Akkreditierungsbericht

Hochschule	HAW Kiel, Fachbereich Wirtschaft			
Studiengang (Name/Bezeichnung) ggf. inkl. Namensänderungen	**Cybersicherheit**			
Abschlussgrad / Abschlussbezeichnung	**Bachelor of Science (B.Sc.)**			
Studienform	Präsenz	☒	Fernstudium	☐
	Vollzeit	☒	Intensiv	☐
	Teilzeit	☐	Joint Degree	☐
	Dual	☐	Kooperation § 19 MRVO	☐
	Berufs- bzw. ausbildungsbegleitend	☐	Kooperation § 20 MRVO	☐
	Industriebegleitet	☐		
Studiendauer (in Semestern)	7 Semester			
Anzahl der vergebenen ECTS-Punkte	210			
Bei Master: konsekutiv o. weiterbildend				
Aufnahme des Studienbetriebs	Wintersemester 2026/27			
Aufnahmekapazität pro Jahr (Max. Anzahl Studierende)	30			
Durchschnittliche Anzahl der Studienanfänger pro Jahr	Studienbetrieb hat noch nicht begonnen			
Durchschnittliche Anzahl der Absolvent*innen pro Jahr	Studienbetrieb hat noch nicht begonnen			

Akkreditierung	☒
Reakkreditierung Nr. (Anzahl)	Erstakkreditierung

Akkreditierungsbericht vom	19. Dezember 2025 Stand: 19.01.2026

Inhalt

Verfahren und Grundlagen der Akkreditierung

Verfahren:

Die HAW Kiel ist seit 2013 systemakkreditiert. Die implementierten Verfahren der Akkreditierung (Reakkreditierung) gewährleisten, dass die Studiengänge der HAW Kiel den aktuellen Standards and Guidelines for Quality Assurance in the European Higher Education Area sowie dem Hochschulgesetz (SH) und der Studienakkreditierungsverordnung SH 2018 entsprechen. Im Akkreditierungsprozess wird geprüft, ob alle Studiengänge der Hochschule die notwendigen formalen Kriterien (z.B. Studienstruktur und Studiendauer, Studiengangsprofile oder Modularisierung) sowie die fachlich-inhaltlichen Kriterien (z.B. Qualifikationsziele und Abschlussniveau sowie ein schlüssiges Studiengangskonzept und eine adäquate Umsetzung) erfüllen.

Die Akkreditierungsverfahren werden auf der Basis modellierter Prozesse einheitlich realisiert. Der Prozess/das Verfahren ist analog zu üblichen Programmakkreditierungen entwickelt worden. Die einzelnen Prozessschritte sind von der Studiengangsidee über die Erstellung, Prüfung und Weiterentwicklung des Grob- und Feinkonzepts des Studiengangs bis zum akkreditierten Studiengang abgebildet. Der Prozess wird begleitet durch eine ausgewählte Anzahl unterstützender Dokumente (z.B. Vorlagen zur Gliederung des Grob- und Feinkonzepts, Checkliste für den Selbstbericht, Meilensteinplanung, Informationen für die externen Gutachter*innen/Prüfauftrag), durch die die Fachbereiche und die externen Gutachter*innen bestmöglich in ihrer Arbeit unterstützt werden sollen.
Die Gruppe der Gutachter*innen wird entsprechend der erforderlichen Fachlichkeit zusammengestellt und setzt sich aus mindestens drei professoralen Gutachter*innen (i.d.R. Universität und zwei einer HAW/Fachhochschule), einer*einem Vertreter*in aus der einschlägigen Berufspraxis und einer*einem Student*in (extern, entsandt durch den studentischen Akkreditierungspool) zusammen.

Die Vorortbegehung dauert einschließlich der Vorbereitung der Gutachter*innen 1,5 Tage.

Grundlagen:

Staatsvertrag über die Organisation eines gemeinsamen Akkreditierungssystems zur Qualitätssicherung in Studium und Lehre an deutschen Hochschulen (Studienakkreditierungsvertrag)

Landesverordnung zur Regelung der Studienakkreditierung des Landes Schleswig-Holstein (Studienakkreditierungsverordnung SH)

Hochschulgesetz Schleswig Holstein.

Ergebnisse auf einen Blick

Studiengang: Cybersicherheit, B. Sc.

Entscheidungsvorschlag zur Erfüllung der formalen Kriterien gemäß Prüfbericht:
Die formalen Kriterien sind erfüllt *(siehe Darstellung in Kapitel 1).*

Entscheidungsvorschlag des Gutachtergremiums zur Erfüllung der fachlich-inhaltlichen Kriterien gemäß Gutachten:
Die fachlich-inhaltlichen Kriterien sind erfüllt *(siehe Darstellung in Kapitel 2).*

Die Gutachter*innen sprechen folgende **Empfehlung** aus:

Empfehlung 1: Es wird empfohlen, die Angabe der Lehrsprachen im Diploma Supplement kritisch zu prüfen. Sollten dort künftig zwei Lehrsprachen ausgewiesen werden, müsste im Wahlbereich mindestens ein entsprechendes Lehrangebot in englischer Sprache integriert werden.

