Premium E-mail Deliverability Audit Rapport

Analyse: jan-karel.nl

Opgesteld voor: **Test**

Door: **BasisHost**

Datum: **3 april 2026**

Inhoudsopgave

Management Samenvatting

Totaalscore: **35/100** (35%) — Cijfer: **F**. Er zijn significante verbeterpunten geïdentificeerd. Hoewel enkele basismaatregelen aanwezig zijn, zijn er kritieke hiaten. Een gestructureerd verbeterplan wordt sterk aanbevolen.

Aandachtsgebieden: **DKIM** (0%), **DMARC** (0%), **Server Security** (33%).

Top aanbevelingen: Corrigeer de SPF syntax; Configureer DKIM signing; Voeg een DMARC record toe.

Let op: Uw score valt in de categorie 'Kritiek'. Direct actie is noodzakelijk.

Totaalscore

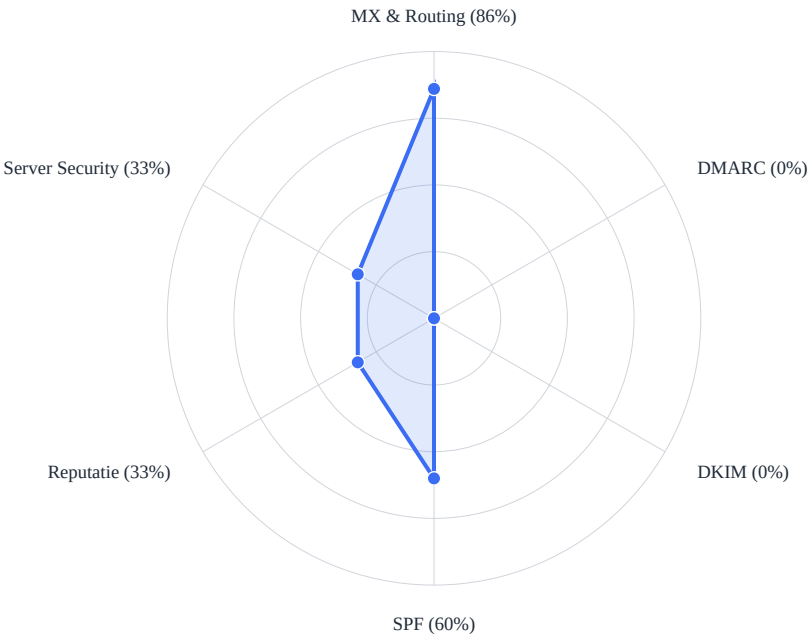
35 / 100

Cijfer: F

Onderwerp	jan-karel.nl
Totaalscore	35/100 (35%)
Cijfer	F
Rapportdatum	03-04-2026

Scores per Categorie

SPF	60%
DKIM	0%
DMARC	0%
MX & Routing	86%
Server Security	33%
Reputatie	33%


MX & Routing (86%)
DMARC (0%)
DKIM (0%)
SPF (60%)
Reputatie (33%)
Server Security (33%)

SPF — 60%

Wat is dit? SPF controleert welke servers namens uw domein e-mail mogen versturen. Zonder juiste SPF-instelling kunnen uw e-mails in spam belanden of kunnen oplichters zich als u voordoen.

Wat betekent deze score? Uw spf is voldoende, maar er zijn meerdere punten die verbeterd moeten worden om risico's te verkleinen.

Check	Status	Waarde	Advies
SPF record aanwezig	✓ PASS	Ja	
SPF syntax geldig	✗ FAIL	Nee — syntaxfouten gedetecteerd	Controleer het SPF record op typefouten en ongeldige mechanismen
SPF lookup limiet (<=10)	✓ PASS	1 lookups	
SPF beleid (-all)	✗ FAIL	Geen all-mechanisme gevonden	Voeg -all of ~all toe aan het einde van je SPF record
Geen dubbele SPF records	✓ PASS	Ja — 1 SPF record	

DKIM — 0%

Wat is dit? DKIM voegt een digitale handtekening toe aan uw e-mails, zodat ontvangers kunnen verifiëren dat het bericht echt van u afkomt en onderweg niet is gewijzigd.

Wat betekent deze score? Uw dkim scoort kritiek laag. Directe actie is vereist om ernstige risico's te voorkomen.

Check	Status	Waarde	Advies
DKIM selector gevonden	✗ FAIL	Nee — geen DKIM records gevonden voor gangbare selectors	Configureer DKIM signing bij je e-mailprovider en publiceer het DKIM record in DNS
DKIM key sterkte	✗ FAIL	N.v.t.	Configureer eerst DKIM
Meerdere DKIM selectors	✗ FAIL	N.v.t.	Configureer eerst DKIM

DMARC — 0%

Wat is dit? DMARC combineert SPF en DKIM en vertelt e-mailproviders wat ze moeten doen met verdachte berichten. Dit beschermt uw merk tegen e-mailfraude.

