Analiza gov.rs domena

www.bezbedanbalkan.net

Agenda

1. Šta je DNS?
2. Šta je DNS zapis?
3. Šta je eMail server?
4. Šta je MX zapis?
5. Šta je SPF zapis?
6. Šta je DKIM zapis?
7. Šta je DMARC zapis?
8. Šta je “domain spoof” napad?
9. Kakve veze sve ovo ima sa gov.rs domenom?
10. Kako se odbraniti od “spoof” napada?
11. Bonus
12. Zakljucak
13. Reference

Šta je Domain Name Server (DNS)?

- Sistem imena domena (DNS) je telefonski imenik Interneta. Korisnici pristupaju informacijama na mreži preko imena domena, kao što su bezbedanbalkan.net ili google.com. Web pretraživači komuniciraju preko Internet protokola (IP) adresa. DNS prevodi imena domena u IP adrese tako da korisnici mogu da učitavaju Internet resurse.

- Svaki uređaj povezan na Internet ima jedinstvenu IP adresu koju druge mašine koriste da pronađu uređaj. DNS serveri eliminišu potrebu da korisnici pamte IP adrese kao što je 192.168.1.1 (tip IPv4) ili složenije novije alfanumeričke IP adrese kao što je 2400:cb00:2048:1::c629:d7a2 (tip IPv6).

Šta je DNS zapis?

- Kada korisnik unese ime domena u svoj pretraživač, ta akcija “poziva” DNS zapis u okviru tog imena domena.

- DNS zapisi mogu biti razni, neki od njih su:
  1. A - zapis je ono što upućuje imena domena na IP adrese. „Zapis“ znači „zapis adrese“ i najčistiji je oblik DNS-a. Zapis A omogućava korisnicima da unesu lako prepoznatljivo ime domena i da i dalje budu usmereni na IP adresu.
  2. CNAME - ili „kanonsko ime“, preusmerava jedan domen na drugi, omogućavajući vam da ažurirate samo jedan A zapis svaki put kada napravite promenu. Na primer, CNAME zapis dozvoljava „bezbedanbalkan.net“ da preuzme „www.bezbedanbalkan.net“ sa „www“ ispred.
  3. I mnogi drugi.

- Za ovu temu, fokus je na MX, SPF, DKIM i DMARC DNS zapise.

Šta je E-Mail server?

- E-Mail sever je sistem čija je funkcija razmena poruka.
- Da bi E-Mail server uspešno dostavio poruku na drugi server, neophodno je podesiti između ostalog i DNS zapise.
- DNS zapisi na E-Mail serveru pored pronalaženja IP adrese drugog email servera, omogućavaju i razne vrste zaštita.

Šta je MX DNS zapis?

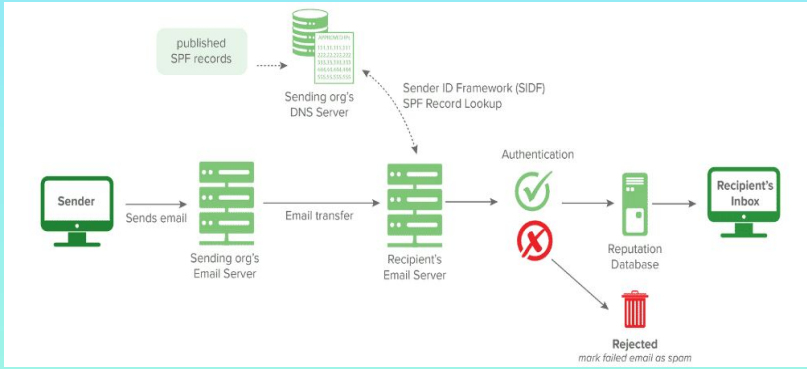
- „Unos razmenjivača pošte“ ili MX unos je zapis koji usmerava elektronsku poštu na drugi server.
- U suštini, zapis navodi kako bi elektronska pošta trebalo da se usmerava kada se pošalje na adresu vašeg domena.

Šta je SPF zapis?