Informationen zur Hochschule und zur Einbettung des Studiengangs

Die HAW Kiel entstand 1969 aus dem Zusammenschluss mehrerer staatlicher Ingenieurschulen und Höherer Fachschulen. In der Geschichte ihrer Vorgängerbereiche kann sie jedoch auf eine über 100-jährige Tradition zurückblicken. Ihr Campus liegt direkt an der Förde. Frischen Wind gibt es hier gratis, und frische Ideen sind Verpflichtung.
Mit über 7.500 Studierenden ist die HAW Kiel die größte Fachhochschule in Schleswig-Holstein. Leistungsstark, innovativ, regional verankert und international ausgerichtet. Wer hier studieren möchte, kann aus einem breiten Fächerspektrum der Fachbereiche Agrarwirtschaft, Informatik und Elektrotechnik, Maschinenwesen, Medien / Bauwesen, Soziale Arbeit und Kindheitspädagogik, Gesundheit, sowie Wirtschaft wählen. In Kooperation mit Universitäten besteht die Möglichkeit der Promotion u. A. auch im Rahmen des neu geschaffenen Promotionskollegs.
Das Lehr- und Forschungsprofil der HAW Kiel ist geprägt von einer starken Anwendungsorientierung, Interdisziplinarität und einer engen Verzahnung mit der regionalen Wirtschaft und Gesellschaft. Die Fachbereiche Wirtschaft sowie Informatik und Elektrotechnik bilden hierbei zentrale Säulen, die traditionell an der Schnittstelle von Technologie und betriebswirtschaftlicher Anwendung agieren.
Der geplante Bachelor-Studiengang „Cybersicherheit" fügt sich nahtlos und mit hoher Priorität in das Studienangebot der Hochschule ein. Mit dem Studiengang reagiert die HAW Kiel vorausschauend auf eine tiefgreifende und vielschichtige Problemlage, die sich aus ökonomischer Notwendigkeit und gesellschaftlicher Priorität, Fachkräftemangel und einer strategischen Lücke im regionalen Bildungsangebot zusammensetzt.
Durch die Bündelung der Expertisen aus den Fachbereichen Wirtschaft (Management, Organisation, Prozesse, Risikomanagement etc.) und Informatik und Elektrotechnik (technische Systeme, Netzwerke, Kryptografie, Software etc.) verkörpert der Studiengang den interdisziplinären Kern des Hochschulprofils. Er trägt maßgeblich dazu bei, das Profil der Hochschule als führende Institution für angewandte Wissenschaften in einem zukunftsweisenden und gesellschaftlich hochrelevanten Themenfeld zu schärfen und langfristig zu festigen.

Allgemeine Informationen zum Fachbereich (Studienangebot, Personal, Ausstattung) und Kurzporträt des Studiengangs

Der Studiengang wird in einer paritätischen Kooperation der Fachbereiche Wirtschaft sowie Informatik und Elektrotechnik getragen. Beide Fachbereiche verfügen über eine langjährige Expertise in der Ausbildung von Fach- und Führungskräften und weisen ein breites Studienangebot auf.
Der Fachbereich Wirtschaft bietet Bachelor- und Masterstudiengänge insbesondere in Betriebswirtschaft und Wirtschaftsinformatik an. Er zeichnet sich durch eine praxisnahe Lehre aus, die durch zahlreiche Kooperationen mit Unternehmen, den Einsatz von Lehrbeauftragten

aus der Praxis und eine starke Betonung von Projektarbeiten geprägt ist. Personell ist der Fachbereich mit Professorinnen und Professoren aus allen relevanten Feldern der Betriebswirtschaftslehre und Wirtschaftsinformatik ausgestattet. Die sächliche Ausstattung umfasst moderne Seminarräume, PC-Pools und eine umfassende Bibliothek.
Der Fachbereich Informatik und Elektrotechnik deckt mit seinen Studiengängen eine große Bandbreite von der klassischen Informatik/Informationstechnologie/Computer Sciences über Medieningenieurwesen und Wirtschaftsingenieurwesen bis hin zu Mechatronik und Elektrotechnik ab. Der Fachbereich verfügt über eine exzellente personelle Ausstattung mit Expertise in Forschung und Lehre in Bereichen wie technische Systeme, Softwareentwicklung, Datenkommunikation etc. Der Fachbereich verfügt über eine Vielzahl moderner Labore (z. B. für Rechnernetze), die für eine anwendungsorientierte Ausbildung unerlässlich sind.

Kurzprofil des Studiengangs

Hintergrund und Zielgruppe: Durch die Digitalisierung wird IT immer relevanter für Wirtschaft und Gesellschaft, während diese gleichzeitig in immer größerem Maße miteinander vernetzt sind. Die Gefahr von Cyberangriffen durch hochprofessionell, global vernetzt agierende Täter*innen wächst dabei von Jahr zu Jahr. Angriffe können immensen wirtschaftlichen und gesellschaftlichen Schaden erzeugen, wichtige Dienstleistungen lahmlegen und der digitalen Souveränität einer Gesellschaft entgegenstehen. Der geplante Bachelor-Studiengang „Cybersicherheit" richtet sich dabei an Studienbewerber*innen, welche die erforderlichen Kompetenzen zum vernetzten Handeln in der Verteidigung vor Cyberangriffen und der Stärkung der Resilienz von Organisationen gegen solche Angriffe erwerben wollen. Der neue Studiengang bereitet Absolvent*innen dabei auf ein vielfältiges Berufsfeld im privaten oder öffentlichen Sektor vor.
Interdisziplinäre Ausrichtung: Cybersicherheit ist keine rein technische Aufgabe. Stattdessen sind der Schutz von Organisationen inklusive ihrer Daten und Prozesse als Ganzes zu betrachten und dabei neben technischen Themenfeldern auch Aspekte des organisationalen oder individuellen Verhaltens zu berücksichtigen, sowohl bei Angriffen als auch für Schutzmaßnahmen. Der Studiengang Cybersicherheit wird daher gemeinsam vom Fachbereich Wirtschaft und vom Fachbereich Informatik und Elektrotechnik angeboten, hinsichtlich des Lehrangebots sind beide Fachbereiche zu gleichen Anteilen beteiligt. Die Zusammenarbeit dazu wird im Rahmen einer Kooperationsvereinbarung zwischen den Fachbereichen transparent und verbindlich dargestellt.
Inhalte und Aufbau des geplanten Studiengangs: Das Studienkonzept verzahnt in höchstem Maße Theorie und praktische Anforderungen. Es wird ein umfassender Einblick in Aspekte der Cybersicherheit und dem weiteren Themenfeld der digitalen Resilienz von Organisationen gegeben. Die Absolvent*innen des Studiengangs erlernen die notwendigen Kompetenzen aus der Informatik und der Wirtschaftsinformatik, um die Sicherheit und Resilienz von Organisationen, Systemen, Netzwerken und Informationen zu planen und zu gewährleisten. Dieses wird dabei aus strategischer Perspektive (z. B. Management durch CISO und CIO), der Perspektive aus Sicht von Systembetreibenden (z. B. Sicherheit in Netzwerken),

Entwickler*innen (z. B. angewandte Kryptografie), weiteren Fachkräften (z. B. Penetration Testing), regulären IT-Anwender*innen (z. B. Umgang mit Zugangsdaten) aber auch aus

