Zaštita operativnog sistema i mrežne infrastukture mail servera

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

Sadržaj- **Kod procedure instalacije mail servera primjenom bezbjedonosnih mehanizama konfiguracije operativnog sistema i mrežnih resursa obezbjeđujemo da se u produkcijskom radu mail servera izbjegne veoma veliki postotak intervencija administartora koji su prouzrokovani bezbjedonosonim incidentom. Prilikom konfiguracije mail servera administrator sistema neophodno je da podesi parametre operativnog sistema, mrežne infrastukture i da ih prilagodi eventualnim budućim nadogradanjama istog. U ovome radu detaljno ćemo opisati pravilnu konfiguraciju mail servera sa posebnim osvrtom na zaštitu operativnog sistema, mrežne infrastukture i zaštite od zlonamjernih softvera**

Ključne riječi: Operativni sistem, mrežna infrastuktura,mail server.

I. UVOD

Mail server koristi resurse operativnog sistema koji je po pravilu najčešće konfigurisan na taj način da se koristi u opšte namjene. Osnovni prvi korak kod zaštite mail servera podrazumjeva da se obezbjedi operativni sistem čije resurse koristi. Pravilnom i optimalnom procedurom konfiguracije operativnog sistema obezbjeđujemo da se u produkcijskom radu mail servera izbjegnu mnoge buduće prijetnje. Prilikom konfigurisanja operativnog sistema, neophodno je onemogućiti sve usluge i aplikacije i osposobiti samo one koje su neophodne za rad mail servera. Administratori sistema ukoliko se ne pridržavaju bezbjedonosnih pravila i procedura koje su na snazi u njihovim organizacijama kao rezultat imaju da puno više vremena provode na aktivnostima na podešavanju servera kao bi on optimalno radio kao hardverska platforma mail servera.

II. ZAŠTITA OPERATIVNOG SISTEMA

A. Konfiguracija operativnog sistema

Prilikom konfiguracije novih servera koji će opsluživati mail jedne organizacije administrator sistema treba da preduzme korake kako bi uvrstio identifikovane bezbjedonosne potrebe organizicaije koje će prilagoditi trenutnom stanju informacionog sistema i prilagoditi ih eventualnim budućim nadogradanjama istog. Minimalni koraci kod obezbjeđivanja operativnog sistema obuhvata sljedeće korake:

- Analiza, identifikovanje i uklanjanje nepotrebnih servisa i aplikacija koje se ne koriste za rad mail servera.
- Identifikacija i podjela prava pristupa internih i eksternih korisnika koji imaju pravo pristupiti serveru, servisima i aplikacijama koje se nalaze na njemu.
- Izvršavati redovno ažuriranje operativnog sistema i instaliranje novih verzija pojedinih modula operativnog sistema u skladu sa obavještenjima vendora koji je isporučio taj softver ili zajednice koja brine o razvoju softvera ako je u pitanju otvorena platforma.
- Instalacija softvera i redovna nadogradnja istog koji ima funkciju otkrivanja zlonamjernih programa.
- Obezbjeđivanje test platforme za instalaciju novih verzija i zakrpa operativnog sistema kako ne bi došlo do prestanka rada produkcijskog servera izazvanih instalacijom novog softvera.
- Izraditi plan obuke i konstantno nadograđivati znanje administratora sistema

Administrator sistema može iskoristiti dobre prakse koje važe za operativni sistem kada je u pitanju nadogradnja mail servera koje obrađujemo u nastavku ovog pasusa. Kao i za operativni sistem, potrebno je instalirati samo neophodne usluge i eliminisati poznata osjetljiva područja pomoću „zakrpa“ ili ažuriranjem. Administratori trebaju da prate izdanja novih verzije softvera za „krpljenje“ operativnih sistema i da ih primjene na operativni sistem koji opslužuje mail server. Veoma bitan korak jeste da se tačno definišu metodi autentifikacije i autorizacije korisnika bilo da se radi o unutrašnjim ili vanjskim korisnicima mail sistema. Potrebno je da se izrade mehanizmi kontrole pristupa mail serveru na sistemu sa jasno definisanim odgovornostima i redosljedom koraka šta treba da se preduzme ukoliko se desi bezbjedonosni incident, [1].

