De mens buitenspel

De mens buitenspel

25 manieren om je AI zelf te laten doorwerken, veilig en robuust

Floris Knol

Floris Knol

ISBN 978-94-0395-097-6

Eerste druk, 2026

Omslagontwerp: Floris Knol

© 2026 Floris Knol

Uitgegeven via Bookmundo

Niets uit deze uitgave mag worden verveelvoudigd of openbaar gemaakt zonder voorafgaande schriftelijke toestemming van de auteur.

Bij het maken van dit boek is gebruikgemaakt van AI-hulpmiddelen.

Inhoud

Voorwoord 7

1. Waarom de mens vaak de rem is 9

DEEL I. TOEGANG

2. Een eigen mailadres voor je agent 17

3. Inloggen, uitloggen en sessies bewaren 23

4. Eenmalige codes 29

5. Geheimen buiten de chat 37

6. Koppelen zonder plugin: de API zelf 43

7. Waar geen API is: de browser als koppeling 49

DEEL II. GRENZEN

8. Jouw veiligheidsregels als harde grenzen 55

9. Meten of je agent kan ontsnappen 61

10. Een poort voor wat de agent verstuurt 67

11. Een logboek dat alles vastlegt 73

12. Menscheck als instelling, niet als gewoonte 79

DEEL III. DOORLOPEN

13. Werk voorbereiden zodat de agent je niet stoort 85

14. Alle vragen in een keer, dan door 91
15. Doorlopen als je computer uit staat 97
16. Herstarten, een zetje, hervatten 103
17. Herstellen na een storing bij de aanbieder 109
18. Een wachtrij en een bord 115

DEEL IV. KOSTEN

19. Goedkoper als het doorstampt 121
20. Plafonds per dag en per agent 127
21. Minder tokens 133

DEEL V. OP AFSTAND EN KWALITEIT

22. Bijsturen vanaf je telefoon 139
23. Een overzicht van wat er draait 145
24. Meldingen die ertoe doen 151
25. Toetsen die je agent zelf draait 157
26. Van losse klus naar vaste rol 163

TOT SLOT

27. Een middag om te beginnen 169
Wantzel Studio en meer 177

Voorwoord

Ik laat AI-agents dagelijks echt werk doen. Wie dat doet, loopt steeds tegen hetzelfde aan: een account dat een code per sms wil, een website zonder koppeling, een agent die stilstaat omdat hij op een antwoord van jou wacht. Voor elk van die problemen is een aanpak die je in een middag neerzet. Dit boek zet ze naast elkaar, 25 in totaal.

Voor wie is dit boek?

Voor wie al met een AI-assistent als ChatGPT werkt en wil dat het werk doorgaat terwijl je er niet naast zit. Je hoeft niet te programmeren, en er staat geen code in dit boek. Elk hoofdstuk legt het idee uit en geeft je een prompt die je aan je AI-agent geeft, zoals Claude Code. De agent bouwt het; jij controleert of het werkt. Je moet wel durven een opdracht aan een AI-agent te geven en na te kijken wat er terugkomt; waar iets meer van je vraagt, staat dat in het hoofdstuk. Het is een boek voor knutselaars: voor wie het wil uitproberen, kapot wil maken en weer heel wil krijgen.

Het bedrijf in dit boek

Alle voorbeelden spelen bij Lindeboom Fietsen, een verzonnen fietsenbedrijf dat tweedehands fietsen opknapt en online verkoopt. De mensen, de agents en de gebeurtenissen zijn verzonnen. De problemen zijn dat niet: ze komen uit mijn eigen werk en uit wat anderen die met AI werken tegenkomen.

Gereedschap

Ik noem concrete gereedschappen, zoals Playwright, een programmeerassistent in de terminal, een authenticator-app en een server. Versies en menu's veranderen. Wat blijft, is het idee erachter; zoek de huidige instructie erbij als een knop anders heet.