Wat betekent deze score? Uw dmarc scoort kritiek laag. Directe actie is vereist om ernstige risico's te voorkomen.

Check	Status	Waarde	Advies
DMARC record aanwezig	✗ FAIL	Nee — geen DMARC record gevonden	Voeg een DMARC TXT record toe op _dmarc.jouwdomein.nl, bijv. v=DMARC1; p=quarantine; rua=mailto:dmarc@jouwdomein.nl
DMARC beleid (p=)	✗ FAIL	N.v.t.	Voeg eerst een DMARC record toe
Rapportage URI (rua)	✗ FAIL	N.v.t.	Voeg eerst een DMARC record toe
Subdomain beleid (sp=)	✗ FAIL	N.v.t.	Voeg eerst een DMARC record toe

MX & Routing — 86%

Wat is dit? MX & Routing controleert of uw e-mailservers correct zijn geconfigureerd zodat berichten betrouwbaar worden afgeleverd.

Wat betekent deze score? Uw mx & routing is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
MX records aanwezig	✓ PASS	Ja — mx01.mail.icloud.com, mx02.mail.icloud.com	
MX redundantie	✓ PASS	2 MX records — redundant	
MX prioriteit configuratie	■ WARN	Alle MX records hebben dezelfde prioriteit	Stel verschillende prioriteitswaarden in voor failover (bijv. 10 en 20)
E-mail provider detectie	✓ PASS	Apple iCloud	

Server Security — 33%

Wat is dit? Server Security beoordeelt de beveiliging van uw mailserver: versleuteling, certificaten en bescherming tegen afluisteren.

Wat betekent deze score? Uw server security scoort onvoldoende. Er zijn serieuze tekortkomingen die zo snel mogelijk opgepakt moeten worden.

Check	Status	Waarde	Advies
Blacklist check	✗ FAIL	IP 17.57.156.30 staat op: zen.spamhaus.org	Neem contact op met je hostingprovider om je IP van de blacklist(s) te laten verwijderen: zen.spamhaus.org
Reverse DNS (PTR)	✓ PASS	Ja — mx02.mail.icloud.com	
STARTTLS support	? INFO	Verbinding naar mx01.mail.icloud.com:25 timeout	Poort 25 is mogelijk geblokkeerd; controleer de firewall-instellingen

Reputatie — 33%

Wat is dit? Reputatie beoordeelt hoe e-mailproviders (Gmail, Outlook) uw domein beoordelen. Een slechte reputatie betekent dat uw e-mails vaker in spam terechtkomen.

Wat betekent deze score? Uw reputatie scoort onvoldoende. Er zijn serieuze tekortkomingen die zo snel mogelijk opgepakt moeten worden.

Check	Status	Waarde	Advies
SMTP banner check	? INFO	Timeout bij verbinding met mx01.mail.icloud.com:25	Poort 25 is mogelijk geblokkeerd
MX certificaat	? INFO	Timeout bij verbinding met mx01.mail.icloud.com:25	Poort 25 is mogelijk geblokkeerd
Algehele authenticatie	■ WARN	Slechts 1 van 3 authenticatiemethoden geconfigureerd	Configureer SPF, DKIM en DMARC voor optimale deliverability
Consistente forward/reverse DNS	✓ PASS	Consistent — mx01.mail.icloud.com → 17.57.156.30 → mx01.mail.icloud.com	

Aanbevelingen

Geprioriteerde aanbevelingen op basis van de analyse.

Prio	Categorie	Titel	Beschrijving	Doorlooptijd
Hoog	SPF	**Corrigeer de SPF syntax**	Je SPF record bevat syntaxfouten die ervoor kunnen zorgen dat het genegeerd wordt. Gebruik een SPF validator om de fouten op te sporen.	30 minuten
Hoog	DKIM	**Configureer DKIM signing**	DKIM voegt een cryptografische handtekening toe aan je e-mails, waardoor ontvangers kunnen verifiëren dat berichten niet zijn aangepast. Stel DKIM in bij je e-mailprovider.	1 uur
Hoog	DMARC	**Voeg een DMARC record toe**	DMARC bouwt voort op SPF en DKIM en bepaalt wat er moet gebeuren met ongeautoriseerde e-mails. Begin met p=none en rua voor monitoring.	30 minuten
Hoog	Server Security	**Laat je IP van de blacklist verwijderen**	Je mailserver IP staat op een of meer blacklists. Dit heeft een negatieve impact op deliverability. Neem contact op met je hostingprovider.	1-4 uur
Hoog	Reputation	**Completeer je e-mailauthenticatie**	Voor optimale deliverability en bescherming tegen spoofing moeten SPF, DKIM en DMARC alle drie geconfigureerd zijn.	2-4 uur
Middel	SPF	**Verscherp het SPF beleid**	Gebruik -all (hard fail) in plaats van ~all voor strengere bescherming. Dit voorkomt dat ongeautoriseerde servers e-mail kunnen verzenden namens je domein.	15 minuten

