Markus Schneider, Elias Heftrig, Sinisa Dukanovic, Thomas Dexheimer

Weiterbildung zur Cybersicherheit

Angesichts der Bedrohungslage und zunehmender Risiken kommt es nicht nur auf technische Schutzmaßnahmen an, sondern auch auf das Wissen und die erworbenen Fähigkeiten der handelnden Akteure in Bezug auf Cybersicherheit. Jedoch entwickelt sich Cybersicherheitswissen rasant weiter und kann auch schnell altern. Um Schritt zu halten und Anforderungen erfüllen zu können, ist kontinuierliche Weiterbildung notwendig. Nichtwissen und falsches Handeln können schwerwiegende Folgen haben. Doch unterschiedliche Aufgaben erfordern verschiedene Kompetenzen.

Dr.-Ing. Markus Schneider

ist stellvertretender Institutsleiter und Leiter der Weiterbildung Cybersicherheit am Fraunhofer SIT & Nationalen Forschungszentrum für Angewandte Cybersicherheit ATHENE in Darmstadt.
E-Mail:
markus.schneider@sit.fraunhofer.de

Elias Heftrig, M.Sc.,

ist Mitarbeiter am Fraunhofer SIT & Nationalen Forschungszentrum für Angewandte Cybersicherheit ATHENE in Darmstadt im Bereich Weiterbildung Cybersicherheit.

E-Mail: elias.heftrig@sit.fraunhofer.de

Dipl.-Inform. Sinisa Dukanovic

ist Mitarbeiter am Fraunhofer SIT & Nationalen Forschungszentrum für Angewandte Cybersicherheit ATHENE in Darmstadt im Bereich Weiterbildung Cybersicherheit.
E-Mail:
sinisa.dukanovic@sit.fraunhofer.de

Dipl.-Inform. Thomas Dexheimer

ist Mitarbeiter am Fraunhofer SIT & Nationalen Forschungszentrum für Angewandte Cybersicherheit ATHENE in Darmstadt im Bereich Weiterbildung Cybersicherheit.
E-Mail:
thomas.dexheimer@sit.fraunhofer.de

1 Die Ausgangslage

Die Anforderungen an Organisationen in Bezug auf Cybersicherheit haben sich in den letzten Jahren dramatisch verändert. Der Versicherungskonzern Allianz sieht in Cyberangriffen weltweit das größte Geschäftsrisiko für Organisationen.[1] Laut BSI ist die Lage bzgl. Cybersicherheit sehr angespannt.[2] Der Digitalisierungstrend hat die Angriffsfläche für Organisationen stark vergrößert; die Schäden durch Cyberangriffe können immens sein. Sie können kritisch für die Erreichung von zentralen Organisationzielen sein und sogar Wettbewerbsfähigkeit und Existenz bedrohen. Die Entwicklung und Nutzung neuer Technologien schreitet schnell voran, ebenso wie die Weiterentwicklung des Ökosystems auf Angriffsseite in der Cyberkriminalität. Neue Angriffsmethoden gehen mit neuen Kaskadenrisiken einher, z. B. durch Manipulationen in Lieferketten. Daraus entstehen große Herausforderungen, will man eine Organisation gegen diese Bedrohungen wappnen.

Angemessene technische Vorkehrungen sind unerlässlich, sie sind jedoch für den wirksamen Schutz von Organisationen meistens nicht hinreichend. Es braucht Menschen, die auf für sie relevante Aspekte der Cybersicherheit gut vorbereitet sind und über das notwendige Wissen verfügen, so dass sie für ihre Organisation geeignete Entscheidungen treffen können. Die Perspektiven, Aufgaben, Profile und Ziele dieser Personen unterscheiden sich bisweilen deutlich. Entscheidungen im Zusammenhang mit Cybersicherheit werden in der Praxis auf verschiedenen Organisationsebenen getroffen, von der Führungsebene für strategische Belange bis hin zu technisch-operativen Einheiten.

