AI-Risiken von Drittanbietern: Ein ganzheitlicher Ansatz zur Bewertung von Anbietern

Während AI für viele Unternehmen zum Rückgrat moderner Geschäftsprozesse wird, entwickeln bisher nur wenige Unternehmen AI-Systeme selbst. Stattdessen verlassen sie sich auf Drittanbieter, um AI-Lösungen in ihre tägliche Arbeit zu integrieren. Dies erfordert einen grundlegenden Wandel in der Art und Weise, wie Unternehmen die Risiken ihres AI-Einsatzes bewerten und managen.

Paradigmenwechsel bei der Bewertung von Lieferanten

Die meisten Unternehmen haben Strategien für das Risikomanagement von Drittanbietern (Third Party Risk Management, TPRM), aber diese traditionellen TPRM-Workflows müssen sich weiterentwickeln, um mit der dynamischen Integration von AI Schritt zu halten.

Ein isolierter Ansatz für die klassischen Dimensionen des Drittanbieter-Risikomanagements (z. B. Datenschutz, Sicherheit, Ethik, Geschäftskontinuität, usw.) sind für Unternehmen nicht mehr sinnvoll. Dies gilt auch für den Einsatz von AI bei Drittanbietern. Das unterstreicht die Notwendigkeit, Drittanbieter ganzheitlicher zu bewerten.

Der technische Rahmen: Bewertung von AI-Systemen und -Komponenten

Das Verständnis der technischen Details von AI-Systemen ist die Grundlage für eine solide Bewertung. Die Untersuchung der zugrundeliegenden Technologie deckt potenzielle Risiken auf, die mit Lösungen von Drittanbietern verbunden sind:

- **Datenattribute**

AI-Systeme benötigen eine große Menge an Daten – Verantwortliche müssen wissen, welche Attribute diese Datensätze haben. Die Bewertungen dieser sollten Klarheit über die Datenqualität, die Quellen der Trainingsdaten, das Eigentum an den Daten, die Versionierung und Rückverfolgbarkeit der Daten schaffen.

- **Modelattribute**

Weiterhin müssen Verantwortliche sich über das Modell selbst im Klaren sein. Ist das verwendete Modell ein Basismodell? Welche Lernmethode wird genutzt? Welche Biases können auftreten und wie ist die demographische Parität? Wie autonom ist das Modell und wie viel menschliche Aufsicht ist erforderlich?

Auch wenn das System außer Haus entwickelt oder bereitgestellt wird, tragen Betreiber die Verantwortung für die von Ihnen verwendeten Daten und Modelle – daher ist es wichtig, die Antworten auf diese Fragen gut zu dokumentieren.

AI-Governance-Rahmenwerke: Umgang mit der Einhaltung von Vorschriften und Anforderungen

AI-Governance-Praktiken sind eine entscheidende Komponente für die verantwortungsvolle Nutzung von AI, nicht nur für die eigene interne AI-Governance. Es wird zunehmend wichtiger, auch das Rahmenwerk des Anbieters zu bewerten, um einen besseren Einblick in die Compliance-, Rechts- und Ethikaspekte seiner Praktiken zu erhalten.

Globale Verordnungen, wie der EU AI Act, führen zunehmend spezifische Anforderungen an Akteure ein. So müssen beispielsweise Anbieter von AI-Systemen mit hohem Risiko eine Konformitätsbewertung durchführen. Auch wenn Unternehmen, die AI von Drittanbietern nutzen, nicht in diese Kategorie fallen, müssen sie sich dennoch an diesen Rahmenwerken orientieren, um die Einhaltung der Vorschriften sicherzustellen.

Umsetzung eines ganzheitlichen Bewertungsansatzes

Der Nutzen eines ganzheitlichen Bewertungsansatzes geht über die bloße Einhaltung von Vorschriften hinaus. Die Vermeidung rechtlicher und ethischer Fallstricke im Zusammenhang mit AI-Systemen ist entscheidend für den Aufbau von Kunden- und Mitarbeitervertrauen.

Es mag aufwändig erscheinen, zusätzlich zu den eigenen Verantwortlichkeiten im Bereich der AI-Governance auch noch Drittanbieter bewerten zu müssen, aber dieser Prozess muss nicht bei null beginnen. Die Operationalisierung von AI-Governance-Bewertungen umfasst kleinere, praktische Schritte, wie die Integration von AI-Governance in bestehende TPRM-Workflows. Tools, wie die TPRM-Lösung von OneTrust, unterstützen bei der Vereinfachung dieses Prozesses und bieten einen umfassenden Überblick über die Einführung von AI-Komponenten.

AI-Risikomanagement: Mehr als nur Drittparteien

Während das Bewusstsein für die Risiken durch Drittanbieter im Bereich AI wächst, ist es wichtig zu betonen, dass ein verantwortungsvoller Umgang damit weit über diese Herausforderung hinausgeht. Unternehmen stehen vor der Aufgabe, einen Rahmen zu schaffen, der nicht nur die Bewertung und Minderung von Drittparteienrisiken umfasst, sondern auch die zentralisierte Verwaltung und Überwachung von AI-Systemen sowie der Daten, die zum Trainieren von Algorithmen für maschinelles Lernen verwendet werden. Mit der AI-Governance-Lösung von OneTrust können Sie diesen Rahmen verwirklichen und damit ein Ökosystem bilden, das auf Transparenz, Vertrauen und Innovation aufbaut.

Marco Barone, Senior Counsel Data Privacy, CIPP/E, CIPP/US, CIPM, FIP