

ONDERZOEK

Onderzoek onder NOAB-administratiekantoren, 2026

Openbare telling van DNS- en HTTPS-records bij actieve NOAB-kantoren

In de periode van 1 tot en met 7 oktober 2026 vroeg 68,6% van de 854 unieke domeinen van actieve NOAB-kantoren ontvangers niet om valse mail te blokkeren of in quarantaine te zetten. SPF staat bij de meeste kantoren wel. Het gat zit in het DMARC-beleid.

68,6% geen afdwingend DMARC-beleid

31,4% vraagt ontvangers te blokkeren of te quarantainen

62,4% SPF eindigt op -all

61 domeinen op 10 of meer SPF-lookups

854 unieke domeinen. 893 kantoren met een eigen domein. 919 actieve kantoren in het openbare portaal.

NovaMX B.V. · Beverwijk

Peilperiode: 1 tot en met 7 oktober 2026

Publicatie: 8 oktober 2026

Inhoud

Wat onafhankelijk hier betekent	3
1. Aanleiding	3
2. Populatie	3
3. Methode	3
4. DMARC-beleid	4
5. RUA en RUF	4
6. SPF	5
7. SPF-lookups en flattening	6
8. DNSSEC, HTTPS en transport	8
9. Regio	9
10. Wat dit voor een kantoor betekent.....	11
11. Conclusies.....	12
12. Wat deze meting niet zegt.....	12
Over NovaMX	12

Wat onafhankelijk hier betekent

NovaMX heeft deze meting zelf uitgevoerd. Niemand in de branche heeft de opdracht gegeven, de telling betaald of de uitkomsten gezien vóór publicatie. De bron is het openbare NOAB-kantorenportaal plus openbare DNS en één HTTPS-verzoek per eigen domein. Kantoren zijn niet gekozen omdat ze wel of geen klant van NovaMX zijn.

NovaMX levert ook mailbeveiliging, waaronder DMARC-rapporten en SPF-flattening. Dat belang staat hier, zodat de lezer het kan meewegen. De cijfers in dit rapport zijn tellingen, geen aanbieding. Een kantoor wordt nergens bij naam genoemd.

1 Aanleiding

Administratie- en belastingadvieskantoren versturen facturen, aangiften en betalingsverzoeken uit naam van het kantoor. Als een buitenstaander een bericht kan laten lijken alsof het van dat domein komt, kan een klant een rekeningnummer wijzigen omdat de afzender er vertrouwd uitziet.

Of die buitenstaander slaagt, hangt voor een deel af van records die iedereen kan opvragen. SPF is de gepubliceerde lijst van systemen die namens het domein mogen versturen. DMARC is een aparte instructie aan de ontvangende mailserver: wat te doen als een bericht die controle niet haalt, en waar een rapport naartoe mag. DNSSEC beschermt de antwoorden op die vragen tegen vervalsing onderweg. Dit rapport telt die publieke signalen voor één afgebakende beroepsgroep.

2 Populatie

NOAB is de branchevereniging voor administratie- en belastingadvieskantoren en noemt circa 1.100 aangesloten kantoren. In de periode van 1 tot en met 7 oktober 2026 toonde het openbare kantorenportaal 919 actieve kantoren. Dat is de populatie van dit rapport: een telling van die lijst, geen steekproef uit een groter bestand.

Van die 919 kantoren hadden 21 geen website in het portaal, en 5 een adres op een platform of sociaal netwerk. Die laatste groep heeft geen eigen maildomein om te beoordelen. Over blijven 893 kantoren met een eigen domein, samen 854 unieke domeinen. Een deel van de kantoren deelt een domein. Daarom staan landelijke mailcijfers per domein, en regionale cijfers per kantoor: elk kantoor krijgt de score van zijn domein.

Dit rapport gaat alleen over de kantoren op die lijst. Kantoren die er niet op staan, zijn niet geteld en worden hier niet vergeleken.

3 Methode

Per eigen domein is in de periode van 1 tot en met 7 oktober 2026 het volgende opgevraagd, alleen via gewoon DNS-verkeer en één HTTPS-verbinding naar de vermelde website:

- SPF op het organisatiedomein: de verzendlijst, en hoeveel DNS-verwijzingen (lookups) in de hele keten zitten.
- DMARC op `_dmarc`: het beleid `p=`, en of `rua` of `ruf` een mailto-adres voor rapporten bevat.
- Of er een MX-record is.
- Of de parent een DS-record heeft. Dat betekent dat DNSSEC is gedelegeerd, niet dat de keten ook valideert.
- MTA-STS als `TXT v=STSV1` op `_mta-sts`, en TLS-RPT als `TXT v=TLSPRV1` op `_smtp._tls`.
- Of de vermelde website een geldig TLS-certificaat heeft, en of een antwoord HSTS meestuurt.

