# КАКО УМАЊИТИ РИЗИК ОД ПРИЈЕМА ФИШИНГ ИМЕЈЛ ПОРУКА

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

# СТАТИСТИЧКИ ИЗВЕШТАЈИ

Након појаве интернета и његовог прихватања у пословној кореспонденцији, електронска пошта је постала најчешће коришћена функција која је омогућила тренутно слање и примање порука.

Према статистичким извештајима [1] број налога електронске поште расте из године у годину, па је у 2019. износио 5.5 милијарди. Број порука електронске поште послатих у једном дану је износио 246.5 милијарди уз предвиђање да ће расти 5% годишње.

# ПРЕТЊЕ

На основу Прегледа тржишта телекомуникација и поштанских услуга у Републици Србији у 2018. Години, који је РАТЕЛ сачинио и за област безбедносних ризика у ИКТ системима, стање информационе безбедности у свету показује да је фишинг на четвртом месту најчешћих претњи, са забележеним трендом раста.

Фишинг је сајбер напад који примарно користи технике социјалног инжењеринга са циљем да завара жртве. Поруке које се шаљу могу да садрже злонамерну датотеку, линк који корисника преусмерава на интернет страницу са злонамерним садржајем, или упутство које наводи жртву да сама проузрокује сајбер инцидент.

Фишинг је до те мере заступљен да је чак 75% држава чланица ЕУ открило случајеве фишинга. Преко 90% инфекција малвером и 72% повреда података потичу управо од фишинг напада.

Посматрајући период од 2011. године, напади на мобилне телефоне у овом облику, из године у годину расту за 85%.

Посебан проблем су фишинг поруке које, као своје примарне мете препознају запослена лица у финансијском сектору или људским ресурсима. Циљ напада је крађа новца нападнуте организације. У периоду од октобра 2013. године до маја 2018. године, пријављено је чак 78.000 оваквих напада уз штету од 12,5 милијарди америчких долара.

Најчешћи прилози у оваквим електороснким поштама су: наруџбеница, плаћање, фактура, потврда, рачун, савет, трансфер.

Најчешће употребљаване речи су: плаћање (13,8%), хитно (9,1%), захтев (6,7%), пажња (6,1%), битно (4,8%), поверљиво (2,0%), хитан одговор (1,9%), трансфер (1,8%), битно ажурирање (1,7%) и пажња (1,5%).

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

# КАКО УМАЊИТИ РИЗИК?

Постоје три механизма за проверу електронске поште који могу смањити ризик од примања порука са лажиране адресе (енг. spoofing), као и од компромитације вашег пословања и то су:

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

Имплементирањем ових механизама, учинићете да домен који користите за електронску пошту буде тежи за лажирање, а системи који буду примали поруке од вас ће бити сигурни да стижу из поузданог извора.

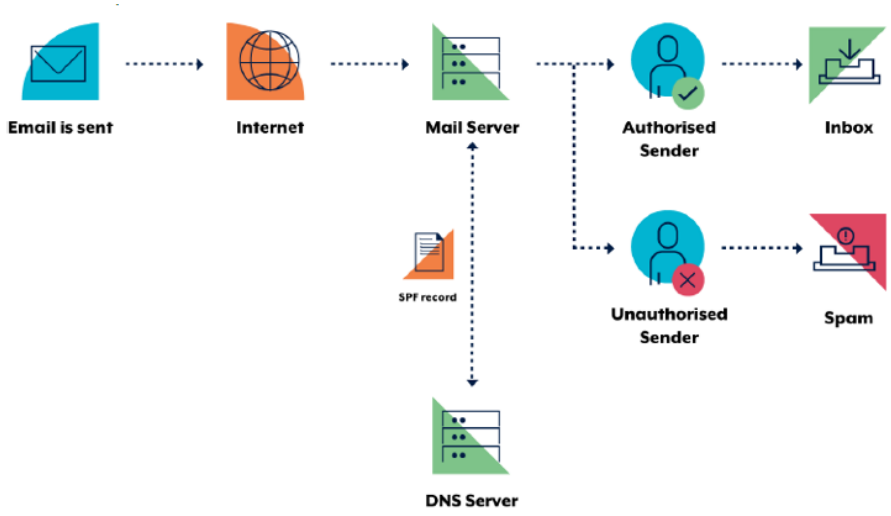
Ови механизми за заштиту система за слање и пријем електронске поште, омогућавају успешно одбијање већине тренутно актуелних фишинг напада, а њиховом применом превентивно делујете на потенцијалну злоупотребу ваших адреса електорнске поште и тиме доприносите бољем имиџу и репутацији ваше компаније.