Hoe het boek is opgebouwd

Het boek heeft vijf delen: toegang, grenzen, doorlopen, kosten, en op afstand en kwaliteit. Je kunt bij elk deel beginnen, maar de inleiding legt uit hoe elk hoofdstuk werkt en wat veilig en robuust betekent. Lees die eerst.

Floris Knol

1. Waarom de mens vaak de rem is

Marijke Lindeboom heeft Lindeboom Fietsen, een fietsenbedrijf met een werkplaats waar tweedehands bakfietsen worden opgeknapt en een webwinkel waar ze worden verkocht. Sinds een paar maanden werkt ze met vier AI-agents: Wiel kijkt in de portalen van de leveranciers, Spaak leest de klantenmail, Ketting doet de administratie en Bel werkt 's nachts de winkel bij. Op de eerste dag ging het goed. Op de tweede dag begon het te wringen.

Wiel stond stil omdat hij bij een leverancier niet meer was ingelogd. Spaak had een antwoord klaarstaan en wachtte op toestemming. Ketting vroeg om een code die naar Marijkes telefoon was gestuurd. Bel had 's nachts een vraag over een foto en wachtte tot ze wakker werd. Marijke zat de hele dag naast haar agents, en dat was precies wat ze niet wilde.

Dit boek gaat over die dag, en over alles wat ze eraan deed.

De mens in de loop

Je hoort vaak dat er een mens in de loop moet zitten. Dat klopt voor een belangrijk deel. Een agent die zonder toezicht betalingen

doet, mails verstuurt en bestanden verwijdert, gaat vroeg of laat iets doen wat je niet wilde.

Maar kijk naar wat de mens in de loop in de praktijk doet. Hij is degene die op "toestaan" klikt. Hij typt de code in. Hij logt opnieuw in. Hij beantwoordt de vraag die de agent om drie uur 's nachts stelde, de volgende ochtend om acht uur. Hij is de schakel in de keten die het langzaamst is, die slaapt, die op reis is, die in een vergadering zit. Elke keer dat de agent op hem wacht, staat het werk stil.

Het gevolg zie je bij bijna iedereen die met AI knutselt. Je begint enthousiast, je agent doet in een uur wat jou een middag kostte, en na een week zit je zelf de hele dag klaar om hem verder te helpen. Je hebt een assistent gekregen die je niet kunt loslaten. Het werk gaat sneller dan voorheen, en het houdt je net zo bezig.

Dit boek gaat over de stap daarna: de mens uit de loop halen. Jij blijft de baas, jij blijft de grenzen bepalen en jij kijkt achteraf naar wat er gebeurde. Maar je zit er niet meer tussen. De agent loopt door, ook als jij slaapt, in de trein zit of met een klant praat.

Wat veilig en robuust betekent

De titel heeft twee woorden die ertoe doen. Elk wordt in dit boek op een eigen manier uitgewerkt.

Veilig betekent dat de agent alleen doet wat jij hebt toegestaan, ook als niemand meekijkt. Dat bereik je door de grenzen buiten de agent te leggen: in rechten, in mappen, in een poort voor alles

wat naar buiten gaat. Een regel in een prompt is een verzoek. Een regel in de omgeving is een grens. Veilig betekent ook dat je kunt nakijken wat er gebeurde: een logboek dat de agent niet kan wijzigen, en een zelftest die laat zien dat de grenzen houden.

Robuust betekent dat het blijft werken als er iets tegenzit. Een sessie die verloopt, een code die gevraagd wordt, een aanbieder met een storing, een limiet die vol is, een agent die vastloopt zonder het te melden. Een robuuste opzet merkt dat zelf op, probeert een volgende route en laat het je alleen weten als het ertoe doet.

Die twee horen bij elkaar. Een agent die zonder jou doorloopt en geen grenzen heeft, is een risico. Een agent met grenzen die bij de eerste storing stilvalt, is een agent die toch weer om jouw aandacht vraagt. Het boek behandelt beide.

