

De verborgen **AI-risico's** waar niemand jouw voor waarschuwt



Inhouds- opgave

03

Inleiding

04

Risico 1: Geen
richtlijnen, geen regels

05

Risico 2: Je verliest de
controle over jouw data

06

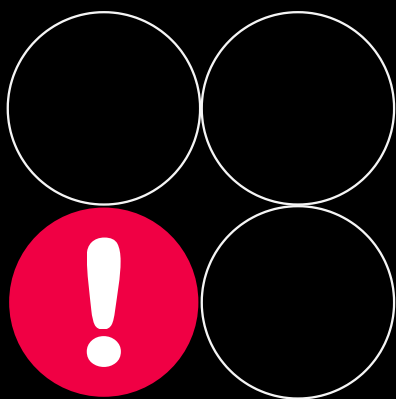
Risico 3: AI geeft niet
altijd correcte informatie

07

Risico 4: AI wordt ook
tegen jouw gebruikt

08

Conclusie



Inleiding

De meeste bedrijfsleiders zitten vandaag in dezelfde situatie. AI-tools worden steeds vaker gebruikt op de werkvloer, maar weinig organisaties staan stil bij de mogelijke gevolgen.

Vaak ontbreken duidelijke afspraken, richtlijnen en controle. Daardoor is er weinig zicht op hoe AI wordt gebruikt en welke informatie ermee wordt verwerkt. Meestal lijkt alles goed te werken. Tot er iets misgaat.

Wanneer krachtige technologie zonder duidelijke structuur wordt ingezet, ontstaan er risico's. De vier risico's in dit e-book zijn vandaag al aanwezig in veel organisaties, alleen zijn ze vaak nog niet zichtbaar.

In dit e-book ontdek je welke risico's AI met zich meebrengt, hoe ze zich tonen in de dagelijkse praktijk en welke stappen je kunt zetten om ze onder controle te houden zonder jouw team af te remmen.





Risico 1:

Geen richtlijnen, geen regels

AI-tools zijn niet via een aankoopproces of IT-goedkeuring binnengekomen. Ze zijn vaak gratis, eenvoudig toegankelijk en binnen enkele minuten in gebruik. Daardoor kunnen medewerkers ermee aan de slag zonder dat iemand binnen de organisatie hiervan op de hoogte is.

Het grootste risico zit niet in de technologie zelf, maar in het ontbreken van duidelijke afspraken. Misschien gebruikt iemand AI om offertes op te stellen, terwijl een collega vertrouwelijke notities laat samenvatten of klantgegevens invoert voor een rapport. Iedereen werkt op zijn eigen manier, omdat er geen richtlijnen zijn.

Zonder beleid maakt elke medewerker zelf de afweging wat wel en niet kan. Die keuzes sluiten niet altijd aan bij elkaar, jouw bedrijfswaarden of wettelijke verplichtingen. En omdat er vaak geen overzicht is, worden problemen meestal pas opgemerkt wanneer er al iets fout is gegaan.

Hoe krijg je weer controle?

- ▼ Breng eerst in kaart welke AI-tools jouw medewerkers gebruiken en waarvoor. Zo krijg je snel zicht op de grootste risico's.
- ▼ Leg daarna een duidelijk AI-beleid vast: welke tools zijn toegestaan, welke informatie niet gedeeld mag worden en wie AI-gegenereerde inhoud controleert.
- ▼ Zorg ten slotte dat iedereen het beleid kent en toepast.





Risico 2: Je verliest de controle over jouw data

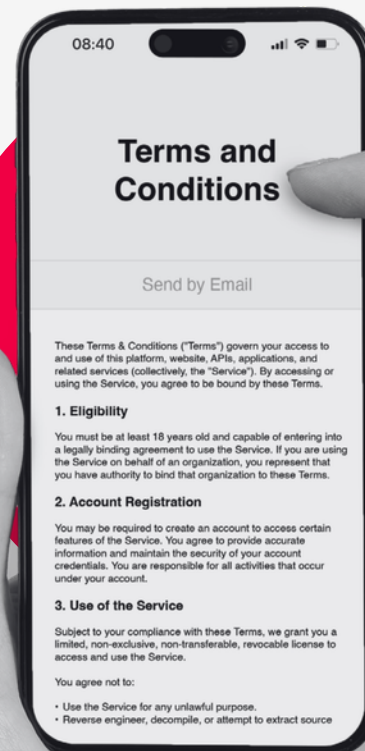
Wanneer medewerkers AI gebruiken, werken ze vaak niet in een afgeschermded bedrijfsomgeving. Ze delen informatie met externe platformen, elk met hun eigen voorwaarden en regels rond gegevensopslag. In veel gevallen is niet duidelijk wat er met die informatie gebeurt nadat ze is ingevoerd.

Het risico ontstaat op twee niveaus. Enerzijds kunnen medewerkers onbewust gevoelige informatie delen, zoals klantgegevens, financiële cijfers of interne plannen. Anderzijds heb je vaak weinig controle over hoe AI-platformen die gegevens bewaren of verwerken.

Juist doordat dit gebeurt tijdens dagelijkse werkzaamheden, blijft het risico vaak onopgemerkt.

Hoe krijg je weer controle?