# SENDER POLICY FRAMEWORK (SPF)

SPF [2] представља стандардизовани начин за верификацију порука електронске поште ради детектовања лажних порука.

Имплементира се објављивањем SPF записа у DNS-у да би се на тај начин идентификовала листа валидних IP адреса сервера за посматрани домен. Када *mail* сервер примаоца добије поруку, покреће се процес верификације идентитета *mail* сервера пошиљаоца коришћењем објављеног SPF записа. Уколико сервер пошиљаоца није дефинисан као ауторизовани пошиљалац у SPF запису, верификација ће бити неуспешна, а порука одбачена (смештена у сандуче за нежељену пошту) јер то значи да је адреса пошиљаоца лажирана.

На слици 1 је овај процес графички приказан [3].




Слика 1. Графички приказ SPF

За додатне информације о имплементацији препоручујемо: RFC 7208 [4].

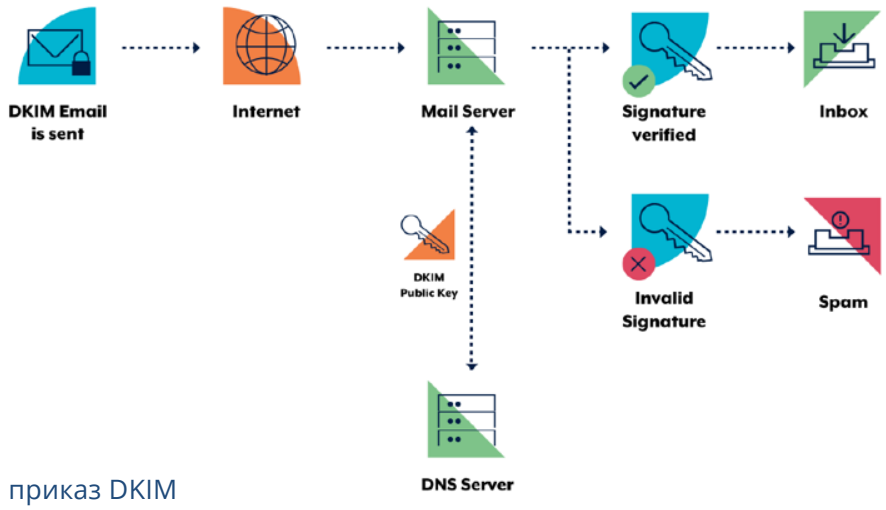
[2] RFC7208
[3] Malicious Email Mitigation Strageties, Australian Government, april 2019
[4] https://tools.ietf.org/html/rfc7208

# THE DOMAIN KEYS IDENTIFIED MAIL (DKIM)

DKIM [5] протокол омогућава криптографско потписивање порука тако да прималац може проверити да ли је порука мењана након слања.

Користи се асиметрична криптографија, односно јавни и приватни кључ. Приликом слања порука електронске поште, сервер, приватним кључем, дигитално потписује одабране делове заглавља и тело поруке, потпис смешта у DKIM заглавље и уз поруку шаље примаоцу. По пријему поруке, прималац уз помоћ јавног кључа који се налази у DNS запису проверава DKIM потпис поруке. Уколико је порука стигла у непромењеном облику, потпис ће бити валидан. У случају да је порука промењена или лажирано неко од потписаних поља, потпис неће бити валидан, а порука одбачена (смештена у сандуче за нежељену пошту).

На слици 2 је овај процес графички приказан [6].