Dem stehen der Fachkräftemangel für Cybersicherheitsaufgaben und die damit einhergehende Überlastung des vorhandenen Personals gegenüber. Hinzu kommt das Erfordernis, das in der Organisation vorhandene Cybersicherheitswissen auf dem aktuellen Stand zu halten. Die Dynamik der Wissensentwicklung in der Cybersicherheit als Querschnittsthema ist höher als in ande-

1 Allianz: Allianz Risk Barometer – Identifying the major business risks for 2025. Januar 2025, https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

2 BSI: Die Lage der IT-Sicherheit in Deutschland 2024. 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

ren Bereichen der Informations- und Kommunikationstechnologie: Für neue Anwendungstechnologien ist zwangsläufig neues Wissen relevant, Obsoleszenzzeiträume sind kürzer, neue Rechtsakte verlangen Reaktionen.

Gute und einschlägige Ausbildungen, wie z.B. ein Informatikstudium, sind zwar notwendig, jedoch können diese das erforderliche Wissen angesichts der Entwicklungsdynamik und der Spezialisierung der Anforderungen der Praxis nicht über längere Zeiträume abdecken. Deshalb sind neben einer guten Ausbildung Weiterbildungen wichtig. Aufgrund des großen Bedarfs an Weiterbildungen ist inzwischen am Markt ein großes und unübersichtliches Angebot entstanden.

2 Cybersicherheitswissen abstrakt

Im Folgenden gehen wir auf besondere Aspekte des Wissens in der Cybersicherheit ein, die Implikationen für den Bedarf an Weiterbildungen haben, und vergleichen diese mit anderen IuK-Bereichen.

2.1 Klassifikation nach Lebenszyklen

Bei den Lebenszyklen des Wissens gehen wir von folgender Klassifikation aus:

- **Kurzfristiges Wissen:** Inhalte in dieser Wissenskategorie entstehen in der Regel *ad hoc* und können unverzügliche Reaktion erfordern. Beispiele sind potenzielle Bedrohungsinformationen aufgrund gefundener Schwachstellen. Solche Inhalte können auch nach kurzer Zeit wieder veraltet sein, z. B. innerhalb weniger Wochen und Monate wie etwa bei Workarounds zur Absicherung von Schwachstellen, bis Patches oder Updates zur Verfügung stehen.
- **Mittelfristiges Wissen:** Inhalte dieser Wissenskategorie entstehen in etwas größeren zeitlichen Abständen. Üblicherweise erfordern sie in den meisten Fällen keine sofortige Reaktion, sondern erlauben Planungen mit zeitlichem Vorlauf. Typische Beispiele für diese Kategorie sind neue Anwendungstechnologien, aus denen sich neben neuen Funktionen auch neue Bedrohungen ergeben, oder neue Cybersicherheitswerkzeuge bzw. neue Versionen von Werkzeugen. Die Zeiträume, in denen solches Wissen altert, können bei wenigen Jahren liegen. Auch neue rechtliche Vorgaben können dieser Kategorie zugeordnet werden.
- **Langfristiges Wissen:** Solches Wissen hat üblicherweise viele Jahre Bestand. Dazu gehören Grundlagen wie kryptographische Primitive und Protokolle oder grundlegende Prinzipien wie etwa *Separation of Duties*, *Least Privilege* oder *Need to Know*. Solches Wissen wird in der Regel im Studium vermittelt und strukturiert bei Fachkräften die mentalen Modelle für das effektive und effiziente Erlernen und Einordnen von Inhalten des mittel- und kurzfristigen Wissens.

Viele der Inhalte, die für die Abwehr von kritischen Bedrohungen relevant sind, gehören zur Kategorie des mittel- und kurzfristigen Wissens. Angemessene Weiterbildungen der Fachkräfte tragen hier zur Reduktion von Risiken bei. Auch wenn kurzfristiges Wissen, wie z. B. Informationen zu Zero Day Exploits, auch außerhalb von Weiterbildungen aufgebaut werden muss, so tragen kontinuierliche Weiterbildungen dazu bei, dass Fachkräfte selbständig entsprechende Ereignisse einordnen und adäquat reagieren können.