Middel	DKIM	**Upgrade DKIM key naar 2048 bits**	Een langere DKIM key biedt betere bescherming tegen spoofing. Genereer een nieuw 2048-bit key-pair en publiceer het in DNS.	1 uur
Middel	DMARC	**Verscherp het DMARC beleid**	Upgrade je DMARC beleid naar p=quarantine of p=reject voor actieve bescherming tegen spoofing. Analyseer eerst de DMARC rapporten.	30 minuten
Middel	DMARC	**Voeg DMARC rapportage (rua) toe**	Met de rua tag ontvang je dagelijks rapporten over wie e-mail verzendt namens je domein. Dit is essentieel om problemen te detecteren voordat je het beleid verscherpt.	15 minuten
Laag	DKIM	**Voeg extra DKIM selectors toe**	Meerdere DKIM selectors maken key-rotatie eenvoudiger en bieden redundantie. Dit is vooral belangrijk als je meerdere e-mailsystemen gebruikt.	1-2 uur
Laag	DMARC	**Stel een subdomain DMARC beleid in**	Zonder een expliciet sp= beleid erven subdomeinen het hoofdbeleid. Stel sp=reject in om spoofing via subdomeinen te voorkomen.	15 minuten
Laag	MX & Routing	**Configureer MX prioriteiten**	Stel verschillende prioriteitswaarden in zodat e-mail correct wordt gerouteerd en er automatische failover is bij problemen.	15 minuten

Bijlage: Invoergegevens

Domein	jan-karel.nl

Bijlage A: Begrippen en Afkortingen

Onderstaande lijst verklaart de belangrijkste termen en afkortingen die in dit rapport worden gebruikt.

Term	Betekenis
AVG	Algemene Verordening Gegevensbescherming — Europese privacywetgeving (ook wel GDPR).
BCP	Business Continuity Plan — plan om bedrijfsprocessen voort te zetten bij verstoringen.
BIA	Business Impact Analysis — analyse van de gevolgen van uitval van systemen of processen.
CISO	Chief Information Security Officer — eindverantwoordelijke voor informatiebeveiliging.
CVE	Common Vulnerabilities and Exposures — gestandaardiseerd identificatiesysteem voor kwetsbaarheden.
DKIM	DomainKeys Identified Mail — digitale handtekening die bewijst dat een e-mail echt van uw domein afkomt en onderweg niet is gewijzigd.
DMARC	Domain-based Message Authentication — beleid dat e-mailproviders vertelt wat ze moeten doen met e-mails die niet voldoen aan SPF/DKIM.
DRP	Disaster Recovery Plan — plan voor herstel van IT-systemen na een calamiteit.
EDR	Endpoint Detection & Response — beveiligingssoftware die verdachte activiteit op werkstations en servers detecteert en blokkeert.
IAM	Identity & Access Management — beheer van digitale identiteiten en toegangsrechten.
IR-plan	Incident Response Plan — vastgelegde procedures voor het afhandelen van beveiligingsincidenten.
MFA	Multi-Factor Authenticatie — inloggen met twee of meer verificatiestappen (bijv. wachtwoord + app-code).
MX-record	DNS-instelling die aangeeft welke server de e-mail voor uw domein afhandelt.
NIS2	Network and Information Security Directive 2 — Europese richtlijn die cybersecurity-eisen stelt aan essentiële en belangrijke entiteiten.
NIST CSF	National Institute of Standards and Technology Cyber Security Framework — internationaal raamwerk voor cybersecurity.
PAM	Privileged Access Management — beheer en beveiliging van accounts met verhoogde rechten.
RPO	Recovery Point Objective — maximaal acceptabel dataverlies, uitgedrukt in tijd.
RTO	Recovery Time Objective — maximaal acceptabele tijd om een systeem te herstellen na uitval.
SIEM	Security Information & Event Management — systeem dat beveiligingslogs verzamelt, correleert en alarmeert.
SOC	Security Operations Center — team dat 24/7 beveiligingsincidenten monitort en afhandelt.
SPF	Sender Policy Framework — lijst van servers die namens uw domein e-mail mogen versturen. Voorkomt dat anderen zich voordoen als u.
XDR	Extended Detection & Response — geïntegreerde detectie over endpoints, netwerk en cloud.

Dit rapport is opgesteld door **BasisHost**.

Rapport gegenereerd op 3 april 2026. De resultaten zijn gebaseerd op door de klant verstrekte informatie. Dit rapport vervangt geen professionele security audit of pentest. BasisHost is niet aansprakelijk voor beslissingen genomen op basis van dit rapport zonder aanvullend professioneel advies.