



## **ISC2-Studie: Die Einführung von KI gewinnt an Dynamik und verbessert die Karrierechancen für Cybersecurity-Experten in Deutschland**

*Die neueste ISC2-Studie zur Cybersicherheitsbelegschaft zeigt, dass Cybersecurity-Experten ihre KI-Kenntnisse erweitern – zum Vorteil der Unternehmen und ihrer eigenen Karrierechancen.*

**Alexandria/München, 3. Februar 2026** – Die „[ISC2 Cybersecurity Workforce Study 2025](#)“ der weltweit führenden gemeinnützigen Mitgliederorganisation für Cybersecurity-Experten [ISC2](#) verdeutlicht die Auswirkungen von KI. Die Ergebnisse der Umfrage unter 16.029 Cybersecurity-Experten weltweit zeigen, dass der Einsatz von KI in diesem Berufsfeld weiter an Dynamik gewinnt. Die Studie untersucht, wie 515 Cybersecurity-Experten in Deutschland die Entwicklung ihrer Aufgabenbereiche angesichts der zunehmenden Komplexität der Bedrohungslage einschätzen und wie sie die Entwicklung von KI-Kompetenzen priorisieren, um sich auf die Zukunft vorzubereiten.

Die Einführung von KI schreitet unter den Befragten in Deutschland schneller voran als unter den Befragten weltweit: 35 Prozent geben an, dass sie bereits KI-Tools integriert haben, verglichen mit 28 Prozent weltweit. Insgesamt befinden sich 77 Prozent der Befragten in Deutschland in einer Phase der KI-Einführung – von der Integration über das Testen bis hin zur ersten Bewertung – gegenüber 68 Prozent der Befragten weltweit. Dazu gehören 25 Prozent in Deutschland, die ausgewählte Tools vor der vollständigen Einführung aktiv testen (gegenüber 19 Prozent weltweit).

Die Antworten zeigen eine größere Übereinstimmung zwischen Deutschland und den globalen Ergebnissen, wenn es um die Erwartungen hinsichtlich der Auswirkungen von KI auf den Beruf des Cybersecurity-Experten geht. So glauben beispielsweise 75 Prozent der deutschen Befragten, dass KI zu spezialisierteren Cybersecurity-Funktionen führen wird, verglichen mit 73 Prozent weltweit. 71 Prozent der in Deutschland tätigen Cybersecurity-Experten (72 Prozent weltweit) prognostizieren einen steigenden Bedarf an strategischen Funktionen und Fähigkeiten. Gleichzeitig glauben 69 Prozent (weltweit 66 Prozent), dass KI einen Bedarf an breiteren, allgemeineren Fähigkeiten in allen Bereichen der Cybersicherheit schaffen wird.



KI rangiert weiterhin ganz oben unter den gefragtesten Fähigkeiten. Unter den Fachkräften, die angaben, dass ihr Unternehmen einen oder mehrere Bedarf an Cybersicherheitskompetenzen hat, nennen 43 Prozent in Deutschland KI als einen Bereich, in dem zusätzliche Fähigkeiten erforderlich sind, verglichen mit 41 Prozent weltweit. Der Bedarf an Weiterbildungen wird sowohl in Deutschland als auch weltweit einheitlich angegeben: Fast die Hälfte der deutschen und globalen Befragten (48 Prozent) arbeitet derzeit daran, ihre KI-bezogenen Fähigkeiten zu erwerben und zu erweitern, um in einer KI-gesteuerten Welt relevant oder „zukunftsicher“ zu bleiben. Darüber hinaus informieren sich 35 Prozent (in Deutschland und weltweit) über mögliche Schwachstellen und Exploits in KI-Lösungen.

Die Ergebnisse deuten darauf hin, dass KI den Bedarf an Fachkräften im Bereich Cybersicherheit in erster Linie durch die Weiterentwicklung von Fähigkeiten und Denkweisen in bestehenden Rollen beeinflussen wird. Zusammengenommen deuten diese Trends auf einen klaren und wachsenden Bedarf an kontinuierlicher Weiterqualifizierung der Fachkräfte im Bereich Cybersicherheit hin.

Die vollständige Studie und weiterführende Handlungsempfehlungen für Führungskräfte und Organisationen, stehen hier zum Download bereit:

[2025 ISC2 Cybersecurity Workforce Study](#)

### **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](mailto:koleary@isc2.org)

TC Communications

Arno Lucht, +49 157 52443749

Thilo Christ, +49 171 6220610

Alexandra Schmidt, +49 170 3871064

[ISC2@tc-communications.de](mailto:ISC2@tc-communications.de)