Operativni sistem koji nije u potpunosti „zakrpljen“ predstavlja bezbjedonosnu prijetnju jer može biti ugrožen od strane zlonamjernih korisnika ukoliko mu se može pristupiti za vrijeme dok se preduzima akcija krpljenja.

Prilikom puštanja u rad novih mail servera administratori sistema trebaju da preduzmu sljedeće korake:

- Isključiti ga sa mreže
- Izolovati server u poseban LAN (ukoliko nisu u mogućnosti da ga isključe sa mreže)
- Dodijeliti drugi mrežni opseg od produkcijskog dok se vrši akcija instalacije (ukoliko nisu u mogućnosti da ga isključe sa mreže)
- Koristiti uređaje kao što su USB i DVD kao medij za skladištenje instalacijskog softvera kako bi se izbjegao mrežni prenos podataka na server.
- Deaktivirati portove za administraciju kojima se može pristupiti sa udaljene lokacije, (postepeno aktivirati one portove koji su neophodni za produkcijski rad neposredno poslije priključenja instaliranog servera na LAN i VLAN mrežnu infrastukturu)

Kao što smo naveli u predhodnom paragrafu operativni sistem i mail server se može konfigurisati na način da se zakrpe automatski preuzimaju. Ova opcija je sa stanovišta bezbjednosti veoma neracionalna jer serveri ne bi trebali biti konfigurisani na taj način. Veoma je važno da se prije puštanja u produkcijsko okruženje novi softver na serveru istestira na testnom okruženju koje je identično kao produkcijsko.

B. Uklanjanje neophodnih servisa ili softvera

Instalacija mail servera treba da se izvrši na namjenskom serveru čija je hardverska konfiguracija optimizovana za ovu vrstu servera. Od velike važnosti je da se operativni sistem koji opslužuje server na kojem se nalazi mail server oslobođen od nepotrebnog memorijskog i CPU opterećenja. Optimalan način da oslobodimo resurse na serveru je da se odeaktiviraju sve usluge i aplikacije kao i da se aktiviraju samo one koje su neophodne za mail server. Usluge i aplikacije koje treba onemogućiti su po pravilu podrazumjevani web server, servisi direktorija kao što je LDAP, djeljenje mrežnih uređaja kao što su štampači, usluge bezičnog umrežavanja, mogućnost povezivanja na server sa udaljene lokacije kao što je Telnet i sl.. Prilikom instalacije operativnog sistema preporučuje se tkz. Minimalna instalacija, koju je moguće pokrenuti na većini savremenih verzija operativnog sistema. Sa stanovišta bezbjednosti od administratora sistema očekuje se da ukloni nepotrebne servise i aplikacije jer postoji mogućnost da napadač pokuša da izmjeni postavke i aktivira onemoguće usluge i time ugrozi sistem. Ako administrator želi da poboljša bezbjednost on ima nekoliko opcija da to uradi. Prva opcija je da smanji na minimum broj novih usluga na hostu jer svaka nova usluga postaje potencijalni novi put za napadača. Druga opcija je da se smanjenjem broja servisa smanjuje broj logova koje administrator treba da izfiltrira. I treća opcija je da izvrši analizu da li su eventualne dodatne usluge kompatibilne sa samim mail serverem. Administrator u skladu sa politikom bezbjednosti svake organizacije donosi odluku koje usluge će onemogućiti na mail sreveru. Većina dodatnih usluga odnosi se na udaljeni pristup korisničkom direktoriju organizacije i glavnoj konzoli za administraciju mail servera. Ove usluge mogu se aktivirati stalno i povremeno i to zavisi od odluke svake organizacije kada se optimalno procjene koji su rizici i prednosti aktiviranja dodatnih usluga.