Sicht von Angreifenden (z. B. Durchführung von Social Engineering und Ethical Hacking) anwendungsorientiert betrachtet.
Struktur des Curriculums: Der Studiengang stützt sich stark auf bestehende Module insbesondere aus den Bachelor-Studiengängen Informatik und Wirtschaftsinformatik (105 LP plus Wahlmodule). Um das Thema Cybersicherheit durchgehend im gesamten Studium zu verankern, sind neue Module im Umfang von 30 LP (plus Wahlmodule) vorgesehen: In der Verantwortung des Fachbereichs Wirtschaft insbesondere „Einführung in Cybersicherheit" (1. Semester), „Cybersicherheit und menschliches Verhalten" (2. Semester), „Cybersicherheit und resilienz von Organisationen" sowie „IT-Recht und Datenschutz" (beide 5. Semester); in der Verantwortung des Fachbereichs IuE insbesondere „Grundlagen derKryptografie" (3. Semester) und „Ethical Hacking and Penetration Testing" (4. Semester). Diese Vorlesungen können z. T. auch in anderen Studiengängen als Wahlmodule dienen, um das Thema Cybersicherheit interdisziplinär auch in weiteren Studiengängen der Hochschule besser zu verankern.
Praxisanteile und Vertiefung: Bereits im Laufe des Studiums erhalten die Studierenden regelmäßig die Möglichkeit, ihre Fähigkeiten und neu erlangten Kompetenzen in der Praxis einzusetzen. Der Studiengang beinhaltet ein Praxisprojekt Cybersicherheit im 4. Semester, wo die bisherig erworbenen Kenntnisse und Fähigkeiten in konkreten Aufgabenstellungen z. B. aus Partnerunternehmen erprobt werden. Zudem ist im 6. Semester ein berufspraktisches Studiensemester vorgesehen. Die Studierenden können zudem ihr Interessengebiet in vier Wahlmodulen im 4. und 7. Semester vertiefen und dabei aus einem breiten Curriculum wählen, welches sowohl technische Themen (z. B. Digitale Forensik) als auch ManagementThemen (z. B. Risiko- und Krisenmanagement) vorsieht.

Zusammenfassende Qualitätsbewertung des Gutachtergremiums, Gesamteindruck

Die Gutachter danken herzlich für die Einladung und die insgesamt sehr positiven Eindrücke während des Audits. Besonders hervorzuheben ist die durchdachte inhaltliche Ausrichtung und der gut strukturierte curriculare Aufbau des geplanten Studiengangs Cybersicherheit. Das zugrunde liegende Konzept ist überzeugend, und die Begründung für die Einführung des Studiengangs ist sorgfältig und klar in den Unterlagen aufbereitet. Die Gutachter sind der Ansicht, dass der Studiengang sowohl auf die aktuellen Anforderungen des Arbeitsmarktes als auch auf die Bedürfnisse der Absolvent*innen sehr gut eingeht. Die Module und deren Zusammenstellung wurden ebenfalls positiv bewertet. Der Studiengang ist so konzipiert, dass er praxisorientierte Inhalte gut mit theoretischen Grundlagen kombiniert. Dabei wurde ein hoher Praxisbezug betont, der in der Cybersicherheit von entscheidender Bedeutung ist. Der Bedarf an gut ausgebildeten Fachkräften im Bereich Cybersicherheit ist aus der Perspektive der Gutachter offensichtlich und auch aus der praktischen Erfahrung heraus sehr groß. Der

Kontakt zwischen den Lehrenden und den Studierenden der beiden beteiligten Fachbereiche scheint sehr gut zu sein, was sich positiv auf die Zufriedenheit der Studierenden auswirkt.

Trotz dieser insgesamt sehr positiven Einschätzungen gibt es einige Hinweise, Impulse und eine Empfehlung, die zur weiteren Verbesserung des Studiengangs beitragen könnten. Ein wesentlicher Aspekt ist die Notwendigkeit, die Absolventen mit Kompetenzen auszustatten, die sie dazu befähigen, sich auch in dynamischen und sich schnell verändernden Themenfeldern wie der Cybersicherheit langfristig zurechtzufinden. Die Gutachter betonen, dass die Studierenden lernen sollten, sich kontinuierlich in neue, technische Themenfelder einzuarbeiten, die in den kommenden Jahren von Bedeutung sein könnten. Für die Laborarbeit empfehlen die Gutachter, auch praxisnahe Szenarien wie Disaster Recovery, Krisenstab-Simulationen oder Datenschutzthemen in den Mittelpunkt zu stellen, um den Studierenden die realen Herausforderungen der Cybersicherheit näherzubringen.
Ein weiterer Vorschlag betrifft die theoretische Informatik: Die Grundlagen der Berechenbarkeit und Komplexitätstheorie sollten berücksichtigt werden, da diese Themen für das Verständnis der Cybersicherheit von grundlegender Bedeutung sind. Im Hinblick auf den Übergang zum Masterstudium wird geraten, eine Öffnungsstrategie zu entwickeln, die den Studierenden einen reibungslosen Übergang zu bestehenden Masterprogrammen im eigenen Haus ermöglicht. Im bestehenden Modulangebot (z.B. im Wahlbereich) könnten Themen wie Ethical Hacking, Network Hacking, Penetration Testing und Post-Quantum-Kryptographie (PQC) stärker integriert werden, um den Studierenden aktuelle und zukunftsrelevante Themen näherzubringen. Dabei könnte es sinnvoll sein, für die gemeinsam mit anderen Studiengängen belegten Module, spezialisierte Laborinhalte zu entwickeln, die auf Cybersecurity-spezifische Themen wie Penetration Testing und KI-gestützte Angriffe fokussieren. Ein weiterer Punkt betrifft das Wahlmodul „Cybersicherheit aktuell". Es wird empfohlen, dieses Modul als Pflichtmodul im mittleren Abschnitt des Studiums zu verankern und inhaltlich stärker auf aktuelle Sicherheitslücken, Gesetzgebungsverfahren und neue Sicherheitsverfahren wie Post-Quantum-Sicherheitsverfahren auszurichten. Zudem sollte die Einführung von Tutorien für die grundlegenden Informatikmodule, wie sie bereits angedacht ist, unterstützt werden.

Die sprachliche Ausrichtung des Studiengangs verdient ebenfalls besondere Beachtung. Angesichts der internationalen Relevanz der Cybersicherheit und der zentralen Bedeutung der englischen Sprache in diesem Bereich empfehlen die Gutachter, englischsprachige Wahlmodule zu integrieren. Dies ist besonders wichtig, da im späteren Berufsleben ein fundiertes Verständnis englischer Fachtexte und technischer Anleitungen unerlässlich ist. Zudem sollte, da im Diploma Supplement zwei Lehrsprachen ausgewiesen werden, mindestens ein englischsprachiges Wahlmodul angeboten werden.

