Campaign readiness report

Dit rapport combineert email-authenticatie en website-gedrag rond verzending. We gebruiken “bewijs” (metingen/headers) waar beschikbaar en geven concrete next steps.

Campaign Readiness Report

Scan ID: 7ddb62c6-7c43-40ba-83b9-184afa6e11a1 · Generated: 2026-01-20T18:14:56.255Z

Headline

High risk: fix authentication and stability before sending.

Verdict: **high** · Confidence: **low** · Ready: **No**

BLOCKERS

Blockers are issues that materially reduce deliverability or campaign performance. Fix these first.

- **DKIM record not detected via DNS.**
- **SPF record is missing.**
- **DMARC is missing.**

Hard blockers: 3

WARNINGS

Warnings are not always blockers, but they often explain score drops or inconsistent performance.

- None

Website performance & cache behavior

Mailproviders en security gateways prefetch-en vaak links (zeker bij B2B). Daarom kijken we niet alleen naar “gemiddeld”, maar naar **voorspelbaarheid** en **cache-gedrag** tijdens de send-window. Standaard richtlijn:

- **TTFB**: < 800–1200 ms is meestal prima; boven 1200 ms wordt het vaak “traag”.
- **Cache**: idealiter zie je bij herhaalrequests vaker **HIT** i.p.v. DYNAMIC/MISS/BYPASS.
- **Stability**: geen timeouts/5xx en geen grote uitschieters.

No website evidence captured yet.

Email authentication (SPF, DKIM, DMARC)

Deze drie bepalen of mailbox providers je mail vertrouwen.

- **SPF**: welke servers mogen namens je domein verzenden.
- **DKIM**: cryptografische handtekening; bewijst integriteit & herkomst.
- **DMARC**: policy + reporting; dwingt alignment af en helpt spoofing voorkomen.

Standaard doel: **SPF pass**, **DKIM pass**, en DMARC naar **quarantine/reject** zodra alles aligned is.

Control	Current (client)	Target (recommended)
SPF	missing	pass · lookup ≤ 10 · end with -all (after validation)

Control	Current (client)	Target (recommended)
DKIM	missing	pass · aligned with From-domain · stable selector
DMARC	missing	quarantine/reject · aligned · rua reporting enabled

Inbound verification (real-world headers)

DNS-checks zijn “theorie”. Inbound headers zijn “praktijk”: je ziet wat mailbox providers **daadwerkelijk** observeerden (Authentication-Results, DKIM-Signature, Received-chain). Dit maakt je scan audit-proof en €30 waardig: je kunt fixes aantonen met bewijs.

No inbound verification captured yet (send a test mail to the unique verify+scanId address to populate this).