Wat te doen als je mailserver op een blacklist staat

Algemeen Beheer · https://autorespond.nl/docs/wat-te-doen-als-je-mailserver-op-een-blacklist-staat/

Wat te doen als je mailserver op een blacklist staat

Soms komt een e-mail niet aan bij één of enkele van je contacten, omdat het IP-adres waarmee de mail op dat moment werd verstuurd op een blacklist staat bij de ontvangende provider. Dit herken je aan bouncemeldingen met teksten als “blocked using” gevolgd door de naam van een blacklist. Goed om te weten: onze mails worden verstuurd via een grote mailprovider met een pool van wisselende IP-adressen. Een blokkade geldt dus voor het IP-adres van dát moment; een volgende mail gaat vaak al via een ander adres.

Wat is een blacklist

Een blacklist is een lijst van IP-adressen die tijdelijk of permanent worden geblokkeerd door mailproviders omdat ze verdacht gedrag hebben vertoond. Dit kan gebeuren bij grote mailproviders vanwege het volume e-mails dat wordt verstuurd.

Sommige DNS-gebaseerde blacklists zijn niet breed erkend of betrouwbaar. Ze kunnen hele IP-ranges van grote e-mailproviders blokkeren, ongeacht de reputatie van individuele afzenders. Deze blacklists hebben vaak geen transparante criteria voor het plaatsen op de lijst of een eerlijk proces om eraf te komen.

De meeste grote mailproviders zoals Gmail, Outlook en Yahoo gebruiken deze blacklists niet voor filtering, dus de impact op je algehele bezorging is meestal minimaal. Wel kunnen kleinere of regionale providers ze gebruiken, wat kan leiden tot blokkering bij enkele ontvangers.

Hoe herken je een blacklist probleem

In de bouncemelding zie je teksten zoals:

- “blocked using bl.cloud86-dnsbl.io”
- “Service unavailable; Client host blocked”
- “listed in blacklist”

Het IP-adres dat wordt genoemd is een van onze mailservers, niet jouw eigen IP-adres.

Wat kun je doen

Stap 1: reset de bounce-status van het contact. Open het contact, zet de status van **Bounced** terug naar **Geabonneerd** en verstuur de mail opnieuw (of laat de volgende mail uit de reeks gewoon lopen). Omdat de verzending via wisselende IP-adressen loopt, komt de mail in veel gevallen dan gewoon aan.

Stap 2: controleer je eigen DNS-instellingen. Blijft het bij dezelfde ontvanger misgaan, dan ligt de oorzaak meestal niet bij het IP-adres maar bij de reputatie van jouw afzenderdomein. Ontvangende providers kijken naar de SPF-, DKIM- en DMARC-records van je domein; ontbreekt daar iets of staat er een oud record (bijvoorbeeld nog van je vorige mailsysteem), dan is dat de structurele fix. Hoe je die records controleert lees je in de gids over het voorkomen van het belanden in de spam. Twijfel je, mail dan naar support met je domeinnaam; wij kijken de records dan met je na.

Stap 3: bedenk of de ontvanger je mail wel wil. Het kan zijn dat de ontvanger je e-mail eerder als spam heeft gemarkeerd. Ga er dus niet zomaar vanuit dat je deze relatie alsnog kunt mailen. Is het een klant van wie je zeker weet dat die je mails wil ontvangen, adviseer dan om:

1. Jouw afzenderadres toe te voegen als veilige afzender in hun e-mailclient
2. Te controleren of de e-mail mogelijk in de spam-map is beland

Blijft het probleem daarna bestaan, mail dan naar support met het e-mailadres van de ontvanger en de volledige bouncetekst; dan kijken wij mee.

Wat doet Autorespond

Wij bewaken de verzendreputatie van het platform doorlopend. Een de-listing aanvragen bij zo’n blacklist doen we bewust niet: de verzend-IP-adressen wisselen, dus het vrijgeven van één adres heeft geen blijvend effect. Wat wél helpt, doen we samen met jou: de bounce resetten (stap 1) en je DNS-records op orde brengen (stap 2). Dat laatste is bijna altijd de echte oplossing, en die werkt voor álle ontvangers.

Voorkomen van blacklistings

Om blacklistings te minimaliseren:

- Mail alleen naar relaties die expliciet toestemming hebben gegeven
- Schoon inactieve relaties regelmatig op
- Gebruik altijd een duidelijke afmeldlink in je emails
- Spreidt grote mailings over meerdere uren
- Volg best practices om spam te voorkomen