- Bezbednosna tehnologija kao što je “Sender Policy Framework” (SPF) može se pokazati od neprocenjive vrednosti u svetu opterećenom onlajn napadima i neželjenim porukama.
- Sajber bezbednost je glavna briga za sve, od pojedinaca i preduzeća do državnih organa.
- Bezbednosni rizici kao što su lažiranje e-pošte, phishing napadi, neželjena pošta i druge zlonamerne šeme postali su sve prisutniji, ciljajući podatke, aplikacije, mreže i ljude.
- Kao rezultat toga, vlasnici sajtova mogu patiti u smislu izgubljenih podataka, novca, reputacije i poverenja kupaca.
- Elektronska pošta je jedan od najlakših puteva napada.
- SPF je popularna tehnika validacije elektronske pošte koja može pomoći u odbrani ovih napada, otkrivanjem lažiranja elektronske pošte, i sprečavanjem neželjene pošte.
- Korišćenje SPF zapisa takođe može pomoći u sprečavanju da vaši e-mailovi budu označeni kao neželjeni od strane drugih servera pre nego što dođu do ciljane publike.

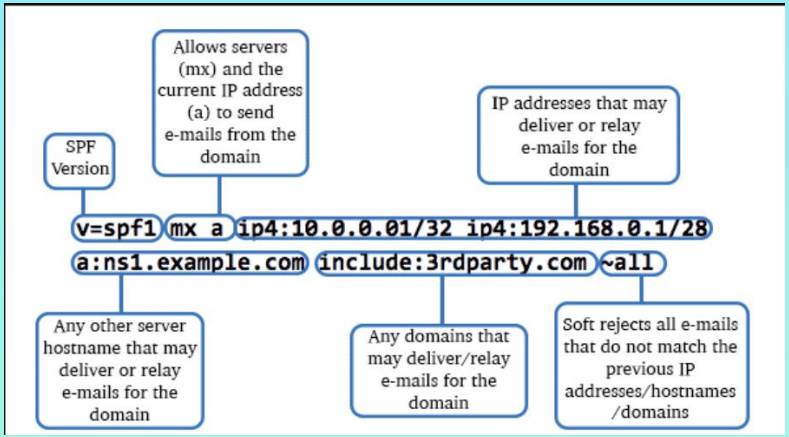
Šta je SPF zapis?

- Pre nego što dođemo do toga šta je SPF zapis, hajde da prvo razumemo SPF.
- Okvir smernica pošiljaoca (SPF) odnosi se na metod provere autentičnosti elektronske pošte koji je dizajniran da uoči falsifikovane adrese pošiljaoca tokom isporuke elektronske pošte.
- Napadači često lažiraju adrese pošiljaoca, čineći da izgledaju originalno, kao adresa običnog korisnika.
- SPF može pomoći u otkrivanju ovih poruka stavljajući ih u karantin, ili izbacujući ih iz njihovih napada.
- SPF omogućava serveru na prijemnoj strani da proveri da li poruka e-pošte koja izgleda da dolazi sa datog domena zapravo potiče sa ovlašćene IP adrese tog domena. Lista koja sadrži sve ovlašćene IP adrese i hostove za određeni domen može se naći u DNS zapisima tog domena.



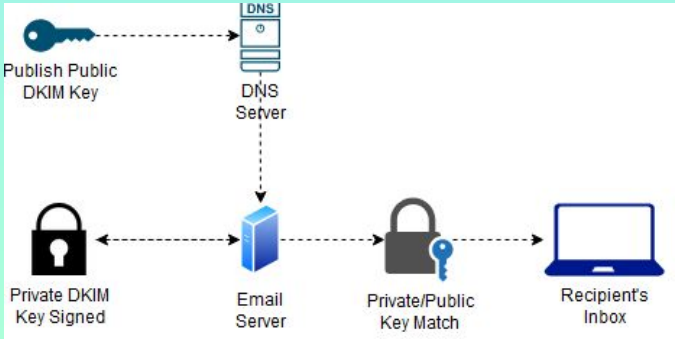
Šta je SPF zapis?

- SPF zapis je vrsta TXT zapisa objavljenog u datoteci DNS zone, koja sadrži listu svih ovlašćenih servera pošte koji mogu da šalju elektronsku poštu u ime vašeg domena. To je implementacija SPF-a koja se mora dodati vašem DNS-u da bi se pomoglo u identifikaciji i ublažavanju neželjenih elektronskih poruka od slanja zlonamernih elektronskih poruka sa falsifikovanim adresama u ime vašeg domena.
- Spameri sprovode lažiranje elektronske pošte tako što kreiraju elektronsku poštu koristeći falsifikovane adrese pošiljaoca, jer većina servera elektronske pošte ne vrši autentifikaciju. Zatim uređuju adresu pošiljaoca elektronske pošte tako što falsifikuju zaglavlja, čineći da izgleda kao da su poruke poslate sa vašeg domena.
- Ovaj proces se naziva lažiranje i omogućava pošiljaocima neželjene pošte da prevare korisnike i dobiju njihove privatne podatke i nanose štetu reputaciji.
- Danas skoro svi zlonamerni mejlovi nose lažne adrese. Kao rezultat toga, ljudi čije adrese elektronske pošte su napadači ukrali trpe oštećenje reputacije, gube vreme na popravljanje odbijenih poruka, stavljaju svoje IP adrese na crnu listu, itd.
- Zbog toga je podešavanje SPF zapisa neophodno da biste poboljšali isporuku i bezbednost vaše e-pošte.



