knowbe4

NEDERLAND

Van Agentic Risk naar Human Wins

Inleiding

Nederlandse organisaties bevinden zich inmiddels voorbij de fase van experimenteren met AI. Autonome AI-agents en geautomatiseerde workflows worden steeds vaker ingezet om bedrijfsprocessen uit te voeren en beslissingen te ondersteunen.

Tegelijkertijd blijkt uit onderzoek van KnowBe4 dat veel organisaties moeite hebben om grip te houden op het gebruik van deze technologie. Het rapport 'From Agentic Risk to Human Wins' laat zien waar de grootste risico's liggen, welke blinde vlekken organisaties hebben en hoe goed zij voorbereid zijn op een toekomst waarin mensen en AI-agents steeds nauwer samenwerken.

1. Organisaties verliezen grip op AI-gebruik

Hoewel AI steeds vaker onderdeel uitmaakt van de formele IT-omgeving, ontstaat tegelijkertijd een groeiende laag van ongecontroleerde 'Shadow AI'. Voor securityteams vormt dit een uitdaging: wat niet zichtbaar is, kan ook niet worden beschermd.

De belangrijkste bevindingen zijn:

- 84% van de ondervraagde Nederlandse organisaties maakt gebruik van AI-tools, terwijl 58% autonome AI-agents inzet die zelfstandig acties kunnen uitvoeren binnen bedrijfsprocessen.
- 50% van de organisaties heeft geen duidelijke governance rond het gebruik van AI, ondanks dat deze technologie inmiddels breed wordt ingezet binnen bedrijfsprocessen.
- 27% van de medewerkers zegt zelf AI-tools te gebruiken wanneer goedgekeurde alternatieven ontbreken of als te beperkend worden ervaren.
- 81% van de medewerkers weet dat informatie die wordt ingevoerd in AI-tools opgeslagen of gebruikt kan worden op manieren die gevoelige bedrijfsinformatie blootstellen.

Highlights

- **Ontdek de governancekloof:** Krijg inzicht in de omvang van Shadow AI en waarom AI-gebruik binnen organisaties vaak plaatsvindt zonder formele governance- of beleidskaders.
- **Beoordeel de opkomst van agentic AI:** Ontdek welk percentage van de organisaties autonome AI-agents inzet die zelfstandig acties kunnen ondernemen, en welke beveiligingsrisico's dit met zich meebrengt.
- **Breng het psychologische strijdtoneel in kaart:** Leer hoe het dreigingslandschap is verschoven naar hyperrealistische, door AI gegenereerde deepfakes en waarom de meeste medewerkers erkennen dat zij hierdoor succesvol misleid zouden kunnen worden.
- **Identificeer de werkelijke menselijke risico's:** Bekijk de gegevens waaruit blijkt hoe cognitieve overbelasting en operationele frictie medewerkers ertoe aanzetten om veiligheidsprocedures te omzeilen, wat leidt tot een aanzienlijk deel van de beveiligingsincidenten.
- **Evalueer uw paraatheid:** Begrijp wat de 'gouden standaard' voor securityvolwassenheid inhoudt en ontdek of securityleiders zich weerbaar genoeg achten om opkomende AI-gedreven dreigingen het hoofd te bieden.

2. De impact van ongecontroleerd AI-gebruik is al zichtbaar

Het gebrek aan toezicht op AI-gebruik is niet alleen een toekomstig risico. Veel organisaties ervaren vandaag al de gevolgen.

De belangrijkste bevindingen zijn:

- 50% van de cybersecuritybeslissers zegt dat ongeautoriseerde software en AI-applicaties de beveiligingspositie van hun organisatie in de afgelopen twaalf maanden negatief hebben beïnvloed.
- 48% noemt het veilig beheren van AI-tools en AI-agents de grootste uitdaging bij het beperken van mensgerelateerde cyberrisico's.

3. Weinig organisaties hanteren een volwassen aanpak

Ondanks de toenemende aandacht voor cybersecurity blijkt slechts een kleine groep organisaties in staat om risico's rondom mensen en AI-agents geïntegreerd te beheren.

De belangrijkste bevindingen zijn:

- Slechts 6% van de organisaties heeft het hoogste volwassenheidsniveau bereikt: een geïntegreerde aanpak die menselijke en AI-gerelateerde cyberrisico's gelijktijdig beheert.
- 50% van de cybersecuritybeslissers voelt zich zeer goed voorbereid op onverwachte of nieuwe AI-gerelateerde dreigingen in de komende twaalf maanden.

4. AI-gedreven aanvallen vormen een nieuwe uitdaging

Naast de risico's van ongecontroleerd AI-gebruik laat het onderzoek zien dat AI ook verbeterde aanvalsmethoden mogelijk maakt.

De belangrijkste bevindingen zijn:

- 90% van de medewerkers vindt dat deepfake-video's en -audiobestanden inmiddels zo realistisch zijn dat het lastig is om te bepalen welke informatie nog te vertrouwen is.
- 67% van de medewerkers denkt mogelijk slachtoffer te kunnen worden van een deepfake-oplichting op het werk.
- Toch noemt slechts 16% van de cybersecuritybeslissers AI-gestuurde aanvallen als de belangrijkste factor die het cyberrisico voor hun organisatie in de komende twaalf maanden zal vergroten.

Conclusie

De Nederlandse arbeidsmarkt verandert snel. Medewerkers en AI-agents vormen steeds vaker één geïntegreerde werkomgeving. Daardoor moeten organisaties ook anders naar cybersecurity kijken.

In deze nieuwe digitale werkplek worden verantwoordelijkheden, besluitvorming en handelingsruimte anders verdeeld, wat leidt tot fundamentele veranderingen in organisatorische processen en werkwijzen. Daardoor volstaat het niet langer om werk te begrijpen vanuit traditionele organisatorische structuren.

Organisaties zullen opnieuw moeten definiëren hoe werkzaamheden worden uitgevoerd, welke rollen verschillende actoren vervullen en welke gedeelde normen, waarden en verwachtingen daarbij horen.

knowbe4

KnowBe4, Inc. | Stadsplateau 25, 3521AZ, Central Park Building, Utrecht, Netherlands
+31 (0)30 7996074 | www.KnowBe4.com | Sales@KnowBe4.com