Kas ettevõtte e-mailid jõuavad kirjasaajale õigesti kohale

SPF, DKIM ja DMARC on kolm tehnoloogiat, mis aitavad vältida ettevõtte saadetud e-posti märkimist rämpspostiks ja tagavad kirja soovitud kasutajale kohale toimetamise.

Tähelepanu vajab e-maili turvalisus ja *e-mail spoofing*[1]. Ettevõtte juhina ei peagi sa teadma, et mis on **SPF**, **DKIM** ja **DMARC**. Kuid oluline on uurida välja, et kas ettevõtte IT osakond on selles osas kõik vajalikud meetmed kasutusele võtnud ja *olgu mainitud, et kõik need kolm DNS kirjet korraga ja kõigil ettevõttega seotud domeenidel*!

Milleks seda seadistada vaja on? **Tegevus on vajalik, et piirata identiteedi ülevõtmist ja teie ettevõtte mõne juhtiva isiku nimel kergelt e-maili saatmise võimalust piirata.** Nende DNS kirjete samaaegne seadistamine aitab tõhusalt kaitsta teie ettevõtet e-kirjade pettuste eest ja tagada, et olulised kirjad saajatele *spam/junk* kausta ei jõuaks või keegi pahalane ettevõtte tegevjuhi või finantsjuhi või müügijuhi nimel kirju välja ei saadaks.

1. **SPF** (*Sender Policy Framework)* on nimekiri serveritest, millel on õigus teie ettevõttega seotud domeeni nimega e-posti saata. Tuleb koostada ammendav loend kõigist teenustest, kes tohivad teie ettevõtte nimel kirju saata, loendist välja jäänud allikad ja neist edastatavad kirjad ei saa ega ka tohi enam saajale kohale jõuda.
2. **DKIM (***DomainKeys Identified Mail*) lisab väljuvale e-postile digitempli, mis võimaldab vastuvõtjal kontrollida saatja õigust domeeni nimel e-posti saata. See tuleb lisada igale e-maili väljasaatvale teenusele. Näiteks Outlook O365, veebiserver, uudiskiri, majandustarkvarast arvete või tellimuse kinnitamise saatmisel jne
3. **DMARC** (*Domain-based Message Authentication Reporting and Conformance*) kinnitab, et SPF ja/või DKIM on kasutusel ning võimaldab tellida raporteid väärkasutuse või reeglitele mitte vastavate kirjade kohta. Samuti määrab SPF ja DKIM reeglitele mittevastavate kirjade ka garantiini panemist (näiteks *spam* kaustas jõuab kohale) või keelab sootuks teie ettevõtte domeeni nimel võltsitud kirjade kohalejõudmise.

Ülevaatlik skeem juhendis kirjeldatud tegevustest

Oluline on tähele panna e-posti autentimise protokollide (SPF, DKIM, DMARC) olulisust ja teostada nende korrektne seadistamine kõigis teie ettevõtetes ja kõigi ettevõttega seotud domeenides. Korrektselt seadistatud autentimiskirjed aitavad kaitsta ettevõtet e-posti pettuste, rämpsposti ja turvariskide eest ning tagada e-posti usaldusväärsus ja kättetoimetatavus.

Oluline on seadistada see kõigile ettevõttega seotud domeenidele,

ka neile domeenidele, millelt tegelikult e-maile välja ei saadetagi.

Ilmselt on nii ootuspäraselt mittetöötava e-maili liikluse osas kui ka ettevõtte nimel võltsitud kirjade saatmisel mõjutatud nii ettevõtte maine kui ka selle suhtluspartnerid, kes võivad puutuda kokku petturlike e-kirjadega või kogeda e-kirjade kättetoimetamise probleeme. Näiteks, et kas on mõni oluline kiri jäänud kätte saamata või on see leitud SPAM kaustast? See näitabki ilmekalt, et kirja saatja peaks nende eeltoodud ettevõtte domeeni DNS-seadistustega tegelema, et e-maili saajad saaksid vajalikud e-kirjad ootuspäraselt ja õigesti kätte!

[1] Email spoofing: what is it and how to stop it? https://cybernews.com/secure-email-providers/email-spoofing/

Kes on mõjutatud, kui seadistused jätta tegemata?

Halvasti või vigaselt seadistatud SPF-, DKIM- ja DMARC-kirjed võivad mõjutada mitmeid erinevaid osapooli:

1. **Ettevõte:** domeeni omanik – ettevõte ise on peamine osapool, kes võib saada mõjutatud, kui tema e-posti autentimise kirjed pole korrektselt seadistatud. See võib kahjustada ettevõtte mainet, suurendada turvariske ja põhjustada e-kirjade kättetoimetamise probleeme. (*kiri ei lähe sootuks kohale või leitakse SPAM kaustast* või keegi pahalane kirjutab kirju teie ettevõtte nimel)
2. **Kliendid ja partnerid:** halvasti seadistatud e-posti autentimise kirjed võivad mõjutada ka ettevõtte kliente ja partnereid. Kliendid võivad saada rämpsposti või petlikke e-kirju, mis näivad olevat pärit ettevõtte alt, mis võib kahjustada nende usaldust ettevõtte vastu. Partnerid võivad samuti kogeda e-kirjade kättetoimetamise probleeme või turvariske, saades justkui e-kirja teie ettevõttelt ja selle usalduse pinnalt toimub pahatahtlik tegevus.
3. **Vastuvõttev e-posti teenusepakkuja:** halvasti seadistatud e-posti autentimise kirjed võivad mõjutada ka vastuvõtvaid e-posti teenusepakkujaid. Kui e-posti kirjed pole korrektselt seadistatud, võivad teenusepakkujad tõlgendada ettevõtte e-kirju kahtlastena või märgistada need rämpspostina, mis võib viia e-kirjade kohaletoimetamise probleemideni või nende blokeerimiseni. Google, Microsoft ja Yahoo [2] on jõuliselt otsa lahti teinud ja tõkestavad kirjade ootuspärast kohalejõudmist domeenidelt, mis on seadistamata.
4. **E-posti kasutajad:** lõppkasutajad võivad olla mõjutatud, kui halvasti seadistatud e-posti autentimise kirjed põhjustavad nende e-kirjade kohaletoimetamise probleeme või kui nad saavad rämpsposti või petlikke e-kirju, mis näivad olevat pärit ettevõtte alt.

Kokkuvõttes võivad halvasti või vigaselt seadistatud SPF-, DKIM- ja DMARC-kirjed mõjutada kõiki osapooli, kes on seotud ettevõtte e-posti kommunikatsiooniga, ning põhjustada mitmeid negatiivseid tagajärgi, sealhulgas mainekahjustusi, turvariske ja kättetoimetamise probleeme. Seetõttu on oluline hoolikalt jälgida ja hallata e-posti autentimise kirjeid, et tagada ettevõtte e-posti turvalisus ja usaldusväärsus.

[2] Understanding Gmail and Yahoo DMARC Requirements https://dmarcian.com/yahoo-and-google-dmarc-required/

Sisukord

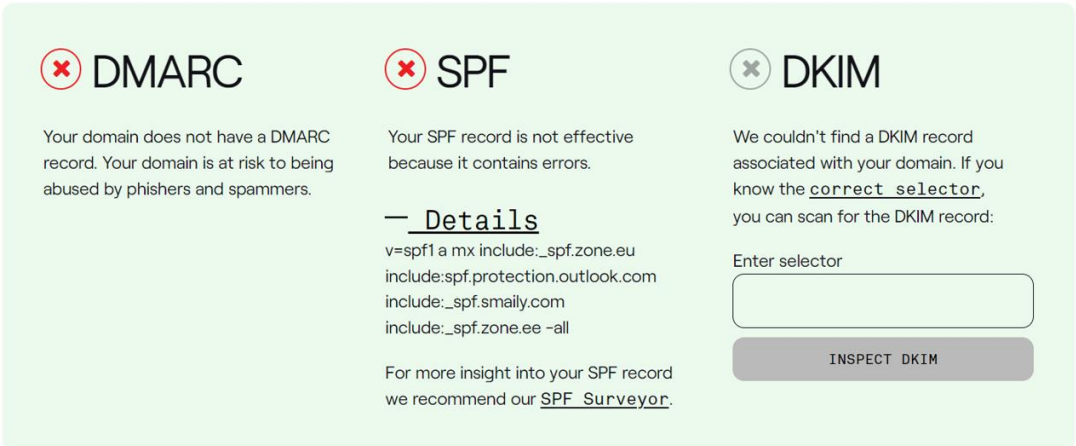
Testime e-maili saatmist ja seadistusi

Ettevõtte domeenide DMARC-i, SPF-i ja DKIM-i konfiguratsiooni õigesti seadistamise testimiseks saab kasutada mitmeid tööriistu ja meetodeid. Järgnevalt on toodud mitmed sammud ja tööriistad ettevõttega seotud domeenide esmaseks kontrollimiseks.

Kuidas näeb välja seadistamata domeen

Testi seda näiteks Dmarcian tööriistaga, kus saad esmase vastuse, et kas sinu ettevõtte domeeni vaade on samuti punane ja kas on välja toodud probleemikohad? Märka, et alloleva lingi pealt peaks avanema vaade, kus selguks, et nii DMARC SPF ja DKIM on õigesti seadistatud. Ilmselt esimene vaade ei ole kohe ootuspärane ja võib sarnaneda näidispildiga.

Vaata üle: https://dmarcian.com/domain-checker/?domain=**ettevõttedomeen.ee**
(kirjuta siia ettevõtte domeen, mida soovid testida)



Testime e-maili saatmist mail-tester'iga

Varasem test andis ülevaate domeeni kirjete üldisest olemasolust ja võimalikest esmasel tuvastusel esile kerkinud parendamist vajavatest leidudest. Järgnevalt on mõistlik testida iga e-maili saatvat teenust eraldiseisvalt!

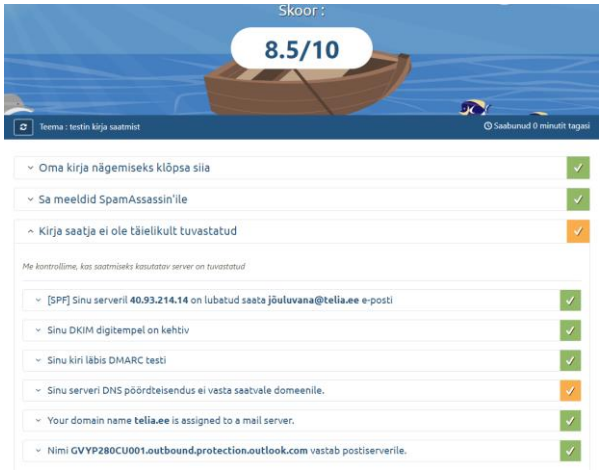
Mail-tester.com on veebiteenus, mis võimaldab kasutajatel testida ja analüüsida e-kirjade saatmise kvaliteeti. Teenus hindab e-kirjade SPF, DKIM ja DMARC kirjeid, kontrollib e-kirjade sisu rämpspostifiltrite suhtes ning annab tagasisidet parandamiseks, et tagada e-kirjade edukas kohalejõudmine. Seal olevaid soovitusi on mõistlik kõiki jälgida ja teenustel korda seadistada.

Mõistlik on saata erinevate e-maili väljasaatvate teenuste pealt test kirjad mail-tester.com toodud unikaalse e-maili peale.

Teeme koos testi – kas sinu e-post näib spämmina?

Jälgime, et kas vajalikud kirjad kasutajatele kohale jõuavad või esineb e-maili saatmise seadistuses puudusi, mida on üldjuhul lihtne eemaldada, kui on teada, et mis täpselt mureks on.

Saadame näiteks test arve (mis platvorm seda saadab, *tihti võib olla, et lisaks ühele majandustarkvarale saadab mingi süsteem veel kliendi nimel arveid välja*), testime turunduse poolelt uudiskirjade saatmist (kui neid saadetakse), veebilehe ankeedi või teeme kontakti ankeedi kinnitusmaili testi, saadame testiks e-poe tellimuse kinnituskirja, personaliosakonnast palgateatise ja testime samuti Outlook'ist igapäevasel viisil kirja saatmist jne...