2.2 Einflussfaktoren und Entwicklungsdynamik

Es gibt eine Reihe von Faktoren, die die Entwicklungsdynamik und die Weiterentwicklung des Cybersicherheitswissens und den damit verbundenen Bedarf nach Weiterbildungen in der Cybersicherheit vorantreiben. Im Folgenden werden einige dieser Einflussfaktoren dargestellt:

- **Fachkräftemangel und Überlastung:** Der Mangel an Cybersicherheitsfachkräften besteht bereits seit vielen Jahren.[3,4] Im Jahr 2024 lag die Lücke weltweit bei ca. 4,8 Millionen Fachkräften bei insgesamt ca. 5,5 Millionen Beschäftigten.[5] Daraus folgt zwangsläufig eine Überlastung für die beschäftigten Personen. Hinzu kommt, dass der Umfang der Aufgaben nicht geringer wird. So ist beispielsweise die Anzahl registrierter CVE drastisch angestiegen.[6] Waren es im Jahr 2016 noch 6.500 CVE, so wurden 2023 bereits 29.200 registriert. In den letzten 25 Jahren hat sich die Anzahl der jährlich gefundenen CVE jeweils über Zeiträumen von 4-5 Jahren ungefähr verdoppelt. Dabei ist die Anzahl der als kritisch und hoch bewerteten CVE ähnlich stark gestiegen wie die Zahl der CVE insgesamt; deren Anteil liegt bei ca. 40%-43%. Die verfügbaren Fachkräfte müssen dies bewältigen. Mit wichtigen und jeweils aktualisierten Fachkenntnissen kann ihnen das effektiver und effizienter gelingen, so dass sich durch Weiterbildung Überlastungen reduzieren lassen, da sie in kürzerer Zeit richtige Entscheidungen treffen können.
- **Angriffsfläche und Komplexität:** Die Digitalisierung hat die Angriffsfläche für Organisationen deutlich vergrößert. Neue Technologien werden zügig übernommen, was zu neuen Einstiegsstellen für Angriffe führt. Anwendungen sind üblicherweise offen für technische Integration. Neue IT-Architekturen in Verbindung mit verschiedenen Hosting-Modellen tragen dazu bei, dass IT-Systeme für die Bewertung der Cybersicherheit unübersichtlich werden.[7,8] Dies geht einher mit gewachsenen, heterogenen Systemlandschaften, Dokumentationsdefiziten, verschiedenen Betriebssystemen und Programmiersprachen, mehr Schnittstellen und Abhängigkeiten.
- **Technologische Entwicklung:** Die technologische Entwicklung wird von neuen Funktionen und dem Druck des Marktes vorangetrieben. Mit neuen Produkten und Diensten ergeben sich zwangsläufig auch neue Angriffsmöglichkeiten. Diese Entwicklungsdynamik führt dazu, dass es auch für Universitäten herausfordernd ist, mit der Weiterentwicklung der Cur-

3 R. Vogel: Closing the Cybersecurity Skills Gap. Salus Journal, Vol. 4, No. 2, 2016, https://journals.csu.domains/index.php/salusjournal/article/view/59/54

4 Robert R. Ackermann: Too few cybersecurity professionals is a gigantic problem for 2019. Techcrunch. 27. Januar 2019, https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/

5 ISC²: Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen. September 2024, https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen

6 Siehe https://www.cve.org

7 N. Gelernter, H. Schulmann, M. Waidner: External Attack-Surface of Modern Organizations. Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, 2024

8 Verizon: 2025 Data Breach Investigations Report – Executive Summary. Verizon, 2025, https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf

ricula Schritt zu halten, so dass die grundständige Ausbildung oft nicht hinreichend schnell auf die Anforderungen der Industrie reagieren kann.[9] Doch auch wenn Curricula schnell angepasst werden, vergeht Zeit, bis die universitäre Ausbildung hinreichend viele Fachkräfte auf den Markt bringt.[10] Um dies abzufedern, braucht man berufsbegleitende Weiterbildungen.