Sta je DKIM zapis?

- DKIM (Domain Keys Identified Mail) je tehnika autentifikacije elektronske pošte koja omogućava primaocu da proveri da li je elektronska poruka zaista poslata i autorizovana od strane vlasnika tog domena.
- Ovo se radi tako što se elektronskoj pošti daje digitalni potpis.
- Ovaj DKIM potpis je zaglavlje koje se dodaje poruci i zaštićeno je šifrovanjem.
- Kada primalac (ili sistem koji prima) utvrdi da je imejl potpisan važečim DKIM potpisom, sigurno je da delovi elektronske pošte među kojima je i telo poruke, i prilozi, nisu izmenjeni.
- Obično, DKIM potpisi nisu vidljivi krajnjim korisnicima, provera se vrši na nivou servera.
- Primena DKIM standarda će poboljšati isporuku elektronske pošte.
- Ako koristite DKIM zapis zajedno sa DMARC-om (pa čak i SPF), takođe možete zaštititi svoj domen od zlonamernih e-poruka poslatih u ime vaših domena.
- Međutim, u praksi se ovi ciljevi postižu efikasnije ako koristite DKIM zapis zajedno sa DMARC (pa čak i SPF).
- DMARC i DMARC Analyzer koriste i SPF i DKIM.
- Zajedno pružaju sinergiju i najbolji rezultat za sigurnost i isporuku e-pošte.

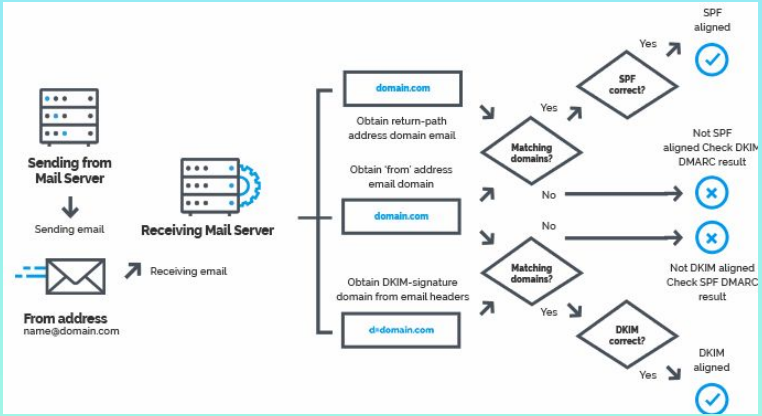


Sta je DMARC zapis?

- DMARC, ili „Provera autentičnosti poruka zasnovanih na domenu, izveštavanje i usklađenost“, je protokol za autentifikaciju elektronske pošte dizajniran da zaštiti vaš domen od korišćenja za lažiranje elektronske pošte. Koristi *Sender Policy Framework* (SPF) i *Domain Keys Identified Mail* (DKIM) za utvrđivanje autentičnosti poruke elektronske pošte.

- Jednostavno rečeno, omogućava pošiljaocima elektronske pošte da navedu kako da rukuju elektronskim porukama. Pošiljaoci imaju opciju da pošalju elektronske poruke u fasciklu sa neželjenim sadržajem, ili da ih potpuno blokiraju.

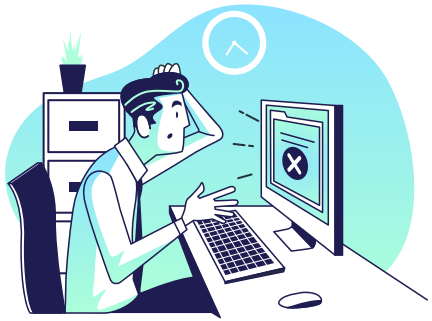
- Ulaganjem u DMARC tehnologiju, pružaoci internet usluga (ISP), državne institucije i preduzeća mogu bolje da identifikuju zlonamerne korisnike i spreče zlonamerne elektronske poruke da uđu u prijemno sanduče svojih klijenata i korisnika.



