

Büchel, Jan; Engels, Barbara; Engler, Jan

Research Report

Cybersicherheit: Kompetenzen gefragter denn je

IW-Kurzbericht, No. 39/2025

Provided in Cooperation with:

German Economic Institute (IW), Cologne

Suggested Citation: Büchel, Jan; Engels, Barbara; Engler, Jan (2025) : Cybersicherheit: Kompetenzen gefragter denn je, IW-Kurzbericht, No. 39/2025, Institut der deutschen Wirtschaft (IW), Köln

This Version is available at:

<https://hdl.handle.net/10419/318330>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

Cybersicherheit: Kompetenzen gefragter denn je

Jan Büchel / Barbara Engels / Jan Engler, 25.04.2025

Cyberangriffe treffen deutsche Unternehmen immer stärker – und die reagieren. Zwischen 2019 und 2024 hat sich die Zahl der Online-Stellenanzeigen, in denen Cybersicherheitskompetenzen gefordert werden, von 117.000 auf 203.000 deutlich erhöht. Kompetenzen rund um digitale Sicherheit sind für eine funktionierende Wirtschaft und Verwaltung zentral geworden.

Die Bedrohungslage im Cyberraum verschärft sich. Die fortschreitende Digitalisierung führt zu einer größeren Angriffsfläche für Cyberkriminelle, welche immer effektivere Angriffsmethoden einsetzen. So ist die IT-Sicherheitslage in Deutschland besorgniserregend (BSI, 2024). Zwei Drittel der Unternehmen sehen sich durch potenzielle Cyberattacken in ihrer Existenz bedroht (Bitkom, 2024a). Die wirtschaftlichen Schäden durch Cyberangriffe sind beträchtlich. Der Gesamtschaden durch Cybercrime betrug 2024 laut Bitkom rund 179 Milliarden Euro (ebenda). Dies verdeutlicht die Dringlichkeit für Unternehmen, in Cybersicherheitsmaßnahmen zu investieren. Unternehmen können etwa Tools zur Cyberabwehr von externen Dienstleistern erwerben oder in entsprechend qualifiziertes Personal investieren – in Form von Weiterbildungen oder Neueinstellungen.

Investitionen in IT-Sicherheit steigen

Tatsächlich haben Unternehmen ihre Investitionen in IT-Sicherheit erhöht. 2024 stiegen die Ausgaben für IT-Sicherheitsmaßnahmen im Vergleich zum Vorjahr um

