Smjernice i prakse za bezbjednost Email sistema

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

Sadržaj— **Email sistemi izloženi su različitim metodama ugrožavanja bezbjednosti koji postaju sve teži za otkrivanje i umanjivanje učestalosti njihovog pojavljivanja. Napadi i zlonamjerne aktivnosti mutiraju u skladu sa razvojem IT usluga i tehnologija. U savremenim javno-privatnim organizacijama, Email postaje primarni vektor za bezbijednosne prijetnje kao što su virusi, phishing, spam, zlonamjerni softver kao i napadi odbijanjem usluga. Blokiranje ili kompromitovanje mail komunikacije može izazvati ekonomsku štetu ili narušiti ugled, što je za jednu organizaciju neprihvatljivo. U ovome radu detaljno ćemo opisati mehanizme za primjenu smjernica za kontrolu i odgovarajućih upravljačkih praksi neophodnih za pravilno funkcionisanje i održavanje zaštićenog mail sistema.**

Ključne riječi: Email sistem, Smjernice i upravljačke prakse

I. UVOD

U proteklih nekoliko godina, kada je u pitanju planiranje smjernica i upravljačkih praksi Email sistema u savremenim privatno-javnim organizacijama primjećen je nedostatak sistematskog pristupa koji se odnose na bezbjednost projektovanja, implementiranja i funkcionisanja Email sistema.

Sistematski pristup realizacije gore navedenih komponenti daje nam mogućnost da izvučemo tehnološki maksimum iz softvera koji podržava produkcijski Email sistem. Takođe, ovakvim pristupom ostvaruje se krajnji cilj korisnika a to je da postojeći Email sistemi koji rade na specifičnim hardverskim arhikteturama budu optimizovani na potencijalne razvoje i nadogradnju kako bi softverski pratile izdavanje novih verzija arhiktetura.

Veoma često javne organizacije iz razloga što nepružaju Email usluge vanjskim organizacijama, koristeći autentifikovanu bezbjednu komunikaciju između građana i institucija da bi se pojednostavilo kreiranje novih javnih usluga ili usluga trećih lica gube veoma velika novčana sredstva i troše vrijeme građana.

II. BEZBJEDONOSNE PRIJETNJE

U proteklih nekoliko godina, Email je postao jedno od najvažnijih sredstava za poslovnu i privatnu elektronsku komunikacij. Brza ekspanzija i opšta prihvaćenost ovakvog vida komunikacije sa bezbjedonosnog aspekta ima i svoju cijenu. Email postaje primarna meta napada zlonamjernih korisnika uz kombinaciju korištenja softverskih alata i tehnologija napada kao što su spam, virusi, zlonamjerni softver, pecanje *(eng. phishing)* , napadi odbijanjem usluga i sl. Istovjetne osobine koje čine email globalnim alatom komunikacije, čine ga osjetljivim i na nenamjernu i na namjernu zloupotrebu.

Gore navedene bezbjedonosne prijetnje kao posljedicu imaju brz odgovor organizacija koje kroz periodično ažuriranje i instalaciju softverskih zakrpa njihovih postojećih bezbijednosnih sistema, kao i permanantan monitoringa i blagovremenu nabavku novih izdanja softvera i hardvera sistemski predviđaju potencijalne osjetljive tačke sistema. Ovakvim pristupom organizacije tipično reaguju na svaku prijetnju pojedinačno umjesto da razmatraju pitanje bezbjednosti kroz jedinstvenu Email arhikteturu, [1].

Bezbijednosni mehanizme možemo da nabavimo na tržištu i oni funkcionišu optimalno unutar svoje sfere djelovanja ali moramo biti svjesni da postoje i svojstvena ograničenja u kreiranju „krpljenja“ za ta rješenja koja se nekada preklapaju, a nekad ne. Sa stanovišta bezbjednosti neko ko je vlasnik Email sistema potrebno je da preuzme potpunu kontrolu nad dolazno-izlaznim mrežnim saobraćajem kroz sve komponente korporativne mreže. To podrazumijeva povezivanje mrežnih filtera i bezbjedonosnih politika u specijalizovan kompaktan sistem za sprovođenje bezbjednosti zasnovano na tačnom definisanju ko su korisnici sistema sa jasno definisanim privilegijama na sistemu. Veoma je teško optimizovati složene elemente Email sistema da funkcionise na jednostavan i fleksibilan način, [7].

