ISC2 Cybersecurity Workforce Study: Cybersecurity-Budgets bleiben angespannt und der Bedarf an Fachkräften wächst

Die Studie von ISC2 zeigt, wie Personal- und Budgetkürzungen das wahrgenommene Sicherheitsrisiko erhöhen, während die schnelle Einführung von KI die Anforderungen an Fähigkeiten verändert und neue Karrieremöglichkeiten schafft.

Alexandria/München, 4. Dezember 2025 – ISC2, die weltweit führende gemeinnützige Mitgliederorganisation für Cybersecurity-Profis, hat heute die Ergebnisse ihrer „2025 Cybersecurity Workforce Study“ veröffentlicht, die eine Rekordzahl von 16.029 Fachleuten aus der Cybersecurity-Branche befragte. Das Vorjahr war von einer Welle von Entlassungen, Budgetkürzungen sowie Einstellungs- und Beförderungsstopps geprägt. Die Daten für 2025 zeigen jedoch, dass sich die wirtschaftlichen Bedingungen, die Auswirkungen auf Cybersecurity-Teams haben, stabilisiert haben: 43 Prozent der deutschen Befragten (global* 36 Prozent) melden Budgetkürzungen und 23 Prozent (global 24 Prozent) Entlassungen.

Budgetengpässe im Bereich Cybersecurity bleiben ein wichtiger Treiber für Personalmangel, so die Studie. 38 Prozent der deutschen Befragten (global 29 Prozent) geben an, dass ihre Organisationen nicht genügend Talente finden, um ihre Teams adäquat zu besetzen, während 25 Prozent (global 33 Prozent) sagen, dass sie es sich nicht leisten können, Personal mit den benötigten Fähigkeiten einzustellen, um ihre Organisationen angemessen abzusichern. Infolgedessen sind in Deutschland 72 Prozent der Befragten (global 71 Prozent) der Meinung, dass eine Reduzierung des Sicherheitspersonals das Risiko eines Sicherheitsvorfalls erheblich erhöht.

Hauptsorge: Fachkräftemangel übertrifft die Personalanforderung

Die Studie zeigt weiterhin, dass trotz des anhaltenden Personalmangels die Fachkräftelücke mehr Sorgen bereitet als die Anzahl der Mitarbeiter. Mit 93 Prozent haben mehr als neun von zehn Befragten in Deutschland (global 88 Prozent) in ihren Organisationen mindestens einen bedeutenden Cybersecurity-Vorfall aufgrund eines Fachkräftemangels erlebt und 77 Prozent (global 69 Prozent) geben mehr als einen Vorfall an.

In Deutschland geben weniger Befragte an, dass sie mindestens einen Qualifikationsbedarf haben (90 Prozent in Deutschland gegenüber 95 Prozent weltweit). Auch geben sie mit 40 Prozent deutlich seltener als ihre Kollegen weltweit (60 Prozent) an, dass sie kritische oder erhebliche Qualifikationslücken haben. Im Jahresvergleich hat sich in Deutschland jedoch eine bemerkenswerte Veränderung vollzogen: Der Anteil derjenigen, die kritische oder erhebliche Qualifikationslücken angeben, ist um 11 Prozentpunkte gestiegen.

„Es findet ein Wandel statt. Die Daten des diesjährigen Berichts machen deutlich, dass die drängendste Sorge für Cybersecurity-Teams nicht die Anzahl der Mitarbeiter, sondern die Fähigkeiten der Mitarbeiter ist“, sagte Debra Taylor, kommissarische CEO und CFO von ISC2. „Mangelnde Fähigkeiten erhöhen das Cybersicherheitsrisiko und stellen die Geschäftskontinuität infrage. Gleichzeitig sehen wir, dass neue Technologien wie KI weniger als Bedrohung für die Arbeitsplätze wahrgenommen werden als erwartet. Stattdessen sehen viele Cybersecurity-Profis die KI als eine Chance für ihre berufliche Weiterentwicklung. Sie setzen KI-Tools ein, um Aufgaben zu automatisieren, und investieren ihre Zeit, um mehr zu lernen und ihre Expertise im Umgang mit und der Absicherung von KI-Systemen zu demonstrieren.“