Sta je domain spoof napad?

- Prevara e-pošte je uobičajen sajber napad u kojem se izmanipulisana elektronska pošta šalje prerušena kao da potiče iz pouzdanog izvora. Pošto su zaglavlja lažnih elektronskih poruka falsifikovana, primaoci veruju da dolaze od poznatog pošiljaoca.
- Cilj lažnih elektronskih poruka je da nateraju primaoce da otvore, proslede i odgovore na ove takozvane legitimne elektronske poruke. Kao takvo, lažiranje je popularan trik koji se koristi u kampanjama za *phishing* i neželjenu poštu, jer je veća verovatnoća da će ljudi otvoriti mejlove za koje se čini da dolaze od poznatih pošiljalaca.
- Evo nekoliko uobičajenih razloga zašto akteri pretnji koriste lažiranje e-pošte:
    1. Oni mogu sakriti pravo ime pošiljaoca.
    2. Njihove zlonamerne e-poruke mogu da izbegnu stavljanje na crnu listu filterima e-pošte.
    3. Oni mogu da koriste lažiranje za krađu identiteta.
    4. Oni mogu imitirati osobu ili posao koji primalac veoma dobro poznaje.
- Ako ste vlasnik imena sajta, lažiranje e-pošte može biti prilično štetno za identitet vašeg brenda i bezbednost vaših korinika.
- Dobra vest je da su zapisi kao što je DMARC dizajnirani da se suprotstave napadima lažiranja e-pošte.

Kakve ovo ima veze sa GOV.RS domenom?



Problem?

GOV.RS domen **nema** implementiran DKIM i DMARC zapis, čime je omogućeno lažno predstavljanje domena sa kog dolazi email poruka!

Rešenje!

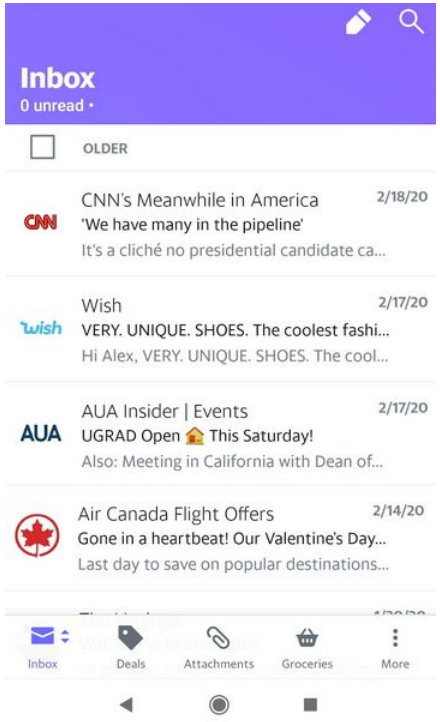
Implementacija DMARC tehnologije!

Kako se odbraniti od spoof napada?

Implementacijom DNS zapisa:

- SPF
- DKIM
- DMARC

Bonus, implementacija BIMI zapisa



- BIMI zapis je tip DNS zapisa koji se koristi za prikazivanje logotipa kompanije unutar prijemnog sandučeta elektronske pošte ako je elektronska pošta legitimna.

- Zapisi o identifikaciji poruke indikatora brenda (BIMI) predstavljaju napor čitave industrije da se logotipi brenda koriste kao indikatori koji pomažu primaocima elektronske pošte da prepoznaju i izbegnu lažne poruke.
- Ovo je bonus jer se placa ~1.000e godišnje.

Zaključak?

- Državne institucije već godinama pokazuju slabost u razumevanju informacionih tehnologija (IKT), kao i u odlučnost da se ovi problemi reše.
- Zbog ovoga, podaci građana republike Srbije su u riziku svakodnevno.
- Najstrašnija stvar u celoj priči je to što se gov.rs domen koristi za većinu državnih sajtova. Spisak adresa možete na primer videti ovde: https://securitytrails.com/list/apex_domain/gov.rs

P.S: ideja da se proveri gov.rs je potekla iz phishing kampanje koju je prenela it-klinika

Reference

- https://www.cloudwards.net/what-are-dns-records/
- https://www.makeuseof.com/what-is-a-dmarc/
- https://kinsta.com/knowledgebase/spf-record/
- https://mxtoolbox.com/dmarc/details/bimi-record/what-is-a-bimi-record
- https://mxtoolbox.com/dmarc/dkim/setup/how-to-setup-dkim
- https://securitytrails.com/
- https://www.it-klinika.rs/