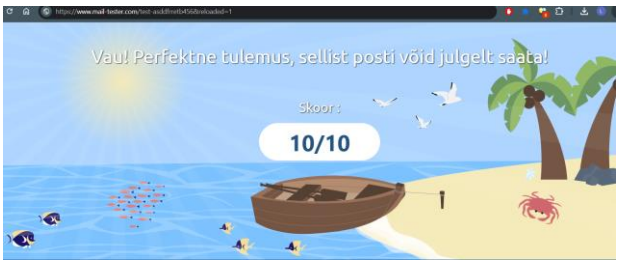
Nagu eelnevalt välja sai toodud, siis mõistlik on e-maili kirjade saatmist testida kõigi ettevõtte domeenide ja teenuste jaoks eraldi, kasutades näiteks https://www.mail-tester.com/ teenust, kus saadetakse iga teenuse pealt eraldi testkiri uue genereeritud test-e-maili aadressi peale, mille raporteid ja e-maili saatmise kvaliteeti saab eraldi analüüsida.

Kuidas e-kirja kohalejõudmist testida

- Loetle üles kõik ettevõtte poolt kasutatavad domeenid ja teenused, mis e-maile nende pealt ettevõtte nimel välja saadetakse.
    - Jälgi, et kas vajalikud kirjad kasutajatele kohale jõuavad. Näiteks arve, mis platvorm seda saadab, uudiskirjad, kui neid saadetakse, veebilehe kinnitusmail või form jne...
- Kirjuta testkirjad https://www.mail-tester.com/ toodud e-maili aadressile.
    - Selleks ava mail-tester veebileht ja saad sealt unikaalse testimise aadressi ning seejärel saada näiteks majandustarkvarast toodu e-mailile näidisarve. Vajuta nuppu „**Seejärel vaata tulemust**„. Saadud tulemus võiks olla ca 9/10 või parem. 😉
    - Võta uues aknas (*tabis*) lahti uuesti Mail-tester esileht, seal genereeritakse uus e-maili aadress. Saada sinna näiteks Outlookist näidis e-maili. Kontrollin uuesti tulemust.
- Korda seda kõigi teenustega, millelt tead, et ettevõtte domeenilt kirju välja peaks saatma. **Märka:** seda protsessi tuleb korrata kõigi ettevõtte domeenidega, mis kirju välja saadavad.

Iga e-maili välja saatev teenus, igalt erinevalt domeenilt, on vaja eraldi läbi testida.
Näiteks ettevõtte turundusliku uudiskirja ootuspärane kohalejõudmine ei aita majandustarkvarast arvel kohale jõuda, sest ilmselt neid saadavad erinevad tarkvarad.

Märka, et mail-tester e-maili testitulemus võiks olla minimaalselt üheksa punkti kümnest või lausa tulemusega kümme. Kui mõne teenuse testimisel (näiteks arve saatmisel) on saadud tulemus halvem, siis tehtud test näitab võimalikud murekohad (*vajadusel lase kellelgi tehnilisemal isikul testi tulemusega tutvuda*) , millele peaks tähelepanu pöörama ja seadistused korda tegema, vastasel juhul muidu suure tõenäosusega samast allikast saadetud päris kirjad ei pruugi samuti alati kirja saajale ootuspäraselt kohale jõuda. Tavapärane on olukord, kus turundustiim imestab, et miks just Teie ettevõtte uudiskirjade avamise statistiline protsent on nõnda madal või raamatupidaja jällegi helistab kadunud arve pärast, et miks see saajale kohale pole jõudnud, ühiselt leides selle siis spämm kaustast.



Kui vajate abi testi tulemuste tõlgendamisel või DNS kirjete hilisemal seadistamisel, siis palun saata testi tulemused ka meile (*iga testi alla tekib link, mida saab soovi korral jagada - kui testi tulemus on kehvem kui 9/10 st* 😉) Vaatame koos peale ja leiame lahenduse. Märka, et testi tulemus säilib seal mail-tester serveris üsna lühikest aega ja hiljem testitud tulemust ja seisu tagasiulatuvalt näha ei saa ja tuleb teostada vajadusel samal viisil uus test.

SPF (*Sender Policy Framework*)

Paljudel ettevõtetel on SPF DNS kirje ilmselt mingil viisil olemas. Kogemus näitab, et see on seadistatud aastaid tagasi ja ei sisalda kõiki tänasel päeval kliendi nimel e-maile saatvaid teenuseid ja on vaja kaasajastada teenuste SPF kirjeid, mis on ajas ilmselt muutunud. Samuti on varasemalt tihti tehnilisel seadistajal jäänud tähelepanuta, et näiteks mis vahet on SPF kirjes „*~all and -all*“ seadistusel. Harvad ei ole ka juhud, kus „ *-all*“ on kirjutatud SPF kirjes tähelepanematusest mitu korda, mis teeb süntaksi serverite jaoks nö katki ja loetamatuks, ning kõike peale esimese „*-all*“ järgset seadistuses toodut tegelikult arvesse ei võetagi.

Kontrolli SPF kirje kehtivust ja olemasolu:

https://dmarcian.com/spf-survey/?domain=**ettevõttedomeen.ee**

Selles valguses tasub värske pilguga uuesti iga ettevõttega seotud domeeni SPF kirje üle vaadata ja vajadusel täiendused teha.

SPF kirje seadistamise plaan

SPF-kirje seadistamine nõuab täpset mõistmist ettevõtte e-posti infrastruktuurist ja sellest, millised serverid võivad volitatult ettevõtte nimel e-kirju saata. Siin on mõned näited ja ettepanekud selle kohta, kuidas SPF-kirjeid seadistada ning milliseid küsimusi ettevõte peaks endale esitama:

1. **Määratlege lubatud e-posti serverid:** Tehke kindlaks kõik ettevõtte domeeni alt saadetavad e-kirjade serverid. See võib hõlmata ettevõtte enda servereid, kolmanda osapoole teenusepakkujaid või turundus- ja majandusplatvorme ning e-poodi jne. Näiteks isegi *printer-kombain-scanner* võib saata scannitud pildi e-maile.
2. **Koguge serverite IP-aadressid:** Hankige kõigi volitatud serverite IP-aadressid, mida kasutatakse e-posti saatmiseks. See võib hõlmata nii IPv4 kui ka IPv6 aadresse. (IP aadressid koguda siis *nende teenuste kohta, millel puudub include:teenusenimetus valmis seadistus*)
3. **Kontrollige olemasolevaid SPF-kirjeid:** Kui teie domeenil on juba SPF-kirje, kontrollige ja veenduge, et kõik volitatud serverid ja teenused oleksid loetletud ja et SPF-kirje oleks õigesti konfigureeritud (sh piisav reegli rangus „*soft fail ~all vs hard fail -all*“).
4. **Lisage uued serverid ja teenused SPF-kirjesse:** Kui teie ettevõttel on uusi e-posti saatvaid servereid ja teenuseid või kui olete lisamas uusi teenusepakkujaid (*näiteks võtsite kasutusel uue majandustarkvara*), lisage need vastavalt SPF-kirjesse. Samuti eemaldage loendist teenused, mida tegelikult ei kasuta enam.
5. **Testige SPF-kirjeid:** Pärast SPF-kirje seadistamist tehke kindlasti põhjalik test, et kontrollida, kas e-posti saatmiseks kasutatavad serverid vastavad SPF-kirje nõuetele ja et kirje töötab ootuspäraselt. Kontrolli siit: https://dmarcian.com/spf-survey/?domain=**ettevõttedomeen.ee**

Kokkuvõttes on SPF-kirje seadistamine oluline samm e-posti turvalisuse tagamisel. Ettevõtte peaks tagama, et kõik volitatud serverid ja teenuspakkujad oleksid korralikult loetletud SPF-kirjes ning regulaarselt kontrollima ja vajadusel uuendama SPF-kirjeid vastavalt ettevõtte e-posti infrastruktuuri muutustele.

Etteruttavalt märka: Kui kõigi toimingute järgselt on kõik õigesti seadistatud, mis tähendab, et DMARK kirjes on märgitud p=reject ja sp=reject (*outright rejects all emails that fail the DMARC check*) ning aspf=s (*Strict Mode*) ning SPF kirjes on kasutatud (*-all*), siis saate luua olukorra, kus ettevõtte nimel piiratakse lubamatutel teenustel e-maile välja saata. Samas tähendab see ka seda, et ilma SPF ja DKIM kirje lisamiseta uusi teenuseid ei saa, ega tohigi kasutuse võtta, mis tõkestab ettevõtte nimel *e-mail spoofing* pahatahtliku [3] kasutamise.

[3] Email spoofing: what is it and how to stop it? https://cybernews.com/secure-email-providers/email-spoofing/

Näide soovituslikust ootuspärasest SPF kirjest

See kirje peaks sisaldama siis kõiki teenuseid, mille alt sellelt domeenilt ettevõtte nimel e-kirju välja saadetakse. Selles näidisena **toodud SPF kirje loetelus (teie ettevõtte domeenis) peavad olema KÕIK teenused**, mida selle domeeni juures e-mailide saatmisel kasutatakse. Kui midagi on jäänud alltoodud näites väljatoodud viisil kirjeldamata, siis nende teenuste kaudu kirjade saatmine võib mitte töötada ootuspäraselt. Kontrollige üle, et näiteks CRM tarkvara, e-pood või täiendav majandustarkvara või uudiskirjade saatmise teenus on siis SPF lubatud teenuste loetelus ettevõtte kasutusel olevas domeenis olemas.

Näide: v=spf1 a mx include:_spf.zone.eu include:spf.protection.outlook.com include:_spf.smaily.com include:mail.zendesk.com a:directo.gate.ee ip4:123.12.21.321 -all

- a tähistab, et veebilehe IP märgitakse lubatud kirjasaajate loendis
- mx viitab e-maili teenuste kirje peale, et seal toodu oleks igaks juhuks ka esile toodud
- spf.protection.outlook.com antud juhul kasutaks ettevõte Office 365 e-maili lahendust
- _spf.zone.eu viide Zone Media e-maili lahendusele
- _spf.smaily.com viitab uudiskirja saatmise lahendusele
- mail.zendesk.com näitab, et nende domeeni alt saadetakse samuti Zendesk tarkvarast kirju
- directo.gate.ee arved ning tellimuse kinnitused saab saata majandustarkvara kaudu
- IP4 aadressi kujul on viidatud ka näiteks üks server, mis kliendi nimel kirju välja saadab
- Sarnasel viisil tuleb koostada ammendav ja mitte midagi välistav loetelu allpool viidatud SPF kirjete loendi alusel, just need teenused, mida klient päriselt igapäevaselt oma e-mailide saatmiseks kasutab. *(SPF list sisaldab just ja ainult neid lubatud allikaid, millelt päriselt klient e-maile saadab*)

  Vaata lisaks Süntaks, mida SPF reeglis kasutada: https://dmarcian.com/spf-syntax-table/

Kontrolli SPF kirjes viidatud teenuseid

Vaata, et kas ettevõttes on kasutusel mõni allolev teenus, mida ettevõte tegelikult kasutab oma domeenilt e-mailide saatmiseks ja kas see on kindlasti SPF kirjes välja toodud. Kontrolli samuti, et viidatud süntaks oleks täpselt sama, kuna ajas on teenuspakkujate SPF kirjete lausendid muutunud. *(Näiteks include:sendsmaily.info on muutunud include:_spf.smaily.com vastu)*

Kõige kindlam on see üle kontrollida otse teenuspakkuja käest, kus tavaliselt on neil veebilehel viide õige seadistuse kohta. Näiteks uudiskirjade teenuspakkuja Smaily on koostanud sellise juhendi https://smaily.com/et/help/juhendid/konto-seaded/spf-ja-dkim-kirjete-lisamine/

Tuntud postiteenuste soovituslikud SPF klauslid

Allikas	kirje
Amazon SES	include:amazonses.com
Directo ERP äritarkvara	a:directo.gate.ee
Excellent Standard Book	a:smtp2.excellent.ee
Google GSuite	include:_spf.google.com
mail.neti.ee	include:_netblocks.neti.ee
Mailchimp	include:servers.mcsv.net
Mailgun	include:mailgun.org
Mailjet	include:spf.mailjet.com
Mandrill	include:spf.mandrillapp.com
Microsoft	include:spf.protection.outlook.com
Radicenter	include:_spf.radicenter.eu

Sendgrid	include:sendgrid.net
Smaily	include:_spf.smaily.com
SMTP2go	include:spf.smtp2go.com
Zendesk	include:mail.zendesk.com
Zone Eesti	include:_spf.zone.eu
Telia	include:_netblocks.neti.ee include:teliaklm.ee
Telia MLX	include:_spf.mlxplus.com
veebimajutus.ee / Elkdata	include:mail.spf.elkdata.ee
Sinu oluline e-maili teenus	Uuri teenuspakkujalt, et milline kirje tuleb SPF reeglile lisada!

