Computer-use agents voor MKB

8 vragen die je IT-leverancier moet kunnen beantwoorden

Dit is geen technische audit. Het zijn acht vragen die je in een gewoon gesprek kunt stellen aan je IT-leverancier of automatiseringspartner. Aan de antwoorden merk je snel of die het onderwerp echt heeft doorgrond, of dat het verkooppraat is.

Computer-use agents zijn AI-systemen die zélf met software-interfaces werken — klikken, typen, navigeren. Sinds Anthropic in oktober 2024 *Computer Use* uitbracht en OpenAI in januari 2025 met *Operator* (nu in ChatGPT als agent mode) volgde, is dit een product-laag geworden. Microsoft Copilot Studio biedt het inmiddels aan, met keuze tussen OpenAI's en Anthropic's modellen. Google trok in mei 2026 de stekker uit Project Mariner en vouwde de techniek in Gemini Agent — een nuchter signaal dat de screenshot-route op schaal nog niet stabiel is.

Voor het MKB is dit het moment om vragen te gaan stellen, niet om alles meteen te bestellen.

1. Bij dít proces: is computer use plan A of plan B?

Wat je wilt horen: ze beginnen met de vraag of er een API of MCP-koppeling bestaat. Bestaat die, dan daar inzetten. Computer use is duurder, langzamer en breekbaarder dan een directe koppeling. Een leverancier die meteen "ja, dat doen we met computer use" zegt zonder de API-vraag te stellen, mist het hele punt.

2. Welk model draaien jullie en waarom?

Wat je wilt horen: ze kennen de keuze. Anthropic's Computer Use (Claude Sonnet 4.5 of nieuwer), OpenAI's CUA (via de Responses API), of via een laag erbovenop zoals Microsoft Copilot Studio. Ze kunnen uitleggen waarom ze voor jouw werkproces voor het ene of het andere kiezen — en hebben een onderbouwde mening over kosten per stap.

3. Hoe regelen jullie human-in-the-loop voor onomkeerbare acties?

Wat je wilt horen: een helder verhaal dat een agent nooit zelfstandig betalingen doet, contracten ondertekent, mails verstuurt naar externe partijen of bestanden verwijdert. Dat soort acties stoppen bij een goedkeuringsstap met een mens erin. Wie zegt "het model maakt zelden fouten", snapt het niet — bij een foutkans van ongeveer 25 % op een industriebenchmark is "zelden" niet goed genoeg.

4. Hoe houden jullie de kosten per run beheersbaar?

Wat je wilt horen: een vooraf afgesproken kostencap per run, monitoring op het aantal stappen, en een afspraak over wat er gebeurt als een agent vastloopt in een lus. Microsoft Copilot Studio rekent bijvoorbeeld 5 credits per stap. Bij tweehonderd stappen per run praat je al over serieus geld. Een leverancier zonder kostenbewaking laat dat ongemerkt oplopen.

5. Wat doen jullie als de UI bij de leverancier verandert?

Wat je wilt horen: een proces. Welk team merkt het op, hoe snel wordt de prompt of agent-configuratie bijgewerkt, en wat is de tussenliggende oplossing — terug naar handmatig, of een gedegradeerde flow. Computer use is robuuster tegen UI-wijzigingen dan klassieke RPA, maar niet immuun.

6. Hoe loggen jullie wat de agent feitelijk heeft gedaan?

Wat je wilt horen: iedere stap wordt vastgelegd — welk scherm, welke klik, welke invoer, welk resultaat. Met screenshots waar het kan. Voor compliance, voor verantwoording aan je accountant en voor je eigen rust. Een agent zonder audittrail mag niet in productie. Punt.

7. Welke credentials gebruikt de agent en hoe zijn die opgeslagen?

Wat je wilt horen: een aparte service-account voor de agent — niet jouw persoonlijke admin-login hergebruikt. Credentials in een keyvault of vergelijkbaar versleutelde opslag. Toegang strikt beperkt tot precies wat de agent nodig heeft, op precies de URL's en applicaties die ertoe doen. Geen "even mijn wachtwoord erin zetten". Draai om en loop weg als dat het voorstel is.

8. Wat is jullie pilot-aanpak?

Wat je wilt horen: één werkproces eerst, in *suggest-only*-modus (de agent stelt voor, jij accordeert), met een meetbaar succescriterium — percentage geslaagde runs, gemiddelde looptijd, kosten per run — en een vooraf afgesproken go/no-go-moment. Een leverancier die meteen tien processen tegelijk wil automatiseren, doet jouw bedrijf geen plezier.

Hoe verder

Beantwoordt je leverancier vijf of meer vragen overtuigend, dan kun je met vertrouwen aan een pilot beginnen. Komen ze er bij de helft niet uit, dan is dat geen reden om weg te lopen — wel een reden om eerst dat gesprek te voeren voor er iets gebouwd wordt.

Twijfel je over de antwoorden die je krijgt? Even sparren mag altijd. Een uur, geen verkopers-script, gewoon kijken of het bij jouw werkproces past — en zo nee, wat dan wél.

Spies Creations
WordPress · Laravel · integraties · AI-koppelingen voor MKB

Stephan Spies · stephan@spiescreations.nl · spiescreations.nl