III. MAIL KLIJENT ZAŠTITA NA SERVERU

Bezbjedno instaliranje operativnog sistema mail servera podrazumjeva pravilnu konfiguraciju, kontrolu pristupa serveru i aplikacijama. Veoma je važno da se koriste filteri sadržaja, zlonamjernih softvera i zaštita od spama. Upotreba PKI infrastukture (*eng. Public Key Infrastucture*) je obavezna u cilju obezbjeđivanja povjerljivosti kako bi se podržali integritet i nemogućnost poricanja u procesu razmjene poruka između korisnika mail sistema. Korištenje sigurnosnih protokola uz upotrebu autentifikacije, šifrovanja za pristup e mail sistemu i na strani klijenta i na strani servera je danas standard u savremenim mail sistemima, [4].

A. Optimizacija operativnog sistema mail servera

U ovome dijelu rada obradićemo dio koji se tiče procedura i koraka koji su potrebni da se izvrše od strane administratora kada je instalacija operativnog sistema završena. Optimizacija operativnog sistema je jedan od prvih koraka koje administarator treba da preduzme na mail serveru poslije njegove instalacije. Prvi korak je da administrator izvrši bezbjednu instalaciju aplikacije za Email i konfiguriše odgovarajuće politike prava pristupa korisnika na sistem, [3]. Kao što smo naveli u predhodnom poglavlju administrator je završio akcije puštanja u rad samo neophodnih usluga, aplikacija i skripti koje su neophodne za rad mail servera i uklonio one komponente koje su mu trebale u procesu instalacije operativnog sistema. Ovom gore navedenom akcijom administrator je uklonio većinu osjetljiv tački za napad zlonamjernih korisnika na mail sistem. Drugi korak je instalacija samog mail servera koji podrazumjeva određene akcije i to:

- Preuzeti sa weba ili instalacionog medija softver mail servera na odgovarajući host koji će opsluživati mail server
- Analizirati i nakon usaglašavanja s bezbjedonosnom politikom organizacije izvršiti sva krpljenja i ažuriranja, a posebno ona koja se odnose na bezbjednost.
- Izvršiti particonisanje disk prostora kako bi se kreirao namjenski disk prostor da bi se odvojili elektronski poštanski sandučići od file sistema koji koristi operativni sistem i aplikacije mail servera.
- Ukoliko predhodna opcija nije moguća postoji mogućnost preusmeravanje sadržaja elektronskih poštanskih sandučića na drugi server.
- Ukloniti svu dokumentaciju proizvođača sa servera.
- Obrisati sve fajlove koji su ostali kao dio instalacije operativnog sistema i nisu potrebni za rad operativnog sistema.

- Provjeriti da li SMTP, POP, i IMAP baneri usluga (a po potrebi i drugi) prijavljuju tip i verziju mail servera i operativnog sistema. Ukloniti te informacije ako to omogućava mail server.

B. Optimizacija kontrole pristupa mail serveru

Postoji nekoliko parametara kontrole pristupa koje je administrator sistema potrebno da konfiguriše kako bi zaštitio informacije na mail serveru. Prvi parametar odnosi se na ograničenje pristupa aplikaciji mail servera na tačno definisan dio računarskih resursa. Drugi parametar je kompleksniji gdje se korisnicima ograničava pristup kroz dodatne kontrole pristupa koje provodi mail server. Drugi korak podrazumjeva specifična znanja koja se odnose na detaljniji nivo kontrole pristupa. Ovakvom primjenom odgovarajućih kontrola pristupa, administrator može zaštititi osjetljive i ograničene informacije koje se nalaze na mail serveru. Ograničavanjem prostora za pristup računarskim resursima kao što su fajlovi kroz mehanizam kontrole pristupa administrator sistema preventivno djeluje na eventualni DoS napad na mail server. Ovim mehanizmima kontrole pristupa ograničava se pristup fajlovima koji čuvaju osjetljive podatke kao što su *hash* fajlovi lozinki i drugi fajlovi koji se koriste u procesu autentifikacije, fajlovi koji sadrže informacije o ovlaštenjima koja se koriste pri kontroli pristupa, konfiguracioni fajlovi kao i fajlovi u kojima se nalaze informacije o kriptografskim ključevima koji se koriste za usluge povjerljivosti, integriteta i nemogućnosti poricanja, [6].