Seadista domeeni teenuspakkuja juures SPF kirje

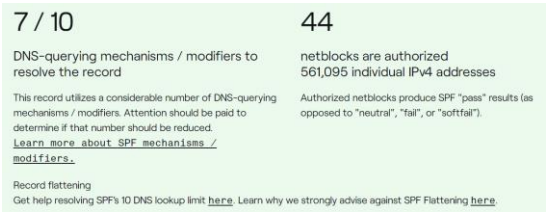
Igal domeenil on majutuseks kasutusel teenuspakkuja, kelle iseteeninduse kaudu saab vajalikud DNS täiendused teostada. Näiteks Zone Media majutuse SPF ja DKIM ning DMARK muutmise juhendi leiab siit: https://help.zone.eu/kb/spf-kirje/ ja igal teenuspakkujal on üsna samataoline võimalus soovi korral ise seadistusi korrastada. Samas, kui ei tunne kindlalt nende seadistuste tegemisel, siis pöördu abisaamiseks spetsialisti poole.

Vigaselt seadistatud DNS kirjed toovad pigem kahju kui kasu.

Tehniline: liiga palju DNS loops'e

Oluline on jälgida, et üle kümne DNS lookup osa SPF-kirjes kirjeldada ei ole mõistlik ja seda tuleb kindlasti tähele panna.

Kuidas parandada ja õigesti SPF kirjet kirjutada, sellel veebilehel on välja toodud mõned soovitused https://dmarcian.com/spf-best-practices/.



DKIM (*DomainKeys Identified Mail*)

DKIM-kirjete (*mitmuses*) seadistamine on oluline samm e-posti turvalisuse tagamisel, kuna see võimaldab vastuvõtja serveritel kontrollida, et kas e-kiri on saadetud domeeni omaniku poolt volitatud saatja poolt ja kas see on saadetud muutumatuna. DKIM aitab vähendada e-posti võltsimise riski ning suurendab e-kirjade usaldusväärsust. Enne DKIM-kirje(te) seadistamist tuleb siiski hoolikalt jälgida juhiseid ja veenduda, et olete järginud kõiki vajalikke samme õigesti.

Märka: oluline on meeles pidada, et kui iga domeeni kohta on üks DMARC kirje ja üks SPF kirje, kuhu koondatakse kõik vajalik süntaks kokku. Siis DKIM kirjeid võib olla iga domeeni kohta mitmeid, sõltuvalt kui palju on e-maili saatvaid teenuseid.

DKIM kirje tuleb seadistada iga ettevõtte nimel e-maili välja saatva teenuse kohta, mis seda tehniliselt võimaldab. Allolevalt mõned näited, et kuidas seda seadistatakse. DKIM võti koostatakse DNS kirjetes viisil: „***teenusenimetusevõti._domainkey.ettevottedomeen.ee***“

Kontrolli DKIM kirje kehtivust ja olemasolu:

https://dmarcian.com/dkim-inspector/?domain=**ettevõttedomeen.ee**&selector=**teenusevõtmenimetus**

Office 365 kontoritarkvara

DKIM kirje selector: O365 DKIM on kättesaadav **selector1** ja **selector2** kirje (**Märka:** *mõlemad peavad olema seadistatud ja andma nö rohelise tulemuse eelviidatud dkim inspector testiga*).

1. **O365 Tenantis:** kontrolli, millised domeenid (ja alamdomeenid) on kliendil MS365-s valideeritud
2. Kontrolli iga domeeni DKIM seadistust https://security.microsoft.com/dkimv2 ja kui DKIM kirje puudub, siis lisa (seadistades pakutavad C-NAME kirjed konkreetse domeeni DNS-i ja aktiveerides seejärel need omakorda DKIM MS365 adminnis)
   Märka, et DKIM kirje peab tegema konkreetse domeeni peale, mitte ainult xyz-onmicrosoft-com – vastasel juhul „*DKIM aligment rate*“ kukub! Selles sammus ilmselt vajad O365 e-maili teenuspakkuja tuge DKIM võtmete seadistamisel (kellel on admin juurdepääs Tenantile ja domeeni DNS kirjetele).

Juhend: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dkim-configure

- **Kirje Selector 1:**
  - **Hosti nimi (***Name/Host/Alias***)**: selector1._domainkey.yourdomain.com
  - **CNAME kirje (***Value/Answer/Destination***)**: selector1-yourdomain-com._domainkey.yourdomain.onmicrosoft.com
- **Kirje Selector 2:**
  - **Hosti nimi (***Name/Host/Alias***)**: selector2._domainkey.yourdomain.com
  - **CNAME kirje (***Value/Answer/Destination***)**: selector2-yourdomain-com._domainkey.yourdomain.onmicrosoft.com

Need kirjed on üliolulised, kuna neid kasutatakse teie domeenist väljaminevate meilide DKIM-i allkirja kontrollimiseks.

Directo majandustarkvara

DKIM kirje selector: majandustarkvara kasutab DKIM kirjet võtmega: **directo** *(directo._domainkey.ettevottedomeen.ee)*

Kui jätta see seadistamata, siis see võib kaasa tuua tagajärje, et näiteks Directo majandustarkvarast arved, tellimuse teavitused ja kinnituskirjad ei pruugi ootuspäraselt kohale klientidele minna ja võivad nö spämmina märgistatud saada.

Juhend: https://wiki.directo.ee/et/kui_meilid_tulevad_tagasi

Standard Books majandustarkvara

DKIM kirje selector: majandustarkvara kasutab DKIM kirjet võtmega: ***smtp4*** *(smtp4._domainkey.ettevottedomeen.ee)*

Kui jätta see seadistamata, siis see võib kaasa tuua tagajärje, et majandustarkvarast arved, tellimuse teavitused ja kinnituskirjad ei pruugi ootuspäraselt kohale klientidele minna ja võivad nö spämmina märgistatud saada.

Juhend: https://www.excellent.ee/kasutajatugi/programmist-saadetud-e-mail-tuleb-saajalt-veateatega-tagasi-spf-fail-not-authorized-mis-pohjusel/

Smaily uudiskirjad

DKIM kirje selector: uudiskirju saad kontrollida näiteks **blue.smly** ja **green.smly**
Märka: *mõlemad võtmed peavad seadistatud olema*

Kui jätta see seadistamata, siis see võib kaasa tuua selle, et Smaily uudiskirjad ja teavitused ning kinnituskirjad ei pruugi ootuspäraselt kohale klientidele minna ja võivad nö spammi minna või ei jõua saajale üldse kohale.

Juhend: https://smaily.com/et/help/juhendid/konto-seaded/spf-ja-dkim-kirjete-lisamine/

MailChimp

DKIM kirje selector: uudiskirjad saab kontrollida **mte1** ja **mte2**

Märka: ilmselt *mõlemad peavad seadistatud olema*

Kui jätta see seadistamata, siis see võib kaasa tuua selle, et Mailchimp uudiskirjad ja teavitused ning kinnituskirjad ei pruugi ootuspäraselt kohale klientidele minna ja võivad nö spammi minna või ei jõua saajale üldse kohale.

Juhend: https://mailchimp.com/developer/transactional/docs/authentication-delivery/

Zone Media

DKIM kirje selector: saab kontrollida **zone**

Kui jätta see seadistamata, siis see võib kaasa tuua selle, et veebilehelt (kontaktiorm kirjad või e-poe arved näiteks) kirjad ei tule saajale ootuspäraselt kohale ja võivad nö spammi minna. Samuti, kui kasutatakse Zone webmail e-maili lahendust, siis on oluline DKIM (ja spf) seadistada.

Juhend: https://help.zone.eu/kb/dkim/

Zendesc tarkvara

DKIM kirje selector: Zendesc seadistusi saab kontrollida **zendesk1** ja **zendesk2**
Juhend: https://support.zendesk.com/hc/en-us/articles/4408822303386-Digitally-signing-your-email-with-DKIM#topic_k3v_gfv_rk

Mandrillapp

DKIM kirje selector: Seadistusi saab kontrollida **mandrill**
Juhend: https://dmarcly.com/blog/how-to-set-up-spf-and-dkim-for-mandrill

Amazonses

Juhend: https://docs.aws.amazon.com/ses/latest/dg/send-email-authentication-dkim.html

Mõni muu tarkvara, mida igapäevaselt emailide saatmiseks kasutad

Eeldus: saadad e-maile välja oma ettevõtte domeeni pealt, mitte ei kasuta teenuspakkuja e-maili domeeninimega aadressi nimekuju.

Uuri tarkvara või teenuse pakkujalt, et kuidas seadistada ettevõtte domeenile SPF ja lisada DKIM võti, et teenust asjakohaselt kasutada saaks. Tuntumad teenuspakkujad leiab ka Google kaudu otsides fraasi „*tarkvaranimi SPF DKIM selector*“ ja ilmselt esimeste tulemuste hulgas on vajaminev juhend olemas.

MS-Modern-Auth

Teatud e-maile väljasaatvad teenused toetavad samuti Office 365 Modern Auht lahendust. Selliselt saab e-mailid edastada nö API kaudu ja liidestada see otse Microsofti Tenantiga.

Merit

Juhend: https://www.merit.ee/juhend/muud/MS-Modern-Auth-Aktivas.pdf

Directo

Directo seadistamine office365 jaoks (*vaadata üle, et see oleks õigesti tehtud või kasutada eeltoodud SPF kirje ja DKIM võtme juhendit, mis kasutab kirjade saatmiseks Directo serverit*)

- Server smtp.office365.com:25
- SSL/TLS: StartSSL/SSL/TLS
- MFA (multi factor authentication) puhul tuleb luua Directo jaoks app password
- Microsoft 365 admin center > Users > Active user > [Kasutaja] > Mail > Manage email apps
- Siit peab valitud olema Authenticated SMTP
- Kui saatmisel tekkib viga näiteks ERR: 334

Juhend: https://wiki.directo.ee/et/office365_334

Mõni teine tarkvara – MS Modern Auth lahendus

Ilmselt mõned teised tarkvarad võimaldavad sarnasel viisil võtta kasutusele otse MS Modern Auth lahendus. Uuri selle kohta konkreetse tarkvara pakkuvalt teenuspakkujalt.

DMARC (*Domain-based Message Authentication, Reporting, and Conformance*)

DMARC ehk petiste tuvastamise süsteem. Zero Trust Email – lihtsamalt öeldes tähendab *Zero Trust* seda, et kasutajaid, seadmeid, võrke, teenuseid ja tarkvara ei tohiks loomupäraselt usaldada. See mudel nõuab privilegeeritud juurdepääsu ja lakkamatut identiteedi kinnitamist. DMARC põimib SPF ja DKIM tehnoloogia ühtseks e-posti aadresside võltsimist *keerulisemaks tegevaks* poliitikaks.

DMARC poliitikaga saab e-posti vastuvõtja serverile teada anda, et SPF ja/või DKIM kontrollide ebaõnnestumisel tuleb valida üks järgmistest tegevustest:

- e-kiri panna karantiini (rämpsposti postkasti);
- e-kiri tagasi lükata;
- e-kiri läbi lasta, kuid saata selliste kirjade kohta domeeni haldajale raport.

Küberturvalisuse seisukohast on oluline ka e-mailide spoofing-kaitse. Teadupärast on pahalasel lihtne e-kirju võltsida – see tähendab, et saata e-kirju, mis teesklevad, et need pärinevad kelleltki teiselt.