Abschließend lässt sich sagen, dass der Studiengang insgesamt sehr positiv bewertet wird. Die Gutachter heben besonders die durchdachte Konzeptualisierung hervor. Sie empfehlen, die genannten Hinweise und Impulse/Empfehlungen zu berücksichtigen, um den Studiengang weiter zu optimieren und sicherzustellen, dass er auch künftig den wachsenden

Anforderungen der Cybersicherheit gerecht wird und die Studierenden optimal auf die Herausforderungen des Arbeitsfeldes vorbereitet.

1 Prüfbericht: Erfüllung der formalen Kriterien

(gemäß Art. 2 Abs. 2 SV und §§ 3 bis 8 und § 24 Abs. Studienakkreditierungsverordnung SH)

1.1 Studienstruktur und Studiendauer

(§ 3 Studienakkreditierungsverordnung SH)

Dokumentation/Bewertung

Der Studiengang „Cybersicherheit" ist als grundständiges Vollzeit-Präsenzstudium konzipiert. Die Aufnahme erfolgt jährlich einmal zum Wintersemester. Die Regelstudienzeit beträgt sieben Semester (210 LP). Nach erfolgreichem Abschluss wird der akademische Grad „Bachelor of Science" (B.Sc.) verliehen. Der Aufbau des Studiums orientiert sich in Teilen an bestehenden Informatik- bzw. Wirtschaftsinformatik-Studiengängen der HAW Kiel.

Entscheidungsvorschlag für den Studiengang

Das Kriterium ist erfüllt.

Damit entspricht der Studiengang den Anforderungen gemäß § 3 Studienakkreditierungsverordnung SH.

1.2 Studiengangsprofil

(§ 4 Studienakkreditierungsverordnung SH)

Dokumentation/Bewertung

Der Studiengang „Cybersicherheit" ist ein allgemeiner Studiengang ohne weitergehende formale Spezialisierungsrichtung innerhalb des Studiengangs.
Die Abschlussarbeit (Thesis) hat einen Umfang von 10 Leistungspunkten, was einem studentischen Arbeitsaufwand von 300 Stunden entspricht. Sie wird im 7. Semester angefertigt und durch ein Kolloquium mit einem Umfang von 5 Leistungspunkten ergänzt.
Die Thesis soll zeigen, dass die Studierenden in der Lage sind, eine praxisrelevante Problemstellung aus dem Bereich der Cybersicherheit nach angewandten wissenschaftlichen Methoden selbstständig zu bearbeiten. Die Themen können sowohl aus dem technischen als auch aus dem organisatorisch-managementorientierten Bereich der Cybersicherheit stammen. Da der Bachelorstudiengang primär anwendungsorientiert ausgerichtet ist, werden Abschlussarbeiten häufig in Kooperation mit Unternehmen oder öffentlichen Einrichtungen vergeben, um einen hohen Anwendungsbezug zu gewährleisten.

Entscheidungsvorschlag für den Studiengang

Das Kriterium ist erfüllt.

Damit entspricht der Studiengang den Anforderungen gemäß § 4 Studienakkreditierungsverordnung SH.

1.3 Zugangsvoraussetzungen und Übergänge zwischen den Studienangeboten

(§ 5 Studienakkreditierungsverordnung SH)

Dokumentation/Bewertung

Die Zugangsvoraussetzungen für den Studiengang richten sich nach den allgemeinen Bestimmungen des schleswig-holsteinischen Hochschulgesetzes und der Satzung der HAW Kiel.
Der Studiengang ist zulassungsbeschränkt mit 30 Studienplätzen pro Jahr konzipiert. Aufgrund der erwarteten Nachfrage ist eine Zulassungsbeschränkung in Form eines Numerus Clausus (NC) vorgesehen, analog zu den etablierten Bachelor-Studiengängen Informatik und Wirtschaftsinformatik an der HAW Kiel.
Um den Studierenden den Einstieg zu erleichtern und mögliche Defizite im Hinblick auf die erwarteten Eingangsqualifikationen, insbesondere in der Mathematik, auszugleichen, wird ein Mathematik-Brückenkurs im Fachbereich Informatik und Elektrotechnik angeboten, deren Teilnahme allen Studienanfänger*innen empfohlen wird. Darüber hinaus sind in den ersten Semestern die Module so gestaltet, dass sie grundlegendes Wissen systematisch aufbauen.
Neben Deutsch als Unterrichtssprache sind ausreichende Englischkenntnisse für das Studium dringend empfohlen, da insbesondere der Austausch in der internationalen Gemeinschaft aus Forschenden und Praktiker*innen (z. B. entsprechende Veröffentlichungen von Sicherheitsfirmen) ein großer Teil der relevanten Inhalte auf Englisch verfasst sind. Diese Kenntnisse lassen sich jedoch z. B. auch durch entsprechende Sprachkurse über das Zentrum für Sprachen und Interkulturelle Kompetenz (ZSIK) erwerben, beispielsweise im Rahmen des Moduls zur interdisziplinären Lehre im 1. und 2. Semester.

Entscheidungsvorschlag für den Studiengang

Das Kriterium ist erfüllt.

Damit entspricht der Studiengang den Anforderungen gemäß § 5 Studienakkreditierungsverordnung SH.

1.4 Abschluss und Abschlussbezeichnung

(§ 6 Studienakkreditierungsverordnung SH)

Dokumentation/Bewertung

Nach erfolgreichem Abschluss des Studiums wird der Abschlussgrad „Bachelor of Science", abgekürzt „B. Sc.", verliehen. Die Abschlussbezeichnung ist international anerkannt und qualifiziert sowohl für den direkten Berufseinstieg als auch für die Aufnahme eines weiterführenden Masterstudiums. Auskunft über das dem Abschluss zugrunde liegende Studium im Einzelnen erteilt das Diploma Supplement, das Bestandteil jedes Abschlusszeugnisses ist.

Entscheidungsvorschlag für den Studiengang

Das Kriterium ist erfüllt.

Damit entspricht der Studiengang den Anforderungen gemäß § 6 Studienakkreditierungsverordnung SH.

