E-mail anti-spam

Teknisk guide til opsætning af SPF, DKIM og DMARC for at sikre optimale leveringsrater for e-mails fra webCRM, ved brug af Mailjet.

For at sikre jer optimal leveringssikkerhed for e-mails sendt fra webCRM ved brug af Mailjet og for at undgå at ende i spamfiltre har vi lavet en guide med tekniske opgaver der kan udføres for at øge leveringssikkerheden. Denne guide fokuserer primært på udsendelse af e-mails fra webCRM systemer hvor Mailjet er slået til, men du kan også sende e-mails fra webCRM via din egen e-mail server, se afsnit 4. Udsendelse af e-mails fra egen e-mail server.

For at sende masse-e-mails fra webCRM, såsom nyhedsbreve, invitationer og påmindelser før arrangementer, skal I som minimum gennemføre trin 1 om omsætning af SPF records. Vi anbefaler også kraftigt at I gennemfører trin 2 omhandlende DKIM. Når det er gennemført, vil I også blive flyttet til en IP-adresse med bedre rating end den I starter på, og dermed yderligere optimerer leveringssikkerheden.

Hvis du ønsker at forbedre jeres setup yderligere, kan I gennemføre trin 3 og implementere DMARC autorisering. Det kræver ændringer på, både jeres og vores side og koster en times konsulenthjælp.

1. SPF records

Sender Policy Framework (SPF) er et e-mailvalideringssystem designet til at forhindre e-mail spam ved at opdage når nogen forsøger at sende på vegne af andre ved at verificere afsenderens IP-adresse. SPF tillader administratorer at specificere hvilke servere der har tilladelse til at udsende e-mails på jeres vegne ved at oprette en specifik SPF record i en DNS-zone. Mail-servere bruger DNS til at tjekke om en e-mail sendt fra et givent domæne, bliver sendt fra en server der er godkendt af domænets administrator.

Opsætningen kræver at I har jeres eget domæne. Hvis jeres e-mailadresser har et offentligt domæne, eksempelvis @hotmail.com eller @gmail.com bør du ikke sende masse-e-mails fra webCRM.

1.1 Teknisk opsætning

For at offentliggøre at du tillader udsendelse af e-mails på vegne af jer fra jeres webCRM system, skal du oprette eller tilrette jeres SPF record til at inkludere **“include:spf.webcrm.com”**. Nogle DNS-udbydere tillader at du selv kan gøre dette, ellers skal du kontakte jeres DNS udbyder og bede dem tilføje det.

SPF record formater kan variere, så du bør kontakte din IT-afdeling eller DNS udbyder for at finde ud af hvilket format I benytter.

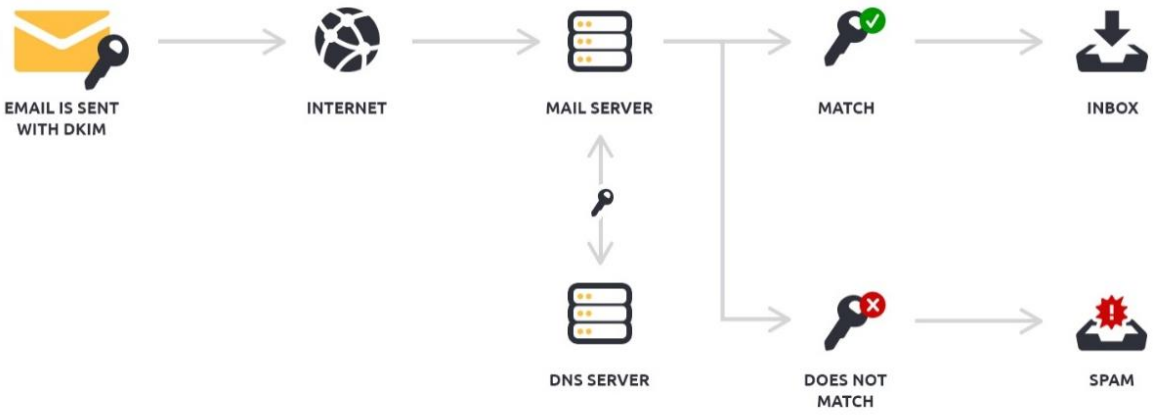
Eksempel på SPF record der tillader webCRM og Mailjet samt din egen e-mail server at udsende e-mails:

"v=spf1 ip4:111.222.333.444 include:spf.webcrm.com -all", hvor 111.222.333.444 er jeres egen servers IP-adresse, hvis I har en.
Hvis I har Office 365, kan SPF recorden se således ud: *v=spf1 include:spf.protection.outlook.com include:spf.webcrm.com +a +mx ~all*

2. DKIM

DKIM står for "Domain Keys Identified Mail". Det er en krypteringsmetode der bruges af e-mailservere til at finde ud af om e-mailen kommer fra et autoriseret system og forhindrer spammere i at stjæle identiteter fra legitime brugere.

DKIM tilføjer en unik signatur til e-mailen for hver e-mail du sender. Signaturen er specifik for jeres domæne og genereres med en privat nøgle. Den tilsvarende offentlige nøgle tilføjes til en DNS record for jeres domæne. Når en e-mailserver modtager din e-mail, tjekkes den offentlige nøgle for at se om din private nøgle var brugt til at generere e-mail signaturen. Hvis ikke din private nøgle var brugt bliver e-mailen anset for at være spam.



2.1 Teknisk opsætning

For at opsætte DKIM for jeres domæne skal du først bekræfte ejerskabet af domænet ved enten at oprette en DNS record eller placere en tom tekstfil, med et navn givet af webCRM, i roden af jeres web-server. Efter det skal I oprette en TXT-fil i jeres DNS med en DKIM værdi givet af webCRM.

I skal selv kunne oprette og indsætte disse værdier, eller få jeres DNS udbyder til at gøre det, da vi ikke kan hjælpe med disse trin. Hvis vi kunne gøre det på vegne af jer, ville valideringen ikke have nogen betydning, da spammere i så fald kunne gøre det samme.

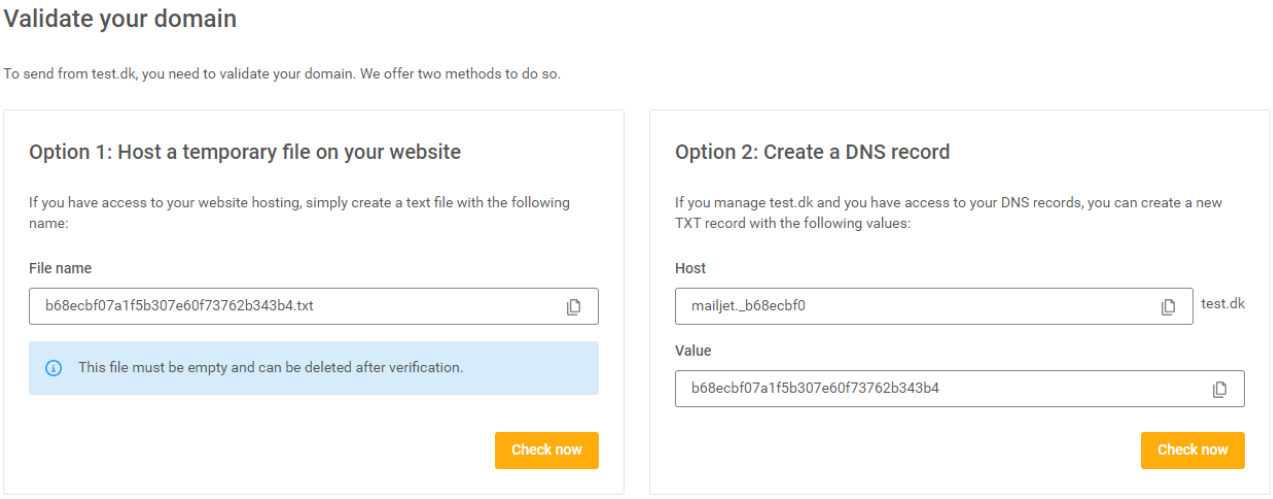
Ønsker I at opsætte DKIM så kontakt support@webcrm.com for at få hostname, public key og TXT værdi til opsætningen. Når I har udført disse trin skal I vende tilbage til os så vi kan bekræfte domæneejerskabet og opsætningen af SPF of DKIM og flytte jer til en bedre IP adresse at udsende fra.