Een lookup in de SPF-telling is één van deze termen: `include`, `a`, `mx`, `ptr`, `exists` of `redirect`, ook als die term in een genest `include` staat. `ip4`, `ip6` en `all` tellen niet. Dat is dezelfde grens als in RFC 7208: bij 10 of meer van die termen mag een ontvanger het SPF-resultaat als permanente fout behandelen. De waarschuwing bij 8 of 9 is de grens die de NovaMX-portalcheck ook gebruikt, omdat een wijziging bij een mailplatform een kantoor dan over de 10 kan duwen.

Niet gemeten: DKIM, omdat de selector niet betrouwbaar uit DNS alleen volgt. Niet gemeten: of één `mx`-term meer dan 10 adresrecords teruggeeft, en of meer dan twee lookups leeg terugkomen. Niet gemeten: softwareversies, open poorten, of de inhoud van dossiers. Een tijdsoverschrijding telt niet mee als "afwezig". Bij DMARC was dat aantal nul.

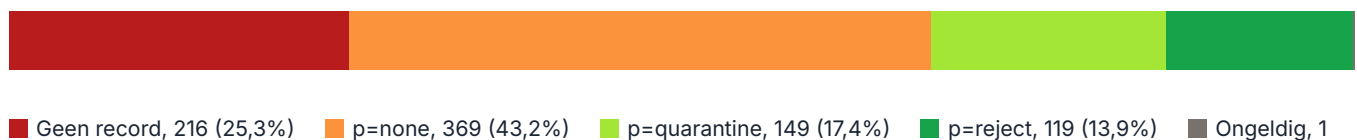
4 DMARC-beleid

DMARC staat in een apart DNS-record en heeft een beleid, geschreven als `p=`. Dat beleid is de vraag aan de ontvanger. Van de 854 domeinen heeft 68,6% geen beleid dat ontvangers vraagt een verdacht bericht te weren. Die uitkomst bestaat uit drie groepen.

Geen record (216 domeinen, 25,3%). Er is geen DMARC-instructie. Ontvangers beslissen zelf wat ze met een bericht doen dat de afzendercontrole niet haalt.

`p=none` (369 domeinen, 43,2%). Het record bestaat. Het beleid vraagt ontvangers het bericht gewoon af te leveren, ook als de controle faalt. Dat is een monitorstand, en alleen bruikbaar als er ook een rapportadres in staat. Zonder dat adres komt er niets terug. Daarover gaat de volgende paragraaf.

Afdwingend (268 domeinen, 31,4%). Daarvan staat `p=quarantine` op 149 domeinen (17,4%) en `p=reject` op 119 (13,9%). Quarantine vraagt de ontvanger het bericht als verdacht te behandelen, meestal door het apart te zetten. Reject vraagt het bericht te weigeren. Eén record was ongeldig.



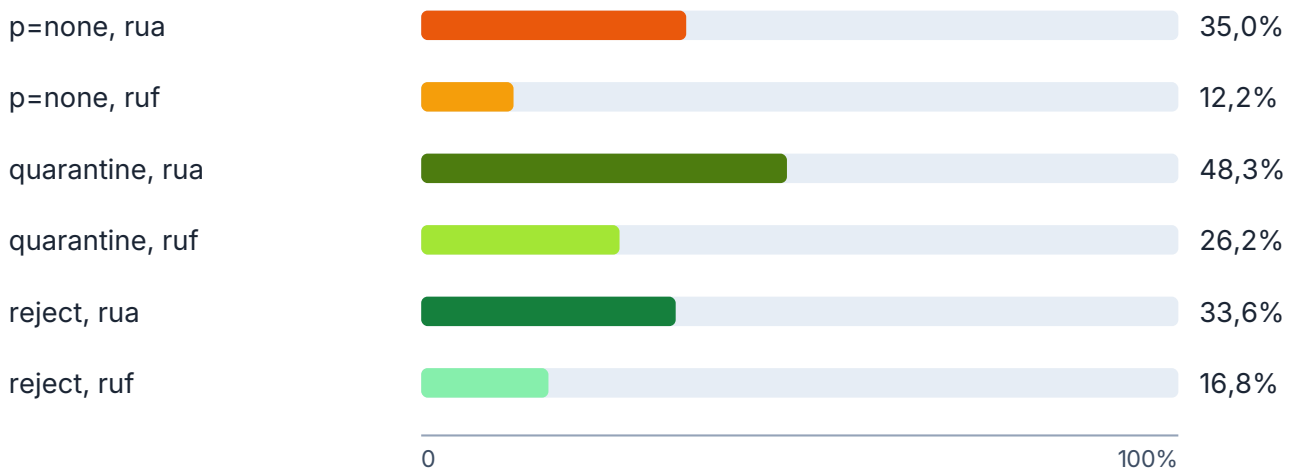
Figuur 1. DMARC-beleid op 854 unieke domeinen.