Kas pahalane saab saata e-kirja näiteks jouluvana@sinuettevõttedomeen.ee pealt?

Jah, kui seda küsimust kahtlevalt küsima pead, siis ilmselt pigem saab,

kui selleks eeltööna vajalik DMARC, DKIM ja SPF on vajalikul viisil seadistamata!

Pettuste vastu võitlemiseks saate väljaminevaid e-kirju digitaalselt DKIM abil allkirjastada, millega saate tõestada, et e-kiri tuli tegelikult kelleltki teie organisatsioonist, mitte pahalaselt, kes teeskleb, et on teie organisatsiooni kuuluv kirjasaatja ja kirss tordile on karmisisuline DMARC kirje, mis selle jõustab. Peale e-maili teenuse õiget seadistamist, seejärel DKIM võtmega allkirjastamine toimub serveris automaatselt ja kasutaja ei pea selleks ise midagi tegema.

DMARC kirje loomiseks peavad olema täidetud kaks olulist tingimust. SPF kirje peab olema korrektselt seadistatud ja DKIM võtmed domeenile lisatud.

- **Kontrolli –** SPF- ja DKIM-kirjeid (*eelnevad peatükid*): Enne DMARC-i konfigureerimist veendu, et domeeni jaoks oleksid SPF ja DKIM kirjed korrektselt seadistatud. **Need DNS kirjed on DMARC-i eeltingimused.**
- **Loo –** DMARC-kirje: DMARC-kirje loomiseks pead lisama oma domeeni DNS-ile TXT-kirje

Näide karmimast DMARC kirjest:

Name	Type	Content
_dmarc.example.com	TXT	v=DMARC1; p=**reject**; sp=**reject**; adkim=**s**; aspf=**s**; rua= mailto:dmarc_agg@vali.email; fo=1;

Ideaalpilt oleks, et kõigi ettevõtete kõigil domeenidel oleks just selline seadistus. Praktikas ilma täiendavaid seadistusi tehes võib pigem tekkida olukord, kus hinnanguliselt pooled ettevõtte domeenidelt edastatavad e-mailid ei jõuaks enam ootuspäraselt e-maili saajatele kohale, kuna teenused ei ole kas SPF kirjes või DKIM võtmena vajalikud viisil kirjeldatud.

See on küll ideaalne ja ootuspärane DMARC reegli seadistus, kuid palume ilma eelnevaid teste ja vajaminevaid seadistusi nõnda karmi DMARC reeglit kohe mitte kasutada. Ennem tuleb mitu eeldust täita, kus SPF kirjes on kõik vajalikud teenused ja kõigile neile teenustele DKIM võtmed seadistatud!

- **p=*reject*** näitab, et meiliserverid peaksid tagasi lükkama meilid, mille DKIM- ja SPF-kontrollid ebaõnnestuvad. Saab veel kirjutada *quarantine* ja *none*. Samas, reject ei lase lubamatuid kirju kliendi nimel saata ja need ei jõua saajale kohale. *Quarantine* määrab selle, et kiri jõuab küll kohale, kuid testi põrudes ilmselt SPAM kaustast leiab saadetud kirja üles. ***None* on ajutine kirje**, mida kasutatakse vaid kaardistuse hetkel, mis hiljem tuleb kindlasti kas *quarantine või reject vastu vahetada.*

  Märka: *niikaua kuni DMARK kirjes on p=none, siis see tähendab, et KÕIK E-KIRJAD LASTAKSE KIRJA SAAJALE LÄBI ja pahalasel on lihtne ettevõtte domeeni nimel võltskirju saata.*

Tihti eksitakse ka selle osas, et üritades kaitsta alamdomeenide pealt kirjade väljasaatmist ja pannakse ***ekslikult sp=none,*** *mis tegelikult tähistab seda, et ettevõtte alamdomeenide nimel võib kõike teha ja pahalased rõõmustavad, sest kõik kirjad jõuavad kohale! Näiteks yannatorry@email.ettevõttedomeen.ee või yannatorry@security.ettevõttedomeen.ee aadresside pealt.*

- **adkim=s** tähistab midagi, mida nimetatakse joondusrežiimiks. Sel juhul on range joondusrežiimiks seatud "s". Range joondusrežiim tähendab, et DMARC-kirjet sisaldava meilidomeeni server peab täpselt ühtima meili päises Saatja (FROM) oleva domeeniga. Kui ei, siis DKIM-i kontroll nurjub.
    - DMARC lisaväljad nagu adkim=r; , need tuleb korra üle kaaluda. Nagu näed, hetkel eelenvas näites on üks R asendatud S parameeriga. S= Specifies "Alignment Mode" for DKIM signatures. Authorized values: "r", "s". "r"
        - ***Relaxed Mode****", allows Authenticated DKIM d= domains that share a common Organizational Domain with an email's "header-From:" domain to pass the DMARC check. "s", or "*
        - ***Strict Mode****" requires exact matching between the DKIM d= domain and an email's "header-From:" domain.*
        - Siinjuures näiteks mõne ettevõtte puhul võib selle jätta selle Relaxed Mode, sest näiteks kui EI SAA kõiki DKIM-parameetreid kõigile kirju välja saatvatele teenustele külge panna (nad ei toeta seda veel) ja see reegel ei saa seeläbi nõnda karm olla, muidu need kirjad ei jõua saajatele kohale, mille DKIM ei läbi kirja vastuvõtja juures DKIM-testi.

- **aspf=s** teenib sama eesmärki kui adkim=s, kuid SPF-i joondamiseks.
    - *aspf=s; Specifies "Alignment Mode" for SPF. Authorized values: "r", "s". "r",- "Relaxed Mode" allows SPF Authenticated domains that share a common Organizational Domain with an email's "header-From:" domain to pass the DMARC check. "s", or "Strict Mode" requires exact matching between the SPF domain and an email's "header-From:" domain.*
    - Ilmselt see saab ja peab olema S (strict), sest kõik SPF loendis olevad kliendi nimel e-maili saatvad teenused peavad täielikult vastama ja seal nö lubatud kirjasaajate listis mitte esinevad teenuspakkujad ja IP-aadressid siis saavad kirja saatmise KEELU

- **rua=mailto:dmarc@example.com:** See osa määratleb aadressi, kuhu saadetakse DMARC-i aruanded, mis sisaldavad üksikasjalikku teavet e-kirjade autentimise tulemuste kohta.

- **ruf=mailto:dmarc-forensic@example.com:** See osa määratleb aadressi, kuhu saadetakse DMARC-i aruanded, mis sisaldavad täiendavat teavet kahtlaste e-kirjade kohta.

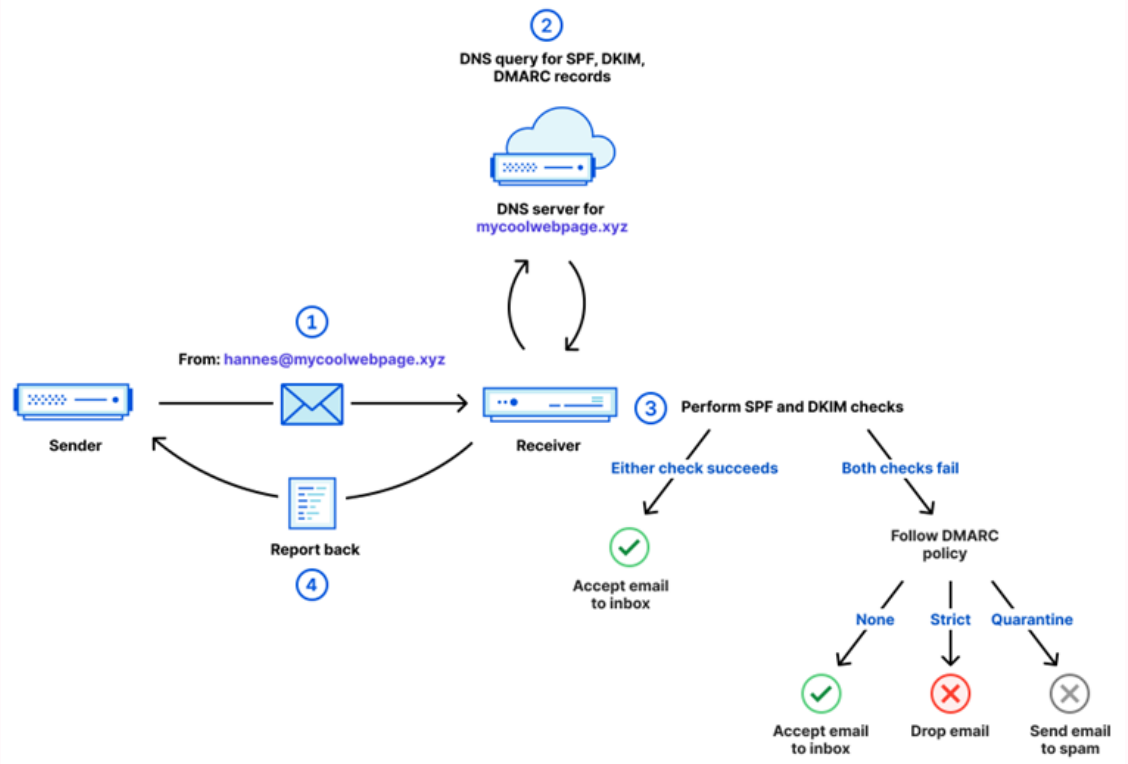
- **sp=none:** See osa määratleb, kuidas käidelda e-kirju, mis ei vasta SPF ALAM domeenide autentimisnõuetele. "None" tähendab, et SPF kontrollimine toimub, kuid puudub tegelik poliitika, mida rakendada. Eelenvalt oli juttu, et none osa saab kasutada ajutiselt kaardistuse hetkel, hiljem on mõistlik see reject peale määrata.

Oluline on tähele panna, et aspf on mõistlik määrata S (strict), sest eeldame, et SPF-nimekirjas on kõik vajalikud ja ainult lubatud teenused, mis kirju seadistatava domeeni pealt tohivad välja saata, kuid adkim on samas mõistlik jätta R (relax), sest üldjuhul kõiki kirju välja saatvaid teenuseid tihti ei saa katta DKIM võtmega (nad näiteks ei toeta seda võimalust, kasutusel on aegunud tarkvara jmt). Kui see siiski on võimalik, et ettevõttes on piiratud määr SPF-kirjeid ja need kõik teenused saab DKIM-võtmega katta, siis adkim=s on igati asjakohane.

DMARC-kirje seadistamine on oluline samm e-posti turvalisuse tagamisel, eriti kui kasutate juba SPF- ja DKIM-autentimist. DMARC annab teile täiendava kontrolli selle üle, kuidas teie domeeni alt saadetud e-kirju käideldakse, ning võimaldab teil saada teavet kahtlaste tegevuste kohta.

Kokkuvõttes võimaldab DMARC-kirje teil täpselt kontrollida, kuidas käidelda teie domeeni alt saadetud e-kirju ning suurendada e-posti turvalisust ja usaldusväärsust. Enne DMARC-kirje seadistamist tuleb aga hoolikalt kaaluda teie ettevõtte vajadusi ja tagada, et olete valinud sobiva poliitika vastavalt teie e-posti turvavajadustele.

Pildil on illustratsioon sellest, et kuidas *none*, *reject* ja *quarantine* märge mõjutab kirjade saajale kohalejõudmist, kui SPF ja/või DKIM võtmete kontroll ebaõnnestub.



