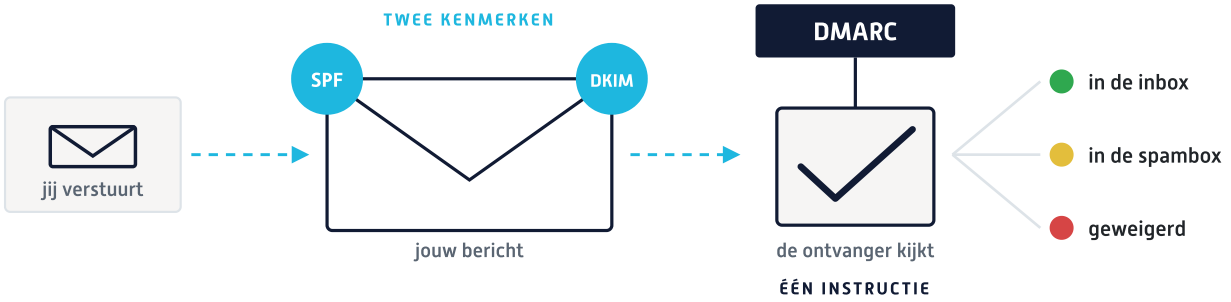
JE UITSLAG, UITGELEGD

Twee kenmerken en één instructie

Je hebt je domein bij ons laten controleren en daar een uitslag van gekregen. Maar wat betekent die eigenlijk?

Het gaat om twee vragen. **Kan iemand zich per e-mail voordoen als jouw bedrijf?** En **komen jouw eigen offertes, facturen en nieuwsbrieven betrouwbaar aan?** Die twee hangen aan dezelfde knoppen.

Je hoeft niet te weten hoe die knoppen werken — wel of ze goed staan. Het zijn er drie: twee **kenmerken** op de post zelf, en één **instructie** aan de ontvanger over wat hij moet doen als een kenmerk niet klopt. Je uitslag gaat over meer dan deze drie; de rest leggen we uit op **rijsict.nl/e-mailcheck**.



KENMERK 1

SPF

De lijst van verzendpunten

Hierin staat welke servers namens jouw domein mogen versturen: je mailprovider, je boekhoudpakket, je nieuwsbriefdienst. Komt een bericht ergens anders vandaan, dan klopt dit kenmerk niet.

Ontbreekt het? Dan kan de ontvanger niet nagaan of de verzender bij jou hoort.

KENMERK 2

DKIM

Het zegel op de brief

Je mailserver zet een digitale handtekening op elk bericht. De ontvanger controleert die tegen een sleutel in jouw domein. Zo weet hij dat de post echt van jou komt én onderweg niet is veranderd.

Ontbreekt het? Dan sta je zwak bij doorgestuurde post: daar werkt SPF vaak niet meer, en DKIM wel.

DE INSTRUCTIE

DMARC

Wat de ontvanger moet doen

Hier zeg jij wat er moet gebeuren met post die de kenmerken niet haalt: niets doen, naar de spambox, of weigeren. En je vraagt om rapportage, zodat je ziet wie er namens jou verstuurt.

Staat het op niets doen? Dan grijpt DMARC niet in, en laat je het aan de spamfilters van de ontvanger over.

Waarom één kenmerk niet genoeg is

Een bericht doorstaat DMARC als **SPF óf DKIM klopt én het gecontroleerde domein past bij de naam die de ontvanger in het afzenderveld ziet**. Eén van de twee lijkt genoeg, maar dat is het niet: zodra een bericht wordt doorgestuurd werkt SPF vaak niet meer, en is DKIM het enige dat nog overeind kan blijven. Ontbreekt dat, dan belandt jouw eigen post in de spambox terwijl je dacht dat alles goed stond.

Wat jouw DMARC-stand betekent

De instructie kent vier standen. Ze lopen van **“je hebt nooit iets gezegd”** tot **“wat niet klopt, komt er niet in”**. In de uitslag die je van ons kreeg, staat op welke stand jouw domein nu staat.



Geen record er staat niets	**“Je hebt de ontvanger nooit iets verteld.”** Hij doet maar wat: elke ontvanger bedenkt zelf of hij jouw post vertrouwt. Je hoort het ook niet als iemand jouw naam misbruikt.
p=none meekijken	**“Je kijkt mee, maar laat alles door.”** De ontvanger controleert netjes, ziet dat het niet klopt, en bezorgt het alsnog. Het slot zit op de deur, maar niemand draait hem om.
p=quarantine naar de spambox	**“Twijfelgevallen gaan naar de spambox.”** Vervalste post komt niet meer in de inbox, maar is nog wel te vinden. Een goede tussenstap.
p=reject weigeren	**“Wat niet klopt, komt er niet in.”** De ontvanger neemt het bericht niet aan. Dit is waar je naartoe wil.

DMARC werkt bij ontvangers die het toepassen; de grote partijen doen dat. Bij “meekijken” grijpt DMARC zelf niet in — gewone spamfilters blijven wel hun werk doen.