Osnovni izazovi za organizaciju koji prestavljaju minimum zahtijeva na koje je potrebno obratiti posebnu pažnju a vezana su za bezbjednost Email sistema uključuju sljedeće :

- Zaštiti povjerljive i osjetljive informacije koje se prenose između mail servera i klijenta a koje nisu šifrovane a iste se mogu presresti od strane zlonamjernih korisnika. Jednostavan primjer takvih informacija su informacije o korisničkom imenu, lozinki i tekst poruka .
- Ako imamo činjenicu da Email nije autentifikovana tehnologija, informacije koje se nalaze u email porukama mogu se izmijeniti u nekoj tački komunikacije između pošiljaoca i primaoca. Potrebno je preduzeti tehničke korake kako bi se napadačima otežala akcija prekida komunikaciong kanala između pošiljaoca i primaoca
- Greške (*eng.bugs)* u email arhitekturi mogu se koristiti da se ugrozi server i dobije pristup resursima mreže u kojoj se nalazi Email arhitektura. Primjeri ovakve vrste napada uključuju dobijanje privilegija pristupa fajlovima i folderima

koji nisu javni, a nalaze se unutar mail servera i omogućavaju da se aktiviraju izvršne komande na mail serveru.

- Sprečavanje napada odbijanjem usluge tkz. DoS napad, koji može biti usmjeren na Email server koji odbija autorizovane korisnike ili ih sprečava da koriste email server.
- Spriječiti da se Email sistem koristi kao sredstvo za društveni inženjering, koji može omogućiti napadaču da iskoristi korisnike unutar organizacije za sakupljanje informacija.
- Upoznati autorizovane korisnike da ne šalju osjetljive informacije putem email-a ako nisu šifrovane iz razloga što takva akcija može izložiti organizaciju zakonskim sankcijama ukoliko pojedine osjetljive informacije dođu u posjed trećih lica.
- Spriječiti da organizacioni mail server bude iskorišten od strane hakera kao *host* za napad na druge vanjske organizacije.

III. OPŠTE SMJERNICE ZA UPRAVLJANJE EMAIL SISTEMIMA

A. Planiranje instalacije sistema i angažovanja osoblja

Imajući u vidu činjenicu da bezbjednost Email-a prilično složena, i to je akcija kojom se moramo baviti u početnom planiranju i dizajnu prije podukcijske primjene i same distribucije rješenja. Plan primjene koji je detaljniji kao krajnji rezultat ima mogućnost da budući Email sistem brzo odgovori na svaku eventualnu kriznu bezbjedonosnu situaciju, [1]. Izrada detaljnog plana pomaže administratorima na sistemu da naprave optimalan balans iskoristivosti na relaciji performanse sistema-rizici. Organizacija treba planirati i angažovanje osoblja kada se radi o sljedećim kritičnim pitanjima i to:

- Da se izvrši angažman specijalizovanog tehničkog osoblja tj. Administratora sistema u kojem bi se tačno definisala podjela prava i uloga na sistemu (npr. administratori sistema i mail servera, administratori mreže, službenici zaduženi za bezbjednost informacionog sistema),
- Da se definišu minimalani tehnički zahtjevi za vještinama i obukama koji se zahtijevaju od odabranog osoblja,
- Veoma je bitno da se angažuju administratori koji su na raspolaganju organizaciju 24/7 u slučaju nepredviđenih sitacija
- Da se izradi plan edukacije i usavršavanja administratora za rad na sistemu.

B. Procedure upravljanja bezbjednošću

Procedure upravljanja su od veoma velikog značaja za optimalno upravljanje organizacijskim mail serverom. Bezbijednosne procedure obuhvataju identifikovanje sredstava informacionog sistema, dokumentaciju, implementaciju politike i smjernice neophodne da bi se osigurali povjerljivost, integritet i dostupnost resursa informacionog sistema.