- **Asymmetrie:** Cybersicherheit ist geprägt durch einen Wettlauf zwischen Verteidiger- und Angreiferseite. Um hinreichend schnell reagieren zu können, braucht die Defensive aktuelles Wissen. Sie muss alle Angriffswege im Blick haben und diese absichern; ein Angreifer hingegen muss nur einen Einstiegspunkt finden.
- **Bedrohungslandschaft:** Angreifer agieren stark professionalisiert. Es hat sich inzwischen eine international agierende Schattenwirtschaft für kriminelle Leistungen zu Cyberangriffen entwickelt. Auch im Jahr 2024 haben in Deutschland Angriffe, insbesondere mit Ransomware, weiter stark zugenommen.[11] Das für Kriminelle sehr einträgliche und risikoarme Handeln hat dazu geführt, dass inzwischen jede größere kriminelle Vereinigung im Bereich Cyberkriminalität aktiv ist.[12] Die Bedrohungslage verschärft sich weiter durch die geopolitische Lage und durch zwischenstaatliche Konflikte.
- **Regulatorische Anforderungen:** Für Organisationen gibt es immer mehr verbindliche Rechtsakte mit Bezug zur Cybersicherheit, z. B. die Datenschutzgrundverordnung, den Cyber Resilience Act oder NIS2. Fachkräfte müssen diese Anforderungen kennen und verstehen, wie diese unter Berücksichtigung weiterer Erfordernisse, wie z. B. deren Wirtschaftlichkeit, erfüllt werden können. Dies kann dazu führen, dass erprobte Vorgehensweisen plötzlich angepasst werden müssen.

Diese Einflussfaktoren machen Cybersicherheit zu einem der am schnellsten evolvierenden Felder in der IuK-Technologie. Dies verlangt, dass Fachkräfte bereit für lebenslanges Lernen sein müssen, dass ihre Arbeitgeber in die Weiterbildung investieren und dass auch die Weiterbildungsanbieter ihre Angebote bedarfsorientiert weiterentwickeln. Das effektive Zusammenwirken dieser Rollen trägt zur Wettbewerbsfähigkeit in Deutschland und Europa bei.[13] Gerade bei unvorhergesehenen Technologiesprüngen ist die kurzfristige Weiterentwicklung des Wissenskanons jedoch herausfordernd.[14]

2.3 Vergleich

Der Vergleich in Tabelle 1 unterstreicht, warum gerade für Weiterbildungen in der Cybersicherheit ein besonderer Bedarf besteht.

Tab. 1 | Vergleich des Weiterbildungsbedarfs in der Cybersicherheit mit anderen IuK-Bereichen

	Cybersicherheit	Andere IuK-Bereiche
Evolutionstreiber	Bedrohungslage	Marktanforderungen, Funktionen
Vorhersehbarkeit	Geringer	Höher
Halbwertszeit taktisches Wissen	Wenige Monate	Wenige Jahre
Halbwertszeit strategisches Wissen	Wenige Jahre	Viele Jahre
Reaktionszeit	Kurz	Länger
Dokumentation	Oft unvollständig	Umfangreich, strukturiert
Obsoleszenz	Abruptes Aufgeben	Gradueller Übergang

Dies verdeutlicht, dass Weiterbildungen in der Cybersicherheit in kürzeren Zyklen notwendig sind, als dies in anderen IuK-Bereichen der Fall ist. Was gestern noch nach kanonischem Wissen korrekt war, kann morgen obsolet sein. Wissen muss regelmäßig auf den aktuellen Stand gebracht werden.

3 Adressaten für Weiterbildung

War Cybersicherheit früher den IT-Abteilungen vorbehalten, so ist es heute für verschiedene Funktionsträger in Organisationen relevant. Hierzu zählen neben den für die operative Cybersicherheit verantwortlichen Personen, wie z. B. IT-Administratoren, auch Personen, die in der strategischen Planung von Organisationen aktiv sind. Für die Risikovorsorge in Organisationen und die hierfür notwendige Verbesserung der Widerstandsfähigkeit gegen Cyberangriffe sind zahlreiche präventive Maßnahmen notwendig, die geplant und organisiert werden müssen. Hierfür trägt die Ebene der Entscheider die Verantwortung. Aber auch IT-Anwender ohne technischen Hintergrund tragen zur Sicherheit ihrer Organisation bei, indem sie Fallen erkennen (z. B. Phishing) und somit zur Abwehr von Angriffsversuchen beitragen.