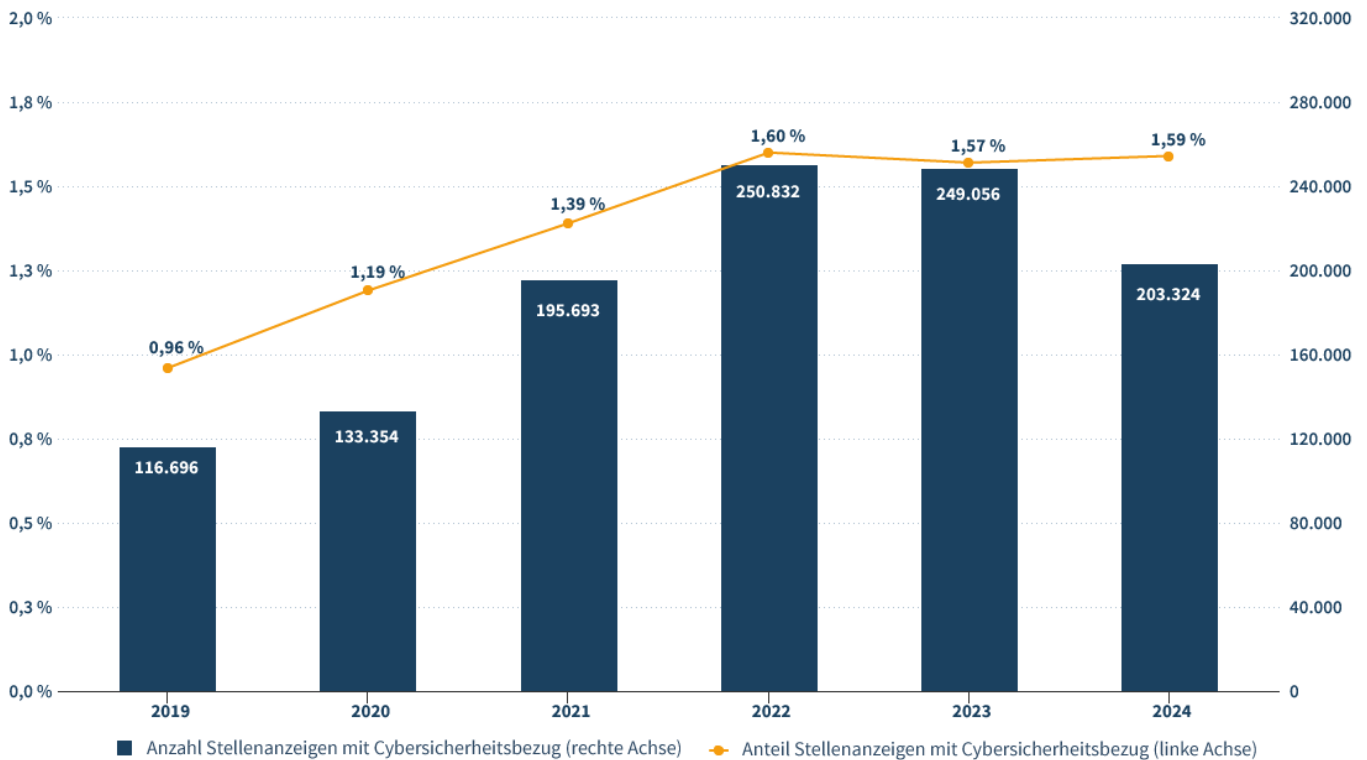
13,8 Prozent auf 11,2 Milliarden Euro (Bitkom, 2024c). Doch die Investitionen können den Mangel an qualifizierten Fachkräften nicht lösen. Laut der IW-Fachkräftedatenbank gab es im Dezember 2024 für etwa drei von zehn offenen Stellen in der Berufsuntergruppe „IT-Netzwerktechnik, IT-Koordination, IT-Administration und IT-Organisation (sonstige Spezialisierung)“, zu der auch Fachkräfte für IT-Security zählen, keine passend qualifizierten Arbeitslosen. Über alle IT-Berufe hinweg könnten laut Bitkom (2024b) bis 2040 insgesamt 663.000 IT-Fachleute fehlen.

Wie stark die Nachfrage deutscher Unternehmen nach IT-Fachkräften speziell mit Cybersicherheitskompetenzen ist, zeigt eine Analyse von Online-Stellenanzeigen. Insgesamt schrieben deutsche Unternehmen zwischen 2019 und 2024 etwa 82 Millionen Online-Anzeigen für Stellen in Deutschland aus. Zur Identifikation der Stellenanzeigen mit Cybersicherheitsbezug wurde ein computerlinguistisches Verfahren angewendet, mit dem bereits in anderen Studien themenbezogene Stellenanzeigen identifiziert werden konnten (Büchel et al., 2025; Büchel/Engler, 2024).