De meeste domeinen publiceren wel een DMARC-record. Dat record vraagt in meerderheid nog niet om ingrijpen.

5 RUA en RUF

Een DMARC-record kan twee soorten rapportadressen bevatten. `rua` is het adres voor verzamelrapporten: welke systemen mail probeerden te versturen uit naam van het domein. `ruf` is het adres voor foutrapporten over afzonderlijke berichten. Alleen een ingevuld `mailto`-adres telt. Een limiet achter het adres, zoals een maximumgrootte, telt nog steeds als een verzoek.

Onder de 638 domeinen mét een DMARC-record vraagt 37,9% om een verzamelrapport en 16,5% om een foutrapport. `ruf` komt in deze meting nergens voor zonder `rua`.



Figuur 2. Aandeel domeinen met een mailto-adres voor rua of ruf, per beleid.

Beleid	Domeinen	rua	ruf	Beide	Geen van beide
p=none	369	35,0%	12,2%	12,2%	65,0%
p=quarantine	149	48,3%	26,2%	26,2%	51,7%
p=reject	119	33,6%	16,8%	16,8%	66,4%

Tabel 1. Rapportverzoeken binnen domeinen die dat beleid publiceren. Percentages zijn van de rij.

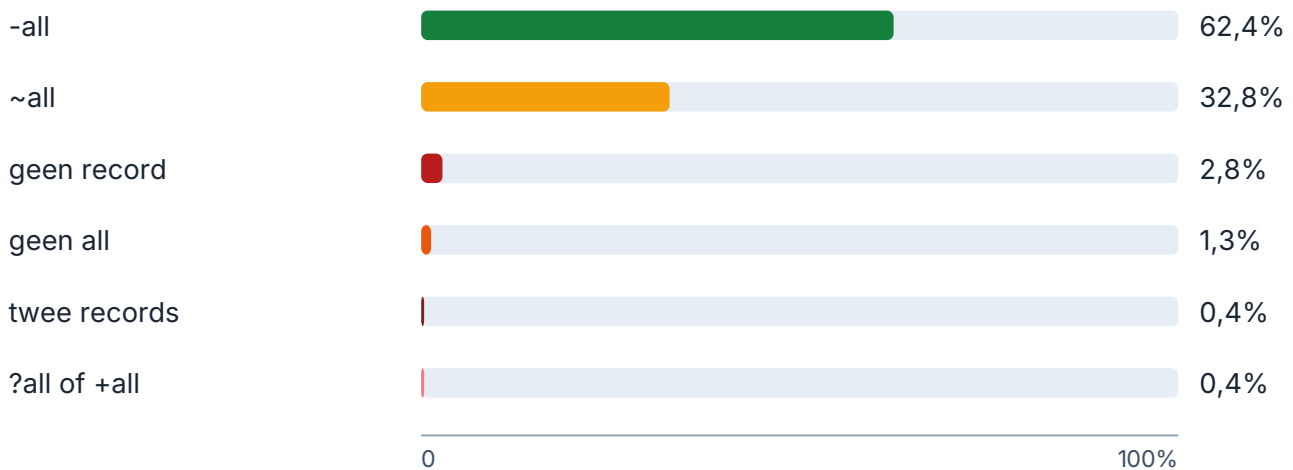
Bij p=none vraagt 65,0% ook geen enkel rapport. Dat record staat aan en levert het kantoor geen informatie.

p=quarantine vraagt het vaakst om rapporten (48,3% heeft rua). Bij p=reject heeft 66,4% geen rapportadres: die kantoren vragen ontvangers te weigeren, maar zien niet wat er vervolgens gebeurt.

6 SPF

SPF is de lijst van systemen die namens het domein mogen mailen. Die lijst eindigt meestal met een afsluiter. -all betekent: wie er niet op staat, mag niet versturen. ~all betekent: wie er niet op staat, is verdacht, maar veel ontvangers leveren zo'n bericht toch af. Zonder afsluiter, of met ?all of +all, beperkt de lijst bijna niemand. Twee SPF-records tegelijk maken de controle ongeldig: ontvangers mogen het resultaat dan negeren.