Da Cybersicherheit ein Querschnittsthema ist, hat es längst große Bedeutung für viele verschiedene Rollen und Aufgaben in Organisationen, nicht mehr nur für stark technisch orientierte Mitarbeitende. Die entsprechenden Weiterbildungen müssen sich inhaltlich an den jeweiligen Zielgruppen orientieren.

4 Verpflichtungen zur Weiterbildung

Weiterbildungen zur Cybersicherheit, z. B. als Schulungen, Übungen oder Trainings, sind nach verschiedenen Rechtsakten für Organisationen verpflichtend. Die spezifische Verantwortung innerhalb einer Organisation zur Erfüllung dieser Anforderungen kann auf verschiedene Rollen verteilt sein (z. B. IT-Sicherheitsbeauftragte, Datenschutzbeauftragte, CISO). Die Gesamtverantwortung im Rahmen der Organisationsverpflichtungen liegt bei der Geschäftsführung oder dem Vorstand. Diese sind üblicherweise auch verpflichtet, die Ressourcen für notwendige Weiterbildungsmaßnahmen zur Verfügung zu stellen (Zeit, Finanzierung). Bei Vernachlässigung von Sorgfaltspflichten, aus denen sich Schäden für die Organisation ergeben, können auch persönliche Haftungsrisiken entstehen, z. B. nach § 93 AktG oder § 43 GmbHG. Weitere Beispiele für Weiterbildungsverpflichtungen bestehen nach dem IT-Sicherheitsgesetz 2.0 mit § 2 Abs. 2 und § 8a, sowie

9 S. Ramezanian, V. Niemi: Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development. IEEE Access, Vol. 12, 2024

10 R. Walendy, M. Weber, S. Becker, C. Paar, N. Rummel: An Evidence-Based Curriculum Initiative for Hardware Reverse Engineering Education. 56th ACM Technical Symposium on Computer Science Education, Februar 2025

11 Siehe Fußnote 2

12 Peter Lau: What, the Hack! brand eins, September 2024, https://www.brandeins.de/corporate-services/projekte/g-data-cybersicherheit-in-zahlen/cybersicherheit-in-zahlen-2024-what-the-hack

13 Fazak Rizvi: Risk Society and Its Implications for Rethinking Lifelong Learning. In K. Evans et al. (eds.): Third International Handbook of Lifelong Learning, Springer International Handbooks of Education, Springer Nature, 2023

14 Jordan Allison: The System's Holding Me Back: Challenges of Teaching Computing in Further Education. 2020 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, 2021

der DSGVO mit Art. 32 Abs.1, Art. 39 Abs. 1 lit. b und Art. 47. Abs. 2 lit. n. Darüber hinaus können branchenspezifische Anforderungen bestehen.

Schulungsteilnahmen sollten im Rahmen von Nachweispflichten dokumentiert und der Wissenstand der Mitarbeitenden aufgrund der hohen Evolutionsdynamik regelmäßig aktualisiert werden.

5 Entwicklungen bei Weiterbildungen

Der Mangel an Fachkräften in der Cybersicherheit, häufig unzureichende Vorbereitungen im Studium auf die Anforderungen der Wirtschaft und der große Bedarf an Weiterbildungen gliedern sich ein in den allgemeinen Fachkräftemangel bei technischen Fächern, wie z. B. den Rückgang der Studienanfänger und die Kritik an der ingenieurwissenschaftlichen Ausbildung in Zukunftsfeldern.[15] Prognosen verheißen wenig Verbesserung an der jetzigen Ausgangslage.[16]

