



ISC2-Studie zeigt, dass Cybersicherheitsteams bei der Einführung von KI vorsichtig vorgehen

*Neue Studie zeigt, dass 30 Prozent der Cybersicherheitsexperten bereits KI-Tools einsetzen,
und liefert Einblicke in die ersten Auswirkungen auf die Teamleistung und Einstellungsentwicklungen*

Alexandria (VA) / München, 16. Juli 2025 – ISC2, die weltweit führende gemeinnützige Mitgliederorganisation für Cybersicherheitsexperten, hat heute ihre Umfrage „[2025 AI Adoption Pulse Survey](#)“ veröffentlicht, in der die Einführung von KI-Sicherheitstools in Cybersicherheitsteams abgefragt wurde. Basierend auf den Erkenntnissen von weltweit 436 Cybersicherheitsexperten in Unternehmen aller Größenordnungen, bewertet die Studie die Auswirkungen der Nutzung von KI auf die Teameffektivität, Einstiegsjobs und die Einstellung von Cybersicherheitsexperten.

„KI verändert die Arbeitsweise von Unternehmen, und die Cybersicherheit bildet dabei keine Ausnahme“, sagt Casey Marks, Chief Qualifications Officer bei ISC2. „Unsere aktuelle KI-Umfrage zeigt ein vorsichtiges, aber wachsendes Interesse an KI-Sicherheitstools, deren Einführung sich in Zukunft voraussichtlich beschleunigen wird. Erfreulicherweise geben 44 Prozent der Experten an, dass die derzeitige oder erwartete Einführung von KI-Sicherheitstools keine Auswirkungen auf die Einstellung von Personal hat. 28 Prozent sehen in KI neue Chancen für Berufseinsteiger. Die Ergebnisse deuten darauf hin, dass KI die Cybersicherheitsexperten unterstützt, indem sie repetitive Aufgaben automatisiert und es ihnen ermöglicht, sich auf sinnvollere Aufgaben zu konzentrieren.“

Einsatz von KI-Sicherheitstools

Laut der AI Pulse Survey haben 30 Prozent der Cybersicherheitsexperten bereits KI-Sicherheitstools in ihre Abläufe integriert, die in der Umfrage als „KI-fähige Sicherheitslösungen, generative KI und/oder agentenbasierte KI für automatische Aktionen“ definiert werden. Darüber hinaus prüft oder testet die Mehrheit (42 Prozent) derzeit deren Einführung, was auf eine starke Dynamik in Richtung einer zukünftigen Implementierung hindeutet. Von denjenigen, die bereits KI-Sicherheitstools nutzen, berichten 70 Prozent von positiven Auswirkungen auf die Gesamteffektivität ihres Teams.

Die fünf Bereiche, in denen KI-Sicherheitstools in kürzester Zeit die positivsten Auswirkungen auf den Betrieb haben werden, wie Verbesserung der Effizienz und Automatisierung zeitaufwändiger Aufgaben, sind:

- Netzwerküberwachung und Intrusion Detection: 60 Prozent
- Endpunktschutz und -reaktion: 56 Prozent
- Schwachstellenmanagement: 50 Prozent
- Bedrohungsmodellierung: 45 Prozent
- Sicherheitstests: 43 Prozent

Die größten Unternehmen mit mehr als 10.000 Mitarbeitern sind führend bei der Einführung von KI-Tools als Teil ihrer Cybersicherheitsmaßnahmen, wobei 37 Prozent diese aktiv nutzen. Dicht dahinter folgen mittelgroße bis große Unternehmen (2.500 bis 9.999 Mitarbeiter) und kleinere Unternehmen (100 bis 499 Mitarbeiter) mit jeweils 33 Prozent Einsatzquote. Im Gegensatz dazu weisen mittelständische (500 bis 2.499



Mitarbeiter) und kleinste Unternehmen (1 bis 99 Mitarbeiter) die niedrigsten Einsatzquoten auf: Nur 20 Prozent jeder Gruppe setzen KI aktiv für Sicherheitszwecke ein. Bemerkenswert ist, dass die kleinsten Unternehmen auch die konservativsten sind: 23 Prozent geben an, keine Pläne zur Evaluierung von KI-Sicherheitstools zu haben.

Unter den Branchen, die KI-Tools für ihre Sicherheitsmaßnahmen einsetzen, evaluieren oder testen, liegen Industrieunternehmen (38 Prozent), IT-Dienstleister (36 Prozent), der Handels-/Konsumgütersektor (36 Prozent) und professionelle Dienstleistungsunternehmen (34 Prozent) an der Spitze. Im Gegensatz dazu weisen Finanzdienstleister und die öffentliche Hand derzeit mit 21 Prozent bzw. 16 Prozent die niedrigsten Akzeptanzraten auf.

Einige Branchen mit den derzeit niedrigsten Akzeptanzraten erwägen jedoch am ehesten die Integration von KI-Tools in der Zukunft. Sowohl im Finanzdienstleistungssektor als auch im Handels-/Verbrauchersektor geben 41 Prozent der Fachleute an, diese Tools aktiv zu evaluieren, während 36 Prozent der Befragten aus dem öffentlichen Sektor dies angeben.

