KAKO UMANJITI RIZIK OD PRIJEMA FIŠING IMEJL PORUKA

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

STATISTIČKI IZVEŠTAJI

Nakon pojave interneta i njegovog prihvatanja u poslovnoj korespondenciji, elektronska pošta je postala najčešće korišćena funkcija koja je omogućila trenutno slanje i primanje poruka.

Prema statističkim izveštajima [1] broj naloga elektronske pošte raste iz godine u godinu, pa je u 2019. iznosio 5.5 milijardi. Broj poruka elektronske pošte poslatih u jednom danu je iznosio 246.5 milijardi uz predviđanje da će rasti 5% godišnje.

PRETNJE

Na osnovu Pregleda tržišta telekomunikacija i poštanskih usluga u Republici Srbiji u 2018. godini, koji je RATEL sačinio i za oblast bezbednosnih rizika uIKT sistemima, stanje informacione bezbednosti u svetu pokazuje da je fišing na četvrtom mestu najčešćih pretnji, sa zabeleženim trendom rasta.

Fišing je sajber napad koji primarno koristi tehnike socijalnog inženjeringa sa ciljem da zavara žrtve. Poruke koje se šalju mogu da sadrže zlonamernu datoteku, link koji korisnika preusmerava na internet stranicu sa zlonamernim sadržajem, ili uputstvo koje navodi žrtvu da sama prouzrokuje sajber incident.

Fišing je do te mere zastupljen da je čak 75% država članica EU otkrilo slučajeve fišinga. Preko 90% infekcija malverom i 72% povreda podataka potiču upravo odfišing napada.

Posmatrajući period od 2011. godine, napadi na mobilne telefone u ovom obliku, iz godine u godinu rastu za 85%.

Poseban problem su fišing poruke koje, kao svoje primarne mete prepoznaju zaposlena lica u finansijskom sektoru ili ljudskim resursima. Cilj napada je krađa novca napadnute organizacije. U periodu od oktobra 2013. godine do maja 2018. godine, prijavljeno je čak 78.000 ovakvih napada uz štetu od 12,5 milijardi američkih dolara.

Najčešći prilozi u ovakvim elektorosnkim poštama su: narudžbenica, plaćanje, faktura, potvrda, račun, savet, transfer.

Najčešće upotrebljavane reči su: plaćanje (13,8%), hitno (9,1%), zahtev (6,7%), pažnja (6,1%), bitno (4,8%), poverljivo (2,0%), hitan odgovor (1,9%), transfer (1,8%), bitno ažuriranje (1,7%) i pažnja (1,5%).

[1] https://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

KAKO UMANJITI RIZIK?

Postoje tri mehanizma za proveru elektronske pošte koji mogu smanjiti rizik od primanja poruka sa lažirane adrese (eng. spoofing), kao i od kompromitacije vašeg poslovanja i to su:

- SPF (Sender Policy Framework),
- DKIM (Domain Keys Indentified Mail) i
- DMARC (Domain-based Message Authentication Reporting and Conformance).

Implementiranjem ovih mehanizama, učinićete da domen koji koristite za elektronsku poštu bude teži za lažiranje, a sistemi koji budu primali poruke od vas će biti sigurni da stižu iz pouzdanog izvora.

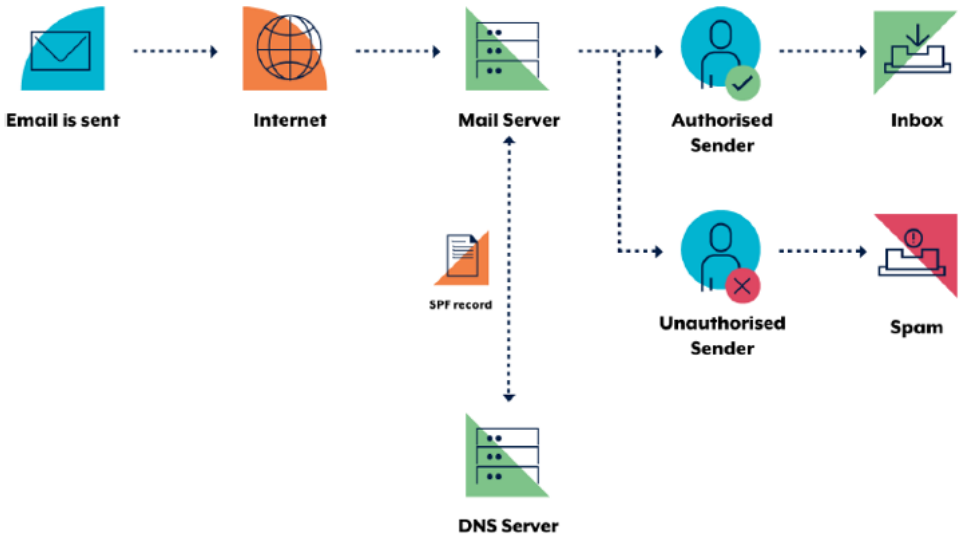
Ovi mehanizmi za zaštitu sistema za slanje i prijem elektronske pošte, omogućavaju uspešno odbijanje većine trenutno aktuelnih fišing napada, a njihovom primenom preventivno delujete na potencijalnu zloupotrebu vaših adresa elektornske pošte i time doprinosite boljem imidžu i reputaciji vaše kompanije.

