Samen aanjagen van vernieuwing

Handreiking beveiligen e-mail

Instellen van SPF, DKIM, DMARC, DNSSEC en DANE

Auteur(s): SURF
Versie: 1.2
Datum: 29 oktober 2024
Kenmerk: Handreiking beveiligen e-mail

Inhoudsopgave

1 Inleiding

E-mail is een van de meest gebruikte communicatiemiddelen ter wereld. Het is een snelle en gemakkelijke manier om met anderen in contact te komen waar iedereen toegang toe heeft. Helaas is e-mail ook een kwetsbaar medium voor aanvallen. Spam, phishing en andere vormen van cybercrime worden vaak via e-mail verspreid. Een van de oorzaken hiervan is dat e-mail zonder aanvullende maatregelen kwetsbaar is voor spoofing: iemand kan zich voordoen als een andere afzender en zo namens jou e-mails versturen. Om spoofing tegen te gaan en het gebruik van e-mail veiliger te maken kun je een aantal maatregelen nemen, zoals het gebruik van SPF, DKIM, DMARC, en DANE voor STARTTLS. In deze handreiking leggen we uit hoe je deze technieken kunt instellen.

1.1 FROM: header en Envelope sender

In e-mailstandaarden zijn er twee belangrijke concepten: het "From:"-adres, zoals weergegeven in de FROM-header en het "Envelope Sender"-adres. Het "From"-adres zie je in de e-mailclient en toont aan de lezer wie de e-mail heeft gestuurd. Het "Envelope Sender"-adres, ook bekend als "Return-Path" of "MAIL FROM", is technisch en geeft aan waar *bounce* berichten naartoe gaan als de e-mail niet afgeleverd kan worden. Dit onderscheid is belangrijk omdat ze niet hetzelfde hoeven te zijn en de verschillende standaarden de authenticiteit van de verschillende adressen beschermen.

1.2 SPF (Sender Policy Framework)

Dit is een techniek die het mogelijk maakt om te verifiëren of een e-mailbericht is verzonden door een geautoriseerde versturende mailserver. SPF werkt door een record in je DNS-zone te plaatsen dat de IP-adressen of hostnamen bevat die mogen worden gebruikt om e-mail namens je domein te verzenden. Wanneer een mailserver een e-mailbericht ontvangt, kan die dit record raadplegen om te controleren of het bericht is verzonden vanaf een van de geautoriseerde IP-adressen. Meer informatie over het configureren van SPF lees je in hoofdstuk 2.

1.3 DKIM (Domain Keys Identified Mail)

Deze techniek maakt het mogelijk om de authenticiteit van een e-mailbericht te verifiëren. DKIM werkt door een digitale handtekening aan een e-mailbericht toe te voegen. Deze handtekening wordt gemaakt met een sleutel die is gekoppeld aan een domein. Een ontvangende mailserver kan dan controleren of het bericht niet meer is veranderd na het zetten van de handtekening. Meer informatie over het configureren van DKIM lees je in hoofdstuk 3.

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

Deze techniek geeft domeineigenaren de mogelijkheid een beleid te definiëren wat een ontvanger moet doen als het afzenderdomein niet minimaal is geauthentiseerd met SPF en/of DKIM. De rapportagemogelijkheid stelt domeineigenaren in staat om rapportages te ontvangen over het gebruik van hun domeinnaam en eventueel misbruik te detecteren. Meer informatie over het configureren van DMARC lees je in hoofdstuk 4.

1.5 DANE (TLSA DNS Authentication of Named Entities)

Mailservers gebruiken (net als websites via HTTPS) TLS om hun verbinding te versleutelen. Met DANE kun je de authenticiteit van TLS-certificaten verifiëren zodat je zeker weet dat niemand de

verbinding onderschept. DANE werkt door een record in je DNS-zone te plaatsen dat de TLS-certificaten bevat die gebruikt mogen worden om verbinding te maken met je servers. Wanneer een versturende en/of ontvangende mailserver een verbinding maakt met je servers, kan die dit record raadplegen om te controleren of het TLS-certificaat bij de server hoort. Zie ook in hoofdstuk 5.