Het bedrijf waarmee je meeleest

De voorbeelden spelen bij Lindeboom Fietsen, het bedrijf van Marijke. Het is verzonnen, en dat blijft het hele boek zo: de mensen en de gebeurtenissen bestaan niet. De problemen waar ze tegenaan lopen wel. Een leverancier met een inlogportaal zonder koppeling, een boekhoudsysteem dat een code per sms vraagt, klantenmail die binnenkomt terwijl iedereen werkt: dat herken je uit je eigen bedrijf, ook als jouw bedrijf iets heel anders doet.

Naast Marijke werken er Bram in de werkplaats, Yara op kantoor en Teun de boekhouder, die twee keer per maand langskomt. Van

de agents kom je Wiel, Spaak, Ketting en Bel tegen. Elk heeft een eigen taak; je ziet er steeds maar een of twee tegelijk.

Hoe elk hoofdstuk werkt

Het boek heeft 25 manieren om de mens uit de loop te halen, verdeeld over vijf delen. Elke manier is een hoofdstuk met dezelfde zes onderdelen, zodat je weet waar je bent:

1. **Het probleem.** Waar je als gebruiker tegenaan loopt, in een situatie die je herkent.
2. W**aarom het je tegenhoudt.** Wat er onder het probleem zit, zodat je het ook in een andere vorm herkent.
3. **De aanpak.** Hoe het werkt, in gewone woorden, en het idee erachter.
4. **Het doe-blok.** Een prompt die je aan je AI-agent geeft, zodat hij het voor je bouwt, met de grenzen waaraan hij zich moet houden en hoe je het resultaat controleert. Elke prompt is aan een AI-agent gegeven in een wegwerpmap voordat hij in het boek kwam.
5. **De valkuilen.** Waar het misgaat en hoe je dat merkt.
6. **De checklist.** Een korte lijst om na te lopen of het staat.

Elk hoofdstuk eindigt met iets dat je dezelfde dag doet. Je kunt de hoofdstukken in volgorde lezen, en de volgorde is bedoeld: wat vooraan staat, maakt wat daarna komt makkelijker. Je kunt ook

beginnen bij het deel waar je het meeste last van hebt. Waar een hoofdstuk iets uit een eerder hoofdstuk gebruikt, staat dat erbij.

Nog één afspraak. Versies en menu's veranderen, dus zoek de huidige instructie erbij als een gereedschap anders heet. Prijzen van aanbieders staan er niet in, want die veranderen sneller dan een boek. En waar iets bij de aanbieder van jouw model anders werkt, kijk je in zijn documentatie; het idee erachter blijft.

Hoe je het veilig doet

Een agent die zelfstandig werkt, maakt ook zelfstandig fouten. Daarom houdt het boek een paar regels vast die in elk hoofdstuk terugkomen:

- Begin met alleen lezen. Geef een agent pas schrijfrechten als je hem hebt zien lezen.
- Geef elke agent het minimum aan rechten dat zijn taak vraagt.
- Houd geheimen buiten de chat en buiten de logs.
- Laat alles wat niet terug te draaien is door een poort lopen.
- Speel elke opzet eerst na op een wegwerpomgeving, en kijk dan pas naar je echte werk.

Dat laatste geldt ook voor de doe-blokken in dit boek. Waar een blok je eigen accounts raakt, staat dat bij het blok, met de proefversie die je veilig kunt doen.

Doe het vandaag: de wachtlijst

Voor het eerste hoofdstuk heb je geen gereedschap nodig, alleen een vel papier of een leeg bestand en een dag.

Zet er twee kolommen op. In de linker schrijf je elke keer dat je agent op jou wacht: een toestemming, een code, een inlogscherm, een vraag, een agent die stilstaat. In de rechter schrijf je wat hij nodig had om zelf door te gaan. Doe dat een werkdag lang, bij elke agent die je gebruikt.