SENDER POLICY FRAMEWORK (SPF)

SPF [2] predstavlja standardizovani način za verifikaciju poruka elektronske pošte radi detektovanja lažnih poruka.

Implementira se objavljivanjem SPF zapisa u DNS-u da bi se na taj način identifikovala lista validnih IP adresa servera za posmatrani domen. Kada mail server primaoca dobije poruku, pokreće se proces verifikacije identiteta mail servera pošiljaoca korišćenjem objavljenog SPF zapisa. Ukoliko server pošiljaoca nije definisan kao autorizovani pošiljalac u SPF zapisu, verifikacija će biti neuspešna, a poruka odbačena (smeštena u sanduče za neželjenu poštu) jer to znači da je adresa pošiljaoca lažirana.

Na slici 1 je ovaj proces grafički prikazan [3].



Slika 1. Grafički prikaz SPF

Za dodatne informacije o implementaciji preporučujemo: RFC 7208 [4].

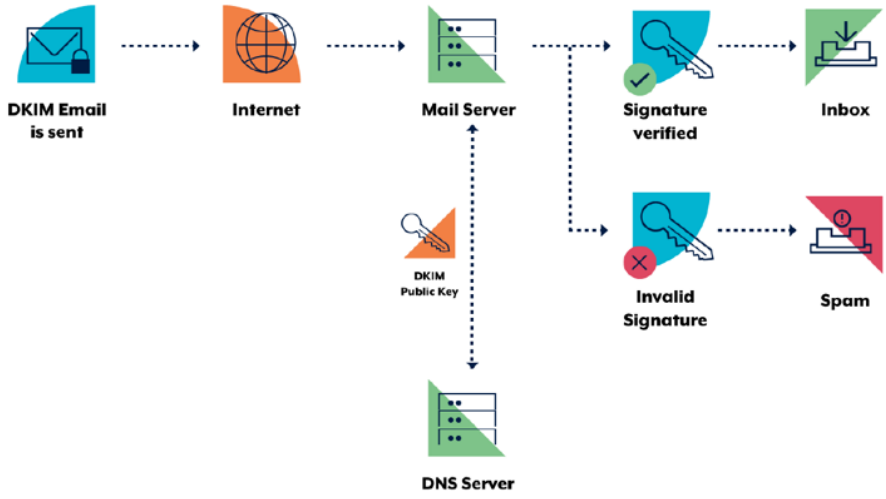
[2] RFC7208
[3] Malicious Email Mitigation Strageties, Australian Government, april 2019
[4] https://tools.ietf.org/html/rfc7208

THE DOMAIN KEYS IDENTIFIED MAIL (DKIM)

DKIM [5] protokol omogućava kriptografsko potpisivanje poruka tako da primalac može proveriti da li je poruka menjana nakon slanja.

Koristi se asimetrična kriptografija, odnosno javni i privatni ključ. Prilikom slanja poruka elektronske pošte, server, privatnim ključem, digitalno potpisuje odabrane delove zaglavlja i telo poruke, potpis smešta u DKIM zaglavlje i uz poruku šalje primaocu. Po prijemu poruke, primalac uz pomoć javnog ključa koji se nalazi u DNS zapisu proverava DKIM potpis poruke. Ukoliko je poruka stigla u nepromenjenom obliku, potpis će biti validan. U slučaju da je poruka promenjena ili lažirano neko od potpisanih polja, potpis neće biti validan, a poruka odbačena (smeštena u sanduče za neželjenu poštu).

Na slici 2 je ovaj proces grafički prikazan [6].



Slika 2. Grafički prikaz DKIM

Za dodatne informacije o implementaciji preporučujemo: RFC 6376 [7].