Illustratsioonid: https://blog.cloudflare.com/tackling-email-spoofing

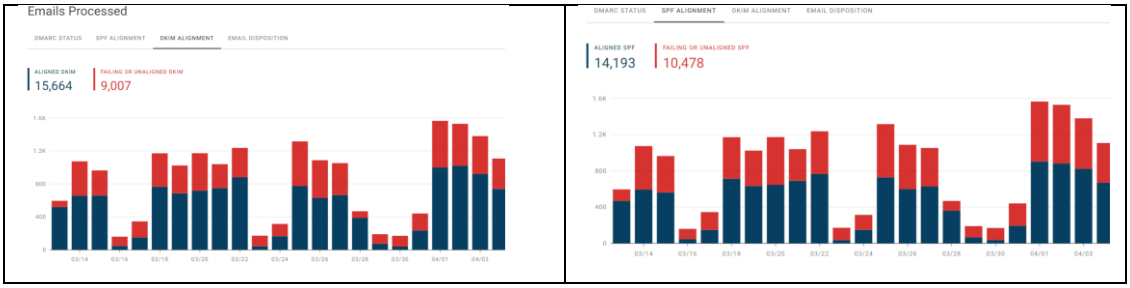
Seadista DMARC monitooring

Mõislik on ettevõttel teha tasuta konto https://www.valimail.com/try-monitor-free/ ,ja seadistada see ja sinna hakkab kogunema statistika, kes ja mis teenused kliendi domeeni(de) nimel kirju välja saadavad. Teatud sagedusega tasub sellele raportile pilk peale heita ja vaadata, et mis uued teenused ja probleemid sealt vastu vaatavad.

(vaata ka teisi teenuspakkujaid nagu näiteks https://dmarcian.com/pricing/)

Kui on DMARC RUA aadressile e-mail peale tellitud XML raportid ja seda veel ei lasta töödelda mõnel teenusel, nagu näiteks Valimail, siis saab need mugavalt avada alloleva tööriistaga, mis teeb saadetud raporti nö inimloetavaks.

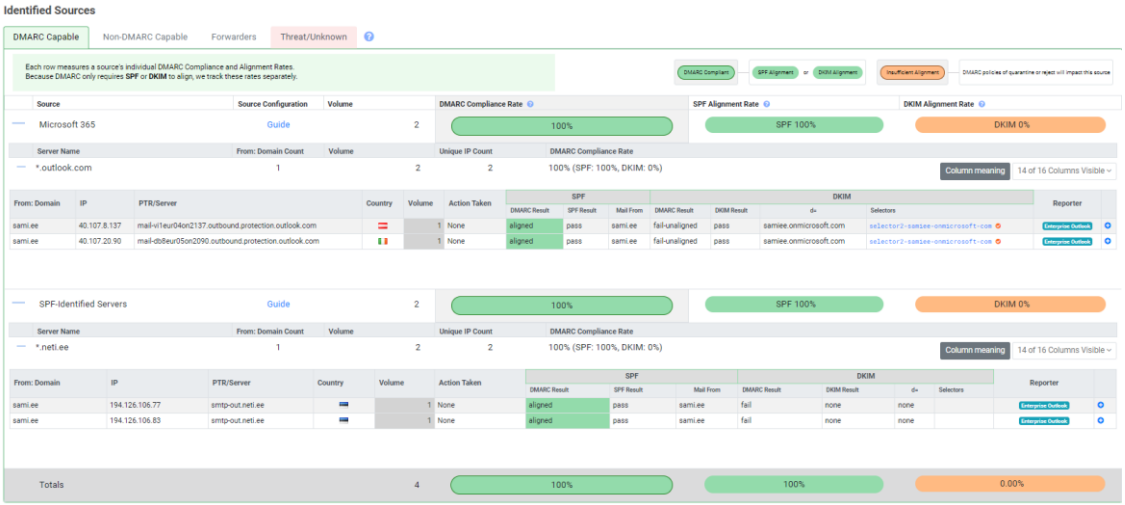
Näiteks allolevast valimail raportist näeb, et kui palju kirju ebaõnnestub SPF või DKIM kirjete ebatäpse või puuduliku kirjeldamise pärast. Kui hetkel see klient seadistaks DMARK reegli p=reject, siis pea pooled kirjad jääks nö kadunuks.



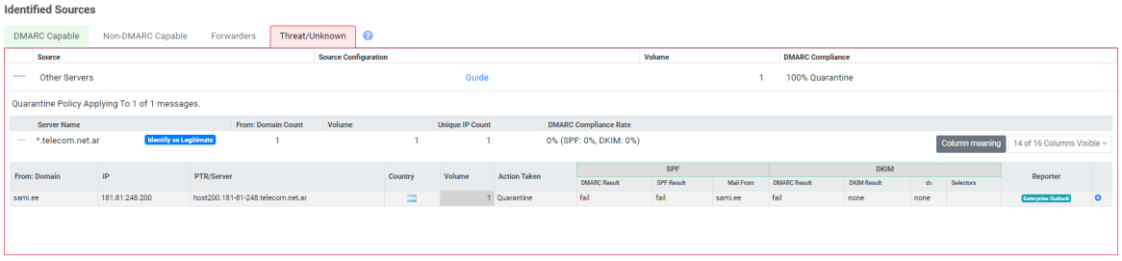
DMARC-aruannete analüsaator https://us.dmarcian.com/xml-to-human-converter/

- Lae DMARK aruande konverterisse saabunud raport ja vaata tulemust. Kui ükshaaval käsitsi ei soovi XML-faile uurida, siis kasuta teenust. Näiteks loo teenuskonto https://dmarcian.com/ lehel ja saad soovi korral 14 päeva tasuta andmeid analüüsida. Selliseid teenuspakkujaid on veel, mille hulgast võib sobiva valida. Näiteks eelnevalt viidatud https://www.valimail.com/

Näiteks selles näitlikus raportis tuvastati, et ükski DKIM ei vasta nõuetele ja ei läbi vajaminevat testi. Lisaks avastati raportit lugedes, et mingi kliendi teenus kasutab mail.neti.ee proxit e-mailide saatmiseks, mis EI OLE mõistlik ja tuleks asendada näiteks O365 kontoga.



Teisest vaadatavast tuvastati, et tegemist on Threat leiuga. Seega, soovitan soojalt raportitele detailselt korra peale vaadata, see annab hea ülevaate tegelikult toimuvast. Oluline on raporti tulemustele peale vaadata ja siis ilmselt leiab sealt samataolisi mõtteid, mida klient endal parendada saab.



Koosta sobiv DMARC reegel

Varasemalt tõime välja soovitusliku karmi DMARC reegli. Kui eeltoodud näites nö karm DMARC reegel kohe kasutamiseks ei sobi, siis saad soovi korral genereerida sobivama DMARC reegli kasutades allolevat tööriista.

- **DMARC Wizard** Kellel täiendav huvi, saab selle (https://dmarcian.com/dmarc-record-wizard/) wizardiga toimetada ja meelepärase DMARC-kirje kokku panna, sest seal on ka selgitused, et mida üks või teine kirjes kasutatav seadistus tegelikult tähendab.

Oluline on vältida olukorda, kus DMARC kirje on püsivalt kujul v=DMARC1; p=none;

Jah, SPF teenuste kaardistuse hetkel on see „*none*“ mõistlik, et kõikidest serveritest kõik kirjad lubatakse kõigile kohale saata, kuid varasemalt pöörasime tähelepanu sellele, et p=none staatusega saab iga pahalane saata teie ettevõtte domeeni nimel e-mail spoofing võltsitud kirju.

Märka, et DMARC kirjes saab olla rohkem seadistusi ja jättes mõne neist lisamata võib tähendada „*Strict Mode*“ reegli asemel hoopis „*Relaxed Mode*“ reegli kasutamist. Eelista DMARC kirjes pigem **Reject** ja **Strict Mode** kasutamist, eeldusel, et oled eelnevalt vajamineva SPF õigesti koostamine, kus on kõik vajaminevad teenused ja serverid loetletud ja DKIM kirjed iga teenuse kohta lisatud. Samuti SPF kirjes kasuta eelistatult „*-all*“ süntaksit. DMARC kirjes võimalusel võta kasutusel RUA, mille kaudu antakse märku kirja saaja serveritele XML-i tagasisidet saata.

Märkus. See ei ole e-posti aadresside loend, kuna DMARC nõuab URI-de loendit kujul "mailto:aadress@example.org".

TAG	DEFAULT	TRANSLATION
v	DMARC1	The DMARC version should always be "DMARC1". Note: A wrong, or absent DMARC version tag causes the entire record to be ignored.
p	none	Policy applied to emails that fails the DMARC check. Authorized values: "none", "quarantine", or "reject". "none" is used to collect feedback and gain visibility into email streams without impacting existing flows. "quarantine" allows Mail Receivers to treat email that fails the DMARC check as suspicious. Most of the time, they will end up in your SPAM folder. "reject" outright rejects all emails that fail the DMARC check.
adkim	r	Specifies "Alignment Mode" for DKIM signatures. Authorized values: "r", "s". "r", or "Relaxed Mode", allows Authenticated DKIM d= domains that share a common Organizational Domain with an email's "header-From:" domain to pass the DMARC check. "s", or "Strict Mode" requires exact matching between the DKIM d= domain and an email's "header-From:" domain.
aspf	r	Specifies "Alignment Mode" for SPF. Authorized values: "r", "s". "r", or "Relaxed Mode" allows SPF Authenticated domains that share a common Organizational Domain with an email's "header-From:" domain to pass the DMARC check. "s", or "Strict Mode" requires exact matching between the SPF domain and an email's "header-From:" domain.
sp	p= value	Policy to apply to email from a sub-domain of this DMARC record that fails the DMARC check. Authorized values: "none", "quarantine", or "reject". This tag allows domain owners to explicitly publish a "wildcard" sub-domain policy.
fo	0	Forensic reporting options. Authorized values: "0", "1", "d", or "s". "0" generates reports if all underlying authentication mechanisms fail to produce a DMARC pass result, "1" generates reports if any mechanisms fail, "d" generates reports if DKIM signature failed to verify, "s" generates reports if SPF failed.
ruf	none	The list of URIs for receivers to send Forensic reports to. Note: This is not a list of email addresses, as DMARC requires a list of URIs of the form "mailto:address@example.org".
rua	none	The list of URIs for receivers to send XML feedback to. Note: This is not a list of email addresses, as DMARC requires a list of URIs of the form "mailto:address@example.org".
rf	afrf	The reporting format for individual Forensic reports. Authorized values: "afrf", "iodef".
pct	100	The percentage tag tells receivers to only apply policy against email that fails the DMARC check x amount of the time. For example, "pct=25" tells receivers to apply the "p=" policy 25% of the time against email that fails the DMARC check. Note: The policy must be "quarantine" or "reject" for the percentage tag to be applied.
ri	86400	The reporting interval for how often you'd like to receive aggregate XML reports. You'll most likely receive reports once a day regardless of this setting

Disclaimer

Oluline on märkida, et kahjuks tihti kasutatakse vaid SPF-kirjet ja jääb ekslik turvatunne, et siis ongi kõik hästi ja ootuspäraselt seadistatud. Tavapäraselt kasutatakse neid kolme DNS-kirjet (*DMARC, SPF ja DKIM*) üheaegselt ja nö korraga ja teineteist toetavana. Vajalik on seadistada kõik need kolm hoolikalt ära. Samuti on levinud ekslik arvamus, et DMARC kirjes p=quarantine määramine on juba parim tulemus ja p=reject kasutamine on justkui kurjast! Selle müüdi peab kummutama! Kui domeeni DNS kirje seadistaja teeb kõik õigesti ja kasutatav e-mailide tehnoloogia ning teenused võimaldavad seda õigesti seadistada, siis pigem peaks eelistama karmi dmarc **p=reject** poliitikat koosmõjus ***aspf=s*** lausendiga. Kui on võimalik kõik DKIM võtmed samuti kõigile e-maili teenustele seadistada, siis soovitav on võtta kasutusele ka ***adkim=s*** range reegel.

Karmima kirje puhul peab märkima, et **SPF-kirjes peavad olema KÕIK vajalikud teenused kirjeldatud**, kes kirju välja domeeni nimel saadavad, ja hästi läheb siis, kui ka **kõigi teenuste kohta on digitempel DKIM samuti olemas.**

Palun ole SPF, DKIM ja DMARC muudatuse tegemisel täpne, sellel tegevusel on SUUR MÕJU JA ULATUS !!!

Ebatäpsused koostatud DNS kirjes võivad süntaksi veana kaasa tuua ootamatu tagajärjed.

Vajadusel konsulteeri asjatundjaga või

palu teostada need täiendused teemat tundval spetsialistil.