- ▼ Controleer welke AI-tools binnen jouw organisatie worden gebruikt en bekijk hoe zij omgaan met gegevensopslag en modeltraining.
- ▼ Leg vervolgens vast welke informatie nooit in AI-tools mag worden ingevoerd, zoals klantgegevens, financiële informatie en interne communicatie.
- ▼ Neem deze afspraken op in hetzelfde AI-beleid als bij risico 1. Wat niet schriftelijk is vastgelegd, wordt zelden consequent gevolgd.



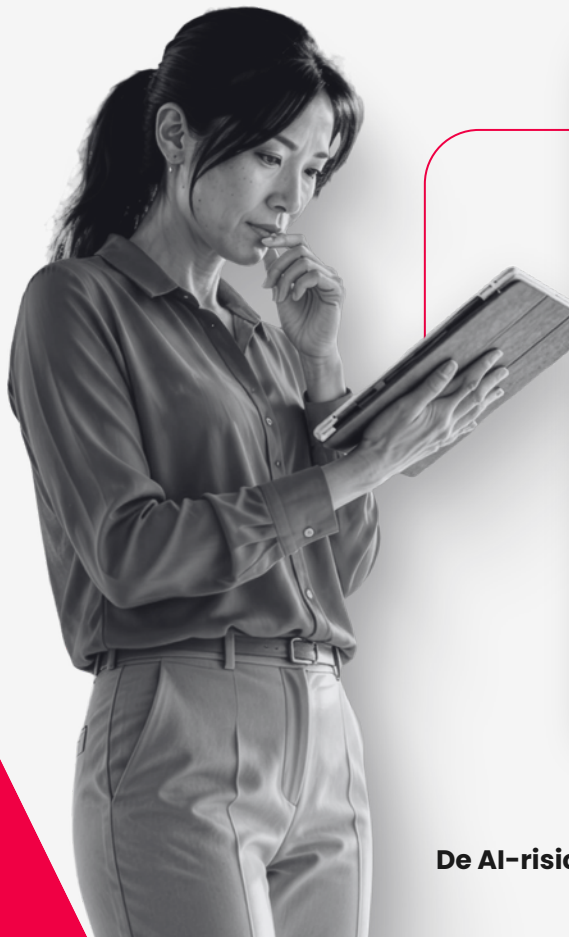


Risico 3:

AI geeft niet altijd correcte informatie

AI-tools zijn ontworpen om overtuigende antwoorden te geven. Het probleem? Die antwoorden zijn niet altijd juist. Ze kunnen foutieve cijfers gebruiken, niet-bestaande bronnen vermelden of informatie verkeerd interpreteren, zonder dat duidelijk te maken.

Voor organisaties kan dat vervelende gevolgen hebben. Onjuiste informatie in offertes, rapporten of klantcommunicatie kan jouw geloofwaardigheid schaden en in sommige gevallen zelfs juridische of financiële risico's veroorzaken.



Hoe krijg je weer controle?

- Voer een duidelijke controleprocedure in voor AI-gegenereerde inhoud. Controleer altijd feiten, cijfers en belangrijke uitspraken aan de hand van betrouwbare bronnen.
- Maak daarnaast duidelijk dat AI een hulpmiddel is, geen eindverantwoordelijke. De medewerker die de inhoud gebruikt, blijft verantwoordelijk voor de juistheid ervan. Dat hoort ook thuis in jouw AI-beleid.



Risico 4: AI wordt tegen jouw gebruikt

Waar de vorige risico's binnen jouw organisatie ontstaan, komt deze bedreiging van buitenaf. En ze wordt steeds moeilijker te herkennen.

Cybercriminelen gebruiken AI om phishingmails, valse facturen en andere vormen van fraude overtuigender te maken dan ooit. Fouten in spelling of vreemde formuleringen zijn vaak verdwenen. Zelfs stemmen kunnen vandaag geloofwaardig worden nagebootst.

Daardoor zijn de waarschuwingssignalen waarop medewerkers vroeger vertrouwden minder zichtbaar. Eén klik op een kwaadwillige link of één foutieve betaling kan al grote gevolgen hebben.

Hoe krijg je weer controle?

- ▼ Zorg ervoor dat jouw cybersecuritytraining aansluit bij de dreigingen van vandaag. Heeft jouw team het afgelopen jaar geen opleiding gevolgd? Dan is de kennis waarschijnlijk al verouderd.
- ▼ Voer daarnaast eenvoudige controleprocedures in voor risicovolle acties. Wijzigingen aan betaalgegevens, betalingen of het delen van gevoelige informatie moeten altijd via een tweede kanaal worden bevestigd.



Conclusie

De vier risico's in dit e-book zijn niet theoretisch. Ze komen vandaag al voor in organisaties die AI gebruiken zonder duidelijke afspraken, controle of inzicht in hoe de technologie wordt ingezet.

Hoe langer AI zonder structuur wordt gebruikt, hoe groter de risico's worden. Met een helder AI-beleid, duidelijke richtlijnen, een controleproces voor AI-gegenereerde inhoud en een moderne aanpak voor cyberdreigingen kun je jouw organisatie veel beter beschermen.

Veel bedrijfsleiders voelen aan dat er iets moet veranderen, maar weten niet goed waar te beginnen. Daar helpen wij bij.

We brengen in kaart hoe AI binnen jouw organisatie wordt gebruikt, waar risico's ontstaan en welke afspraken nodig zijn zodat jouw team AI veilig, verantwoord en consistent kan inzetten.

**Je kent nu de risico's.
Tijd om er iets aan
te doen.**

**Plan vandaag nog een
vrijblijvend
kennismakingsgesprek
van 10 minuten.**