1.5 Modularisierung

(§ 7 Studienakkreditierungsverordnung SH)

Dokumentation/Bewertung

Das Lehrangebot des Studiengangs ist durchgängig modularisiert. Alle Lehrveranstaltungen sind thematisch und zeitlich in Module zusammengefasst, die jeweils mit einer definierten Anzahl von mindestens fünf Leistungspunkten bewertet und meist mit einer Modulprüfung abgeschlossen werden. Die Modulbeschreibungen werden als Anlage C beigefügt als Auszug aus der zentralen Moduldatenbank der HAW Kiel.

Entscheidungsvorschlag für den Studiengang

Das Kriterium ist erfüllt.

Damit entspricht der Studiengang den Anforderungen gemäß § 7 Studienakkreditierungsverordnung SH.

1.6 Leistungspunktesystem

(§ 8 Studienakkreditierungsverordnung SH)

Dokumentation/Bewertung

Der Studiengang umfasst insgesamt 210 Leistungspunkte (LP) nach dem European Credit Transfer and Accumulation System (ECTS). Diese verteilen sich auf sieben Semester, was

einem durchschnittlichen Arbeitsaufwand von 30 Leistungspunkten pro Semester entspricht. Ein Leistungspunkt entspricht einem studentischen Arbeitsaufwand (Workload) von 30 Zeitstunden. Der Gesamtumfang von 210 LP für einen siebensemestrigen Bachelorstudiengang ist konform mit der Studienakkreditierungsverordnung des Landes Schleswig-Holstein sowie der Prüfungsverfahrensordnung (Satzung) der HAW Kiel. In Kombination mit einem dreisemestrigen Masterstudium (90 LP) können 300 LP erworben werden.

Entscheidungsvorschlag für den Studiengang

Das Kriterium ist erfüllt.

Damit entspricht der Studiengang den Anforderungen gemäß § 8 Studienakkreditierungsverordnung SH.

1.7 Anerkennung und Anrechnung

Dokumentation/Bewertung für den Studiengang
Die Anerkennung und Anrechnung von Studienzeiten, Studienleistungen und Prüfungsleistungen, die an anderen Hochschulen in Deutschland oder im Ausland erbracht wurden, sowie von außerhochschulisch erworbenen Kompetenzen erfolgt gemäß der Anerkennungs- und Anrechnungsordnung der HAW Kiel. Zuständig für die Prüfung der Gleichwertigkeit und die Entscheidung über die Anerkennung ist der Prüfungsausschuss des federführenden Fachbereichs Wirtschaft. Ziel ist es sicherzustellen, dass die anzuerkennenden Kompetenzen den im Curriculum definierten Qualifikationszielen entsprechen.

Entscheidungsvorschlag für den Studiengang

Das Kriterium ist erfüllt.

1.8 Besondere Kriterien für Kooperationen mit nichthochschulischen Einrichtungen

(§ 9 Studienakkreditierungsverordnung SH)

Nicht relevant

2 Gutachten: Erfüllung der fachlich-inhaltlichen Kriterien

2.1 Schwerpunkte der Bewertung / Fokus der Qualitätsentwicklung

Dokumentation/Bewertung

Der Bachelorstudiengang Cybersicherheit ist ein neuer Studiengang (Erstakkreditierung). Der Studiengang ist an den Anforderungen des Qualifikationsrahmens für deutsche Hochschulabschlüsse, den Anforderungen der ländergemeinsamen Strukturvorgaben für die Akkreditierung von Studiengängen sowie an den landesspezifischen Strukturvorgaben orientiert.

Bei der Begutachtung standen das Curriculum und die Schlüssigkeit des Studiengangskonzepts im Mittelpunkt. Kritisch hinterfragt und ausführlich diskutiert wurden insbesondere die Aktualität des Curriculums, die angestrebten Kompetenzziele und die vorhandene Ressourcenaustattung. Weitere Informationen befinden sich dazu in den folgenden jeweils einschlägigen Kapiteln.

2.2 Erfüllung der fachlich-inhaltlichen Kriterien

(gemäß Art. 3 Abs. 2 Satz 1 Nr. 4 i.V. mit Art. 4 Abs. 3 Satz 2a und §§ 11 bis 16; §§ 19-21 und § 24 Abs. 4 Studienakkreditierungsverordnung SH)

2.2.1 Qualifikationsziele und Abschlussniveau

(§ 11 Studienakkreditierungsverordnung SH)

Dokumentation

Die Qualifikationsziele des Bachelor-Studiengangs „Cybersicherheit" sind konsequent auf die Entwicklung einer umfassenden, interdisziplinären Handlungskompetenz ausgerichtet und orientieren sich am Qualifikationsrahmen für deutsche Hochschulabschlüsse (HQR) auf Bachelor-Ebene.

Der Bachelor-Studiengang „Cybersicherheit" richtet sich an Studieninteressierte, welche die erforderlichen Kompetenzen zum vernetzten Handeln in der Verteidigung vor Cyberangriffen und der Stärkung der Resilienz von Organisationen gegen solche Angriffe erwerben wollen. Ziel ist daher die Ausbildung von Fachkräften, die in der Lage sind, als interdisziplinäre „Integratoren" zwischen der technischen Ebene (IT-Systeme) und der strategisch-organisatorischen Ebene (Management-Perspektive) zu agieren. Sie sollen nicht nur einzelne Sicherheitsmaßnahmen implementieren, sondern die Cybersicherheit und digitale Resilienz einer Organisation ganzheitlich planen, steuern und weiterentwickeln können.

Der Bereich Cybersicherheit ist ein hochdynamisches Fachgebiet. Zudem besteht eine grundlegende Asymmetrie zwischen Verteidigenden und Angreifenden: Während

Organisationen oder Systeme gegen alle möglichen Angriffe geschützt werden müssen, reicht im Sinne der Analogie des „schwächsten Glieds der Kette" für einen erfolgreichen Cyberangriff oft bereits die erfolgreiche Ausnutzung einer einzelnen Schwäche in einem der ineinandergreifenden sozio-technischen Schutzmechanismen. Daher ist eine besonders breite Qualifikation Studierender in vielen Bereichen nötig.

Das Thema Cybersicherheit wird dabei aus strategischer Perspektive (z. B. Management durch CISO und CIO), der Perspektive aus Sicht von Systembetreibenden (z. B. Sicherheit in Netzwerken), Entwickler*innen (z. B. angewandte Kryptografie), weiteren Fachkräften (z. B. Penetration Testing), regulären IT-Anwender*innen (z. B. Umgang mit Zugangsdaten) aber auch aus Sicht von Angreifenden (z. B. Durchführung von Social Engineering und Ethical Hacking) anwendungsorientiert betrachtet.