Zunächst wurde dafür eine Liste mit deutschen Begriffen und deren englischen Übersetzungen erstellt, die charakteristisch für Cybersicherheitskompetenzen sind. Für diese Liste wurden relevante Fachbegriffe und Schlüsselkonzepte des Themenfeldes Cybersicherheit

Cybersicherheit in Stellenanzeigen

Anzahl der Online-Stellenanzeigen in Deutschland mit Cybersicherheitsbezug und deren Anteil an allen ausgeschriebenen Stellen



Insgesamt 1.148.955 verschiedene Stellenanzeigen mit Cybersicherheitsbezug

Quelle: Institut der deutschen Wirtschaft basierend auf Textkernel-Daten

durch eine systematische Recherche und Analyse öffentlich zugänglicher Quellen zusammengestellt. In einem iterativen Prozess wurde die Auswahl mehrfach überarbeitet, um die Vollständigkeit und Relevanz der Begriffe sicherzustellen. Allgemein verwendete Ausdrücke, die neben dem Bereich Cybersicherheit auch in anderen Kontexten auftreten können, blieben unberücksichtigt. Stattdessen lag der Fokus auf möglichst spezifischen Begriffen wie „ISO 27001“, einer internationalen Norm mit hoher Bedeutung für Cybersicherheitszertifizierung. Schließlich wurde die Liste automatisiert mit den Volltexten der Stellenanzeigen abgeglichen.

Nachfrage nach Cybersicherheitskompetenzen verdoppelt sich

Im Zeitraum von 2019 bis 2024 konnte in insgesamt 1.148.955 Stellenanzeigen ein Cybersicherheitsbezug festgestellt werden. Zwischen 2019 und 2022 ist die Zahl der Online-Stellenanzeigen mit Cybersicherheitsbezug um über 115 Prozent gestiegen – von jährlich rund 117.000 auf über 250.000 (Abbildung). Diese Dynamik wird durch die zunehmende Digitalisierung und steigende Anforderungen an IT-Sicherheit getragen. Insbesondere die Corona-Pandemie, der dadurch

ausgelöste Digitalisierungsschub und die vermehrte Homeoffice-Nutzung können potenzielle Sicherheitslücken aufgedeckt und somit Cybersicherheitsmaßnahmen in den Unternehmen ausgelöst haben.

2024 ist ein Rückgang der absoluten Zahlen zu beobachten: In diesem Jahr werden nur noch rund 203.000 Stellenanzeigen mit Cybersicherheitsbezug verzeichnet – ein Rückgang um etwa 18,4 Prozent im Vergleich zum Vorjahr. Auffällig ist dabei jedoch, dass der relative Anteil an der Gesamtzahl der Stellenanzeigen mit 1,59 Prozent nahezu auf dem Niveau von 2022 bleibt. Insgesamt haben Unternehmen im Jahr 2024 aufgrund der schwächelnden Konjunktur weniger Stellen ausgeschrieben (Tiedemann/Risius, 2025). Der Rückgang der absoluten Anzahl von Cyber-Stellenanzeigen ist vor diesem Hintergrund nicht auf eine sinkende Relevanz der Thematik selbst zurückzuführen.

Ein genauerer Blick auf die ausschreibenden Unternehmen zeigt, dass besonders Behörden mit Sicherheits- und Kriminalitätsbezug sowie Unternehmen aus den Bereichen Energieversorgung und Verteidigung Fachkräfte mit Cybersicherheitskompetenzen suchen. Dies verdeutlicht, dass Cybersicherheit gerade im Bereich

der Kritischen Infrastrukturen (KRITIS) elementar ist – was auch durch die stärkere Regulierung der KRITIS belegt ist. Auch Unternehmen – vor allem große – aus den Branchen IT, Beratung und Automotive möchten gemessen an der Zahl der Online-Stellenanzeigen viele Personen mit Cybersicherheitskompetenzen einstellen. Cyber-Fachkräfte werden grundsätzlich von vielen verschiedenen Unternehmen unterschiedlichster Branchen gesucht, auch weil ihre Kompetenzen vielseitig eingesetzt werden können – etwa in den Bereichen Datenmanagement oder Künstliche Intelligenz (KI).