2 Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is een DNS-record dat aangeeft welke servers e-mail namens je domein mogen verzenden. Door alle mailservers die e-mail verzenden toe te voegen aan je SPF-record, kun je helpen om je e-mail tegen *spoofing* te beschermen, andere mailservers worden dan in principe niet vertrouwd door een ontvanger. SPF beschermt het domein van de *envelope sender.* In dit hoofdstuk lees je hoe je SPF kunt configureren voor jouw instelling.

2.1 SPF-records verschillen per organisatie

De configuratie van SPF hangt af vanaf waar er mail moet worden verstuurd.
Je moet alle IP adressen van applicaties die e-mail verzenden toevoegen aan je SPF-record.
Organisaties maken gebruik van verschillende e-maildiensten en apps voor het verzenden van e-mails, zoals Microsoft 365, SURFmailfilter, Google Workspace, SendGrid, enzovoort. Elke dienst kan een andere set IP-adressen hebben die moeten worden opgenomen in het SPF-record.

2.2 SPF Configuratie

Er zijn verschillende scenario's mogelijk voor het instellen van SPF. Om een indruk te geven van de mogelijkheden beschrijven we hieronder verschillende voorbeelden:

1. Je gebruikt slechts één dienst, om e-mails namens de organisatie te verzenden. In dit scenario voeg je een verwijzing (‘include:’) naar het SPF-record van de dienst toe aan jouw SPF:

   v=spf1 include:_spf.surfmailfilter.nl –all

2. Je wil hier een online leeromgeving (we nemen als voorbeeld BrightSpace) aan toevoegen. Het record ziet er dan zo uit:

   v=spf1 include:_spf.surfmailfilter.nl include:_spf.brightspace.com -all

3. Je heb nog een losse server die mail kan versturen, daarvoor wil je een specifiek IPv4-adres toevoegen, hiervoor gebruik je de ‘ip4’ tag:

   v=spf1 ip4:192.0.2.0 include:_spf.surfmailfilter.nl
   include:a._spf.brightspace.com -all

Naast de hier genoemde voorbeelden is er nog de ‘v’ tag die de versie aangeeft (op dit moment altijd spf1). En wordt naast ‘ip4’ ook ‘ip6’ gebruikt om enkele of reeksen IP-adressen te specificeren.

Opmerking: De beschreven voorbeelden eindigen allemaal in “-all”. Dit geeft aan dat alle overige IP-adressen niet gemachtigd zijn om mail te versturen namens dit domein.

Naast de gegeven voorbeelden zijn er nog veel meer opties bij SPF, zoals een verwijzing opnemen naar andere records in je eigen DNS-zone. Hierboven gegeven voorbeelden vormen het minimum om er mee aan de slag te kunnen, voor uitgebreide opties kijk je bijvoorbeeld op http://www.open-spf.org/SPF_Record_Syntax/.

2.3 Publiceren van een SPF-record

Nadat je het SPF-record hebt gemaakt, moet je het publiceren in de DNS-zone voordat de ontvangende e-mailserver het kan ophalen. Het publiceren van een SPF-record doe je door het maken van een TXT-record in je domein. Dit kun je doen door de volgende stappen te doorlopen:

1. Log in bij de DNS provider. Ga naar de DNS van het domein in kwestie.
2. Als er nog geen SPF-record op het domein aanwezig is, maak er dan een aan.
3. Selecteer TXT voor het Type-dropdownmenu. Voer @ in voor het Host-veld. Voer het SPF-record in als de TXT-waarde. Klik vervolgens op de knop Opslaan. Voor SURFmailfilter alleen is dat: **v=spf1 include:_spf.surfmailfilter.nl –all**

Opmerking: Een limitatie van SPF is dat het interpreteren van een SPF-record maximaal 10 DNS lookups mag genereren. Het kan al snel voorkomen dat je over deze limiet heen gaat. Het kan bijvoorbeeld voorkomen dat een include record weer extra DNS lookups veroorzaakt. Het verdient de aanbeveling om je domeinnaam hierop te monitoren. Bijvoorbeeld met een tool, of handmatig door op internet een tool te vinden die je SPF-record valideert.