Den inhaltlichen Aufbau des Studiengangs prägen drei zusätzliche Perspektiven:

(i) Cybersicherheit ist **keine rein technische Aufgabe** (klassisch oft als „IT-Sicherheit" bezeichnet), sondern eine **interdisziplinäre Aufgabe**. Stattdessen ist der Schutz von Organisationen inklusive ihrer Informationen („Informationssicherheit") und Prozesse als Ganzes zu betrachten und dabei neben technischen Themenfeldern auch Aspekte des organisationalen oder individuellen Verhaltens zu berücksichtigen, sowohl bei Angriffen als auch für Schutzmaßnahmen. Hier bestehen Querbeziehungen zu Themen wie Datenschutz und Risiko- und Krisenmanagement.

(ii) Sicherheit ist eingebettet in das **breitere Themenfeld der Resilienz**. Das Ziel in der Praxis ist häufig, Widerstandsfähigkeit aufzubauen, um z. B. bei einem erfolgreichen Angriff auf ein Unternehmen den Geschäftsbetrieb nicht vollständig einzustellen, sondern soweit wie möglich aufrechtzuerhalten und/oder möglichst zügig organisiert wiederherzustellen. Hier bestehen enge Beziehungen z. B. zu technischer oder digitaler Resilienz, d. h. der Widerstandsfähigkeit auch bei nicht durch Cyberangriffe ausgelösten Ausfällen.

(iii) Fokussierung auf **erfolgreiche Gestaltung und Umsetzung von Sicherheitsmaßnahmen**: Da wie oben beschrieben im Themenbereich Cybersicherheit eine breite Ausbildung notwendig ist, sind gleichzeitig Abwägungen erforderlich, um die Studierbarkeit im Rahmen eines Bachelor-Studiums mit 210 LP zu gewährleisten. Eine der hier vorgenommenen Priorisierungen ist daher, den Studiengang bewusst **nicht** primär darauf auszurichten, Entwickler*innen sicherer Software, Hardware oder Produkte auszubilden. Entscheidungsgrundlage ist, dass in vielen Organisationen nicht die Eigenentwicklung von Software, Hardware oder Produkten im Vordergrund steht, sondern Fachkräfte benötigt werden für den sicheren Einsatz bestehender Softwarelösungen bzw. die Sicherung der gesamten Organisation inklusive aller eingesetzten oftmals eingekauften Anwendungen.

Der neue Studiengang bereitet Absolvent*innen damit auf ein vielfältiges Berufsfeld vor, beispielsweise als:

- Mitarbeiter*in in der IT-Sicherheit: Systematische Planung, Koordination, Durchführung von technischen und organisatorischen Maßnahmen zur Steigerung der Cybersicherheit und digitalen Resilienz.
- Cybersicherheitsberater*in: Beratung von Unternehmen und Organisationen in Fragen der Cybersicherheit, z. B. als Teil des Angebots von IT-Beratungsunternehmen.
- Sicherheitsanalyst*in: Identifizierung von Schwachstellen in Systemen, Netzwerken und Organisationen sowie Entwicklung von Lösungen zur Risikominimierung.
- Cybersicherheitsexpert*in in Behörden wie beispielsweise Regulierungsbehörden.

Langfristige Perspektiven bieten sich mit Weiterbildung bzw. Berufserfahrung beispielsweise in Berufsfeldern wie

- IT-Sicherheitsbeauftragte*r (CISO), verantwortlich für die Entwicklung und Umsetzung von Sicherheitsstrategien in Unternehmen und Organisationen.
- Penetration Tester*in: Durchführung von gewünschten Angriffsversuchen, um technische und organisatorische Sicherheitslücken in Organisationen aufzudecken und zu beheben.
- Forensiker*in: Untersuchung von Cyberangriffen und Aufklärung von Cyberkriminalität.
- IT-Risikomanager*in: Identifikation, Analyse und Überwachung der operationellen Risiken auf Unternehmens- oder Organisationsebene inklusive technischer Risiken (durch Cyberangriffe, aber auch durch Ausfälle etc.)
- IT-Leiter*in (CIO) verantwortlich für die Leitung einer IT-Abteilung inklusive der Sicherheitsmaßnahmen in der IT und darüber hinaus.

Absolvent*innen des Studiengangs „Cybersicherheit" können in einer Vielzahl von Organisationen tätig sein, darunter:

- IT-Unternehmen bzw. -Dienstleistungsunternehmen: Beratung und Dienstleistungen im Bereich Cybersicherheit, Entwicklung von Sicherheitssoftware.
- Wirtschaftsunternehmen aller Branchen und Größen (auch kleine und mittelständische Unternehmen): Schutz von z. B. Kundendaten, Transaktionen, sensiblen Systemen oder kritischer Infrastruktur vor Cyberangriffen.
- Öffentliche Verwaltung inkl. z. B. Strafverfolgung: Schutz von kritischer Infrastruktur und sensiblen Daten.

Die entsprechende Ableitung der Qualifikationsziele erfolgte insbesondere auf Basis der fachlichen Anforderungen, die sich aus der Natur von Cyberangriffen in der Praxis ergeben (z. B. Kombination aus technischen und nicht-technischen Angriffswegen).

Die angestrebten Kompetenzen lassen sich gemäß dem Kompetenzmodell der HAW Kiel auf Basis des HQR in vier Dimensionen gliedern:

1. **Fachkompetenz (Wissen und Verstehen):** Die Absolvent*innen verfügen über ein breites und integriertes Wissen in den Kerndisziplinen:

- **Informatik:** Sie können die fundamentalen Prinzipien von Computern, Betriebssystemen, Programmierung, Algorithmen und Datenstrukturen, Datenbanken und Rechnernetzen beschreiben. *Module: TIN, BS, PROG1, PROG2, AUD, DBN, WA, CN*

- **Wirtschaft und Management:** Sie können die Grundlagen betriebswirtschaftlichen Handelns und die Bedeutung von Geschäftsprozessen, Projektmanagement und IT-Management beschreiben. *Module: ABWL, GPM, PROJ*