24 domeinen (2,8%) hebben geen SPF-record. 533 (62,4%) eindigen op -all. 280 (32,8%) eindigen op ~all. 11 records hebben geen all-term. 3 domeinen publiceren twee SPF-records. 3 records sluiten af met ?all of +all.



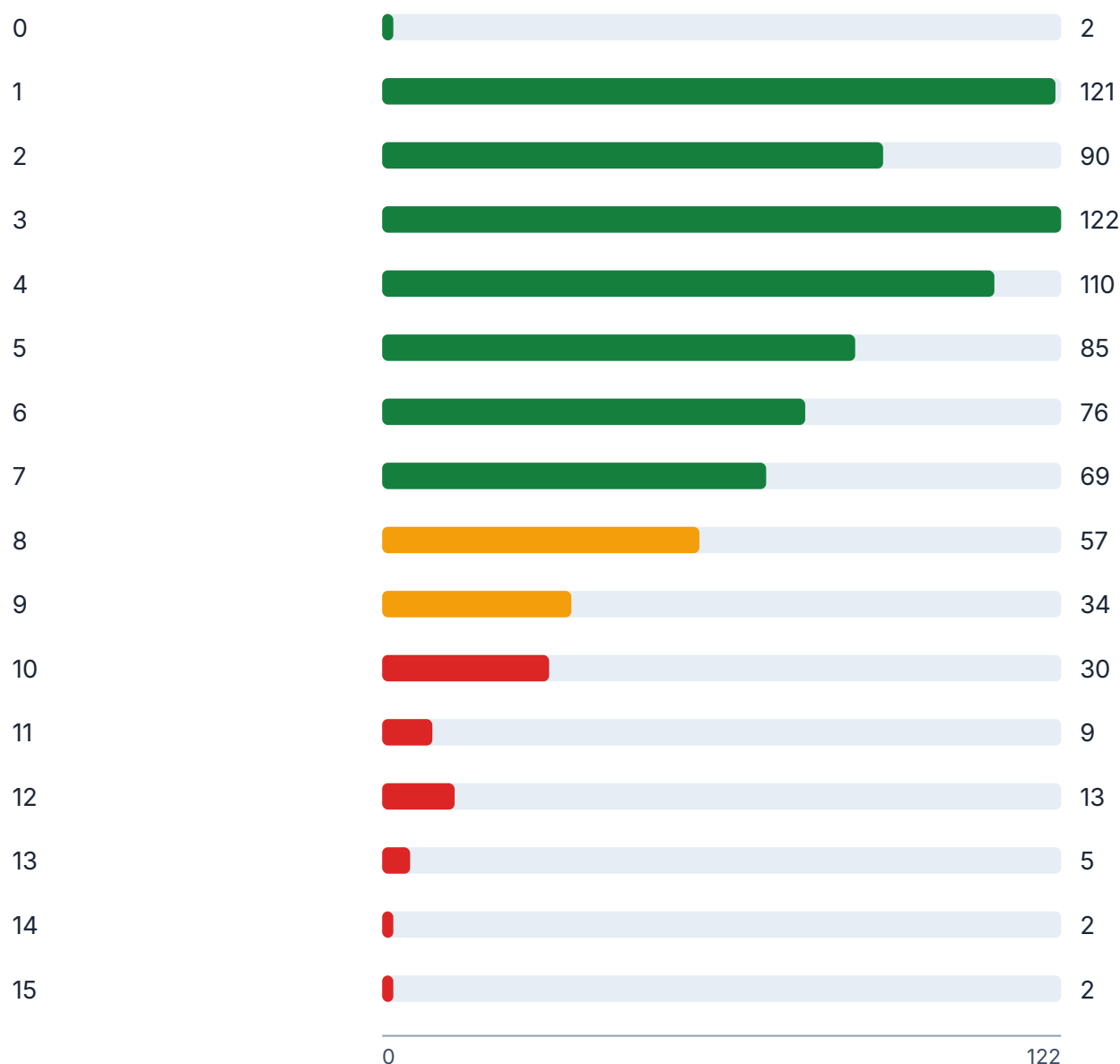
Figuur 3. SPF op 854 unieke domeinen.

SPF zegt wie mag versturen. Zonder afdwingend DMARC blijft een ontvanger vrij om een bericht dat die toets mist toch af te leveren. Een strak SPF-record en een DMARC-beleid van `p=none` zijn twee aparte uitkomsten.