SURFmailfilter biedt hier nog een alternatief voor doordat je dan uitgaande mail van andere systemen via SURFmailfilter kan laten gaan. Je hoeft dan alleen (een “include:” van) de IP-adressen van SURFmailfilter in je DNS op te nemen.

3 Domain Keys Identified Mail (DKIM)

Domain Keys Identified Mail (DKIM) is een beveiligingsstandaard voor e-mailberichten. DKIM werkt door een digitale handtekening aan een e-mailbericht toe te voegen. Deze handtekening stelt een ontvanger in staat om te controleren of het bericht niet is gewijzigd na het zetten van de handtekening. Daarnaast stelt het de ontvanger in staat om te controleren of het domein dat in de handtekening wordt gebruikt onder controle van de versturende partij staat.

DKIM gebruikt een publiek-privaat sleutelpaar. Alleen de verzendende server kent de privésleutel, terwijl de publieke sleutel in DNS wordt gepubliceerd. Zo kan de ontvanger garanderen dat de verzendende server namens het domein mag versturen én het bericht niet is gewijzigd. In dit hoofdstuk wordt hoe je DKIM moet configureren.

3.1 De opbouw van een DKIM-record

Hieronder een voorbeeld van de domainkey die SURF gebruikt om via SURFmailfilter te versturen:

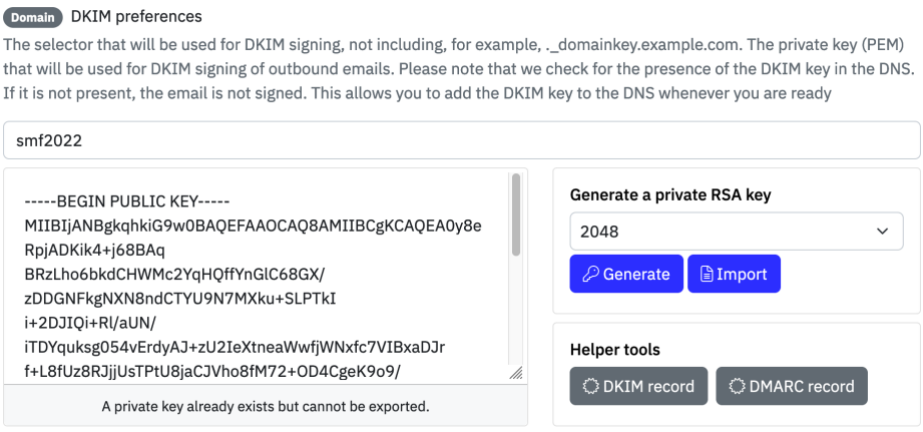
smf2022._domainkey.surf.nl. IN TXT "v=DKIM1; k=rsa; p=MIIBI[…]jANBgkqhkiG9w0BAQEA0y8eRpjADKik4+j6KCZo4O2DXkybokyT89iGXYP3nEPpSLy+yAx A8VHJsY7yFqaKtjjP8VlnTEhp4x6hWHX7DspQIDAQAB"

De tag ‘v’ geeft de versie aan, en ‘p’ de publieke sleutel. Het is een TXT-record die op de locatie _domainkey.domein.nl staat. Om meerdere systemen met verschillende sleutels te kunnen laten ondertekenen staat hiervoor nog een *selector*, in dit geval smf2022. Naast dit record zou bijvoorbeeld nog een ander DKIM-record in de DNS kunnen worden gezet. Bijvoorbeeld *google._domainkey.surf.nl* om Gmail geauthentiseerde mails te kunnen laten sturen.