Слика 2. Графички приказ DKIM

За додатне информације о имплементацији препоручујемо: 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)

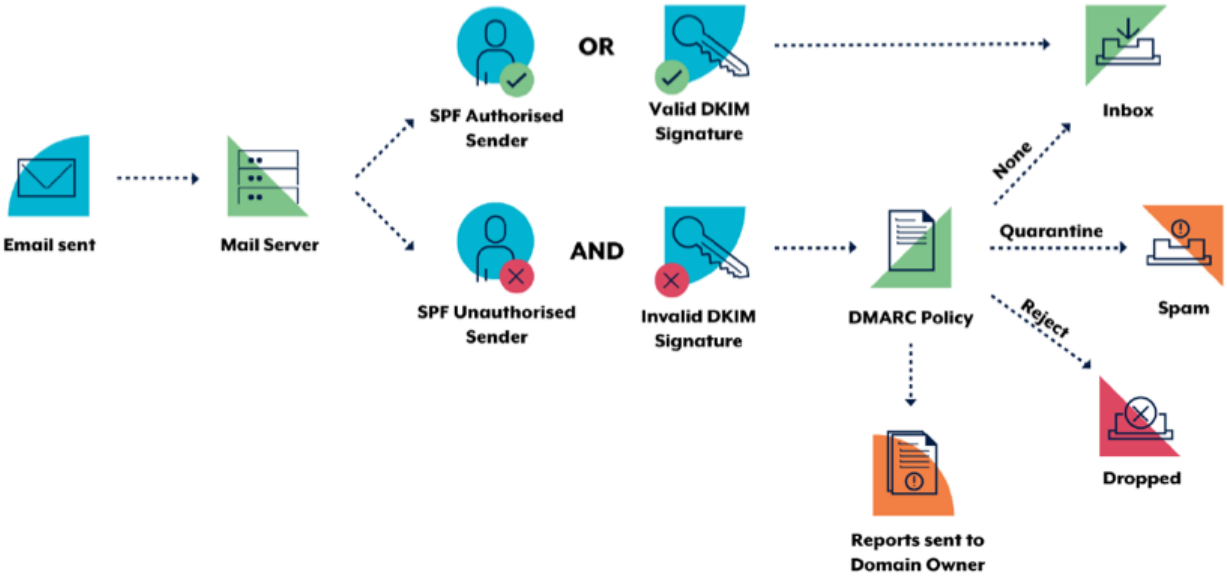
DMARC [8] протокол пружа додатан ниво безбедности комбиновањем SPF и DKIM функционалности, као и полисе којом се дефинише начин поступања у случајевима када верификација пошиљаоца није успешна.

Полису дефинише власник домена и објављује је кроз DNS запис.

Приликом пријема порука са домена, за који је дефинисан DMARC запис, *mail* сервер проверава да ли су испуњени захтеви за верификацију идентитета пошиљаоца (SPF и/или DKIM) у складу са дефиницијом полисе. Уколико је верификација успешна, порука ће бити испоручена, док ће остале бити смештене у сандуче за нежељену пошту, или у потпуности одбачене, у зависности од захтева DMARC полисе. Поред тога, полиса пружа могућност подешавања адресе електронске поште на коју ће се власнику домена слати информације о IP адресама које су покушале да злоупотребе његов домен, чиме се омогућава његово проактивно реаговање и спречавање озбиљнијих напада који лажирају посматрани домен. Највећи ниво заштите се постиже када су имплементиране и SPF и DKIM функционалности заједно са DMARC протоколом.

[8] RFC7489

На слици 3 је овај процес графички приказан [9].




Слика 3. Графички приказ DMARC

DMARC стандард је формиран 2013. године и већ у првој години постојања је помогао да се заштити 60% сандучића електронске поште широм света од фишинга и нежељених порука [10].

За додатне информације о имплементацији препоручујемо: RFC 7498 [11].

# ПРЕПОРУКА НАЦИОНАЛНОГ ЦЕРТ-А

Национални ЦЕРТ препоручује пре примене наведених механизама процену ризика пословања, односно да ли се улагања могу оправдати смањењем ризика од компромитације сигурности.

Уколико поседујете сопствени сервер за слање и пријем електронске поште, неопходно је да се обратите одговорном лицу које је задужено за његово одржавање, односно исправно функционисање.

Исти принцип је неопходно применити и у случајевима када се домен и сервер за слање и пријем електронске поште налазе код хостинг провајдера.

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