Kaitske oma ettevõtet kulukate BEC-rünnakute eest

Tänapäeva digimaailmas on teie ettevõtte turvalisus ja selle maine haavatavam kui kunagi varem. ***Business Email Compromise*** (BEC) rünnakud on osutunud kõige kulukamateks – just sel aastal registreeriti sadu tuhandeid rahvusvahelisi ja RIA poolt samuti riigisisest intsidente, mille tulemuseks on ligikaudu 50 miljardi dollari [4]suurune kahju. Ilmselt on tekkinud kahju ilmselt suurem, sest kõik mõjutatud isikud ja kannatanud ei anna toimunud intsidentidest märku.

Tegevjuhi pettused, andmepüügipettused – need kõik on BEC-i rünnakud. Ja kõige hirmutavam osa? Need ei tugine pahavarale ega pahatahtlikele linkidele, mistõttu on neid traditsiooniliste meilikaitsetööriistade abil uskumatult raske tuvastada.

Tutvu BEC-i rünnakute oluliste ründevektoritega, et õppida:

1. BEC-pettuste toimimise olemusega.
2. Reaalse elu stsenaariumid, nagu tegevjuhi pettus ja valearvete skeemid.
3. Kuidas BEC kasutab inimeste haavatavust (sh sotsiaalne rünnak).
4. Millised on sammud oma ettevõtte kaitsmiseks ja BEC-rünnakute ärahoidmiseks.

Tugevdame koos teie ettevõtte kaitsevõimet. Rääkige see teema oma juhtkonnaga läbi, et aidata rakendada tugevaid e-posti autentimisprotokolle ja takistada BEC-kirjade jõudmist teie meeskonna postkasti.

Loe täpsemalt BEC juhendit:: https://www.valimail.com/blog/essential-guide-to-bec-attacks/

[4] https://www.ic3.gov/Media/Y2023/PSA230609 This annual FBI report also shares that there were 277,918 BEC international and domestic incidents recorded, with an adjusted loss of approximately $50 billion.

Erinevad ettevõttega seotud domeenid

Samas igale domeenile peab eraldi lähenema ja seda oleks hea teha kellegagi koos, kes teab, et mis teenused tegelikult tohivad tööd teha ja millised on lubamatud kirjasaatjad.

Ettevõttel on mitmeid domeene

Oluline on esmalt hinnata oma organisatsiooni e-posti infrastruktuuri suurust ja keerukust. Meilidomeenid on enamikus organisatsioonides jagatud ressurss, mis hõlmab mitut osakonda, kolmandatest osapooltest tarnijaid ja isegi organisatsiooni enda Interneti-rakendusi. Kuna domeenid on jagatud, nõuab edukas DMARC-projekt tugevat osakondadevahelist suhtlust ja selgeid domeenihaldusprotsesse.

DMARC-i juurutamisel on parem kasutada seda kõigis organisatsiooni domeenides, selle asemel et keskenduda üksikutele domeenidele. DMARC-i juurutamine kogu domeeniportfellis tagab organisatsiooni nähtavuse ja juhid saavad uusi tööriistu, mis tagavad, et kõik meilid saadetakse organisatsiooni standardite kohaselt.

Alustuseks koostage kõigi oma organisatsiooni domeenide loend, et saaksite süstemaatiliselt DMARC-i kasutusele võtta. Samuti on oluline mõista, kes organisatsioonis kasutab domeene ja omab selle domeeni kolmandatest osapooltest tarnijaid, kuna vajate nende tuge, et meilivooge ei häiritaks.

.ee domeenid

Nimi	Seisund	Alguse kuupäev	Kehtiv praegu
argipaeva.ee	registreeritud	16.09.2021	jah
autokaubamaja.ee	registreeritud	06.04.2011	jah
comarket.ee	registreeritud	02.11.2020	jah
delice.ee	registreeritud	02.11.2020	jah
digimaailm.ee	registreeritud	06.07.2010	jah
e-kinkekaart.ee	registreeritud	07.03.2022	jah
eselver.ee	registreeritud	18.04.2022	jah
gurmeecatering.ee	registreeritud	12.03.2012	jah
ilu.ee	registreeritud	04.07.2010	jah
kaubamaja.ee	registreeritud	04.07.2010	jah
kiaauto.ee	registreeritud	02.11.2010	jah
kiatammsaare.ee	registreeritud	16.09.2021	jah
kingakaubamaja.ee	registreeritud	30.03.2016	jah
kulinaaritoit.ee	registreeritud	23.12.2014	jah
laadapaevad.ee	registreeritud	16.09.2021	jah
netikaubamaja.ee	registreeritud	06.04.2011	jah
osturalli.ee	registreeritud	06.04.2011	jah
partnerkaart.ee	registreeritud	04.07.2010	jah
selverabc.ee	registreeritud	16.09.2021	jah
shoe.ee	registreeritud	22.02.2017	jah
solaristoidupood.ee	registreeritud	07.03.2022	jah
supersam.ee	registreeritud	07.03.2022	jah
tallinnakaubamaja.ee	registreeritud	18.04.2022	jah
tkmbeauty.ee	registreeritud	16.09.2021	jah
tkmfinants.ee	registreeritud	17.02.2022	jah
tkmgroup.ee	registreeritud	07.11.2013	jah
tkmgrupp.ee	registreeritud	07.03.2022	jah
topsec.ee	registreeritud	07.05.2019	jah
viimsikeskus.ee	registreeritud	09.07.2013	jah

Märka, et igal ettevõttel on tavapäraselt enam kui üks domeen. Jah, põhidomeenilt saadetakse ja võetakse kirju vastu, kuid üsna tavaline on ka see, et ettevõttel on mõned domeenid veel, millelt samuti kirju välja saadetakse.

Näiteks Eesti ettevõtete domeenid leiab https://www.teatmik.ee/ veebilehe otsingust, kus tee otsing kõigi enda kontserni ettevõtete kohta. Sealt tabelist altpoolt leiab peatüki „.ee domeenid“. Märka, et seal loendis on vaid *.ee domeenid ja neile lisaks tasub üle kontrollida kõik ettevõttega seotud .ee, .eu, .com, .lv, .lt, .fi jne domeenid.

Märka, et kirju mitte välja saatvad domeenid tuleb samuti kaitsta (allpool täpsemalt)

Alamdomeenid

Alamdomeen on domeeni osa, mis on eraldiseisev osa suuremast domeenist, näiteks "blogi.sinudomeen.com", kus "blogi" on alamdomeen. Alamdomeen võib olla kasutusel selleks, et eristada erinevaid osi või teenuseid samas domeenisüsteemis. Näiteks võib ettevõte kasutada alamdomeene erinevateks osakondadeks või geograafilisteks piirkondadeks, et luua selgeid ja struktureeritud veebilehti.

Alamdomeen on nö Telia.ee peadomeenile lisaks näiteks https://digitark.telia.ee/ alamdomeen.

Kui ettevõttel on plaanis selle alamdomeeni pealt täiendavalt eraldi e-mailie saata (näiteks toimetus@digitark.telia.ee) , siis tuleb ka see domeen SPF- ja DKIM-kirjena seadistada. Kui kirju saadetakse pigem toimetus@digitark.ee pealt, siis tuleb see domeen vajalikul viisil seadistada kirju välja saatma või keelata kõigi kirjade saatmine sellelt domeenilt, et pahalased ei saaks seda ise ära kasutada.
Oluline on teha iga alamdomeeni jaoks eraldi oma SPF ja DKIM reeglid (kui neilt saadetakse kirju välja) või peadomeeni DMARK kirjes alamdomeenide kasutamine keelata.

Milline on hea DMARK, SPF ja DKIM seadistus?

Ideaalne oleks, kui ettevõttel on IGAL domeenil selliselt tehtud kirjed, mis just selle domeeni kohta käib:

- DMARK kirje: ***„v=DMARC1; p=reject; rua=mailto:dmarc_agg@vali.email; aspf=s; adkim=s; fo=1;“***
    - See reegel lubab kirjasaaja postkasti läbi vaid need e-kirjad, mis on õigesti SPF ja DKIM osas seadistatud. Lubamatutest (volitamata) allikatest saadetud kirju läbi ei lasta ja RUA aadressi kaudu kogutakse kokku Valimail teenuse peale raporteid ja statistikat e-mailide saatmiste kohta, kust saab siis vaadata, et kas kõik on korrektselt seadistatud või mingid kirju saatval teenusel tuleb see teema veel täiendavalt üle vaadata ja seadistada.
- SPF kirjes „***v=spf1 teenus1 teenus2 teenus3 teenus4 teenus5 teenus6 teenus7 teenus8 teenus9 jne -all*“**
    - DKIM kirje **teenus1** kohta (näiteks O365 Outlook kirjad)
    - DKIM kirje **teenus2** kohta (näiteks majandustarkvara arved ja tellimuste kinnituskirjad)
    - DKIM kirje **teenus3** kohta (näiteks uudiskirjad Smaily või Mailchimp vmt)
    - DKIM kirje **teenus4** kohta (näiteks epoe tellimuse kinnituskirjad või veebilehe kontaktivormid)
    - DKIM kirje **teenus5** kohta (näiteks palgaarvestus tarkvara mis saadab palgasedeleid)
    - DKIM kirje **teenus6** kohta (näiteks personalihaldus tarkvara mis saadab puhkuseteateid)
    - DKIM kirje **teenus7** kohta (näiteks Amazoni serveris mingi teenus)
    - DKIM kirje **teenus8** kohta (näiteks klientide broneerimissüsteemi teenus, mille kaudu teevad kliendid aegade broneeringuid ja saavad sealt meeldetuletus ja selle kohta kinnituskirja)
    - DKIM kirje **teenus9** kohta (näiteks CRM, Zendesk, Jira, jmt domeenilt kirju saatev teenus)
    - jne

Kuna saatan peitud detailides, siis võib ettevõttel olla tarkvarasid (näiteks vana majandustarkvara, mis DKIM teenust ei toeta), siis see tähendab, et kõigile teenustele EI SAA DKIM võtit tehnilistel põhjustel teha. Siis peaks DMARK reeglis adkim=s; (*Strict Mode*) asemel kasutama adkim=r; (*Relaxed Mode*) Mis tähistab siis seda, et Strict reegli asemel kasutatakse DKIM kontrollimisel nö madalamat Relaxed turvataset ja lubatake seal nö eksimust.

TAG	TRANSLATION
p	Policy applied to emails that fails the DMARC check. Authorized values: “none”, “quarantine”, or “reject”. “none” is used to collect feedback and gain visibility into email streams without impacting existing flows. “quarantine” allows Mail Receivers to treat email that fails the DMARC check as suspicious. Most of the time, they will end up in your SPAM folder. “reject” outright rejects all emails that fail the DMARC check.
adkim	Specifies “Alignment Mode” for DKIM signatures. Authorized values: “r”, “s”. “r”, or “Relaxed Mode”, allows Authenticated DKIM d= domains that share a common Organizational Domain with an email’s “header-From:” domain to pass the DMARC check. “s”, or “Strict Mode” requires exact matching between the DKIM d= domain and an email’s “header-From:” domain.
aspf	Specifies “Alignment Mode” for SPF. Authorized values: “r”, “s”. “r”, or “Relaxed Mode” allows SPF Authenticated domains that share a common Organizational Domain with an email’s “header-From:” domain to pass the DMARC check. “s”, or “Strict Mode” requires exact matching between the SPF domain and an email’s “header-From:” domain.
sp	Policy to apply to email from a sub-domain of this DMARC record that fails the DMARC check. Authorized values: “none”, “quarantine”, or “reject”. This tag allows domain owners to explicitly publish a “wildcard” sub-domain policy.
fo	Forensic reporting options. Authorized values: “0”, “1”, “d”, or “s”. “0” generates reports if all underlying authentication mechanisms fail to produce a DMARC pass result, “1” generates reports if any mechanisms fail, “d” generates reports if DKIM signature failed to verify, “s” generates reports if SPF failed.