Weiterbildungswissen baut üblicherweise auf dem Grundlagenwissen auf, welches in Ausbildungen vermittelt wurde. Beide Säulen sollen zusammen die anwendungsorientierten Anforderungen von Organisationen stützen, z. B. aus der Wirtschaft oder Behörden. Die von den Organisationen geforderten Kompetenzen sind jedoch vielschichtig und unterscheiden sich jeweils nach den Aufgaben und Funktionen der jeweiligen Personen. In einer in den USA bereits vor mehreren Jahren durchgeführten Untersuchung hat sich herausgestellt, dass die Ausbildung auch an vielen US-amerikanischen Top-Universitäten den anwendungsorientiert ausgerichteten Anforderungen von Organisationen in Bezug auf Cybersicherheit nicht mehr genügt hat.[17] Da man in den

15 Michael Rose: Der lange Abstieg des deutschen Ingenieurs. Frankfurter Allgemeine, 26.5.2025, https://www.faz.net/aktuell/wirtschaft/warum-deutschland-den-anschluss-bei-zukunftstechnologien-verliert-110494175.html

16 M. Pröbster, J. Ehrenreich, G. Käßer-Pawelka, N. Marsden: Beyond Future Skills: Developing Company Personas in Disruptive Transformation Processes. Human-Computer Interaction (HCII 2024), LNCS 14684, Springer, 2024

17 Sarah White: Top U.S. universities failing at cybersecurity education. CSO Online, 25. April, 2016, https://www.csoonline.com/article/555881/top-u-s-uni-

bestehenden Defiziten und dem Fachkräftemangel ein nationales Sicherheitsproblem gesehen hat, wurde in den USA die Initiative *NICE* (National Initiative for Cybersecurity Education) ins Leben gerufen, die vom US-amerikanischen National Institute of Standards and Technology (NIST) organisiert wird.[18] Durch NICE wurde ein abstraktes Kompetenzrahmenwerk erarbeitet, welches die Ausbildung und Weiterbildung in der Cybersicherheit für unterschiedliche Aufgaben in Organisationen strukturiert.[19, 20] Das Rahmenwerk liegt inzwischen in mehreren Revisionen vor; die aktuelle Fassung aus dem Jahr 2025 enthält 41 sogenannter *Work Profiles*, für welche jeweils unterschiedliche Kompetenzen relevant sind, die in Aus- und Weiterbildung behandelt werden sollen.[21]

Eine solche Strukturierung kann in der Praxis hilfreich sein; beispielsweise hilft es Anbietern aus dem Bildungssektor bei der Entwicklung ihrer Curricula, aber auch denjenigen, die für ihre Mitarbeitenden oder für sich selbst in einem unübersichtlichen Markt die passenden Weiterbildungen suchen. Weiterbildungen können sich inhaltlich hinsichtlich vieler Kriterien unterscheiden, z. B. nach der *Zielgruppe* (IT-Fachkräfte mit/ohne Fokus Cybersicherheit, Führungskräfte mit/ohne IT-Hintergrund, Themenverantwortliche Recht/Compliance, IT-Einsteiger), dem *Qualifikationsniveau* (von einfach bis hochspezialisiert), der *Perspektive* (defensiv, offensiv), der *Konzeption* (theoretisch, praktisch, interaktiv), dem *Branchenbezug* (spezifisch für z.B. Health, Banking, Energy, übergreifend) oder dem *Durchführungsrahmen* (präsenz, remote, synchron, self-paced).

In Anlehnung an NICE ist man auch in Europa aktiv geworden und hat das *EU Cybersecurity Skills Framework* (ECSF) entwickelt.[22] Dieses enthält 12 Profile für unterschiedliche Kompetenzen mit unterschiedlichen Schulungsinhalten. In Deutschland steht die Übernahme des ECSF noch am Anfang und es noch nicht abzusehen, ob es sich durchsetzen wird.

Aufgrund der hohen Entwicklungsdynamik in der Cybersicherheit kann man annehmen, dass diese Profile mit ihren Kompetenzen immer wieder verändert und angepasst werden müssen, wie dies auch bereits in der Vergangenheit der Fall war.