3.2 DKIM instellen

Omdat je verzendende server het ondertekenen met DKIM doet, geeft dit systeem je de publieke sleutel en *selector* die gepubliceerd moeten worden. De meeste systemen zullen ook pas beginnen met ondertekenen zodra ze geverifieerd hebben dat het record er staat.

Voor Microsoft365 kijk je (op het moment van schrijven) in het Security Center onder ‘E-mailverificatie-instellingen’. Bij Google kijk je in de Admin console onder ‘Authenticate E-mail’. In SURFmailfilter vind je het DKIM-record dat je kan publiceren onder ‘Outgoing’:



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

DMARC staat voor "Domain-based Message Authentication, Reporting, and Conformance". Het is een e-mailbeveiligingsprotocol dat helpt om het domein in de FROM: header te beschermen, door het beleid van een domeineigenaar te definiëren voor de behandeling van e-mails die niet voldoen aan de authenticatievereisten (SPF óf DKIM). DMARC beschermt de *FROM: header.* In dit hoofdstuk delen we hoe je DMARC voor jouw instelling configureert.

Voordat je DMARC met streng beleid configureert, is het van belang om ervoor te zorgen dat je SPF (Sender Policy Framework) of DKIM (DomainKeys Identified Mail) correct zijn geconfigureerd en goed functioneren. DMARC bouwt namelijk voort op de basis van deze twee technologieën om een effectieve bescherming tegen e-mailspoofing te bieden.

DMARC biedt naast het formuleren van een beleid wat er met ongeauthentiseerde mail moet gebeuren ook de mogelijkheid tot het ontvangen van rapportages over het gebruik van je domeinnaam
Door een "p=none" policy in te zetten wordt door ontvangers wel gecontroleerd of je DKIM en SPF goed hebt ingesteld en rapporteren ze dat aan jou, maar ze doen er nog niks mee. Na analyse van de rapportages en mogelijke benodigde aanpassingen kan je de policy strenger instellen. Verder stelt DMARC dat je minimaal SPF of DKIM moet hebben. Een van beide volstaat dus ook. Wel wordt aangeraden om beide ingesteld te hebben.

4.1 Stappenplan configureren DMARC

De volgende stappen kun je doorlopen om DMARC te configureren.

1. **Begrijp DMARC-recordcomponenten:** Een DMARC-record is een DNS TXT-record dat wordt toegevoegd aan het domein van de afzender. Het DMARC-record bestaat uit verschillende componenten:
    a. **v=**: Geeft de versie van DMARC aan (bijv. "v=DMARC1").
    b. **p=**: Geeft aan wat te doen met falende berichten: none, quarantine of reject.
    c. **rua=**: E-mailadres waarnaar een geaggregeerde rapporten verstuurd kunnen worden
    d. **sp=**: Geeft aan of subdomeinen ook moeten voldoen aan de DMARC-regels.

    De standaard definieert ook nog ruf voor ‘forensic reports’, maar omdat deze (persoons)gegevens over individuele mails bevatten raden we aan om deze niet te vragen. De meeste mailproviders zullen deze sowieso al niet sturen.
2. **Bepaal DMARC-beleid:** Beslis of je DMARC-e-mails zelf wil controleren (p=none), e-mails wilt laten markeren als verdacht (p=quarantine), of wilt laten afwijzen (p=reject) wanneer ze niet voldoen aan SPF óf DKIM. Het doel is om naar “reject” toe te werken.
3. **Maak een DMARC-record:** Maak een TXT-record in de DNS-instellingen van het domein. Het DMARC-record moet er ongeveer als volgt uitzien:

    v=DMARC1; p=reject; rua=mailto:dmarc-reports@example.com; sp=none

    Pas de waarden aan op basis van je specifieke beleid en e-mailadressen voor rapporten.