Procesi koji se tiču aplikacije mail servera potrebno je da se odvijaju pod uslovima koji omogućavaju identifikaciju samo pojedinačnih identiteta korisnika ili grupe korisnika koji imaju restriktivna prava pristupa.

Putem kontrola pristupa domaćem operativnom sistemu mail servera, administrator treba uraditi sljedeće:

- Obezbjediti prostor na hard disku koji bi skladištio privremene fajlove koji nastaju kao produkt rada mail srevera.
- Pristup privremenim fajlovima ograničiti na one procese koji su ih generisali i u kojima su ti fajlovi i nastali.

Mail server ni u kom slučaju ne može sačuvati fajlove van određenog prostora koji je namjenjen za taj mail server i setovan od strane administratora.

IV. ZAŠTITA EMAIL-A OD ZLONAMJERNIH SOFTVERA

U prilozima u elektronskoj pošti postoji veoma velika mogućnost da se nalaze mnogi oblici zlonamjernih softvera, uključujući viruse, crve, trojance, i špijunske softvere—zlonamjerne softvere namijenjene za narušavanje privatnosti korisnika. Zlonamjerni korisnici ili napadači koriste email za isporučivanje napada nultog dana na ciljanu organizaciju prije nego što te osjetljive tačke postanu javno poznate.

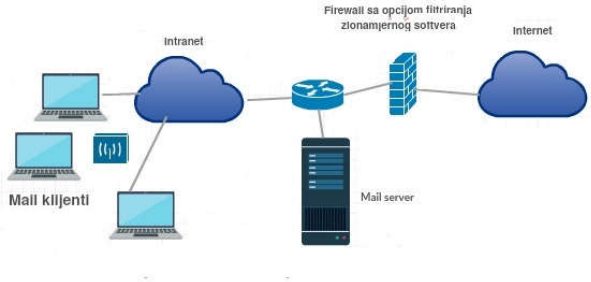
Ovakva kontrola može se upotrijebiti za povećanje privilegija, odobravanje pristupa osjetljivim informacijama, nadgledanje aktivnosti korisnika (npr. kucanja tipki na tastaturi), instaliranje „zadnjih vrata“ i obavljanje drugih zlonamjernih aktivnosti. Jedan od prvih mehanizama odbrane jeste da administrator blokira prijem neke ekstenzije fajlova (*npr.**.exe) putem mail servera. Ovakav način nije efikasan u potpunosti jer napadač ima mogućnost da promjeni ekstenziju zlonamjernog priloga koji pošalje email-om ciljanom korisniku. Da bi se izvršila prevencija instalacije zlonamjernog softvera putem mail priloga potrebno je da se koriste mehanizmi filtriranja. Umjesto da se provjerava samo ekstenzija, filtriranjem se kontrolišu hederi, futeri i drugi identifikacioni aspekti fajla ako je to moguće da bi se identifikovao prilog. Pored dodatnog filtriranja sadržaja, treba uvesti i alatke za skeniranje zlonamjernih softvera (npr. anti-virus softver, softver za blokiranje i prepoznavanje špijunskih softvera) za što efikasniju kontrolu bezbjednosti. Organizacije mogu željeti da razmotre i postavljanje različitih pravila za email-ove koji su porijeklom iz organizacije u odnosu na one koji dolaze van organizacije ili iz pouzdane u odnosu na nepouzdanu organizaciju. Druge prijetnje bezbjednosti mogu se izvući iz zlonamjernih softvera koji se prenose email-om na drugi način. Poruke zasnovane na HTML mogu sadržavati aktivan sadržaj kao što je ActiveX, Java, JavaScript, i Visual Basic Script (VBScript) koji može uticati na klijenta. Poruke zasnovane na HTML često sadrže i drugi neželjeni sadržaj, kao što su spam poruke i pokušaji phishing-a. Phishing se odnosi na upotrebu varljivih računarskih sredstava kako bi se prevarili pojedinci da objave osjetljive lične informacije. Na kraju, moramo razmotriti da takve tehnike filtriranja postaju sve komplikovanije za primjenu ili neefikasne ako su email-ovi šifrovani. Kada se poruka šifruje, bezbijednosne alatke treba da dešifruju poruku prije skeniranja sadržaja. Ovo može biti neizvodljivo zbog velikih zahtjeva u relizaciji i za sobom povlači mnoga pitanja koja se tiču privatnosti. Generalno preopruka je da se ukoliko koristimo šifriranje u velikoj mjeri filtriranje vršimo na krajnjoj tački odnosno na samom klijentu.