Auch andere Länder wie etwa China sehen in der Aus- und Weiterbildung eine zentrale Säule ihrer nationalen Cybersicherheitsstrategie und forcieren diese Entwicklung, da sie Cybersicherheit als Schlüsselkomponente für ihre Innovations- und Wettbewerbsfähigkeit verstehen.[23]

Neben hoher inhaltlicher Qualität wünschen sich Organisationen von den Weiterbildungsangeboten, dass diese inhaltlich zügig auf aktuelle Erkenntnisse reagieren und dass Formate angeboten werden, die sich gut in die praktische Arbeitswelt integrieren lassen und auch zu den Rahmenbedingungen von kleinen und mittleren Unternehmen passen.[24] Von mehr praktischen Komponenten bei der Vermittlung von angewandten Themen erwartet man schnellere und effektivere Lernerfolge.[25, 26]

6 Fazit

Zur Vermeidung von Organisationsverschulden müssen Organisationen darauf achten, dass ihre Mitarbeiterinnen und Mitarbeiter über relevante Fähigkeiten und Wissen in der Cybersicherheit verfügen. Weiterbildungen und die Bereitschaft zum lebenslangen Lernen werden wichtiger. Dem stehen der Mangel an Fachkräften für Cybersicherheit und die „Halbwertszeit" des Wissens vorhandener Fachkräfte gegenüber. Daher müssen Organisationen nicht nur in Hardware, Software und Dienste, sondern auch in Köpfe investieren; und dies angesichts des Fachkräftemangels auch mit dem Risiko, dass man damit die eigenen Fachkräfte, in deren Fähigkeiten man investiert hat, auch attraktiver für potenzielle Wettbewerber macht. Angesichts der immensen Bedrohungen im Cyberraum erscheint dieses Risiko jedoch alternativlos. Der Weiterbildungsmarkt ist inzwischen für die Adressaten sehr unübersichtlich geworden und befindet sich in stetem Wandel, wie die Cybersicherheit selbst. Anbieter von Weiterbildungen sind gefordert, ihre Inhalte auf die Bedarfe abzustimmen und ihre Angebote für die Zielgruppen transparent zu gestalten.

versities-failing-at-cybersecurity-education.html

18 Siehe https://www.nist.gov/itl/applied-cybersecurity/nice

19 R. Petersen, D. Santos, M.C. Smith, K.A. Wetzel, G. Witte: Workforce Framework for Cybersecurity (NICE Framework), Revision 1. NIST Special Publication 800-181, November 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

20 K.A. Wetzel: NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce. Juni 2023, https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8355.pdf

21 Siehe https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions#Publications%20 und https://www.nist.gov/document/nice-framework-components-v200

22 Siehe https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/ad-hoc-working-group-on-the-european-cybersecurity-skills-framework-2023-2025

23 Die Primärquellen der chinesischen Regierung wie etwa die Nationale Cybersicherheitsstrategie von 2016 oder der 14. Fünfjahresplan 2021-25 liegen nicht in Übersetzungen vor, so dass hier nur auf Sekundärquellen verwiesen werden kann wie z.B. Meijiea Chen, Fahong Yu: Research and Practice of Value-added Assessment for Cultivating Cybersecurity Talents in Higher Vocational Colleges. Proceedings of the 2024 3rd International Conference on Artificial Intelligence and Education (ICAIE '24), ACM, April 2025; Junfeng Diao, Xiaoqi Tang, Xu Ding: How do nations around the world navigate the digitalization of vocational education policies? Education and Information Technologies, Springer, April 2025

24 M. Eisenschink, C. Glück, M. Maier, E. Scheuchenpflug, H. Timinger, M. Martens: A new trend in further education? Micro-degrees as a contribution to deal with new paradigms in SMEs. IEEE German Education Conference, 2022

25 G. Gerontakis, I. Voyiatzis, P. Yannakopoulos: Security Operations Center in Education: Building an Educational Environment for Attack and Defense Scenarios. Proceedings of the 26th Pan-Hellenic Conference on Informatics, November 2022, ACM 2022

26 https://www.sit.fraunhofer.de/de/weiterbildungen-allgemein/