Saviynt

2026
CISO AI Risk Report Germany | **Wichtigste Erkenntnisse**

In unserer Umfrage unter mehr als 100 Sicherheitsverantwortlichen traten immer wieder dieselben Bedenken auf. KI-Systeme verfügen bereits über erheblichen Zugriff und das oft mit Berechtigungsstufen, die niemand ausdrücklich vergeben hat. Sie erzeugen Aktivitäten, die schwer nachzuverfolgen sind, verhalten sich in Mustern, die nicht dem menschlichen Verhalten entsprechen und hinterlassen manchmal unvollständige oder nur temporäre Spuren. Für sich genommen ist das nicht katastrophal, erschwert jedoch die grundlegenden Fragen, auf die sich Sicherheitsteams verlassen, nämlich: „Wer hat das getan?“ und „Hätte diese Aktion erlaubt sein dürfen?“

93%

der CISOs geben an, dass KI-Identitäten bereits Zugriff auf kritische Geschäftssysteme haben, doch nur ein Viertel dieser Organisationen steuert diese Zugriffe mit starker Governance. Diese Agenten agieren mit weitreichenden Befugnissen und minimaler Aufsicht.

58%

haben keine vollständige Sichtbarkeit über alle KI-Identitäten, und 11% geben an, Missbrauch kompromittierter KI nicht erkennen und enthalten zu können. KI ist bereits in Umgebungen im Einsatz, die manche Sicherheitsteams nicht überwachen können.

65%

setzen keine umfassenden Zugriffsrichtlinien für KI-Identitäten durch. Im Schnitt verwalten nur 57,8 % ihre KI-Identitäten wie menschliche Benutzer, aber 89 % sind zuversichtlich, dass sie einen kompromittierten Agenten einfangen könnten.

56%

nutzen GenAI-spezifische Access-Monitoring-Tools. Die meisten Organisationen versuchen, das Risiko der Maschinengeschwindigkeit mit fragmentierten Werkzeugen zu bewältigen, die für manuelle Arbeitsabläufe und menschliche Benutzer und nicht für autonome Agenten konzipiert sind.

76%

haben unsanktionierte KI-Tools identifiziert, oft mit eingebetteten Zugangsdaten oder erweiterten Systemzugriffen, die niemand überwacht.

Weitere Information unter ***www.saviynt.com.***