- **Cybersicherheit:** Sie können u. a. Bedrohungslandschaften, Angriffsmethoden, kryptografische Grundlagen (z. B. Algorithmen), technische Sicherheitsmaßnahmen (z. B. Netzwerksicherheit oder sichere Konfiguration von Systemen), organisatorische Rahmenwerke (z. B. ISMS oder Methoden des Risikomanagements) oder Vorgehensmodelle (z. B. beim Penetration Testing), relevante rechtliche Rahmenbedingungen (z. B. Datenschutz), die Rolle menschlichen Verhaltens (z. B. Social Engineering und Sicherheitskultur) und Sicherheitsprinzipien (z. B. Security by Design) beschreiben. *Module: ECS, CSMV, GKR, EHP, CSRO, ITRD, PPCS*

- **Mathematische Grundlagen:** Sie beherrschen mathematische Grundlagen, die in den grundlegenden und weiterführenden Themen der Informatik, Wirtschaft sowie Kryptografie eingesetzt werden, können diese wiedergeben und erläutern. *Module: MA1 (-I), MA2-I, STA*

2. **Methodenkompetenz (Einsatz, Anwendung und Erzeugung von Wissen):** Die Absolvent*innen sind befähigt, ihr Wissen zur Lösung komplexer Probleme im Bereich Cybersicherheit und digitaler Resilienz anzuwenden:

- **Analyse- und Problemlösungsfähigkeit:** Sie können komplexe sozio-technische Systeme analysieren, Schwächen der Cybersicherheit oder digitalen Resilienz identifizieren (z. B. mittels Risikoanalyse und dem Verständnis von Penetration Testing), relevante Abwägungen (z. B. Sicherheit gegenüber Wirtschaftlichkeit oder Sicherheit gegenüber Benutzbarkeit) diskutieren und systematisch Lösungen zur Risikominimierung entwickeln. *Module: CSMV, EHP, CSRO, etc.*

- **Gestaltungskompetenz:** Sie können Sicherheitskonzepte und -strategien für Organisationen entwerfen und deren Implementierung planen und begleiten. *Module:*
  CSMV, CSRO, etc.

- **Wissenschaftliches Arbeiten:** Sie sind in der Lage, sich selbstständig in neue Themengebiete einzuarbeiten und Problemstellungen nach wissenschaftlichen Methoden zu bearbeiten, was in der Bachelor-Thesis gipfelt. *Module: PPCS, CSA, T, etc.*

3. **Sozialkompetenz (Kommunikation und Kooperation):** Die Absolvent*innen können effektiv in Organisationen bzw. heterogenen Teams arbeiten.

- **Kommunikationsfähigkeit:** Sie können komplexe technische Sachverhalte (wie z. B. die Implikation von Sicherheitslücken auf die Sicherheit von Systemen oder Organisationen) verständlich aufbereiten und sowohl mit technischen Experten als auch mit dem Management oder nicht-technischen Anwendern zielgruppengerecht kommunizieren, auch unter Kenntnis und Verwendung englischer Fachbegriffe. *Module: PPCS, CSRO, CSA, etc.*

- **Team- und Kooperationsfähigkeit:** Das Curriculum fördert durch zahlreiche Projekt- und Übungsanteile die Fähigkeit zur Zusammenarbeit in interdisziplinären und zum Teil auch interkulturellen Teams, was eine Kernanforderung im Berufsfeld darstellt. *Module: WA, ITRD, CSA, etc.*

4. **Selbstkompetenz (Wissenschaftliches Selbstverständnis und Professionalität):** Die Absolvent*innen entwickeln eine professionelle und verantwortungsbewusste Haltung:

- **Verantwortungsbewusstsein und Ethik:** Sie sind sich der gesellschaftlichen Verantwortung im Themenfeld der Absicherung gegen Cyberangriffe bewusst und reflektieren die ethische Dimension ihres Handelns, z. B. in Bereichen wie Ethical Hacking oder dem Umgang mit sensiblen Daten. *Module: ECS, EHP, ITRD, etc.*

- **Selbstständigkeit und Lernfähigkeit:** Sie können eigenständig und eigenverantwortlich arbeiten und sind in der Lage, im Kontext des lebenslangen Lernens in einem sich stetig weiterentwickelnden Feld wie der Cybersicherheit die eigenen Fort- und Weiterbildungsbedarfe zu beurteilen. *Module: ECS, CSA, PPCS, BS, T, etc.*

Die **Berufsfeldorientierung** wird durch mehrere Bestandteile des Curriculums sichergestellt: Das Praxisprojekt im 4. Semester und das berufspraktisch Studiensemester im 6. Semester bieten intensive Praxiserfahrungen. Es wird eine regelmäßige Einbeziehung von Gastvorträgen z. B. von Praxisvertretern von Unternehmen der Region oder darüber hinaus angestrebt, wofür die bestehenden Hochschulkontakte, die umfangreichen Netzwerke der beteiligten Lehrenden sowie die regionalen Netzwerke (z. B. Fachgruppe IT-Security des Clusters Digitale Wirtschaft Schleswig-Holstein) genutzt werden.

Die **Persönlichkeitsentwicklung** und die Fähigkeit zum **zivilgesellschaftlichen Engagement** werden zum einen durch die Auseinandersetzung mit den ethischen und gesellschaftlichen Implikationen der Cybersicherheit gefördert. Module wie „Cybersicherheit und menschliches Verhalten", „Ethical Hacking and Penetration Testing" sowie „IT-Recht und Datenschutz" schärfen das Bewusstsein für Grundrechte, Privatsphäre und die Verantwortung, die mit der Gestaltung sicherer digitaler Räume einhergeht. Zum anderen dienen die im Curriculum verankerten Module der interdisziplinären Lehre z. B. durch Nutzung der Angebote in den interdisziplinären Wochen der HAW Kiel als Raum zur Persönlichkeitsentwicklung über die Kerninhalte des Studiengangs hinaus.

Diese Qualifikationsziele basieren auch auf dem Leitbild für die Lehre der HAW Kiel[1], insbesondere Leitsatz 1 (Anwendungsorientierung und Interdisziplinarität) und Leitsatz 2 (breitgefächerte Fachkompetenz, Schlüsselkompetenz, Verantwortungsbewusstsein). Die

Qualifikationsziele finden sich im gesamten Curriculum wieder – von der Vision des Studiengangs, über die konkrete Ausgestaltung der einzelnen Module und ihrer Lernergebnisse, bis hin zur grundlegenden Verankerung in der Prüfungsordnung (vgl. Anhang D).