7 SPF-lookups en flattening

Een SPF-lijst verwijst vaak door naar andere DNS-namen, bijvoorbeeld de verzenddienst van het kantoor. Elke zo'n verwijzing is een lookup, ook als die naam zelf weer doorverwijst. Ontvangers mogen stoppen bij 10 lookups. Dan kan de controle als mislukt gelden, ook als de lijst inhoudelijk klopt. Flattening vervangt die verwijzingen door de onderliggende adressen, zodat de lijst onder die grens blijft.

Van de 827 domeinen met precies één SPF-record zitten 61 (7,4%) op 10 of meer lookups. Daar kan SPF voor ontvangers al een permanente fout zijn. Nog 91 (11,0%) zitten op 8 of 9: één extra verzenddienst kan ze over de grens duwen. 673 (81,4%) blijven op 7 of lager. De mediaan is 4. Het hoogste volledig getelde aantal is 15. Bij 2 domeinen brak de keten af voordat de telling compleet was.



Figuur 4. Aantal domeinen per lookup-aantal, bij één SPF-record. Groen is onder 8, amber is 8 of 9, rood is 10 of meer.

Lookups	Domeinen
0	2
1	121
2	90
3	122
4	110
5	85
6	76
7	69
8	57
9	34
10	30
11	9
12	13
13	5
14	2
15	2

Tabel 2. Aantal domeinen per lookup-aantal, bij één SPF-record.

Flattening raakt een minderheid van de domeinen. Het verklaart het verschil bij DMARC niet. Een kantoor met 4 lookups en p=none heeft geen lookup-probleem. Het beleid staat nog op meten, of er is geen meting, als rua ontbreekt.

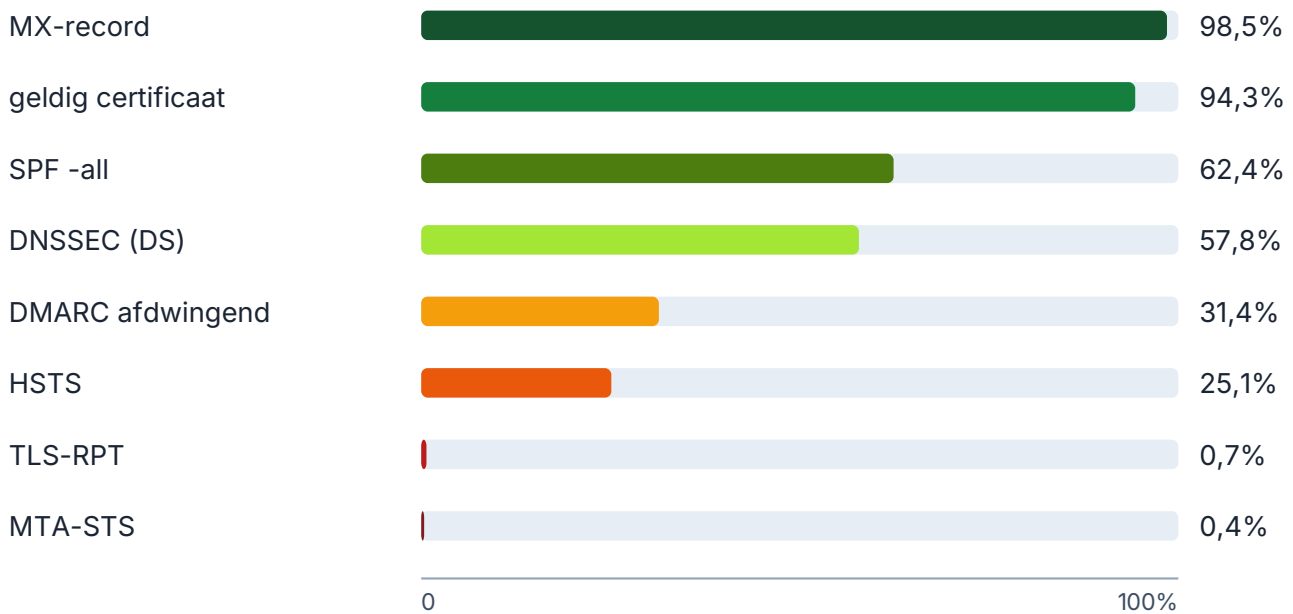
De 3 dubbele SPF-records en de 24 ontbrekende records vallen buiten deze 827. Flattening repareert geen tweede record. Die twee records moeten eerst één record worden.

8 DNSSEC, HTTPS en transport

Bij 57,8% van de domeinen staat een DS-record bij de parent (494 van 854). DNSSEC is daarmee gewoner dan afdwingend DMARC. Een DS-record is geen bewijs dat de handtekeningen in de zone ook kloppen.