Wat een slechte stand concreet betekent

1

Factuurfraude op jouw naam

Een klant van jou krijgt een mail die écht van jullie lijkt te komen — jullie naam, jullie adres, jullie ondertekening — met een factuur en een ander rekeningnummer. Jij hoort het pas als die klant belt dat hij betaald heeft.

2

Je eigen post komt niet aan — en je merkt het niet

Google en Yahoo eisen sinds 2024 SPF, DKIM én een DMARC-record van wie veel post verstuurt — bij Google vanaf zo’n 5.000 berichten per dag naar privé-adressen op gmail.com. Ook daaronder weegt het mee in de filters. Je krijgt **geen foutmelding**: je offerte, factuur of wachtwoordmail wordt stil in de spambox gelegd. Jij ziet een verstuurd bericht, de klant ziet niets.

3

Je ziet het niet gebeuren

Zonder rapportage weet je niet eens óf er al misbruik is. De meeste bedrijven ontdekken het via een klant die vraagt of die rare mail van hen was.

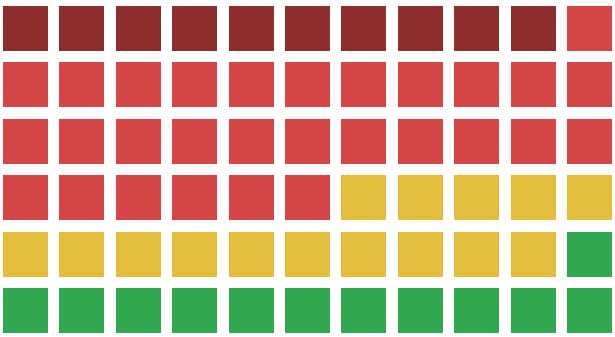
“Meekijken” is een goed begin, geen eindstand

Wie net begint, hóórt op meekijken te staan: eerst een paar weken meten wie er namens jou verstuurt, en dan pas dichtzetten. Wie meteen op weigeren zet, ziet zijn eigen nieuwsbrief verdwijnen. **Het probleem is dus niet dat er “meekijken” staat — het probleem is dat het er bij veel bedrijven al jaren op staat.**

WAT WE OP DE BEURS ZAGEN

Je bent bepaald niet de enige

Voor de beurs hebben we de standhouderslijst langsgelopen en elk domein gemeten, zonder er iemand mee lastig te vallen. Dit kwam eruit.



10 geen record · 29 meekijken · 15 spambox · 12 weigeren

66 standhouders hebben we voorafgaand aan de beurs gemeten, op hun eigen domein.

59% daarvan — 39 bedrijven — had **niets staan dat vervalste post tegenhoudt**: geen record, of de instructie op meekijken.

20 hadden geen DKIM-sleutel op de gangbare selectors van de grote aanbieders — het kenmerk dat juist bij doorsturen overeind blijft.

39 gebruiken Microsoft 365. Zeven van hen tekenden nog met Microsofts eigen naam en niet met hun domein; dan telt DMARC die handtekening niet mee.

Van meekijken naar weigeren, in vier stappen

1 **Meten**

DMARC aan op meekijken, mét rapportage. Twee tot vier weken verzamelen wie er namens jou verstuurt.

2 **Bronnen op orde**

Microsoft 365, je boekhoudpakket, je CRM, je nieuwsbrief, de formulieren op je site: elk krijgt zijn plek in SPF en een eigen DKIM-sleutel.

3 **Naar de spambox**

De instructie op quarantine. Vervalste post komt niet meer in de inbox. Je blijft meekijken in de rapporten.

4 **Weigeren**

De instructie op reject. Vervalste post met jouw domein wordt dan geweigerd door elke ontvanger die DMARC toepast.

Bij elkaar meestal zes tot tien weken, waarvan het meeste wachttijd is. Het echte werk zit in stap 2, en dat is uitzoekwerk — geen techniek.

Het blijft daarna bewegen

Klaar is het nooit helemaal. Er komt een pakket bij, marketing probeert een andere nieuwsbrief, een leverancier wisselt van mailserver — en niemand werkt de records bij. Zo loopt een domein dat ooit goed stond langzaam weer scheef. SPF heeft daarbij een harde grens van tien opzoekingen, waar bedrijven met veel pakketten ongemerkt tegenaan lopen.

En wat dit niet oplost

DMARC stopt iedereen die jouw **exacte domeinnaam** gebruikt. Het stopt niemand die er een nieuwe naast registreert die er bijna hetzelfde uitziet — een streepje erbij, een letter anders. Daar is iets anders voor nodig, en het is goed om te weten dat die twee niet hetzelfde zijn.

Jouw uitslag verbeteren?

Je domein is al gemeten. In een halfuur lopen we die uitslag langs: wat er goed staat, waar het risico zit, wat er moet gebeuren, wat je zelf kunt oppakken en waar wij je bij kunnen helpen. Voorbereiden hoef je niets, en er zit geen verplichting aan.

Bert van Rijssen · bert@rijs.nl
rijsict.nl · check.rijs.nl

Doe de check nog eens, of laat een collega hem doen