Auswirkungen auf die Einstellung und Einstiegspositionen

Die Mehrheit der Befragten stimmt zu, dass KI-Sicherheitstools Auswirkungen auf die Einstellung von Nachwuchskräften im Bereich Cybersicherheit haben werden. Mehr als die Hälfte (52 Prozent) gibt an, dass KI den Bedarf an Nachwuchskräften erheblich oder etwas reduzieren wird. 31 Prozent äußerten sich jedoch optimistischer und glauben, dass KI auch neue Arten von Einstiegs- und Junior-Positionen schaffen oder die Nachfrage erhöhen wird, was dazu beiträgt, den Rückgang an anderen Stellen bei den Einstiegsmöglichkeiten auszugleichen.

Die Befragten äußerten sich optimistisch über die allgemeine Einstellungslage im Bereich Cybersicherheit angesichts der Einführung von KI. Fast die Hälfte (44 Prozent) stimmt zu, dass die Einstellung von Cybersicherheitsexperten in ihrem Unternehmen noch nicht von der Einführung von KI-Sicherheitstools beeinflusst wurde. Im Gegensatz dazu geben 21 Prozent an, dass KI ihre Einstellungspläne und Prioritäten in ihren Unternehmen verändert hat.

Gleichzeitig ist klar, dass KI-Sicherheitstools die Rollen und Verantwortlichkeiten der bestehenden Mitarbeiter neu definieren. Laut der Umfrage geben 44 Prozent der Cybersicherheitsexperten an, dass ihre Unternehmen aktiv die Rollen und Fähigkeiten überdenken, die für die Einführung und Nutzung von KI-Sicherheitstools erforderlich sind.

Der Umfrage-Bericht enthält wichtige Erkenntnisse für Unternehmen und Personalverantwortliche, die sich mit dem wachsenden Einfluss von KI auf die Cybersicherheit auseinandersetzen. Angesichts der kontinuierlichen Weiterentwicklung der KI müssen Unternehmen ein Gleichgewicht finden. Dabei müssen sie ihre Effizienz nutzen und gleichzeitig Investitionen in Einstiegsmöglichkeiten priorisieren, um sicherzustellen, dass die Cybersicherheitsfachkräfte agil, qualifiziert und zukunftsfähig bleiben.

Die vollständigen Umfrageergebnisse, darunter auch Informationen darüber, wie Cybersicherheitsexperten KI-Tools einsetzen und wie sich dies auf die Teameffizienz, Einstiegspositionen und Einstellungstrends auswirkt, finden Sie im vollständigen Bericht [hier](#).



Über die Umfrage „2025 AI Adoption Pulse Survey“

ISC2 führte eine Online-Umfrage durch, um den Einsatz von KI-Sicherheitstools in Unternehmen zu eruieren und die Auswirkungen dieses Einsatzes auf die Teameffizienz, Einstiegsjobs und die Einstellung von Cybersicherheitsexperten besser zu verstehen. Insgesamt nahmen 436 Fachleute in Positionen mit Verantwortung für Cybersicherheit teil. Die Umfrage wurde vom 13. bis 22. Mai 2025 auf die Dashboard-Seiten für Mitglieder von ISC2 gestellt. Für die Zwecke dieser Umfrage wurden KI-Sicherheitstools als „KI-fähige Sicherheitslösungen, generative KI und/oder agentenbasierte KI für automatische Aktionen“ definiert.

+++

Über ISC2

ISC2 ist die weltweit führende Nonprofit-Organisation für Cybersecurity-Experten. Mit über 265.000 zertifizierten Mitgliedern und Partnern setzen wir uns in einer immer stärker vernetzten Gesellschaft für eine sichere Cyberwelt ein. Unsere renommierten Zertifizierungen – darunter die branchenführende CISSP®-Zertifizierung – dienen Fachkräften als Nachweis ihrer Kenntnisse, Fähigkeiten und Kompetenzen in jeder Phase ihrer Karriere. ISC2 setzt Cybersecurity auf die politische und gesellschaftliche Agenda. Wir fördern die Relevanz, Vielfalt und Dynamik der Cybersecurity-Branche durch engagierte Fürsprache, fundiertes Fachwissen und die Schulung und Zertifizierung von Fachkräften. Mit unserer gemeinnützigen Stiftung, dem [Center for Cyber Safety and Education](#), vereinfachen wir den Zugang zu diesem Berufszweig für angehende Nachwuchskräfte.

Erfahren Sie mehr über [ISC2](#) und werden Sie Teil unserer Mission. Vergrößern Sie ihr Netzwerk und folgen Sie uns auf [X](#), [Facebook](#) und [LinkedIn](#).

© 2025 ISC2 Inc. | ISC2, CISSP®, SSCP®, CCSP®, CGRC®, CSSLP®, HCISPP®, ISSAP®, ISSEP®, ISSMP®, CC® und CBK® sind eingetragene Marken von ISC2, Inc.

Pressekontakt:

ISC2
Kiri O'Leary, Corporate Communications Professional
koleary@isc2.org

TC Communications
Arno Lucht, +49 157 52443749
Thilo Christ, +49 171 6220610
Alexandra Schmidt, +49 170 3871064
ISC2@tc-communications.de