[5] RFC6376
[6] Malicious Email Mitigation Strageties, Australian Government, april 2019
[7] https://tools.ietf.org/html/rfc6376

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE PROTOCOL (DMARC)

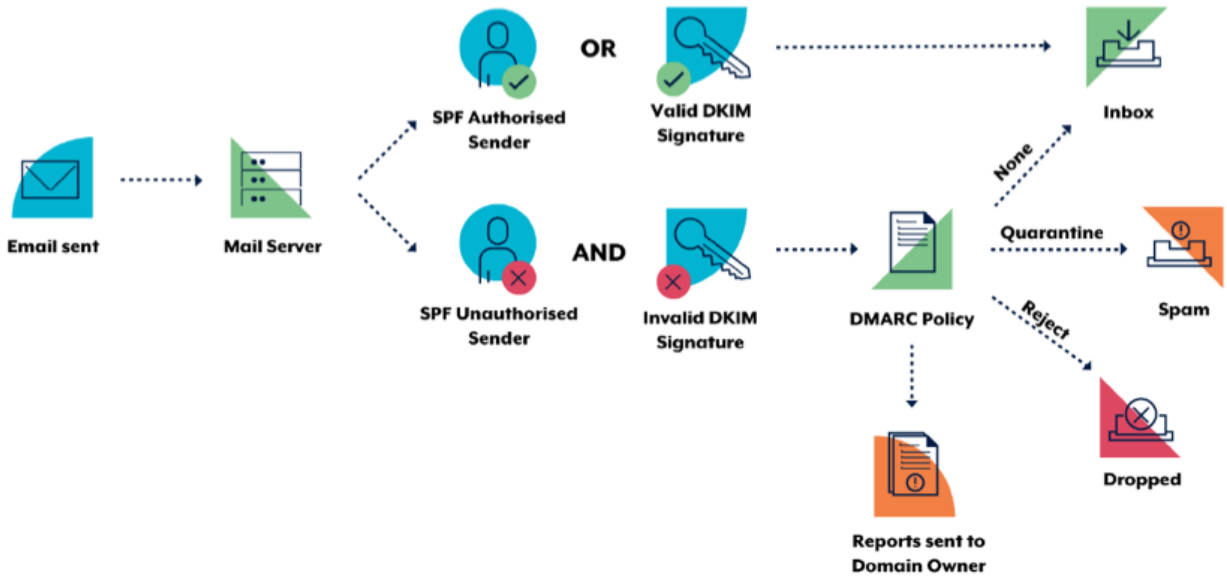
DMARC [8] protokol pruža dodatan nivo bezbednosti kombinovanjem SPF i DKIM funkcionalnosti, kao i polise kojom se definiše način postupanja u slučajevima kada verifikacija pošiljaoca nije uspešna.

Polisu definiše vlasnik domena i objavljuje je kroz DNS zapis.

Prilikom prijema poruka sa domena, za koji je definisan DMARC zapis, mail server proverava da li su ispunjeni zahtevi za verifikaciju identiteta pošiljaoca (SPF i/ili DKIM) u skladu sa definicijom polise. Ukoliko je verifikacija uspešna, poruka će biti isporučena, dok će ostale biti smeštene u sanduče za neželjenu poštu, ili u potpunosti odbačene, u zavisnosti od zahteva DMARC polise. Pored toga, polisa pruža mogućnost podešavanja adrese elektronske pošte na koju će se vlasniku domena slati informacije o IP adresama koje su pokušale da zloupotrebe njegov domen, čime se omogućava njegovo proaktivno reagovanje i sprečavanje ozbiljnijih napada koji lažiraju posmatrani domen. Najveći nivo zaštite se postiže kada su implementirane i SPF i DKIM funkcionalnosti zajedno sa DMARC protokolom.

[8] RFC7489

Na slici 3 je ovaj proces grafički prikazan [9].



Slika 3. Grafički prikaz DMARC

DMARC standard je formiran 2013. godine i već u prvoj godini postojanja je pomogao da se zaštiti 60% sandučića elektronske pošte širom sveta od fišinga i neželjenih poruka [10].

Za dodatne informacije o implementaciji preporučujemo: RFC 7498 [11].

PREPORUKA NACIONALNOG CERT-A

Nacionalni CERT preporučuje pre primene navedenih mehanizama procenu rizika poslovanja, odnosno da li se ulaganja mogu opravdati smanjenjem rizika od kompromitacije sigurnosti.

Ukoliko posedujete sopstveni server za slanje i prijem elektronske pošte, neophodno je da se obratite odgovornom licu koje je zaduženo za njegovo održavanje, odnosno ispravno funkcionisanje.

Isti princip je neophodno primeniti i u slučajevima kada se domen i server za slanje i prijem elektronske pošte nalaze kod hosting provajdera.

[9] Malicious Email Mitigation Strageties, Australian Government, april 2019
[10] https://dmarc.org/press/release-20130206
[11] https://tools.ietf.org/html/rfc7489