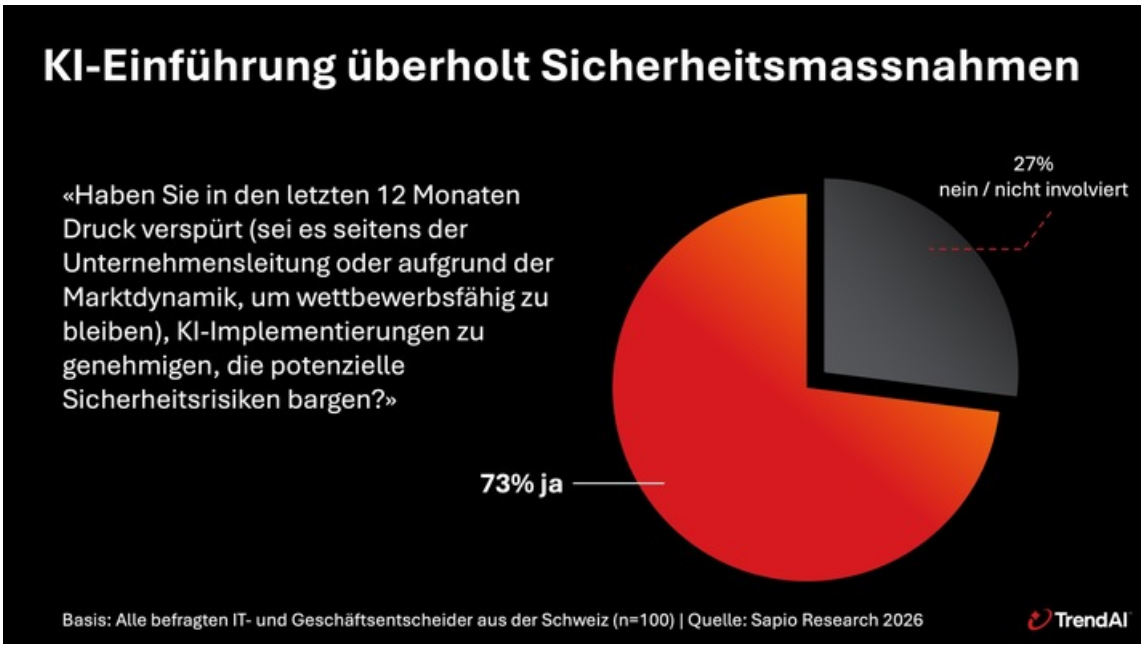
26.03.2026 – 09:01 Uhr

Umfrage: 73 Prozent der Schweizer Unternehmen genehmigen KI-Projekte trotz Sicherheitsbedenken



Umfrage: 73 Prozent der Schweizer Unternehmen genehmigen KI-Projekte trotz Sicherheitsbedenken

Vorbehalte werden zugunsten von Wettbewerbsdruck und internen Forderungen ignoriert

Wallisellen, 26. März 2026 – TrendAI™, ein Geschäftsbereich von Trend Micro und einer der weltweit führenden Anbieter von KI-Sicherheit, veröffentlicht neue Forschungsergebnisse, die zeigen, dass Unternehmen weltweit den Einsatz von künstlicher Intelligenz vorantreiben, obwohl bekannte Sicherheits- und Compliance-Risiken bestehen.

Eine neue globale Befragung von 3.700 Business- und IT-Entscheidern, davon 100 in der Schweiz, ergab, dass 73 Prozent der Schweizer Entscheider (67 Prozent weltweit) bereits unter Druck standen, KI-Projekte trotz Sicherheitsbedenken zu genehmigen. 7 Prozent von ihnen (14 Prozent global) bezeichneten diese Bedenken sogar als „extrem“, wurden aber dennoch übergangen, um mit Wettbewerbern und internen Anforderungen Schritt zu halten.

Der Druck zu einer schnellen KI-Einführung wird ausserdem durch uneinheitliche Governance-Strukturen und unklare Verantwortlichkeiten für KI-Risiken verstärkt. Cybersecurity-Verantwortliche können häufig nur noch auf Entscheidungen zur KI-Einführung reagieren, die von der Unternehmensführung getroffen werden. Das führt oftmals zu Behelfslösungen und einer verstärkten Nutzung nicht genehmigter, sogenannter „Schatten-KI“-Tools.

KI-Einführung überholt Sicherheitsmassnahmen

Unternehmen implementieren KI schneller, als sie die damit verbundenen Risiken verwalten können. Dadurch entsteht eine wachsende Lücke zwischen Ambitionen und Kontrolle. 60 Prozent der Schweizer Befragten (57 Prozent weltweit) geben an, dass sich KI schneller entwickelt, als sie sie absichern können. Gleichzeitig äussern 58 Prozent von ihnen (64 Prozent weltweit) nur geringes bis mittleres Vertrauen in ihre Kenntnisse der rechtlichen Rahmenbedingungen für den Einsatz von KI im Unternehmen.