A. Skeniranje zlonamjernih softvera

Ako posmatramo cjelokupni informaciono komunikacioni sistem koji opslužuje mail sistem sa aspekta skeniranja zlonamjernih softvera najoptimalniji način je da koristimo slojevite odbrambene mehanizme. Ti mehanizmi mogu biti instalirani na dolaznom e mail serveru, na odlaznom mail serveru, na zaštitnom zidu *(eng. Firewall), na (eng.gateway)* mrežnom uređaju koji je isturen kao prva tačka kontakta spoljnog svijeta sa mrežom organizacije i na radnoj stanici korisnika. Generalno, potrebna su najmanje dva nivoa skeniranja zlonamjernih softvera—jedan na nivou radne stanice krajnjeg korisnika i jedan na ostalim gore nabrojanim komponentama. Prilikom pružanja zaštite od zlonamjernih softvera na više nivoa, organizacije treba da razmisle o biranju proizvoda različitih proizvođača. Raznolikost povećava šansu da se blokiraju najnovije prijetnje, jer je vrijeme reakcije svakog pojedinačnog proizvođača na nove prijetnje različito.

B. *Skeniranje mrežnih uređaja*

Filteri za skeniranje zlonamjernih softvera inicijalno se postavljaju na zaštitnom zidu i realizuju se kroz proksi aplikacije. Takođe imamo mogućnost stavljanja filtera na uređaje koji regulišu mrežni saobraćaj a samim time i prolaze kojima cirkulišu email-ovi. Ove dvije akcije stavljanja filtera za skeniranje mrežnih uređaja imaju za rezultat da se zlonamjerni softver može zaustaviti prije kontakta sa serverom koji opslužuje mail server organizacije. U ovom slučaju, bezbijednosni uređaj se postavlja između mail servera i eksterne mreže. On osluškuje saobraćaj na na TCP portu 25 SMTP konekcije, skenira poruku, potom prosljeđuje poruku koje ne sadrži zlonamjeran softver na mail server, koji je konfigurisan za osluškivanje na neprivilegovanom, nekorišćenom portu, prije nego na uobičajenom portu 25. Kod ovoga pristupa imamo pojavu da se usljed konstantnog SMTP striminga smanjuje efikasnost brzine rada kada je u pitanju brzina mrežnog sadržaja koji prolazi na zaštitnoom zidu kao što je prikazano na sl.1. Da bi riješili ovu situaciju poželjno je da se rastereti skeniranje zlonamjernih softvera na namjenske servere.



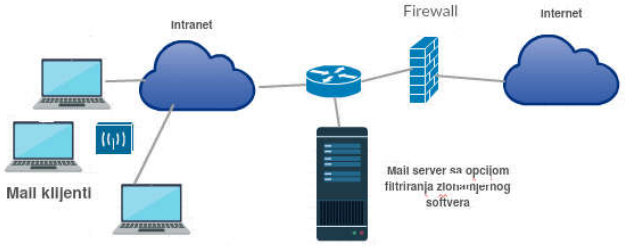
***Slika1**: Primjer filtera na zaštitnom zidu*

Prednosti ovakvog pristupa su kompletno skeniranje saobraćaja toka email-ova, Skeniranje i blokiranje se dešava prije nego što zlonamjerni softveri dođu do mail servera, konfiguracija dolaznih email-ova ne zahtijeva dodatne akcije i obučenost administratora za složene izmjene na konfiguraciji servera kao i omogućeno centralizovano upravljanje politikom skeniranja i filtriranja.

