knowbe4

DEUTSCH

From Agentic Risk to Human Wins Report

Einleitung

Die Unternehmenslandschaft in Deutschland hat die Phase theoretischer KI-Experimente hinter sich gelassen; autonome Agenten und Workflows in Maschinen-Geschwindigkeit führen bereits aktiv Geschäftsabläufe aus.

Doch während Unternehmen eifrig versuchen, Effizienzgewinne zu erzielen, bröckelt die Sicherheitslage. Der Bericht „From Agentic Risk to Human Wins“ von KnowBe4 beleuchtet die kritischen blinden Flecken, psychologischen Schwachstellen und Vorbereitungslücken, mit denen Unternehmen in Deutschland zu kämpfen haben.

Abschnitt 1: Das Schatten KI & Governance-Defizit

Während Unternehmen in Deutschland KI in ihre offiziellen Tech-Stacks integrieren, entsteht in den deutschen Belegschaften eine beträchtliche, unkontrollierte Ebene von „Schatten-KI“. Angreifer sind sich sehr wohl bewusst, dass Sicherheitsteams keine Ressourcen schützen können, die sie nicht sehen.

- 62 Prozent der befragten deutschen Unternehmen setzen autonome KI-Agenten ein, die eigenständig Maßnahmen ergreifen können, doch 48 Prozent von Führungskräften geben zu, dass der Einsatz von KI in ihrem Zuständigkeitsbereich weder genehmigt ist noch einer formellen unternehmensweiten Steuerung unterliegt.
- In Deutschland geben 42 Prozent der Entscheidungsträger im Bereich Cybersicherheit an, dass die unerlaubte Nutzung externer Software und nicht genehmigter KI-Anwendungen ihre Sicherheitslage in den letzten 12 Monaten direkt verschlechtert oder aktiv gefährdet hat.
- Über ein Drittel (37 %) der Mitarbeiter gibt zu, dass sie, sollten die offiziellen KI-Tools des Unternehmens eingeschränkt oder zu langsam sein, aktiv nach eigenen, nicht genehmigten KI-Tools suchen werden, um administrative Sperren zu umgehen.

Highlights

- **Finden Sie die Governance-Lücke:** Erfahren Sie, wie weit verbreitet „Shadow-AI“ ist und warum der Einsatz von KI in Unternehmen oft ohne formelle Governance erfolgt.
- **Bewerten Sie den Wandel hin zu autonomen Agenten:** Erfahren Sie, wie viel Prozent der Unternehmen autonome KI-Agenten einsetzen, die eigenständig Maßnahmen ergreifen können, und welche Folgen damit für die Sicherheit verbunden sind.
- **Sehen Sie sich die psychologische Bedrohungslage an:** Erfahren Sie, wie sich der Bedrohungsvektor zu hyperrealistischen, KI-gestützten Deepfakes verlagert hat und warum die meisten Mitarbeiter zugeben, dass sie erfolgreich getäuscht werden könnten.
- **Identifizieren Sie die Bedrohung für den Menschen:** Sehen Sie sich die Daten an, wie kognitive Überlastung und operative Reibungsverluste Mitarbeiter dazu zwingen, Abstriche zu machen, was einen erheblichen Prozentsatz der Sicherheitsvorfälle verursacht.
- **Bewerten Sie Ihre Verteidigungsbereitschaft:** Verstehen Sie den „Goldstandard“ der Sicherheitsreife und finden Sie heraus, ob sich Sicherheitsverantwortliche resilient genug fühlen, um aufkommende KI-getriebene Bedrohungen zu überstehen.

Abschnitt 2: Deepfakes

Der Angriffsvektor hat sich grundlegend von traditionellem Phishing hin zu hyperrealistischer, KI-gestützter Manipulation verlagert. Die kognitiven Abwehrmechanismen des Menschen versagen angesichts maschinengenerierter Medien.

- Überwältigende 87 Prozent der Beschäftigten in Deutschland geben an, dass Deepfake-Stimmen und -Videos mittlerweile so realistisch sind, dass es schwieriger geworden ist zu wissen, wem man vertrauen kann.
- 55 Prozent der Belegschaften geben offen zu, offen zu, dass sie sich von einem ausgeklügelten Deepfake-Betrug täuschen lassen könnten, bei dem sich der Betrüger als interner Mitarbeiter oder Führungskraft am Arbeitsplatz ausgibt.
- Die Bedrohungslage hat sich von menschlicher Geschwindigkeit zu maschineller Geschwindigkeit gewandelt. Unternehmen in Deutschland sind strukturell nicht auf automatisierte, mehrstufige Angriffe vorbereitet, die Mitarbeiter gleichzeitig über E-Mail, SMS und Kollaborations-Apps ins Visier nehmen.

Abschnitt 3: Operative Reibungsverluste und die Lücke zum „Goldstandard“

Die größte Gefahr geht nicht einfach von hochentwickelten Angriffen aus, sondern vom Zusammenwirken von menschlicher Erschöpfung in stressreichen Unternehmensumgebungen und einem niedrigen Reifegrad der betrieblichen Sicherheit.

- 64 Prozent der Beschäftigten in Deutschland geben zu, dass starker Zeitdruck, kognitive Überlastung und alltägliche Ablenkungen am Arbeitsplatz sie direkt dazu veranlassen, Abstriche zu machen und kritische Sicherheitsfehler zu begehen, selbst wenn sie die Sicherheitsprotokolle genau kennen.
- Deutsche Führungskräfte im Bereich Cybersicherheit bestätigen das Ausmaß dieser Verhaltenslücke und weisen darauf hin, dass bis zu 52 Prozent aller Sicherheitsvorfälle, die in diesem Jahr ihre Perimeter betrafen, durch alltägliche operative Fehler und nicht durch Exploit-Kits ausgelöst wurden.
- Trotz des weit verbreiteten Bewusstseins haben lediglich 20 Prozent der Organisationen ein Reifegradmodell nach dem „Goldstandard“ erreicht – definiert als eine vollständig abgestimmte Kultur, die in der Lage ist, menschliche und agentische Risiken gemeinsam zu bewältigen.
- Zudem fühlen sich nur 94 Prozent der deutschen Sicherheitsverantwortlichen robust genug, um unerwartete oder neu auftretende KI-gesteuerte Bedrohungsvektoren im kommenden Kalenderjahr zu bewältigen.

Fazit

Die Arbeitswelt in deutschen Unternehmen hat sich gewandelt. Mitarbeiter und KI-Agenten bilden nun eine einzige, vernetzte Verteidigungslinie. Das verändert die Vorstellung davon, wie gute Sicherheit aussieht. Unternehmen, die das Sicherheitsbewusstsein, das Verhalten und die Unternehmenskultur auf ein klares Risikobild ausrichten, tun mehr, als nur das Risiko zu managen. Sie schaffen „abgehärtete Ziele“. Die Bedrohungen werden nicht verschwinden, aber sie werden auf besser vorbereitete Unternehmen treffen.

KnowBe4, Inc. | Rheinstrasse 45/46, 12161 Berlin
+49 30 34646 460 | www.knowbe4.com/de/ | Sales@KnowBe4.com