: Jedan primjer centra podataka i framework IDPS-a

Postoje smjernice koje treba razmotriti prilikom izrade Framework mrežnih IDS-a ili IPS-a u centru podataka provajdera ili organizacije i to:

Centri podataka su dizajnirani za međusobnu interkonekciju velike brzine i visoke dostupnosti podataka, te je veoma važno obezbjediti da mrežni IPS senzori ne utiču na te funkcije i da su optimalno integrisani sa obližnjim mrežnim okruženjem. Korišćenje logičkih VLAN interfejsa na senzorima u mreži dizajner framework IPS rješenja imaju fleksibilnost da se bave različitim uslovima primjene. Od krucijalnog je značaja da se izvrši dobro skaliranje učinka i da se održava jednostavnost konfiguracije razmatranjem korišćenja određenih mrežnih IPS senzora ili virtuelnog konteksta za odgovarajuće aplikacije centra podataka. Centri podataka su po pravilu produkciona okruženja koja su pod kontrolom Sistema za upravljanje bazama podataka- RDBMS-a, tako da u kombinaciji sa IPS možemo lakše podesiti i primijeniti preventivne aktivnosti. Imajući u vidu gore navedeno dolazimo do zaključka da elementi IDP-a u kombinaciji sa IPS-om mogu obezbjediti sledeće opšte koristi:

- Bolju zaštitu imovine organizacije: IDP sistemi mogu kontrolisati mrežni saobraćaj dubinski od 3 do 7 nivoa, otkriti šablone određenih napada funkcijom podudarnosti potpisa i verifikovati usklađenosti sa standardima protokola.
- IDP sistemi skeniraju cjelokupan mrežni saobraćaj koji prolazi kroz senzore i mogu dati statističke podatke o tipovima saobraćaja i tokovima i poslati upozorenja ili obavještenja na osnovu pragova i međusobnih veza bezbijednosnih događaja koji se mogu konfigurisati.

Da bi ostvarili optimalnu zaštitu centara podataka potrebno je konfigurisati centralizovanu tačku otkrivanja i prevencije. U poređenju sa sistemom otkrivanja neovlašćenog pristupa putem hosta, mrežni IDPS pruža centralizovanu tačku otkrivanja i prevencije neovlašćenih pristupa jednostavnu za korištenje i administraciju. Ovim pristupom obezbjeđuje se dubinsko logovanje napada i zlonamjernih aktivnosti korisnika kao i funkcionalnost da IDPS obezbjeđuje detaljno logovanje sa informacijama na nivou aplikacije. Opcija memorisanja logova i alarma o napadu je od presudnog značaja prilikom dokazivanja napada. IDPS uključuje i elemente za zaštitu od odstupanja što omogućava identifikovanje i blokiranje pokušaja odstupanja od kontrole, [7].

Evaluacija prijetnji bezbjednosti i njihov uticaj na imovinu organizacije mogu se formalizovati uz pomoć principa za upravljanje rizikom. U nastavku ćemo usvojiti ovaj pristup za evaluaciju koristi od uvođenja IDP sistema u mrežnu infrastrukturu organizacije koja je zadužena za administraciju centara podataka. U skladu sa teorijom o upravljanju rizikom, koristi od uvođenja IDP sistema striktno su vezane za: efikasnost bezbijednosnih kontramjera, vrijednost imovine koja se štiti kao i uticaj uspješnog napada koji bi se pomoću novog sistema mogao blokirati i ublažiti, [3].

Kombinacija gore navedih elemenata određuje vrijednost određenog okruženja. Stoga je najbolji metod za procjenu koristi od novog bezbednosnog rješenja izrada analize rizika ciljanog okruženja i procjena načina na koji bi nove bezbijednosne kontramjere ublažile te rizike. Primjenjujući ovakvu metodologiju, možemo analizirati koje pozitivne efekte uvođenja IDPS rješenja mogu imati IT infrastruktura organizacije i njene on line usluge, [5].

Odnosno, pokušaćemo identifikovati, na kvalitativan način, koji su najviši rizici za IT infrastrukturu organizacije kao što je prikazano u Tabeli 1.