Kaitse domeenid, millelt e-maile ei saadeta

Mõistlik on kaitsta ära need domeenid, mis on ettevõttel olemas, kuid mis kaudu ettevõte ISE kirju välja ei saada. Kõik domeenid peab üle vaatama nagu näiteks need eeltoodud Teatmik lehelt leitud iga ettevõttega seotud domeenid. Mõistlik on koostada ammendava loetelu domeenidest (sh alamdomeenidest), mis on ettevõttega (kontserniga) seotud ja mis nende nimel kirju võivad välja saata.

Kuidas kaitsta domeene, mis e-maile ei saada ega tohigi välja saata

- **SPF** – SPF-i osas on mõistlik seadistada teatud valimi domeenidele reegel "***v=spf1 -all***", mis tähistab seda, et selle domeeni pealt kirju välja **EI TOHI saata ühegi teenuse pealt,**
- **DMARC** – ilmselt on mõistlik kohe ka DMARC-kirje sama karm sinna juurde lisada, mis annab SPF-kirjele mõjuulatuse ja käivitab SPF-reegli. "***v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s;***" ja kui tegelikult tahaks teada, et mis seal domeenidel tegelikult toimub, siis ruf ja rua samuti e-maili peale ära seadistada. (Märka, et kui soovid seadistatavast domeenist erineva domeeni e-maili aadressid lisada, siis tuleb üks DNS-kirje selleks veel lisada (example.net._report._dmarc.example.com IN TXT "v=DMARC1;" on märksõna, millele internetist täiendavalt juurde saad otsida)
- **DKIM** – Soovitatakse isegi domeenidele, mis ei tohi kirju välja saata, lisada tühi DKIM-kirje *tärniga-wildcard kujul *._domainkey.example.com TXT ***v=DKIM1; p=***

Täpsemalt on selgitatud artiklis "*How to protect domains that do not send email*": https://www.cloudflare.com/learning/dns/dns-records/protect-domains-without-email/

Võideldes meilide võltsimise ja andmepüügiga, siis on soovitud tulemuseks kaitstaval domeenil vajalikud kirjed DNS sellised *(lisatakse eraldi igale kaitstavale domeenile):*

```
example.com                    TXT     "v=spf1 -all"
*._domainkey.example.com.      TXT     "v=DKIM1; p="
_dmarc.example.com.            TXT     "v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s;"
```

Võta kasutusele BIMI (*Brand Indicators for Message Identification*)

Kui oled suurem ettevõte ja pead oluliseks, et emailid kasutaja postkastis eriliselt esile tuuakse (*sh lisatakse logo*), siis tasub mõelda BIMI kasutamisele, mis on e-maili turvalisuse ja autentimise standard, mis võimaldab ettevõtetel kuvada oma brändi logo autenditud e-kirjade juures. See aitab tugevdada saatja usaldusväärsust ning suurendada kasutajate teadlikkust ja turvatunnet e-kirju avades. BIMI töötab koos DMARC (*Domain-based Message Authentication, Reporting & Conformance)* protokolliga, mis kontrollib, et e-kirjad pärinevad lubatud domeenidelt.

BIMI eelised:

1. **Tugevdab brändi nähtavust**: Brändi logo kuvamine postkasti vaates aitab kasutajatel kiiresti tuvastada, kes on e-kirja saatnud.
2. **Parandab turvalisust**: BIMI nõuab DMARC-i rakendamist, mis aitab kaitsta domeeni võltsimise ja pettuse eest.
3. **Suurendab kasutajate usaldust**: Selge visuaalne identifitseerimine vähendab riski, et kasutajad avavad petturlikke e-kirju.

BIMI kasutuselevõtmiseks peab ettevõte:

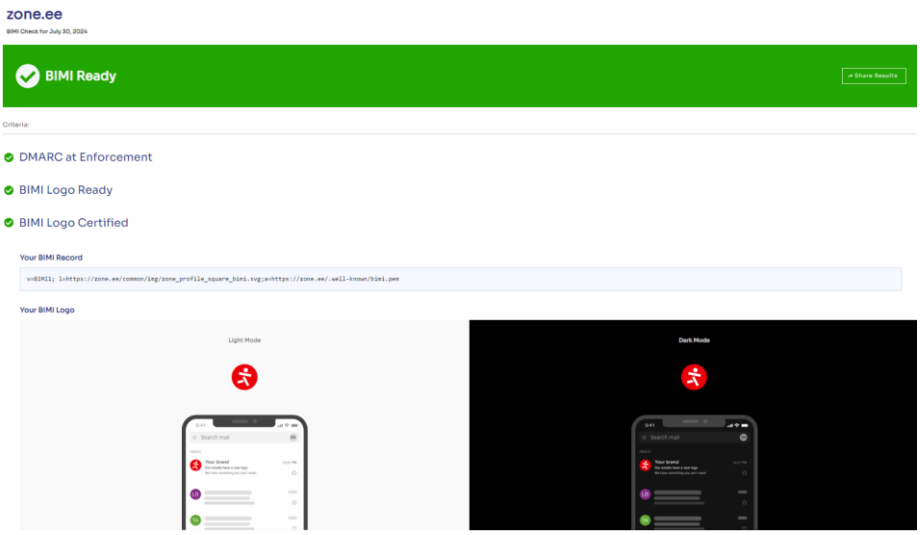
1. **Rakendama DMARC-protokolli**: DMARC peab olema konfigureeritud ja kasutusele võetud domeeni jaoks.
2. **Kinnitama brändi logo**: Logo peab olema esitatud spetsiaalses vektorgraafika vormingus (SVG) ja vastama BIMI spetsifikatsioonidele. Nagu Zone Eesti on teinud https://zone.ee/common/img/zone_profile_square_bimi.svg
3. **Sertifitseerima logo**: Mõned e-posti teenusepakkujad nõuavad logo sertifitseerimist sõltumatu kolmanda osapoole poolt, et kinnitada selle ehtsust (nö tasulise sertifikaati eeldus). nagu Zone Eesti on lisanud https://zone.ee/.well-known/bimi.pem **Märka: eeldus on tasuline domeeni certifikaat!**.

BIMI on oluline samm e-maili turvalisuse ja kasutajate kogemuse parandamiseks, pakkudes nii ettevõtetele kui ka tarbijatele suuremat turvalisust ja usaldust.

Näidis ettevõte BIMI seadistus - Zone Eesti: https://www.mailhardener.com/tools/bimi-validator?domain=zone.ee

Kontrolli oma ettevõtte seadistust: https://domain-checker.valimail.com/bimi

Juhend seadistamiseks: https://www.valimail.com/resources/guides/bimi-email/bimi-checker/



Lülita sisse DNSSEC ettevõtte domeenidel

Lubage oma domeenis DNSSEC, mis vähendab haavatavust DNS-rünnakute suhtes.

DNSSEC (*Domain Name System Security Extensions*) on turvameede, mis lisab DNS-süsteemile autentimise ja tervikluse kontrolli. DNSSEC kasutab digitaalallkirju, et tagada, et DNS-i andmed, nagu IP-aadressid ja domeeninimed, on autentsed ja muutmata, kui nad liiguvad serveritest kasutajateni.

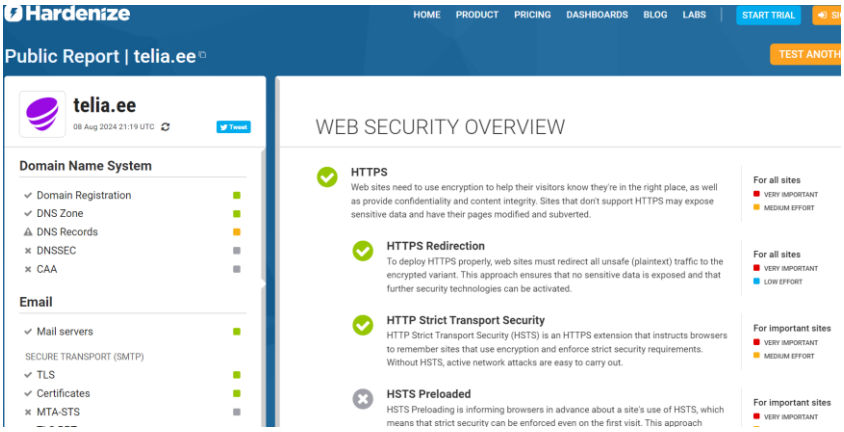
Miks võtta DNSSEC kasutusele?

1. **Turvalisus**: DNSSEC aitab kaitsta DNS-i manipuleerimise, näiteks DNS-i vahemälu mürgitamise (cache poisoning) ja man-in-the-middle rünnakute eest. Need rünnakud võivad suunata kasutajaid võltsitud veebilehtedele, kus kurjategijad võivad varastada isiklikku informatsiooni.
2. **Andmete terviklikkus**: DNSSEC tagab, et DNS-i andmed ei ole muudetud pärast nende algset allkirjastamist. See tähendab, et kasutajad saavad olla kindlad, et saadud DNS-i vastus on täpne ja autentne.
3. **Usaldusväärsus**: DNSSEC-i kasutamine suurendab kogu interneti usaldusväärsust, kuna see tagab, et andmed, mida kasutajad saavad, pärinevad tegelikust ja usaldusväärsest allikast.

Kokkuvõttes on DNSSEC oluline täiendus DNS-süsteemile, mis aitab suurendada interneti turvalisust ja usaldusväärsust, kaitstes kasutajaid pahatahtlike rünnakute eest.

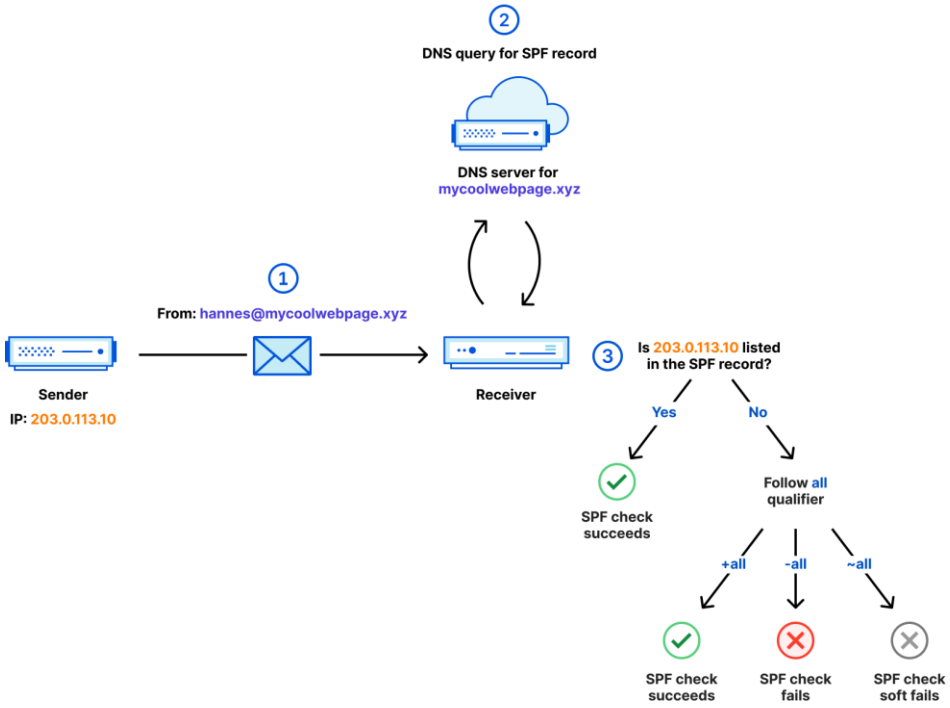
Kontrolli üle samuti teised domeeniga seotud seadistused
(*kõigil ettevõttega seotud domeenidel*):