Auch die Reife von Governance-Strukturen bleibt niedrig. Weniger als ein Drittel (30 Prozent) der Schweizer Unternehmen verfügt bereits über umfassende KI-Richtlinien; 66 Prozent befinden sich noch in der Ausarbeitung entsprechender Vorgaben oder haben gerade erst damit begonnen. Fast die Hälfte (49 Prozent) der Befragten in der Schweiz nennt zudem unklare regulatorische oder Compliance-Anforderungen als Hindernis für eine sichere KI-Nutzung. In der Praxis bedeutet dies, dass KI bereits im operativen Geschäft ausgerollt wird, bevor die Regeln für ihren Einsatz vollständig festgelegt sind.

«Unternehmen fehlt es nicht am Bewusstsein für Risiken, sondern an den Voraussetzungen, um diese wirksam zu

managen», sagt Richard Werner, Security Advisor bei TrendAI. «Wenn die Einführung von KI eher durch Wettbewerbsdruck als durch reife Governance-Strukturen getrieben wird, entsteht eine Situation, in der KI in kritische Systeme integriert wird, ohne dass die notwendigen Kontrollen vorhanden sind. Wir müssen Unternehmen deshalb dabei unterstützen, mit KI solide Ergebnisse zu erzielen und gleichzeitig ihre Geschäftsrisiken im Griff zu behalten.»

Vertrauen in autonome KI bleibt begrenzt

Das Vertrauen in fortschrittliche, autonome KI-Systeme befindet sich weiterhin in einer Reifungsphase. 45 Prozent der Schweizer Entscheider (44 Prozent weltweit) sind optimistisch, dass agentische KI die Cyberabwehr kurzfristig deutlich verbessern wird. Gleichzeit bestehen weiterhin Bedenken beim KI-Einsatz: Fast die Hälfte (48 Prozent) der Befragten hierzulande sehen den Zugriff von KI-Agenten auf sensible Daten als grösstes Risiko. 30 Prozent von ihnen warnen davor, dass manipulierte Prompts die Sicherheit gefährden könnten, während ein Drittel (33 Prozent) eine zusätzliche Angriffsfläche für Cyberkriminelle sieht. Ein ähnlich grosser Anteil (28 Prozent) befürchtet den Missbrauch des Vertrauensstatus von KI-Systemen sowie Risiken durch autonome Codebereitstellung (33 Prozent).

Gleichzeitig gibt ein Drittel der Schweizer Unternehmen an, dass ihnen die notwendige Transparenz oder Auditierbarkeit dieser Systeme fehlt. Das wirft grundlegende Fragen darüber auf, wie Unternehmen eingreifen oder Kontrolle ausüben können, sobald autonome Agenten im Einsatz sind. 33 Prozent der Befragten in der Schweiz unterstützen die Einführung von „Kill-Switch"-Mechanismen für KI, mit denen Systeme im Fall von Fehlfunktionen oder Missbrauch abgeschaltet werden können. Etwa die Hälfte (48 Prozent) ist sich hierzu noch unsicher. Hier zeigt sich ein grundlegendes Problem: Unternehmen bewegen sich in Richtung autonomer KI, ohne sich darüber einig zu sein, wie Kontrolle in kritischen Situationen gewährleistet werden soll.

«Agentic AI bringt Unternehmen eine neue Kategorie von Risiken», ergänzt Rachel Jin, Chief Platform and Business Officer und Head of TrendAI. «Unsere Studie zeigt, dass die zentralen Bedenken bereits klar sind – von der Offenlegung sensibler Daten bis hin zum Verlust von Kontrolle. Ohne Transparenz und Kontrollmechanismen setzen Unternehmen Systeme ein, die sie nicht vollständig verstehen oder steuern können. Dieses Risiko wird weiter zunehmen, wenn sie keine Gegenmassnahmen ergreifen.»

Über die Studie

TrendAI beauftragte SAPIO Research mit der Befragung von 3.700 IT- und Business-Entscheidern in 23 Ländern, die in Unternehmen mit mehr als 250 Mitarbeitenden tätig sind. An der Befragung im Februar 2026 nahmen 200 Geschäfts- und IT-Entscheider aus Deutschland sowie je 100 aus Österreich und der Schweiz teil.

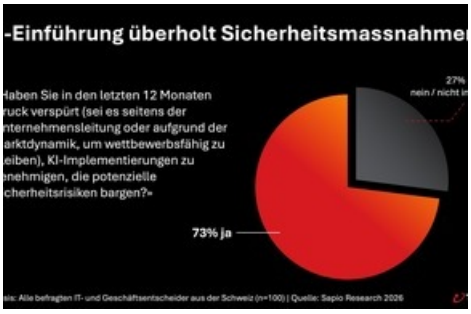
Weitere Studienergebnisse können Sie hier einsehen: https://www.trendmicro.com/explore/trendai-global-ai-study/

Pressestelle TrendAI™
c/o BRAND AFFAIRS AG

Mischa Keller / MSc Business Administration
Partner

Telefon: +41 44 254 80 00
E-Mail: trendmicro-media@brandaffairs.ch
Mühlebachstrasse 8 / 8008 Zürich / Switzerland

Medieninhalte



Diese Meldung kann unter https://www.presseportal.ch/de/pm/100103176/100939206 abgerufen werden.