TABELA I Analiza učinka primjene IDPS-a

Imovina	Potencijalna prijetnja	Uticaj prijetnje	Vjerovatnoća prijetnje	Nivo rizika	Kontramjere uvedene putem IDPS
Baze podataka i evidencije	Neovlašćen pristup, krađa osjetljivih podataka, manipulisan je podacima	Visok	Srednja	Visok	Posebni potpisi za uobičajene napade na baze podataka (npr. SQL injection)
Interne web usluge	Neovlašćen pristup, DoS napadi	Visok	Niska	Srednji	Posebni potpisi za napade na aplikacije, zaštita od Syn-flood, korelacija
Javne internet web usluge	DoS i DDoS napadi, Neovlašćen pristup, napadi na usluge autentifikacije	Visok	Visoka	Veoma visok	Posebni potpisi za napade na aplikacije, zaštita od Syn-flood, korelacija
Email usluge	Spam, virusi, phishing	Nizak	Visoka	Srednji	Elementi anti-virus anti-spam, filtriranje sadržaja
Intrnet sajt	Defacement, DoS napadi	Nizak	Niska	Nizak	Posebni potpisi za napade na aplikacije, zaštita od Syn-flood, korelacije
Unutrašnji računari	Virusi, Trojanci	Srednji	Niska	Srednji-nizak	Anti-virus funkcije, i filtriranje sadržaja i URL

Ako analiziramo gornju tabelu, dolazimo do zaključka da bi se najbolji učinak i najviše koristi dobili primjenom IDPS-a za zaštitu internih i eksternih web servisa, kao i baza podataka provajdera ili organizacije. Ako uzmemo primjer provajdera koji objavljuje nove web usluge na internetu, preporučuje da se primijeni interfejs IDP sistema u internet edge segmentu kako bi se otkrili i spriječili opasnosti i napadi koji dolaze sa interneta.

V. ZAKLJUČAK

Centri podataka provajdera ili organizacije čuvaju većinu ključnih aplikacija i podataka tog provajdera ili organizacije. Kao što smo spomenuli u poglavlju IV, centar podataka okrenut je ka unutrašnjosti, a većina njegovih klijenata je na internoj mreži organizacije. Izuzetak pravilu bili bi centri podataka provajdera koji se eksterno obraćaju klijentima koji mogu biti potrošači ili preduzeća. Kao što je navedeno u predhodnim poglavljima ovoga rada, centri podataka izloženi su raznim metodama ugrožavanja bezbjednosti koji postaju sve teži za otkrivanje i umanjivanje njihovog pojavljivanja. Napadi i zlonamjerne aktivnosti mutiraju u skladu sa razvojem IT usluga i tehnologije. U savremenim javno-privatnim organizacijama, IT infrastruktura i aplikacije postaju ključne komponente u poslovnim procesima ili javnim uslugama. Blokiranje ili kompromitovanje web usluga može izazvati ekonomsku štetu ili narušiti ugled, što je za jednog provajdera ili organizaciju neprihvatljivo. Upotrebom IDPS rješenja imamo situaciju da su centri podataka zaštićeni od zlonamjernih upada trećih strana u cilju kompromitovanja podataka koji se nalaze u centrima podataka.

LITERATURA

[1] http://www.malware-info.com/ pristupljeno: 08.02.2016.)

[2] http://services.seekdotnet.com/knowledgebase/261/What-is-Iframe-Injection.html(pristupljeno: 08.02.2016.)

[3] https://businessresources.mt.gov/Portals/94/shared/IDP/docs/DataCenterIndustryAnalysis.pdf(pristupljeno: 08.02.2016.)

[4] Alazab, Ammar; Hobbs, Michael; Abawajy, Jemal; Khraisat, Ansam; Alazab, Mamoun. Information Management & Computer Security.2014, Vol. 22 Issue 5, p431-449. 19p. DOI: 10.1108/IMCS-02-2013-0007. , Baza podataka: Library, Information Science & Technology Abstracts

[5] By: Patel, Ahmed; Qassim, Qais; Wills, Christopher. Information Management & Computer Security. 2010, Vol. 18 Issue 4, p277-290. 14p.DOI: 10.1108/09685221011079199.

[6] Leonid Stoimenov, Nataša Veljković, Sanja Bogdanović-Dinić, Srđan Nogo and Siniša Macan, Development of e-Government in Serbia and Bosnia and Herzegovina, ICEST 2010, Conference, Ohrid 2010, Macedonia.

[7] S. Nogo, S. Macan, "E-usluge", SMART E-GOVERNMENT konferencija, Beograd, 2009.

ABSTRACT

Data centers are exposed to various methods of security threats that are becoming more and more difficult to reveal and reduce their occurrences. Attacks and malwares mutate as IT services and technologies develop. In modern public-private companies, IT infrastructure and applications are becoming key components in the business processes or electronic public services. Blocking and compromising IT services may cause economic or reputation damage, which is unacceptable for a company. In this paper we will describe in details the “Defense in Depth” approach, which is aiming to provide layered, distributive and miscellaneous security solution by applying multiple security technologies with different possibilities for inspection and control at various points throughout the network.

USE OF THE SYSTEM FOR DETECTING AND PREVENTING UNAUTHORIZED ACCESS TO DATA CENTERS

Srdjan Nogo