2.2 Validering af domæne

For at validere ejerskabet af jeres domæne tilbyder vi to metoder:

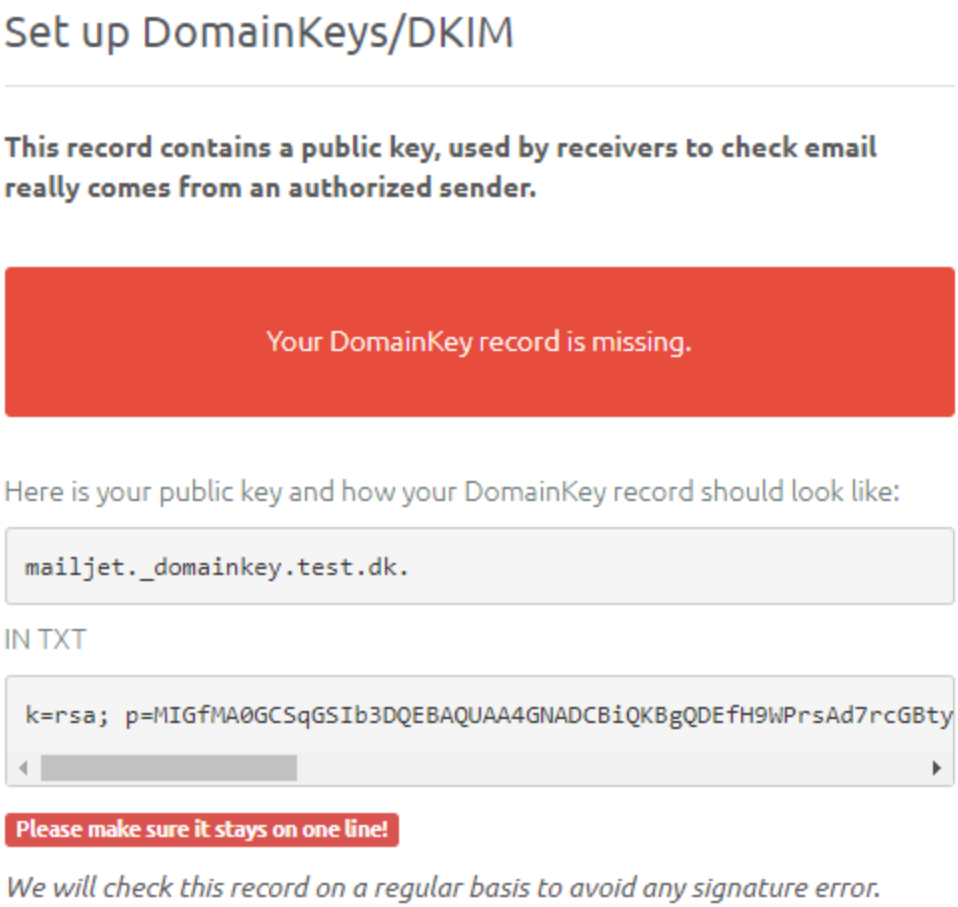
1) Placer en midlertidig fil på jeres website
2) Opret en DNS record.