4. **Monitoring en aanpassing:** Nadat je DMARC hebt geïmplementeerd, is het belangrijk om regelmatig rapporten te controleren en te analyseren om te zien welke e-mails niet voldoen aan de DMARC-regels. Er zijn verschillende aanbieders die software bieden om dit voor je te doen; zoals Postmark, Dmarcadvisor en Dmarcian. Dit helpt je om eventuele onbedoelde gevolgen te detecteren en je beleid indien nodig aan te passen.
5. **Geleidelijke implementatie:** Overweeg om DMARC eerst in een monitoringfase (p=none) in te stellen en rapporten te analyseren voordat je overstapt naar strengere beleidsinstellingen zoals quarantine of reject. Hierdoor krijg je inzicht in de impact op legitieme e-mails.

4.2 DMARC advies voor instellingen

Het is lastig om globaal advies te geven voor DMARC, omdat elke organisatie unieke behoeften, configuraties en beveiligingsvereisten heeft. Toch willen we graag een voorbeeld geven van hoe een goede DMARC policy er volgens ons uitziet en waar een DMARC beleid uiteindelijk minimaal aan moet voldoen:

v=DMARC1; p=reject; rua=mailto:dmarc@voorbeeld.com

Je wilt als eindstadium een situatie bereiken waarin je 100% van de mails afwijst die niet aan de DMARC policy voldoen. Uiteraard wil je ook rapporten hierover ontvangen op het in de policy aangegeven e-mail adres.

Merk op dat DMARC-beleid minstens net zo belangrijk is voor domeinen waar vanaf *geen* mail wordt gestuurd. Hier kan je meteen een p=reject op zetten om er voor te zorgen dat dit domein niet gebruikt kan worden in spoofing en spam.

5 DANE, STARTTLS en DNSSEC

Dit hoofdstuk behandelt DNSSEC, DANE en STARTTLS, drie meer fundamentele technieken voor mailbeveiliging. DNSSEC, wat staat voor Domain Name System Security Extensions, versterkt de integriteit van de DNS, waardoor je ervan verzekerd bent dat je verbinding maakt met de juiste server. Hoewel dit voor SPF, DKIM en DMARC al ten zeerste aan te raden is, is het voor DANE verplicht. DANE, of DNS-based Authentication of Named Entities, bouwt voort op de betrouwbaarheid van DNSSEC om ervoor te zorgen dat de digitale certificaten die servers gebruiken om hun identiteit te bewijzen, authentiek zijn. STARTTLS is een protocol dat de overgang van een onbeveiligde naar een beveiligde verbinding voor e-mailverkeer faciliteert.

Traditionele email is gevoelig voor *man in the middle* aanvallen. Dit trio van standaarden beschermt je hiertegen. In dit hoofdstuk leggen we uit hoe je DNSSEC, DANE en STARTTLS kunt configureren voor jouw instelling om zo een veiligere digitale omgeving te creëren. Daarbij is DANE en STARTTLS meestal al door de leverancier van maildiensten geïmplementeerd, dus lichten we alleen toe hoe je er gebruik van maakt.

5.1 DNSSEC instellen

Bij de meeste registrars is het aanzetten van DNSSEC slechts een enkele klik en in 90% van de gevallen is het niet nodig om zelf keys te genereren en publiceren. We linken naar de meest voorkomende DNS providers binnen onderwijs en onderzoek.

- SURFdomeinen: https://wiki.surfnet.nl/display/SURFdmn/Managed+domein%3A+DNSSEC+aanzetten
- Microsoft: https://learn.microsoft.com/en-us/purview/how-smtp-dane-works#how-can-exchange-online-customers-use-inbound-smtp-dane-with-dnssec-in-preview
- Cloudflare: https://developers.cloudflare.com/dns/additional-options/dnssec/
- Google Cloud DNS: https://cloud.google.com/dns/docs/dnssec-config
- AWS: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html

Microsoft biedt vanaf oktober 2024 ondersteuning voor inbound SMTP DNSSEC en DANE. Outbound DNSSEC was al door Microsoft geïmplementeerd.

