LEAD MAGNET · B2B & PRODUCT MARKETING

MCP-selectie & implementatie checklist

Kies de juiste Model Context Protocol-servers voor jouw marketingstack — en implementeer ze veilig, controleerbaar en met échte impact op je werk.

Hoe je deze checklist gebruikt

Werk de vijf blokken in volgorde af. Doe dit per use-case (bv. "win/loss synthese" of "maandelijkse product-usage rapport"), niet per tool. Zo voorkom je dat je een MCP-park bouwt dat niemand gebruikt.

1. Use-case scherp krijgen

- [ ] Ik heb één concrete use-case beschreven in 1–2 zinnen.
- [ ] Ik weet welke output (rapport, samenvatting, actie) eruit moet komen.
- [ ] Ik weet hoe vaak deze use-case terugkomt (dagelijks / wekelijks / ad hoc).
- [ ] Ik heb bepaald wie de gebruiker is: ikzelf, mijn team, of sales/CS.
- [ ] Ik heb geverifieerd dat deze use-case handmatig te veel tijd kost of te vaak wordt overgeslagen.

2. Data- en toolinventarisatie

- [ ] Ik heb per use-case in kaart welke databronnen nodig zijn (CRM, analytics, docs, ticketing).
- [ ] Ik weet per bron of er een officiële MCP-server bestaat of een betrouwbare community-versie.
- [ ] Ik heb gecheckt wie binnen mijn organisatie eigenaar is van elke bron.
- [ ] Ik heb bepaald of read-only voldoende is, of dat schrijfacties nodig zijn.
- [ ] Ik heb potentiële overlap tussen tools geëlimineerd (geen dubbele bron voor dezelfde vraag).

3. MCP-selectiecriteria

- [ ] De MCP-server wordt actief onderhouden (recente commits, changelog, community).
- [ ] Duidelijke documentatie over scopes, permissions en rate limits.
- [ ] Server draait lokaal of via een vertrouwde host (geen onbekende SaaS-tussenlaag).
- [ ] Authenticatie via OAuth of scoped API-key — geen gedeelde admin-credentials.
- [ ] Logging en observability zijn beschikbaar (welke tool-call is wanneer uitgevoerd).
- [ ] Kosten (compute + API-calls) zijn voorspelbaar en passen bij de use-case-waarde.

4. Veilige implementatie

- [ ] Ik gebruik least-privilege scopes: alleen lezen wat nodig is, alleen schrijven waar nodig.
- [ ] API-keys en tokens staan in een secret manager, niet in een .env-bestand op mijn laptop.
- [ ] Ik heb een aparte technische gebruiker (service account) aangemaakt per MCP-integratie.
- [ ] Gevoelige velden (PII, salarissen, contractwaarden) zijn uitgefilterd of gemaskeerd.
- [ ] Er is een audit-log zichtbaar voor mij én voor security/IT.
- [ ] Ik heb een kill-switch: één plek waar ik toegang binnen 5 minuten kan intrekken.
- [ ] Ik heb met IT/Security afgestemd voor productie-gebruik (niet alleen POC).

5. Adoptie & meten van impact

- [ ] Ik heb een baseline: hoeveel tijd/kwaliteit kostte deze use-case zonder MCP?
- [ ] Ik meet na 2 en 6 weken opnieuw en vergelijk met de baseline.
- [ ] Ik heb een korte SOP (max 1 pagina) waarin staat hoe een collega dezelfde workflow draait.
- [ ] Ik review maandelijks welke MCP-servers écht gebruikt worden en zet ongebruikte uit.
- [ ] Ik documenteer één learning per maand: wat werkt wel, wat niet, en waarom.

Rode vlaggen — stop en heroverweeg

• MCP-server vraagt om admin- of owner-scope terwijl de use-case read-only is.

• Geen mogelijkheid tot logging of audit — je weet niet wat de AI ophaalt of doet.

• Server wordt gehost door een onbekende partij zonder duidelijke voorwaarden.

• Je kunt niet in één klik toegang intrekken.

• De use-case is eigenlijk "ik wil met AI experimenteren", niet een concreet werkprobleem.

Meer frameworks, artikelen en workshops op productmarketeer.nl. Vragen of sparren over MCP-inzet in jouw B2B-stack? Mail twan@productmarketeer.nl.