Vi oplyser jer bade filnavn til mulighed 1 og hostname og værdi til mulighed 2, eksempelvis:



2.3 DKIM-opsætning

For at validere jeres DKIM-opsætning skal du først opsætte jeres SPF record, som beskrevet i afsnit **1. SPF records**. I e-mailen I modtager fra os omkring opsætning modtager I også en offentlig nøgle (public key) og tekst værdi til jeres DKIM record, eksempelvis:



Efter du har oprettet ovenstående I din DNS skal du vende retur til os, så vi kan validere opsætningen. Herefter bekræfter vi at alt er som det skal være, eller bede dig foretage eventuelle ændringer.

3. DMARC-opsætning

DMARC står for "Domain-based Message Authentication, Reporting & Conformance" og er endnu et niveau af e-mail validering. Denne yderligere valideringsprocedure kan først opsættes efter at SPF og DKIM-opsætningen er gennemført. DMARC tillader dig at tilføje endnu et sikkerhedslag for dit domæne og indikerer overfor modtager-servere hvordan de skal reagere hvis SPF og DKIM-valideringen fejler (NB: Ikke alle e-mailservere tager højde for DMARC politikker når de leverer e-mails).

For at indføre en DMARC-politik til et afsenderdomæne er det tilstrækkeligt at tilføje en TXT-record i DNS-zonen på afsenderdomænet, eksempelvis:

Host: *dmarc.yourdomain.com.*
Txt: *v=DMARC1; p=none; pct=100; rua=mailto:yourmail@yourdomain.com; sp=none; aspf=r;*

Du kan læse mere om DMARC-validering i Mailjet's tekniske dokumentation. Aktivering af DMARC-validering for dit domæne koster en times konsulentarbejde for den opsætning der ligger hos os.

4. Udsendelse af e-mails fra egen e-mail server

Et alternativ til at lave ovenstående opsætning er at sende e-mails fra webCRM gennem jeres egen e-mailserver. På den måde er I selv ansvarlige for jeres domænes spam-rating og skal selv sørge for at opretholde en god afsenderskik, for at jeres e-mails vil nå frem. En ulempe ved denne metode er at I ikke kan benytte Mailjet i webCRM, så klik- og åbningsrater kan ikke overvåges og benyttes i webCRM.

Hvis du ønsker at sende e-mails via din egen server, skal du sikre at jeres webCRM system kan tilgå jeres SMPT server ved at tjekke jeres servers autentificeringsmetode. I kan tillade webCRM at udsende e-mails ved enten at sende brugernavn og adgangskode til SMTP-serveren til support@webcrm.com og angive, at I ønsker at sende e-mails fra jeres egen server, eller ved at whiteliste IP-adressen **40.74.40.57**, som webCRM systemet udsender e-mails fra. Hvis I ikke har authentication på jeres SMTP-server, kan I skippe dette trin, men det er ikke anbefalet, da alle i så fald kan udsende e-mails som jer.

Når ovenstående er udført, beder vi jer sende os følgende information på support@webcrm.com:

- E-maildomæne eller IP-adresse, der skal sendes igennem
- Porten der skal sendes igennem
- Hvorvidt I ønsker TLS kryptering slået til eller fra
- (Brugernavn og kodeord, hvis I benytter denne autentificeringsmetode)

Vi laver opsætningen herfra og derefter vil jeres egen e-mailserver blive brugt til udsendelser fra webCRM.

5. Specielle indstillinger for interne e-mails

Nogle kunder har en opsætning, hvor e-mails sendt og modtaget internt i organisationen beskyttes på en særlig måde. Det er typisk indført for at sikre at folk udenfor virksomheden ikke kan identificere sig som en ansat og sende e-mails fra domænet fra andre steder end virksomhedens egne servere.

Det begrænser dog også webCRM fra at sende e-mails til jeres egne e-mailadresser og I skal tillade at e-mails fra IP-adressen **40.74.40.57** kan modtages internt.