Slabosti su sljedeće: Nije efikasan ako se radi o šifrovanim email-ovima, ne nudi zaštitu internoj mreži organizacije osim ako mreža nije konfigurisana tako da SMTP saobraćaj bude prerutiran preko namjenskih skenera prije nego što dođe do mail servera kao i da se može zahtijevati određene modifikacije postojeće konfiguracije mail servera kada se skeniraju odlazni email-ovi.

C. *Skeniranje na samom mail serveru*

Ukoliko ne koristimo prvu opciju koju smo obradili u predhodnom dijelu B. ovoga rada postoji mogućnost da se aplikacija za skeniranje smjesti direktno na mail server. U tom slučaju, aplikacije za skeniranje pregledaju email koji se šalje između internih korisnika, koji obično ne prolaze kroz zaštitni zid /odašiljač email-ova/ uređaj za prolaze email-ova kroz mrežu. Ovaj pristup ima jednu prednost a to je da se smanjuje mogućnost generisanja unutrašnjih (Intranet) zlonamjernih softvera i time povećevamo nivo sigurnosti unutar mreže organizacije. Pojedini mail serveri nude interfejse za programiranje aplikacija *(eng. Application programming interface)* API koji podržavaju integrisanje skeniranja zlonamjernih softvera, filtriranja sadržaja, blokiranja priloga i drugih bezbijednosnih usluga u okviru *(eng. Mail transfer agent)* MTA.



***Slika2:** Primjer filtriranja na samom serveru*

Prednosti ovakvog tehničkog rješenja su da se vrši kompletno skeniranje dolaznih i odlaznih tokova mail-ova da imamo centralizovano upravljanje politikom skeniranja email-ova u jednoj organizaciji kao i dodatni mehanizmi zaštitite email poruke koje se razmijenjuju između internih korisnika. Osnovni nedostaci pristupa filtriranja na samom serveru je što to može zahtijevati određene akcije na postojećoj konfiguraciji mail servera, što nije efikasno ako se radi šifrovanje email-a kao i što se mogu zahtijevati jače konfiguracije servera što ima za posljedicu ulaganje za nabavku istih , [2].

D. *Filtriranje neželjenog sadržaja i spam-a*

Ukoliko e mail-ovi sadrže neželjene sadržaje a da to nije zlonamjerni softver (virusi i sl.) administratori trebaju da upotrebe tehnologiju filtriranja neželjenog sadržaja. Jedan prilog mail-a ili njegov sadržaj može nanijeti više štete nego virus ili pojedini zlonamjerni *.exe fajlovi. Filtriranje sadržaja potrebno je izvršiti i za dolazne i za odlazne mail poruke i primijeniti ga na istim lokacijama na kojima se nalaze skeneri za zlonamjerne softvere, zaštitni zidovi, mail serveri i računari klijenata.

Element filtriranja sadržaja skenira opasne i neodgovarajuće sadržaje i ako se otkriju može preduzeti skidanje sumnjivog aktivnog sadržaja (npr. ActiveX, JavaScript) prekidanje pokušaja spama,phishinga kao i brisanje ili označavanje poruka kao sumnjive. Politika sigurnosti organizacije treba da definiše pojedine ključne riječi i fraze koje se smatraju neprikladnim i povjerljivim da se putem odlaznih email poruka šalju iz organizacije prema spoljnom svijetu. Ovakav pristup filtriranja sadržaja (kao što je spam i lančana pisma) organizaciju može spasiti gubljenja ugleda u poslovnom svijetu i eventualnih sudskih sporova.