Zukünftige Herausforderungen

KI wird im Bereich der Cybersicherheit zunehmend zu einem entscheidenden Faktor. KI-Systeme können Cyberangriffe schnell erkennen und automatisiert darauf reagieren. Vor allem Methoden des maschinellen Lernens, die Mustererkennung und Anomaliedetektion nutzen, ermöglichen eine effizientere Überwachung von IT-Systemen (Sarker, 2021). Dadurch können IT-Fachkräfte entlastet werden, die sich auf komplexere sicherheitsrelevante Fragestellungen konzentrieren. Allerdings verschärft KI auch die Cyber-Bedrohungslage für die Wirtschaft. So nutzen Cyberkriminelle ebenfalls KI, um Angriffe zu skalieren, gezielter durchzuführen oder automatisiert Sicherheitslücken zu finden und auszunutzen. Beispielsweise kann KI Phishing-Angriffe immer überzeugender gestalten, wodurch die Risiken für Unternehmen und ihre Beschäftigten steigen. Es entsteht somit ein regelrechtes „Wettrüsten“ zwischen defensiven und offensiven KI-Anwendungen im Cyberraum (Hidalgo, 2025).

Auch deshalb dürfte die Nachfrage nach Cybersicherheitskompetenzen auch zukünftig hoch bleiben. Zu einer steigenden Nachfrage tragen außerdem die zunehmenden regulatorischen Anforderungen an die Unternehmen bei – etwa im Rahmen der NIS-2-Richtlinie. Um den neuen Vorgaben hinsichtlich erweiterter Meldepflichten und umfassenderer Sicherheitsmaßnahmen gerecht zu werden, brauchen Unternehmen verstärkt qualifizierte Fachkräfte.

Um den steigenden Bedarf zu decken, sind gezielte Maßnahmen erforderlich, die auf mehreren Ebenen ansetzen müssen. Unternehmen, Politik und Bildungsinstitutionen sollten gemeinsam agieren, um die

Cybersicherheitskompetenzen nachhaltig zu stärken. Investitionen in Aus- und Weiterbildung, Umschulung sowie internationale Fachkräftenwerbung sind essenziell, damit Cybersicherheit als Wirtschaftsfaktor nicht an fehlendem Personal scheitert.

Literatur

Bitkom, 2024a, Wirtschaftsschutz 2024, <https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cyber-crime.pdf> [8.4.2025]

Bitkom, 2024b, IT-Fachkräfte 2040: Wo steht die deutsche Wirtschaft?, Berlin, <https://www.bitkom.org/sites/main/files/2024-04/240411Bitkom-Charts-IT-Fachkraeftemangel-2040final.pdf> [8.4.2025]

Bitkom, 2024c, Erstmals mehr als 10 Milliarden Euro für Deutschlands Cybersicherheit, <https://www.bitkom.org/Presse/Presseinformation/10-Milliarden-Euro-Deutschlands-Cybersicherheit> [16.4.2025]

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2024, Die Lage der IT-Sicherheit in Deutschland 2024, Bonn

Büchel, Jan / Engler, Jan Felix / Mertens, Armin / Küper, Malte, 2025, Die Energiewende als Jobmotor. Nachgefragte Arbeitskräfte für die erneuerbaren Energien und die Energieinfrastruktur, Köln

Büchel, Jan / Engler, Jan Felix, 2024, Generative KI in Deutschland. Künstliche Intelligenz in Gesellschaft und Unternehmen, IW-Report, Nr. 23, Köln

Hidalgo, Álvaro, 2025, Smarter Threats, Smarter Defenses: The AI Arms Race in Cybersecurity, <https://www.cyberproof.com/blog/smarter-threats-smarter-defenses-the-ai-arms-race-in-cybersecurity/> [16.4.2025]

Sarker, Iqbal, 2021, CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks, <https://doi.org/10.48550/arXiv.2104.08080> [16.4.2025]

Tiedemann, Jurek / Risius, Paula, 2025, Jahresrückblick 2024 – Engpässe für Energiewende trotz sinkender Fachkräftelücke, Köln