



Messbarer Einfluss mangelnder Fähigkeiten in der Cybersicherheit

Die ISC2 2025 Cybersecurity Workforce Study beleuchtet den Stand des Bedarfs an Cybersicherheitskompetenz in deutschen Unternehmen. Im Vergleich zum globalen Durchschnitt schnitten deutsche Unternehmen in einigen Bereichen schlechter ab und führten Cybervorfälle auf den Kompetenzmangel zurück.

Alexandria/München, 17. Februar 2026 – [ISC2](#), die weltweit führende gemeinnützige Mitgliedervereinigung für Cybersicherheitsfachleute, befragte im Rahmen der internationalen „[2025 Cybersecurity Workforce Study](#)“ 16.029 Experten aus der Cybersicherheitsbranche. Eine zentrale Erkenntnis der Studie ist der spürbare Einfluss des Kompetenzmangels in Bereichen wie KI und Cloud-Sicherheit. Die Ergebnisse zeigen deutlich: Unzureichende Kompetenzen in Cybersicherheitsteams können die Fähigkeit eines Unternehmens beeinträchtigen, sich selbst zu schützen.

In der Studie gaben 92 Prozent der Befragten in Deutschland an, mindestens eine Konsequenz im Bereich Cybersicherheit aufgrund von Kompetenzdefiziten im Team oder im gesamten Unternehmen erlebt zu haben. 77 Prozent der deutschen Teilnehmer berichteten sogar von mehreren Cyberkonsequenzen, die auf den Mangel an Fachkenntnissen zurückzuführen sind. Damit liegt Deutschland über dem globalen Durchschnitt. International erlebten 88 Prozent mindestens eine erhebliche Konsequenz und 69 Prozent mehr als eine Konsequenz aufgrund des Kompetenzmangels.

Neben fehlenden Kompetenzen waren auch Budgets ein Problem

Budgetbeschränkungen in Unternehmen hatten Auswirkungen auf die Abdeckung der benötigten Kompetenzen in den Cybersicherheitsteams. Während 43 Prozent der Befragten in Deutschland (global: 30 Prozent) angaben, dass ihr Unternehmen nicht genug Talente finden konnte, um das Cybersicherheitsteam angemessen zu besetzen, zeigte die Studie auch, dass 26 Prozent der Unternehmen nicht über die notwendigen Budgets verfügten, um Personal mit den erforderlichen Fähigkeiten einzustellen. Aus finanzieller Sicht schnitt Deutschland etwas besser ab als der globale Durchschnitt, wo 33 Prozent der Befragten angaben, dass ihr Unternehmen mit budgetären



Herausforderungen bei der Erweiterung der Cybersicherheitsteams mit bestimmten Fachkenntnissen konfrontiert war.

Das Problem unzureichender Fähigkeiten

Dass Unternehmen keine geeigneten Mitarbeiter finden oder nicht über die Budgets für qualifizierte Cybersicherheitsfachkräfte verfügen, ist die eine Seite der Medaille. Die andere Seite betrifft das Kompetenzniveau der bestehenden Mitarbeiter. In der Studie gaben 90 Prozent der Befragten an, mindestens eine Kompetenzlücke zu haben. Bei der Frage nach kritischen oder erheblichen Kompetenzlücken sank diese Zahl auf 40 Prozent. Global lag dieser Wert bei 59 Prozent. In Deutschland haben sich kritische oder erhebliche Kompetenzlücken über das Jahr sogar verschärft. Im Vergleich zur vorherigen Studie stiegen sie in der 2025-Studie um 11 Prozentpunkte.

Investitionen in Mitarbeiter und deren Kompetenzen

Die Steigerung von Kompetenzen bedeutet nicht zwangsläufig, mehr Personal einzustellen. Zwar kann eine Ausweitung der Mitarbeiterzahl notwendig sein, doch die Stärkung der Cybersicherheitskompetenzen in bestehenden Teams und bei anderen Mitarbeitern ist ein wichtiger und effektiver Weg, um das Unternehmen mit den Fähigkeiten auszustatten, die für neue und sich weiterentwickelnde Technologien und Arbeitsmethoden erforderlich sind. Eine direkte Budgetzuweisung für die Mitarbeiterentwicklung ist eine zentrale strategische Maßnahme: 34 Prozent der deutschen Studienteilnehmer nannten dies als einen Weg, um sie zu motivieren. Die Priorisierung der beruflichen Weiterentwicklung könnte eine effektive Methode sein, um die bestehende Cybersicherheitsbelegschaft zusätzlich zu qualifizieren, anstatt zu versuchen, eine oder mehrere „Alleskönner“-Fachkräfte mit allen benötigten Fähigkeiten einzustellen.

Die vollständige ISC2 2025 Cybersecurity Workforce Study und weiterführende Handlungsempfehlungen für Führungskräfte und Organisationen, um eine widerstandsfähige Cybersecurity-Belegschaft zu unterstützen, steht bereit unter: [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

TC Communications

Arno Lucht, +49 157 52443749

Thilo Christ, +49 171 6220610

Alexandra Schmidt, +49 170 3871064

ISC2@tc-communications.de