841 domeinen (98,5%) hebben een MX-record. De website van het kantoor is een ander vlak: 805 van de 854 sites (94,3%) boden een geldig certificaat. 32 hadden een certificaat dat de controle niet haalde, 15 waren niet bereikbaar op HTTPS, 2 strandden in de TLS-handshake. Van de sites met een geldig certificaat stuurde 26,3% HSTS mee.

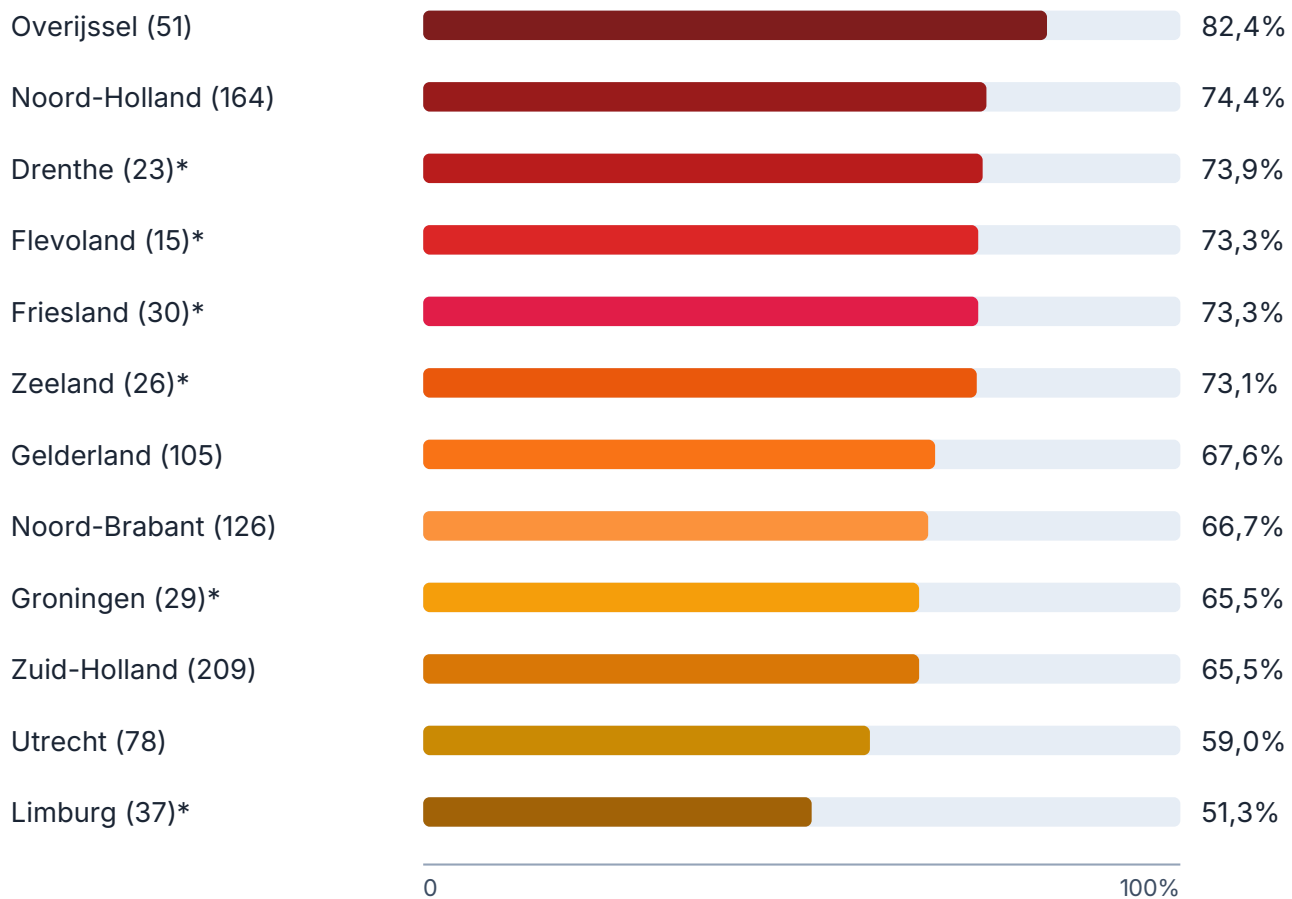
MTA-STTS, de afspraak dat bezorging naar het domein TLS moet gebruiken, stond op 3 domeinen (0,4%). TLS-RPT stond op 6 (0,7%). Dat zijn transportafspraken voor inkomende mail, geen vervanging van DMARC.



Figuur 5. Aandeel domeinen per controle. HSTS, SPF, DNSSEC, MX, het certificaat en DMARC zijn van 854 domeinen. TLS-RPT is van 851, MTA-STS van 852.