Domeeni seadistuste üldtest https://www.hardenize.com/

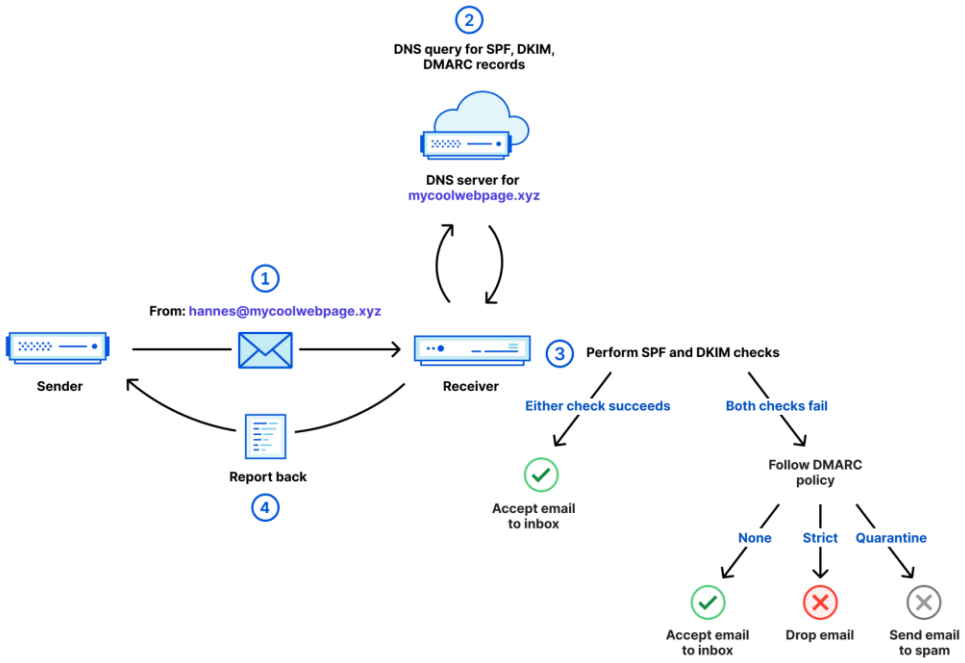


Tehnilist

mida tähendavad SPF-kirjes “-all”, “+all”, “?all” või “~all”



mida tähendavad DMARC-kirjes “*reject*”, “*quarantine*” või “*none*”

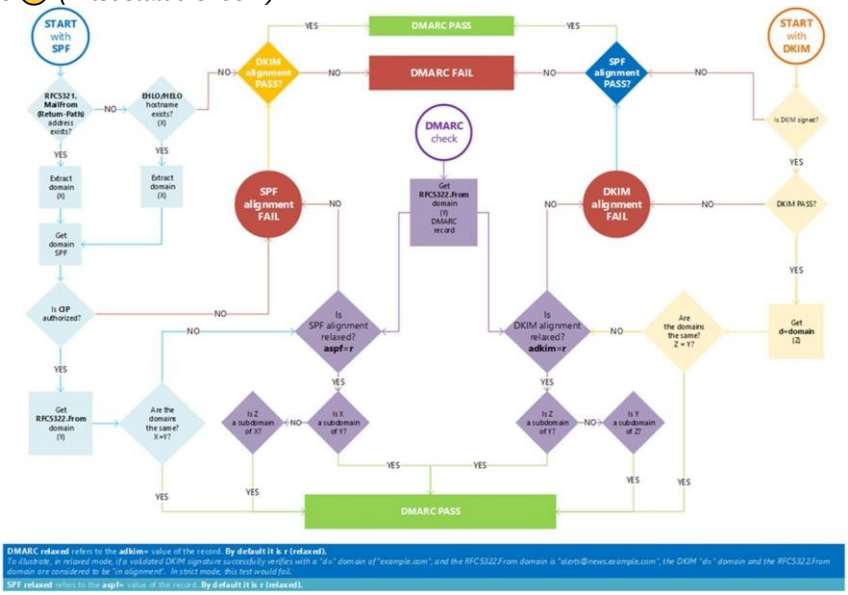


Illustratsioonid: https://blog.cloudflare.com/tackling-email-spoofing

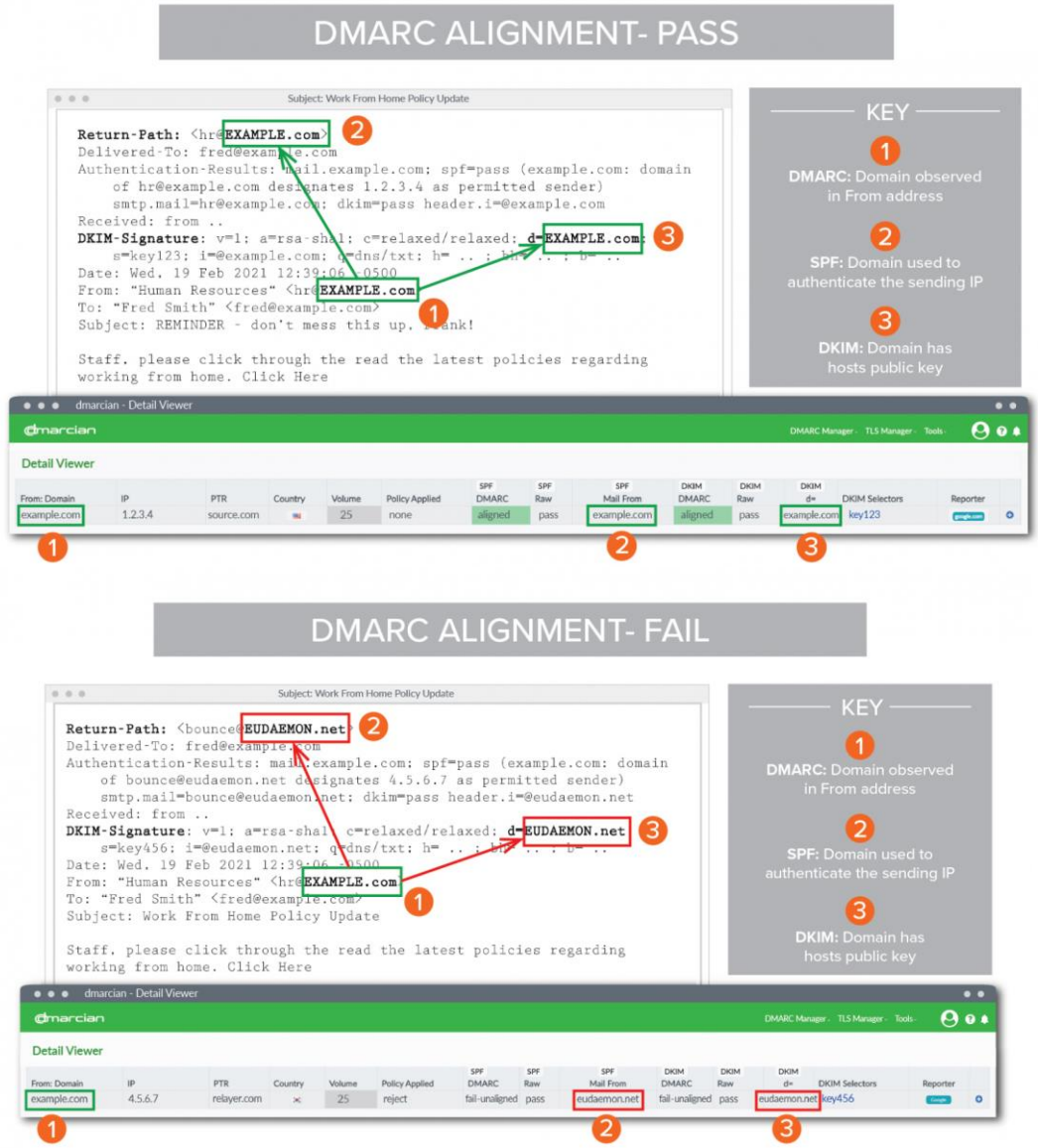
Kuidas toimub e-maili kontrollimine?

Allolev skeem on lihtsalt infoks, et mõista, kuidas toimub e-maili kohalejõudmine ja saatja tuvastamine.

Peab arvestama, et kokku töötavad need üldjuhul selle skeemi järgi, kus üks seadistus tegelikult EI SAA ILMA TEISETA HÄSTI HAKKAMA ja SPF, DKIM ja DMARC seaded täiendavad teineteist 😉 *(lihtsustatud skeem)*



Kuidas tehakse aligment pass või fail test?



Illustratsioonid: https://dmarcian.com/alignment/

Tehnilise tiimi *to-do* list

Vajaminevad esmased ülesandeloend tehnilisele teostajale, et teostada vajalikud toimingud SPF ja DKIM kirjete seadistamiseks erinevate teenuste ja domeenide jaoks:

1. **Teenuste ja domeenide määratlemine:**
   - Koosta nimekiri kõigist teenustest (nt majandustarkvarast saadetavad arved, turunduse uudiskirjad, e-pood jne) ja domeenidest, mida ettevõte kasutab.
2. **SPF ja DKIM kirjete analüüs:**
   - Kontrolli iga teenuse ja domeeni jaoks, millised kirjed on juba olemas ja dokumenteeri need.
   - Selgita välja, millised teenused ja domeenid vajavad SPF ja DKIM kirjete seadistamist ja millised lisakaitset.
   - Kui mõni teenus või domeen ei oma SPF ega DKIM kirjet, märgi need üles.
3. **SPF ja DKIM kirjete loomine:**
   - Looge iga teenuse ja domeeni jaoks SPF ja DKIM kirjed vastavalt teenuspakkuja juhendis toodud nõuetele.
   - Veenduge, et SPF ja DKIM kirjed vastaksid nõutud süntaksile ja ei sisaldaks vigu (testi). ***Märka*****,** et vigane kirje ei tööta ja toob pigem kahju kui kasu!
4. **SPF ja DKIM kirjete lisamine DNS-seadistustesse:**
   - Logige sisse klienti teenindava DNS-halduri või veebiteenuse iseteenindusega või kirjuta e-mail domeeni registripidaja klienditoele.
   - Lisage iga teenuse ja domeeni jaoks SPF ja DKIM kirjed vastavalt dokumentatsioonile.
5. **SPF ja DKIM kirjete testimine:**
   - Tehke DNS-kirjete muudatuste järel testimine, et veenduda, et SPF ja DKIM kirjed on korrektselt konfigureeritud.
   - Saatke test-e-kirju erinevate teenuste kaudu ja kontrollige SPF ja DKIM autentimise õigsust. *Eespool oli juttu mail-tester.com lahendusest.*
6. **Dokumentatsioon ja koolitus:**
   - Dokumenteerige kõik tehtud muudatused ja seadistused.
   - Korraldage vajadusel koolitus või infoüritused meeskonnale, et tagada, et kõik on teadlikud muudatustest ja nende mõjust ning, et antakse kindlasti märku kui miskit ei tööta ootuspäraselt, kuna seadistuse järgselt võib mõni teenus mitte töötada ootuspäraselt .
   - **Märka:** Oluline on mõista, et kui vajaminevad nö karmid seadistused on tehtud, siis iga uue e-maili väljasaatva tarkvara-teenuse kasutusele võtmise juures on vaja teha seadistused ja vajaminevad täiendused iga uue tarkvara kohta.
7. **Järelkontroll:**
   - Tehke järelkontroll paar päeva pärast SPF- ja DKIM-kirjete seadistamist, et veenduda, et kõik toimib nõuetekohaselt ja et pole tekkinud mingeid probleeme. Ilmselt võib ettevõte saata ka teavituse, et mingi teenus ei tööta ootuspäraselt, siis tuleb selle teenuse SPF ja DKIM samuti seadistada.

     rua ja ruf raport on siinjuures abistava iseloomuga leidmaks üles teenused, mis on jäänud esialgu märkamata. Peale seadistust on mõistlik mõni aeg raportitel silm peal hoida. Mõislik on kasutada näiteks valimail.com lahendust, mis aitab saabunud teenuspakkujate raportid inimkeelde tõlkida.
8. **Kliendile tagasiside andmine:**
   - Jagage ettevõtte juhtkonnaga teavet tehtud muudatuste kohta ja veenduge, et ettevõttel poleks tekkinud küsimusi ega probleeme uute seadistustega.

Lõpetuseks soovime tänada kõiki allikaid ja autoreid, kelle teoseid ja artikleid on selles juhendmaterjalis refereeritud. Kasutatud teave on pärit erinevatest usaldusväärsetest interneti allikatest, sealhulgas teadusartiklitest, erialastest blogidest ja ametlikest teenuspakkujate veebisaitidest.