Aan het eind van de dag zie je twee dingen. Je ziet hoe vaak je de rem bent, en dat getal is van jou: geen enkel boek kan het voor je tellen. En je ziet welke wachtmomenten steeds terugkomen. Dat zijn je eerste kandidaten. Hoort een wachtmoment bij toegang, ga dan naar het eerste deel. Wacht je vooral op toestemming, begin dan bij het deel over grenzen. Staat je agent stil zodra je laptop dichtgaat, kijk dan bij doorlopen.

Bewaar de lijst. Je gebruikt hem aan het eind van elk deel om te zien wat er is verdwenen.

Om te onthouden

- De mens in de loop is vaak de langzaamste schakel: hij slaapt, reist en zit in vergaderingen.
- Je blijft de baas en je zit er niet meer tussen: jij bepaalt de grenzen en kijkt achteraf.

- Veilig is dat de agent binnen jouw grenzen blijft, ook als niemand meekijkt.
- Robuust is dat hij doorgaat als iets tegenzit, en je alleen waarschuwt als het ertoe doet.
- Elk hoofdstuk heeft dezelfde zes onderdelen en eindigt met iets dat je dezelfde dag doet.
- Begin met de wachtlijst: schrijf een dag lang op waar je agent op jou wacht.

2. Een eigen mailadres voor je agent

Het probleem

Marijke laat Spaak de klantenmail van de webwinkel lezen. Om dat goed te doen heeft Spaak een account nodig bij het ticketsysteem van de winkel, een account bij de vervoerder en een account bij het platform waar de fietsen worden geadverteerd. Marijke maakte ze alle drie aan met haar eigen mailadres, want dat had ze bij de hand.

Een week later gebeurt wat je kunt verwachten. De vervoerder stuurt een bevestigingsmail, het platform vraagt om een nieuw wachtwoord en het ticketsysteem meldt een verdachte aanmelding. Alles komt in Marijkes inbox, tussen de offertes en de berichten van Bram. Spaak kan er niet bij, dus Spaak staat stil. Marijke zoekt de mail, klikt op de link en plakt hem in het gesprek. Daarna loopt Spaak weer, tot de volgende mail.

Waarom het je tegenhoudt

Een account is van degene wiens mailadres erbij staat. Elke bevestiging, wachtwoordreset, waarschuwing en eenmalige code gaat

naar dat adres. Zet je een account van je agent op jouw adres, dan ben jij de postbode van je agent. Je zit er per definitie tussen.

Er speelt nog iets. Je eigen inbox bevat alles: je bank, je privéberichten, de mail van je boekhouder. Laat je de agent je inbox lezen zodat hij zelf bevestigingen kan afhandelen, dan geef je hem toegang tot dat alles. Een eigen adres voor de agent houdt de toegang klein: hij ziet zijn eigen post en verder niets.

De aanpak

Je geeft elke agent een eigen mailadres en zet elk nieuw account daarop. Dat doe je in vier stappen.

Kies waar het adres woont. Heb je een eigen domein, dan maak je bij je mailaanbieder een extra postvak, bijvoorbeeld `spaak@` met de naam van het bedrijf erachter. Heb je geen eigen domein, dan werkt een gratis postvak bij een bekende aanbieder ook, zolang je er per agent een apart adres van maakt. Eén postvak per agent houdt de post van Wiel gescheiden van die van Spaak, en dan zie je meteen welke agent welke accounts heeft.

Maak toegang die alleen leest en ophaalt. De meeste aanbieders laten je een app-wachtwoord maken, een eigen wachtwoord voor programma's. Dat gebruik je voor de agent, nooit je hoofdwachtwoord. Is het ooit nodig om de toegang in te trekken, dan trek je dat ene app-wachtwoord in en blijft de rest van het postvak werken. Zoek bij je aanbieder naar "app-wachtwoord" en lees de hui-