9 Regio

De provincie volgt uit de postcode van het kantoor. De percentages hieronder zijn kantoorgewogen. Een sterretje betekent minder dan 40 kantoren: dat verschil is te dun voor een harde vergelijking. Flevoland telt 15 kantoren met een eigen domein. Een percentage van nul op p=reject zegt daar weinig, omdat de groep klein is.



Figuur 6. Aandeel kantoren zonder afdwingend DMARC (p=none plus geen record), per provincie. Hoger betekent dat een groter deel ontvangers niet vraagt om te blokkeren of te quarantainen.

Provincie	Kantoren	reject	quarantine	p=none	geen record	zonder dwang	DNSSEC	SPF - all
Overijssel	51	5,9%	11,8%	47,1%	35,3%	82,4%	72,5%	66,7%
Noord-Holland	164	10,4%	15,2%	48,8%	25,6%	74,4%	59,8%	69,5%
Drenthe*	23	8,7%	17,4%	52,2%	21,7%	73,9%	34,8%	52,2%
Flevoland*	15	0,0%	26,7%	60,0%	13,3%	73,3%	66,7%	80,0%
Friesland*	30	16,7%	10,0%	53,3%	20,0%	73,3%	53,3%	43,3%
Zeeland*	26	11,5%	15,4%	34,6%	38,5%	73,1%	53,8%	50,0%
Gelderland	105	14,3%	18,1%	41,9%	25,7%	67,6%	65,7%	65,7%
Noord-Brabant	126	18,3%	15,1%	36,5%	30,2%	66,7%	50,8%	63,5%
Groningen*	29	20,7%	13,8%	41,4%	24,1%	65,5%	51,7%	58,6%
Zuid-Holland	209	12,9%	21,1%	41,6%	23,9%	65,5%	56,9%	57,9%
Utrecht	78	19,2%	21,8%	38,5%	20,5%	59,0%	57,7%	64,1%
Limburg*	37	21,6%	27,0%	37,8%	13,5%	51,3%	54,1%	43,2%

Tabel 3. Kantoorgewogen percentages. Zonder dwang is de som van de afgeronde aandelen p=none en geen record. Een sterretje: minder dan 40 kantoren.

Landsdeel	Kantoren	reject	quarantine	p=none	geen record	DNSSEC
Noord	82	15,9%	13,4%	48,8%	22,0%	47,6%
Oost	171	10,5%	17,0%	45,0%	27,5%	67,8%
West	451	13,1%	19,1%	43,7%	23,9%	58,1%
Zuid	189	18,0%	17,5%	36,5%	28,0%	51,9%

Tabel 4. Landsdelen. Noord is Groningen, Friesland en Drenthe. Oost is Overijssel, Flevoland en Gelderland. West is Utrecht, Noord-Holland en Zuid-Holland. Zuid is Zeeland, Noord-Brabant en Limburg.

Onder de provincies met minstens 50 kantoren heeft Overijssel het laagste aandeel p=reject (5,9%) en het hoogste aandeel zonder DMARC-record (35,3%). DNSSEC is daar met 72,5% het hoogst. Utrecht combineert een hoger aandeel p=reject (19,2%) met het laagste aandeel ontbrekende records onder de grotere provincies. Noord-Brabant heeft vaker geen record (30,2%) en vaker p=reject dan de provincies in de Randstad.

In de landsdelen ligt p=reject tussen 10,5% (Oost, 171 kantoren) en 18,0% (Zuid, 189). West, met 451 kantoren, zit op 13,1% en ligt het dichtst bij het landelijke beeld. De regionale verschillen zijn kleiner dan het landelijke verschil tussen SPF op -all en afdwingend DMARC.

10 Wat dit voor een kantoor betekent

De cijfers beschrijven gepubliceerde records. Ze laten niet zien dat er een vals bericht is verstuurd. Het risico zit in wat een ontvangende mailserver daardoor doet als zo'n bericht er wél is, en in wat het kantoor zelf niet ziet. Voor een administratiekantoor gaat het meestal om een factuur of betalingsverzoek die op het kantoor lijkt.

Geen DMARC, of p=none

Zonder DMARC-record heeft de ontvanger geen instructie. Bij p=none is de instructie: lever het bericht af, ook als de afzendercontrole faalt. In beide gevallen kan een bericht dat eruitziet als post van het kantoor in de inbox belanden. Dat gold voor 68,6% van de domeinen. Het domein vraagt ontvangers dan niet om het tegen te houden.

p=none zonder rapportadres

Een beleid van p=none is alleen een manier om mee te kijken als rua is ingevuld. Zonder dat adres ziet het kantoor niet welke systemen namens het domein proberen te mailen. Dat geldt voor 65,0% van de none-records. Het record staat er, en er komt niets terug.

