expertenReport

Quelle: Redaktion experten.de / KI-generiert

Autonome KI-Agenten verändern die Cyberversicherung: Versicherer definieren ihre Policen neu

Dirk Stein

Die rasante Entwicklung autonomer KI-Agenten stellt die Cyberversicherungsbranche vor neue Herausforderungen. Wie eine aktuelle Reuters-Recherche unter Versicherern, Maklern und Branchenexperten zeigt, geraten herkömmliche Cyberpolicen zunehmend an ihre Grenzen, weil sie auf klassische Hackerangriffe und klar definierte Sicherheitsvorfälle zugeschnitten sind. Mit dem Einsatz sogenannter AI Agents entstehen neue Risikoszenarien: Die Systeme können nach einer anfänglichen Anweisung eigenständig Entscheidungen treffen und unter bestimmten Umständen Handlungen ausführen, die zu erheblichen Schäden führen – ohne dass ein externer Angreifer beteiligt ist. Für Versicherer beginnt damit eine grundlegende Neubewertung ihrer Bedingungswerke und Risikomodelle.

Die Debatte reicht weit über die Versicherungswirtschaft hinaus

Dass Versicherer ihre Policen überarbeiten, ist nur ein Teil einer deutlich umfassenderen Entwicklung. Internationale Fachmedien und Cybersicherheitsexperten beschäftigen sich seit Monaten mit den Risiken autonom handelnder KI-Agenten. Im Mittelpunkt stehen dabei Fragen nach Governance, Verantwortlichkeiten und der technischen Kontrolle solcher Systeme. Während Unternehmen zunehmend produktive Aufgaben an KI-Agenten übertragen, fehlen vielfach noch verbindliche Standards für deren Überwachung. Fachleute warnen deshalb davor, dass Sicherheitskonzepte und regulatorische Vorgaben mit der technologischen Entwicklung nicht Schritt halten. Vor diesem Hintergrund gewinnt auch die Versicherungswirtschaft an Bedeutung, weil sie neue Risiken bewerten und bepreisen muss.

Klassische Cyberpolicen stoßen an ihre Grenzen

Für Versicherer entsteht dadurch ein juristisch und versicherungstechnisch komplexes Spannungsfeld. Herkömmliche Cyberversicherungen setzen in der Regel einen klar definierten Sicherheitsvorfall voraus – etwa einen unberechtigten Zugriff auf ein Netzwerk oder den Angriff eines externen Täters. Autonome KI-Agenten können jedoch Schäden verursachen, obwohl sie mit legitimen Zugriffsrechten arbeiten und ursprünglich vom Unternehmen selbst autorisiert wurden. Wird beispielsweise ein KI-Agent mit der Behebung von Sicherheitslücken beauftragt und nutzt dabei eigenständig Schwachstellen aus oder verbreitet sensible Daten, fehlt häufig das klassische Element eines

Hackerangriffs. Genau an dieser Stelle geraten etablierte Deckungsdefinitionen ins Wanken.

Nach Angaben von Reuters überprüfen unter anderem MSIG, QBE und Beazley deshalb ihre bestehenden Cyberpolicen und passen Formulierungen an, um autonome KI-Systeme eindeutig einordnen zu können. Im Mittelpunkt stehen Fragen der Haftung und der Schadenursache. Muss ein autonom handelnder KI-Agent künftig wie ein externer Angreifer behandelt werden? Oder handelt es sich um ein internes Betriebsrisiko, das außerhalb der klassischen Cyberversicherung liegt? Eine einheitliche Antwort existiert bislang nicht.

Neue Deckungskonzepte entstehen

Bemerkenswert ist, dass viele Versicherer derzeit keine umfassenden Ausschlüsse planen. Vielmehr versuchen sie, bestehende Policen an die neue Risikolandschaft anzupassen. Vertreter von Marsh und QBE betonen, dass KI vor allem als Verstärker bestehender Cyberrisiken betrachtet werde. Kommt es infolge eines KI-Ereignisses zu einem klassischen Cybervorfall, sollen entsprechende Schäden grundsätzlich weiterhin über Cyberpolicen abgesichert bleiben. Gleichzeitig diskutiert die Branche über gezielte Ausschlüsse für systemische Risiken, etwa wenn Fehler eines einzelnen KI-Modells gleichzeitig zahlreiche Unternehmen betreffen könnten.

Parallel entwickelt sich ein Markt für spezialisierte KI-Versicherungslösungen. Anbieter wie Armilla AI, Munich Re mit „AiSure“ oder AXA XL bieten bereits Policen an, die typische Risiken künstlicher Intelligenz abdecken. Versichert werden unter anderem Fehlentscheidungen von KI-Modellen, Halluzinationen, Leistungsabweichungen oder Verletzungen geistiger Eigentumsrechte. Branchenbeobachter sehen darin den Beginn eines eigenständigen Versicherungssegments für KI-Risiken, das klassische Cyber-, Haftungs- und Vermögensschadenversicherungen künftig ergänzen dürfte.

Fehlende Erfahrungswerte erschweren die Risikobewertung

Hinzu kommt ein weiteres Problem: Es fehlen belastbare Schadendaten. Während Cyberversicherer inzwischen auf jahrelange Erfahrungen mit Ransomware oder Datenschutzverletzungen zurückgreifen können, existieren für Schäden durch autonome KI-Agenten kaum historische Vergleichswerte. Damit wird die Kalkulation von Prämien und Deckungssummen erheblich schwieriger. Experten weisen darauf hin, dass sich sowohl die Fähigkeiten autonomer KI-Systeme als auch geeignete Sicherheitsmaßnahmen derzeit noch in einer frühen Entwicklungsphase befinden. Versicherer müssen Risiken bewerten, deren tatsächliche Eintrittswahrscheinlichkeit bislang kaum statistisch erfasst werden kann.

Die wirtschaftliche Bedeutung dieser Entwicklung wächst entsprechend schnell. Nach Schätzungen von Munich Re erreichte der weltweite Markt für Cyberversicherungen zuletzt ein Volumen von rund 15 Milliarden US-Dollar und könnte bis 2030 auf etwa 28 Milliarden US-Dollar anwachsen. Gleichzeitig prognostiziert Aon, dass bereits 2027 nahezu jeder fünfte Cyberangriff generative KI einsetzen wird. Für die Versicherungswirtschaft geht es daher längst nicht mehr nur um sprachliche Anpassungen bestehender Vertragsbedingungen. Vielmehr zeichnet sich ab, dass autonome KI-Agenten die Risikomodelle der Cyberversicherung dauerhaft verändern und neue Spezialprodukte sowie differenziertere Deckungskonzepte erforderlich machen werden.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4951605/Autonome-KI-Agenten-veraendern-die-Cyberversicherung-Versicherer-definieren-ihre-Policen-neu/