Minimalne procedure koje je potrebno imati da bi se osigurala bezbjednost mail servera su:

- Izraditi procjenu rizika i upravljanje rizicima sa jasnom podjelom nivoa rizika (mali, srednji i veliki).
- Definisati standardizovane konfiguracije softvera koje su interoperabilne sa bezbijedonosnom politikom informacionog sistema.
- Obuka osoblja koje je zaduženo za sprovođenje politike bezbjednosti informacionog sistema.
- planiranje nepredviđenih situacija, konstantnog funkcionisanja i plana oporavka.

C. Obezbjeđenje Operativnog sistema

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, [2]. Pravilnom i optimalnom procedurom konfiguracije operativnog sistema obezbjeđujemo da se u produkcijskom radu mail servera izbjegnu mnoge buduće prijetnje. Prilikom konfiguracije novih servera administrator sistema treba da uvrsti bezbjedonosne potrebe organizacije koje će prilagoditi trenutnom stanju informacionog sistema i prilagoditi ih eventualnim budućim nadogradanjama istog. Obezbjeđivanje operativnog sistema obuhvata sljedeće korake:

- Analiza i onemogućavanje nepotrebnih servisa i aplikacija i ako je potrebno totalno uklanjanje istih sa servera.
- Pravilna konfiguracija internih i eksternih korisnika koji imaju pravo pristupiti serveru, servisima i aplikacijama koje se nalaze na njemu.
- Obezbjediti kontrolu sprovođenja procedura koje se odnose na redovno ažuriranje operativnog sistema i instaliranje novih verzija pojedinih modula operativnog sistema.
- Instalacija dodatnog specijalizovanog softvera koji je zadužen za zaštitu operativnog sistema
- Obezbjeđivanje test platforme za testiranje novih funkcionalnosti operativnog sistema kao i cjelokupnog softvera koji je instaliran na radnom okruženju.
- Osiguran dovoljan broj obučenih administratora sa jasnim procedurama koji su to koraci koji se trebaju preduzeti prilikom pojave bezbjedonosnog incidenta.

Prilikom nadogradnje mail servera moguće je koristiti iskustva dobre prakse koji se odnose i na operativni sistem. Kao i za operativni sistem, potrebno je instalirati samo neophodne usluge i eliminisati poznata osjetljiva područja pomoću „zakrpa“ ili ažuriranjem. Obezbjeđivanje aplikacije email servera obuhvata: softver za „krpljenje“ i ažuriranje mail servera, uklanjanje i onemogućavanje nepotrebnih usluga, konfigurisanje autentifikacije i kontrole pristupa za korisnike mail servera i na kraju testiranje bezbjednosti aplikacije mail servera, [3].

D. *Upotreba kriptografije u radu mail servera*

Većina Email sistema koji se nalaze na tržištu konfigurisano je na način da se za razmjenu poruka na relaciji pošiljalac –primalac ne koristi šifrirana komunikacija. Ako koristimo nešifriranu komunikaciju u procesu razmjene podataka izlažemo se napadima korisničkih naloga i omogućavamo napadaču da presretne poruku i da je eventualno izmjeni i pošalje primaocu kao original. Jedan od osnovnih minimuma koji je potrebno preduzeti je da se sesija autentifikacije korisnika šifruje, [5]. Digitalno potpisivanje i šifrovanje cjelokupnog tijela poruke ima za posljedicu povećanje saobraćaja na mrežnoj infrastukturi organizacije. Povećanjem mrežnog saobraćaja otežava se skeniranje svih ulazno izlaznih parametara na mreži i otežava se skeniranje zlonamjernih softvera i filtriranje sadržaja email-ova, a često zahtijeva i značajnu administrativnu podršku. Povećanje saobraćaja ima posljedicu da se bezbjednost mrežne infrastrukture koja igra ključnu ulogu u bezbjednosti mail servera dodatno usložnjava ali se uz pravilno planiranje upotrebe ljudskih resursa i softverskih alata ova sitacija može prevazići. U većini konfiguracija, mrežna infrastruktura se nalazi na prvoj liniji odbrane između interneta i intraneta u kojoj se nalazi mail server. Postoje dva scenarija odbrane, tradicionalni elementi za bezbjednost uređaji koji se zovu 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. Ovakav 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.