Een SPF-lijst die niet afdwingt

Ontbreekt SPF, of eindigt de lijst op ~all, ?all of +all, dan is er geen strikte grens voor wie mag versturen. ~all markeert een onbekende afzender als verdacht, maar veel ontvangers leveren het bericht toch af. Twee SPF-records maken de controle ongeldig, zodat ontvangers het resultaat mogen negeren. Ook een lijst op -all stopt een vals bericht niet vanzelf. Zonder DMARC op quarantine of reject blijft de ontvanger vrij om een bericht dat de lijst mist toch af te leveren.

Te veel SPF-lookups

Bij 10 of meer lookups mag de ontvanger de SPF-controle als mislukt behandelen. Dan kan ook echte mail van het kantoor, zoals een factuur, als fout gelden. Bij 8 of 9 lookups is één extra verzenddienst genoeg om over die grens te gaan. Dat is een ander risico dan een ontbrekend DMARC-beleid: de eigen mail kan breken, terwijl de lijst er wel staat. In deze telling zit 7,4% van de domeinen met één SPF-record op 10 of meer, en 11,0% op 8 of 9.

Reject zonder rapporten

p=reject vraagt ontvangers een falend bericht te weigeren. Zonder rua ziet het kantoor niet welke eigen systemen daardoor worden geweigerd, en ook niet wie het blijft proberen. Handhaven en meekijken zijn twee aparte keuzes. Van de reject-records heeft 66,4% geen rapportadres.

DNSSEC, de website en transport

Zonder DS-record bij de parent zijn de DNS-antwoorden, inclusief SPF en DMARC, onderweg makkelijker te vervalsen. Een DS-record bewijst niet dat de handtekeningen in de zone ook kloppen. Een ongeldig certificaat of het ontbreken van HSTS raakt de website die een klant bezoekt, niet de factuurmail. Zonder MTA-STS publiceert het domein geen eis dat mail naar het kantoor versleuteld wordt afgeleverd. Dat gaat over mail die binnenkomt. In deze telling is dat zeldzaam, en het vervangt DMARC niet.

11 Conclusies

1. Het grootste verschil zit in het DMARC-beleid. 68,6% van de domeinen vraagt ontvangers niet om valse mail te blokkeren of in quarantaine te zetten.
2. SPF ontbreekt zelden. 62,4% eindigt op -all en 2,8% heeft geen SPF.
3. Een DMARC-record van p=none zonder rua is geen monitoring. Dat geldt voor 65,0% van de none-records.
4. Rapporten en handhaving lopen niet gelijk. Quarantine vraagt vaker om rua dan reject. Een reject zonder rua dwingt af, zonder dat het kantoor rapporten ontvangt.
5. SPF-flattening is nodig bij 61 domeinen die de lookup-limiet halen of overschrijden, en verstandig om te plannen bij nog 91 die op 8 of 9 zitten. Het is niet de verklaring voor de DMARC-cijfers.
6. DNSSEC-delegatie (57,8%) en geldige websitcertificaten (94,3%) zijn gewoner dan afdwingend DMARC. HSTS en MTA-STS zijn dat niet.
7. Regio verklaart een deel van de spreiding, vooral Overijssel tegenover Utrecht bij voldoende aantallen. Het verandert de landelijke conclusie niet.

12 Wat deze meting niet zegt

Dit is geen oordeel over de vakinhoud van een kantoor en geen pentest. DKIM is niet gemeten, dus een kantoor kan ondertekende mail versturen terwijl het DMARC-beleid nog op none staat. Een geldig websitcertificaat zegt niets over de mailstream. Een ontbrekend DMARC-record betekent niet dat er deze week een fraude is gepleegd. Het betekent dat ontvangers geen instructie van het domein hebben gekregen.

De lijst met individuele domeinen publiceren we niet. Een kantoor kan zijn eigen domein controleren via de [gratis mailcheck](#). Achtergrond bij de begrippen staat in de gidsen over [DMARC](#), [RUA](#) en [de tien SPF-lookups](#).

Over NovaMX

NovaMX B.V. is gevestigd in Beverwijk en publiceert dit onderzoek onder eigen naam. MailControl, het product voor DMARC-rapporten, beheer van DMARC-beleid en SPF-flattening, staat op de [mailbeveiligingspagina](#). Tarieven staan op de [prijzenpagina](#). Die pagina's zijn geen bijlage bij de cijfers.

Vragen over de methode: contact@novamx.eu.