1. Pas the Time-To-Live (TTL) van je huidige MX-record aan naar 1 minuut en wacht tot de TTL is verstreken voordat je verder gaat.
2. Verbind via PowerShell met Exchange Online: *Connect-ExchangeOnline –UserPrincipalName adminaccount@instelling.nl.*
3. *S*chakel DNSSEC in voor het domein: *Enable-DnssecForVerifiedDomain –DomainName “instelling.nl”.* Kopieer de gegeven output voor het nieuwe MX-record *(DnssecMxValue).*
4. Voeg een nieuw MX-record toe met de gekopieerde output van stap 3, stel de TTL in op 1 minuut en stel de prioriteit in op 20.
5. Verifieer of het nieuwe MX-record naar behoren werkt: https://testconnectivity.microsoft.com/tests/O365InboundSmtp/input
6. Als de test uit stap 6 succesvol is kun je het oude MX-record verwijderen en de prioriteit van het nieuwe MX-record aanpassen naar 0.
7. Verifieer DNSSEC validatie: https://testconnectivity.microsoft.com/tests/O365DaneValidation/input

8. Let op! Heb je ook MTA-STS geconfigureerd? Zorg er dan voor dat je MTA-STS policy (txt file) ook aangepast wordt naar het nieuwe MX-domein om te voorkomen dat mails niet meer arriveren.

DNSSEC is nu geïmplementeerd voor het domein waardoor ook DANE geïmplementeerd kan worden.

5.2 DANE voor STARTTLS instellen voor je mailserver

DANE is een protocol dat alleen werkt als DNSSEC actief is. DANE laat de ontvangende server kijken naar het TLSA-record. In dit record staat vervolgens de public fingerprint van een certificaat waarvan de domeineigenaar aangeeft dat het authoratief is voor de mx records van het domein. Dit kan bijvoorbeeld een *intermediate* certificaat zijn van de CA die het certificaat heeft uitgegeven dat op de server staat, maar kan ook de fingerprint van het certificaat zelf zijn. Je kunt hiervoor dan ook veilig *self-signed* certificaten gebruiken. Hoe je zorgt dat dit gebruikt wordt lees je bij onze collega's van SIDN.

- Postfix: https://www.sidn.nl/en/news-and-blogs/hands-on-implementing-dane-in-postfix
- Exim: https://www.sidn.nl/moderne-internetstandaarden/hands-on-de-implementatie-van-dane-op-exim
- https://learn.microsoft.com/en-us/purview/how-smtp-dane-works#set-up-inbound-smtp-dane-with-dnssec-in-preview

DANE configureren voor Microsoft 365:

1. Verbind via PowerShell met Exchange Online: *Connect-ExchangeOnline –UserPrincipalName adminaccount@instelling.nl.*
2. Schakel DANE in: *Enable-SmtpDaneInbound –DomainName "instelling.nl".* De output moet 'Succes' genereren.
3. Wacht 15-30 minuten voordat je verder gaat met stap 4 in verband met propagatie van het TLSA-record.
4. Verifieer DANE validatie: https://testconnectivity.microsoft.com/tests/O365DaneValidation/input
5. Als er drie groene vinkjes staan bij DNSSEC, TLSA en DANE is de implementatie succesvol.

Bij veel andere email providers wordt dit zowel inkomend als uitgaand standaard voor je geregeld, maar het is goed om dit te controleren.

6 Relevante bronnen

Op het internet is veel informatie te vinden over het beveiligen van email. Enkele relevante en gebruikte bronnen zijn hieronder benoemd. De testtool Internet.nl is een initiatief van het Platform Internetstandaarden, wat zich inzet voor het naleven van de door het Forum Standaardisatie afgesproken internetstandaarden. Zij geven uitgebreide uitleg bij elke standaard. De laatste link geeft nog specifiek advies voor domeinen *zonder* email.

- https://internet.nl/faqs/mailauth/
- https://internet.nl/mail/example.nl/945186/#control-panel-12
- https://www.forumstandaardisatie.nl/vergaderingen/2019/fs-20191211-5a4-opdracht-implementatie-strikte-dmarc-policy