NACHRICHTEN
Österreich

EU-Vorschriften zwingen Unternehmen zur KI- und Cybersicherheits-Kompetenz!

Die EU-Regelwerke AI-Act und NIS2 fordern nachweisbare KI- und Cybersicherheits-Kompetenzen. Unternehmen müssen sich vorbereiten.

Laimgrubengasse 10, 1060 Wien, Österreich - Die neuen EU-Regelungen, die durch den AI-Act und die NIS2-Richtlinie geschaffen wurden, stellen Unternehmen vor erhebliche Herausforderungen, eröffnen aber auch Chancen für eine sicherere und verantwortungsvolle Nutzung von Technologien. Wie die **OTS** berichtet, sind Unternehmen ab dem 2. Februar 2025 verpflichtet, dass ihre Mitarbeitenden über umfassende Kompetenzen im Bereich Künstliche Intelligenz (KI) verfügen. Diese Regelung erstreckt sich auf Personen, die mit Entwicklung, Betrieb und der Anwendung von KI-Systemen betraut sind, und ist Teil der Bestimmungen, die darauf abzielen, digitale Risiken zu minimieren und Sicherheitsstandards zu etablieren.

Risiken verstehen und managen

Der AI-Act kategorisiert KI-Anwendungen nach ihrem Risiko: Unzulässige KI-Systeme werden verboten, während Hochrisiko-KI-Systeme strengen Regulierungen unterliegen. Laut **artificialintelligenceact.eu** müssen Anbieter dieser Systeme ein umfassendes Risikomanagement etablieren, das sich durch den gesamten Lebenszyklus der KI erstreckt. Eine sorgfältige Analyse und Kontrolle von Hochrisiko-KI-Systemen ist unerlässlich, um sicherzustellen, dass sie keine unkontrollierbaren Risiken für die Gesellschaft darstellen. Unternehmen müssen die Verantwortung für die Sicherheit der

in ihren KI-Systemen verwendeten Daten übernehmen und entsprechende Sicherheitsmaßnahmen implementieren.

Beide Regelwerke, AI-Act und NIS2, betonen die Wichtigkeit von Verantwortlichkeit auf Führungs- und Mitarbeiterebene. Führungskräfte sind verpflichtet, nicht nur Sicherheitsmaßnahmen zu genehmigen, sondern auch deren Umsetzung aktiv zu überwachen und haften für Verstöße. Dies ist ein entscheidender Schritt in Richtung verbessertes Risikomanagement in der Nutzung von KI-Technologien und zur Bewältigung der Herausforderungen durch Cyberbedrohungen.

Die NIS2-Richtlinie ergänzt diese Vorgaben, indem sie Unternehmen dazu verpflichtet, Cybersicherheits-Kompetenzen nachzuweisen und entsprechende Schulungen anzubieten. Diese Maßnahmen sind besonders wichtig, um die Resilienz kritischer Infrastrukturen zu stärken, insbesondere in sensiblen Bereichen wie dem Gesundheitswesen und der Energieversorgung. Auch hier sehen die Gesetzgeber strenge Sanktionen vor, um die Einhaltung der Regeln zu gewährleisten.

Details	
Ort	Laimgrubengasse 10, 1060 Wien, Österreich
Quellen	• **www.ots.at** • **artificialintelligenceact.eu**