Frekvencija, sofistikovanost i raznolikost sadašnjih napada na mail server podržavaju ideju da bezbjednost mail servera mora biti implementirana putem slojevitih i raznolikih zaštitnih mehanizama.

IV. BEZBJEDONOSNO PLANIRANJE PRIMJENE MAIL SERVERA

Greške u planiranju i projektovanju arhikteture direktno se projektuju na broj grešaka u bezbjedonosnom sistemu mail servera. Optimalan projekat arhitekture mail servera uključuje detaljno planiranje prije instaliranja, konfigurisanja i primjene. Detaljan projekat će razviti sistem u skladu sa svim politikama organizacije i osigurati da email server bude bezbjedan koliko je to moguće. Ukoliko želimo smanjiti troškove potrebno je da se bezbjedonosni parametri mail servera analizaruju do u detalje prije puštanja u produkciju. Troškovi usklađivanja bezbjednosti rastu srazmjerno povećanju vremenskog intervala nakon implementacije i puštanja u produkciju. Balansiranjem parametara kao što su raspoloživost, perfomanse i upravljanje rizicima koji su uvršteni u plan bezbjednosti daje mogućnost organizaciji da bude fleksibilnija kod donošenja kritičnih odluka kada se desi eventualni bezbjedonosni incident na Email sistemu.

Ukoliko imamo odstupanje od plana vjerovatno se radi o određenim osjetljivim područjima na koja administratori sistema trebaju da obrate posebnu pažnju.

Kada ulazimo u fazu planiranja budućeg mail sistema , mora se uzeti u obzir sljedeće i to:

- Identifikovati namjene mail servera.
- Koja vrsta informacija sa tačno propisanim stepenima povjerljivesti će se čuvati, obrađivati ili prenositi putem mail servera.
- Definisati parametre za bezbjednost tih informacija.
- Definisati zahtjeve za bezbjednost za eventualne dodatne usluge.
- Definisati uslove za izradom rezervnih kopija i procedurom oporavka od nepredviđenih situacija.
- Definisati lokaciju servera unutar mreže.
- Identifikovati dodatne usluge koje su instalirane na mail serveru za upravljanje uslugama (sistem za izradu rezervnih kopija, da li dozvoliti administriranje sa udaljene lokacije, generisanje izvještaja iz log fajlova)
- Definisati koje su to mrežne usluge, klijent i server su instalirani na mail server ili se radi o serveru za podršku (lokalni zaštitni zid, IP tabele itd.)
- Planirati vrste korisnika sa tačno definisanim stepenom autorizacije na sistemu.
- Odrediti način na koji će se administrirati mail serverom (lokalno, sa unutrašnje ili vanjske udaljene lokacije), sa stanovišta bezbjednosti najoptimalnije je da to administracija bude dozvoljena samo iz lokalne mreže.
- odlučiti na koji način će se vršiti autentifikacija korisnika i na koji način će se zaštititi podaci vezani za autentifikaciju

Postoje dva izbora kod odabira softverskog rješenja za realizaciju Email sistema. Prvi je komercijalni softver a drugi je softver otvorenog koda. Kod odabira komercijalnog rješenja, veoma je bitno da se sarađuje sa vendorom tj.da se ispoštuju sva pravila (softverska i hardverska) koja treba ispuniti prilikom instalacije takvog sistema. Ukoliko se odlučimo za otvoreni kod (*eng. Open Source*) veoma je bitno da se što prije počne sa saradnjom sa zajednicom koja je odgovorna za unapređenje i održavanje takvog rješenja, [6]. Drugi pristup kao rezultat ima angažman većeg broja administratora sistema i učestalije akcije nadogradnje softvera.

U većini slučajeva odabir mail servera obično određuje operativni sistem kojim raspolažemo u organizaciji. Ako možemo da biramo operativni sistem, potrebno je da potvrdimo sljedeće osobine operativnog sistema:

- Minimalna izloženost povredljivosti.
- Koje su mogućnosti da se izvrši restrikcija ovlaštenja na administrativnom nivou i na nivou korisnika samo za ovlašćene korisnike,.
- Sposobnost nivoa zaštite u cilju odbijanja pristupa informacijama na serveru ukoliko se ne radi o onim informacijama koje su predviđene da budu dostupne.
- Reduciranje mrežnih usluga koje mogu biti ugrađene u operativni sistem ili softver servera.