KI-Adoption beschleunigt sich und schafft neue Karrieremöglichkeiten

Die Studie zeigt, dass die Einführung von KI unter Cybersecurity-Profis voranschreitet: 35 Prozent der deutschen Befragten (global 28 Prozent) haben bereits KI-Tools in ihre Abläufe integriert. Auch haben sich Cybersicherheitsexperten in Deutschland sich häufiger als ihre Kollegen weltweit mit der Einführung von KI befasst (77 Prozent in Deutschland gegenüber 68 Prozent weltweit) – sei es durch Integration, aktives Testen oder erste Evaluierung. Die Daten deuten auch darauf hin, dass deutsche Cybersecurity-Profis davon ausgehen, dass KI neue Fähigkeiten und Perspektiven im Bereich der Cybersecurity erforderlich machen wird:

- 75 Prozent (global 73 Prozent) glauben, dass KI spezialisierte Cybersecurity-Fähigkeiten schaffen wird.
- 71 Prozent (global 72 Prozent) sagen, dass KI mehr strategische Cybersecurity-Denken erfordert.
- 69 Prozent (global 66 Prozent) sind der Ansicht, dass KI breitere Fähigkeiten innerhalb der Belegschaft verlangt.

KI bleibt im zweiten Jahr in Folge eine der am meisten gefragten Fähigkeiten. In diesem Jahr nennen 43 Prozent der Befragten in Deutschland (global 41 Prozent) KI als die wichtigste erforderliche Fähigkeit, gefolgt von Cloud-Security mit 36 Prozent in Deutschland und global. Mit 48 Prozent arbeitet fast die Hälfte der deutschen als auch der weltweiten Befragten daran, allgemeine KI-Kenntnisse und -Fähigkeiten zu erlangen, während 35 Prozent der deutschen und weltweit Befragten sich über KI-Lösungen für Risikobereiche weiterbilden, um Schwachstellen und Ausnutzungsmöglichkeiten besser zu verstehen.

Trotz Herausforderungen sind Cybersecurity-Profis leidenschaftlich bei ihrer Arbeit

Trotz der wirtschaftlichen Unsicherheit und des Arbeitsdrucks bleiben deutschen Cybersecurity-Profis optimistisch in Bezug auf ihre Rolle in der Branche. Die Forschung zeigt:

- 87 Prozent in Deutschland und global sind der Meinung, dass es immer einen Bedarf an Cybersecurity-Profis geben wird.
- 84 Prozent (global 81 Prozent) sind zuversichtlich, dass der Beruf stark bleiben wird.
- 69 Prozent (global 68 Prozent) sind mit ihrem aktuellen Job zufrieden.
- 84 Prozent (global 80 Prozent) sind leidenschaftlich bei ihrer Arbeit.
- 72 Prozent (global 75 Prozent) sind wahrscheinlich bereit, im nächsten Jahr in ihrer aktuellen Organisation zu bleiben, wobei dieser Wert auf 64 Prozent (global 66 Prozent) sinkt, wenn sie die nächsten zwei Jahre in Betracht ziehen.

Die Studie zeigt jedoch auch, dass Cybersecurity-Profis unter Jobstress und Burnout leiden. Mit 44 Prozent (global 48 Prozent) fühlen sich Fast die Hälfte der Befragten erschöpft, weil sie mit den neuesten Cybersecurity-Bedrohungen und -Technologien Schritt halten müssen und 46 Prozent der deutschen als auch der weltweiten Befragten fühlen sich von der Arbeitsbelastung überwältigt.

Die Studie stellt fest, dass Karrierewachstum und Anerkennung wichtige Faktoren für die Zufriedenheit der Fachleute in der Branche sind. Fast ein Drittel der in Deutschland und weltweit (31 Prozent) nennen Aufstiegsmöglichkeiten als wichtigen Aspekt für ihr berufliches Engagement, während 25 Prozent in Deutschland (global 23 Prozent)

unplanmäßige finanzielle oder leistungsbezogene Belohnungen (z. B. Boni, zusätzliche bezahlte Urlaubstage) als Schlüsselfaktoren für das Engagement ihrer Belegschaft.

Der vollständigen Bericht zur „2025 ISC2 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

* Die im Text genannten globalen Daten schließen deutsche Antworten aus und können von den Zahlen im globalen Bericht abweichen.

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.

Pressekontakt:

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

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