Drugi efikasan način da se smanji broj neželjenih poruka da dospiju do mail servera je korišćenjem lakog protokola za pristup direktorijumu (*eng. Lightweight Directory Access protocol*) LDAP na mrežnom prolazu ili zaštitnom zidu kao mehanizmom za filtriranje. LDAP pretraživač omogućava mrežnom prolazu ili zaštitnom zidu da direktno ispitaju korisnički direktorij organizacije tražeći korisničke informacije. Kada email stigne do mrežnog prolaza ili zaštitnog zida on kontaktira korisnički direktorij da vidi da li je email adresiran na korisnika koji zaista postoji. Ako korisnik nije u direktoriju email se odbacuje i ne dolazi do mail servera.

Veoma veliko opterećenje resursa za organizaciju može da predstavlja pojava velike količine spam poruka. Administrator u cilju zaštite treba osigurati da spam nemože biti poslat sa unutrašnjih mail servera, implementirati filtriranje spama za dolazne poruke kao i blokirati poruke sa servera za koje je poznato da šalju spam. Poželjno je da se u pristupne filtere pamte liste mail servera sa interneta koje se nalaze na crnim listama odašiljača spam-a. Aplikacije mail servera treba konfigurisati kako bi pretraživali više crnih lista i odbili poruke koje su porijeklom sa mail servera koji su na spiskovima. Ovakva konfiguracija na uređajima sa filterima može drastično smanjiti isporuku spam poruka, [5].

V. ZAKLJUČAK

U predhodnim poglavljima opisali smo tehnike koje se tiču instalacije mail server uz upotrebu bezbjedonosnih mehanizama koji su propisani procedurama konfiguracije operativnog sistema i mrežnih resursa. Ovim pristupom obezbjedili smo da se u trenutku kada se mail server pusti u produkcijski rad izbjegne veoma veliki postotak intervencija administartora koji su prouzrokovanim eventualnim bezbjedonosonim incidentom. U poglavlju II smo opisali sve tehničke detalje prilikom konfiguracije mail servera od strane administratora sistem sa posebnim osvrtom na konfiguraciju operativnog sistema servera. Zaključujemo da se bezbjedonosni rizici za cjelokupni sistem smanjuju sa količinom preventivnih mjera koje su preduzete od strane administratora u fazi planiranja kao i konfiguracije operativnog sistema i mrežne infrastukture. Možemo zaključiti da smo u ovome radu definisali jasne smjernica što se tiče zaštite mail servera sa posebnim osvrtom na zaštitu operativnog sistema, mrežne infrastukture i zaštite od zlonamjernih softvera

Literatura

[1] Međunarodna organizacija za standardizaciju (2013) , UNI CEI ISO/IEC 27002:2013

[2] Srđan Nogo, RSS-1-13 upotreba sistema za otkrivanje i sprečavanje neovlaštenih pristupa u centrima podataka, XV međunarodni naučno-stručni simpozijum , INFOTEH Jahorina 2016

[3] Međunarodna organizacija za standardizaciju (2015), UNI CEI ISO/IEC 27033-1:2015

[4] Institut za standarde i tehnologiju (2015), SP 800-131SAr1 , Preporuke za kriptoalgoritme i dužine ključeva Cisco (2015), SAFE referentni vodič

[5] Evropska komisija (2012), "Komunikacija između komisije, Evropskog parlamenta, Savjeta, Evropskog ekonomskog i socijalnog komiteta i komiteta iz regiona: Oslobađanje potencijala računarstva u oblaku u Evropi. "

[6] ENISA (2013), Dobar vodič za praktičnu i bezbjednu primjenu računarstva u gov-oblaku

ABSTRACT

When installing a mail server with usage of security mechanisms that are define with procedure of the configuration for operating system and network resources we ensure that in production environment mail server should avoid a large percentage of intervention by side of administrator caused with security incidents. When configuring the mail server by the system administrator, it is necessary to tune the parameters of the operating system and network infrastructure and adapt them future potential upgrade. In this paper we will describe in detail the proper configuration of mail servers with special focus on operating system security, network infrastructure and protect against malicious software.

PROTECTION OF THE OPERATING SYSTEM AND NETWORK INFRASTRUCTURES OF MAIL SERVER

Srdjan NOGO