- Sposobnost da se upišu u logove odgovarajuće aktivnosti na serveru kako bi se otkrili neovlašćeni pristupi i pokušaji neovlašćenog pristupa.

V. PRAKSE UPRAVLJANJA

Za pravilno funkcionisanje i administriranje zaštićenog mail servera neophodno je da se sprovode određene upravljačke prakse.

Prvi korak primjene upravljačke prakse u organizaciji zahtijeva identifikaciju resursa informacionog sistema. Drugi korak je primjena akcionog plana koji podrazumjeva izradu dokumentacije politika, standarda i procedura koje obezbjeđuju povjerljivost, integritet i raspoloživost resursa informacionog sistema. Treći korak je plan permanetnog monitoringa i nadogradnje sprovođenja akcionog plana u cilju poboljšanja informacionog sistema, [4].

Organizacije treba da implementiraju sljedeće prakse da bi osigurale bezbjednost mail servera:

- **Politika bezbjednosti**: politika bezbjednosti informacionog sistema treba navesti osnovne propise i pravila za bezbjednost informacionog sistema i njihovu planiranu internu svrhu.
- **Kontrola i upravljanje konfiguracijom/izmjenama**: Proces kontrole izmjena obezbjeđuje potvrdu da je sistem dovoljno bezbjedan za upravljanje nakon uvođenja izmjena u hardveru, firmveru i softveru.
- **Menadžment rizika**: Procjena rizika podrazumijeva kvalitativno ili kvantitativno određivanje vrijednosti rizika u odnosu na konkretnu situaciju i prepoznatu prijetnju. Ona obuhvata određivanje obima i metodologije procjene, sakupljanje i analizu podataka vezanih za rizike i tumačenje rezultata analize rizika.
- **Standardizacija aplikacija i operativnih sistema**: neophodno je da organizacija izradi standardizovane bezbijednosne procedure za aplikacije i distribuisane operativne sisteme.
- **Obuka Korisnika**: Program obuke o bezbjednosti je ključan za cjelovit stav organizacije kada je u pitanju bezbjednost. Razvojem svijesti korisnika i administratora kada su u pitanju odgovornosti vezane za bezbjednost i učenjem ispravne prakse pomaže im da promijene svoje ponašanje kako bi se uskladili sa najboljom praksom u oblasti bezbjednosti.
- **Certifikacija:** zaštićen email sistem mora se analizirati kako bi ispunio sve bezbijednosne zahtjeve koje postavi organizacija.

VI. ZAKLJUČAK

Kada je u pitanju planiranje smjernica i upravljačkih praksi Email sistema u savremenim privatno-javnim organizacijama potrebno je primjeniti sistematski pristup koji se odnose na bezbjednost projektovanja, implementiranja i funkcionisanja Email sistema. Kao što smo konstatovali u poglavlju III da je obezbjeđivanje mehanizama bezbjednosti Email sistema prilično složena akcija, neophodno je da obratimo posebnu pažnju u fazi planiranja i dizajna sistema prije podukcijske primjene i same distribucije rješenja. Kao što je navedeno u predhodnim poglavljima ovoga rada blokiranje ili kompromitovanje mail komunikacije može izazvati ekonomsku štetu ili narušiti ugled, što je za jednu organizaciju neprihvatljivo. Da bi se izbjegla takva situacija u radnom okruženju Email sistema primjena smjernica kontrola i odgovarajućih upravljačkih praksi neophodne su za pravilno funkcionisanje i održavanje zaštićenog mail sistema.

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

[7] 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.

ABSTRACT

Email systems 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, Email is becoming key vector for security threats like viruses, phishing, spam, malware and attack Denial of Service. Blocking and compromising mail communication may cause economic or reputation damage, which is unacceptable for a company. In this paper we will describe in details the mechanisms for the implementation of control and appropriate management practices necessary for the proper operation and maintenance of the protected mail system.

GUIDELINES AND PRACTICES FOR THE SECURITY OF E-MAIL SYSTEMS

Srdjan NOGO