Bewertung

Die Qualifikationsziele des Studiengangs sind in der Prüfungsordnung (Anhang 1: „Qualifikationsziele") sowie im Diploma Supplement klar und transparent dargestellt. Die Zielsetzungen auf Studiengangsebene sind eindeutig formuliert und entsprechen den Anforderungen des Qualifikationsrahmens für deutsche Hochschulabschlüsse. Der Studiengang vermittelt ein praxisorientiertes und fundiertes Kompetenzprofil, das die Studierenden optimal auf den Arbeitsmarkt vorbereitet. Besonders hervorzuheben ist die gelungene Kombination von Informatik- und betriebswirtschaftlichen Inhalten sowie die geplant enge Verzahnung mit der regionalen Wirtschaft, die den Studierenden zahlreiche Möglichkeiten zur praktischen Anwendung ihres Wissens bietet. Insgesamt entsprechen die formulierten Qualifikationsziele den Anforderungen des Arbeitsmarktes und tragen dazu bei, die Absolvent*innen auf die Herausforderungen in den künftigen Arbeitsfeldern vorzubereiten. Da es nach aktuellem Stand keinen gleichnamigen Master gibt, sollte für Studierende möglichst transparent dargestellt werden, für welche bestehenden Masterstudiengänge an der HAW man sich mit dem Bachelor Cybersicherheit qualifiziert.

Das Kriterium ist erfüllt.

Der Studiengang entspricht den Anforderungen gemäß § 11 Studienakkreditierungsverordnung SH.

2.2.2 Schlüssiges Studiengangskonzept und adäquate Umsetzung

(§ 12 Studienakkreditierungsverordnung SH)

Mit diesem mehrdimensionalen Kriterium soll zunächst geprüft werden, ob das Curriculum eines Studiengangs im Hinblick auf das Erreichen der Qualifikationsziele adäquat aufgebaut ist, ob Qualifikationsziele, Studiengangsbezeichnung, Abschlussgrad und -bezeichnung und

[1] https://www.fh-kiel.de/fileadmin/data/fachhochschule/leitbild_fuer_die_lehre.pdf

Modulkonzept stimmig aufeinander bezogen sind und entsprechende Lehr- und Lernformen praktiziert werden, die die Studierenden aktiv einbeziehen.

Curriculum

Das Studiengangskonzept ist darauf ausgelegt, die formulierten Qualifikationsziele durch ein schlüssiges, didaktisch durchdachtes und ressourcentechnisch abgesichertes Curriculum zu erreichen. Die Konzeption stellt sicher, dass die Studiengangsbezeichnung, der Abschlussgrad, die Qualifikationsziele und das Modulkonzept stimmig aufeinander bezogen sind.

Didaktisches Konzept: Das didaktische Konzept des Studiengangs lässt sich als anwendungsorientiert und sozio-technisch beschreiben. Es basiert auf der Überzeugung, dass nachhaltige Kompetenz in der Cybersicherheit nur durch die Integration von theoretischem Wissen und praktischer Anwendung entstehen kann. Die Lehr- und Lernformen sind gezielt auf die jeweiligen Modulziele abgestimmt und umfassen ein breites Spektrum:

- Vorlesungen dienen der Vermittlung von grundlegendem und theoretischem Wissen in allen Kernbereichen.
- Übungen und Tutorien, beispielsweise in den mathematischen und wirtschaftlichen Grundlagen, ermöglichen die Vertiefung und Einübung des Gelernten in Kleingruppen.
- Technische Laborpraktika stellen den direkten Bezug zur technischen Praxis her und ermöglichen das „Lernen am System" in einer sicheren, abgeschotteten Laborumgebung.
- Projektarbeiten z. B. in „Fortgeschrittene Programmierung" und insbesondere im „Praxisprojekt Cybersicherheit" fördern die Methoden- und Sozialkompetenz. Die Studierenden arbeiten in Teams an komplexen, praxisnahen Problemstellungen und müssen dabei eigenständig Lösungen entwickeln, dokumentieren und präsentieren.
- Seminare z. B. im Rahmen von Wahlmodulen wie „Cybersicherheit aktuell" fördern den wissenschaftlichen Diskurs und die Fähigkeit zur kritischen Auseinandersetzung mit Fachthemen.
- Praxisanteile im Praxisprojekt (4. Semester), im berufspraktischen Studiensemester (Praktikum im 6. Semester) und ggf. in der Thesis (7. Semester) sehen eine enge Zusammenarbeit mit Unternehmen und öffentlichen Einrichtungen vor, um direkte Einblick in die Berufspraxis zu gewinnen, den Aufbau von Netzwerken zu fördern und die Anwendung des erlernten Wissens auf reale Problemstellungen zu praktizieren. Die Hochschule stellt durch eine*n betreuende*n Professor*in sicher, dass die Inhalte des Praktikums den Qualifikationszielen des Studiengangs entsprechen, die Verantwortung für die Bewertung der Leistung verbleibt bei der Hochschule.

Die Umsetzung der Qualifikationsziele im Curriculum erfolgt durch ein sequenziertes Curriculum. Die ersten drei Semester legen insbesondere die Grundlagen in Informatik, Wirtschaft, Mathematik und Cybersicherheit. Darauf aufbauend werden in den Semestern vier und fünf z. B. die integrativen Cybersicherheits-Module gelehrt, die das Wissen aus den

verschiedenen Disziplinen zusammenführen, wie die Module „Ethical Hacking and Penetration Testing" sowie „Cybersicherheit und -Resilienz von Organisationen". Das „Praxisprojekt Cybersicherheit" im 4. Semester dient als erster großer Integrationspunkt, bei dem die Studierenden üblicherweise eine komplexe Aufgabe z. B. von der Analyse bis zur Lösung bearbeiten müssen. Das berufspraktische Studiensemester im 6. Semester stellt den Transfer des Gelernten in die professionelle Praxis sicher, bevor im 7. Semester mit der Thesis und weiteren Wahlmodulen die akademische Auseinandersetzung abgeschlossen wird.
Ergänzend ist hier insbesondere das Einbeziehen von Künstlicher Intelligenz (KI) bzw. maschinellem Lernen (ML) sowohl in der Lehre bzw. Didaktik und in den Lerninhalten zu erwähnen.
In Bezug auf Lerninhalte sind grundlegende Fähigkeiten zu KI- und ML-Methoden unerlässlich für einen qualifizierenden Abschluss. Daher werden Grundlagen im Modul „Statistik" vorbereitet und im Modul „KI und Machine Learning" sowie ggf. in Wahlpflichtmodulen vertieft.

Gleichzeitig stellt KI in Bezug auf Lerninhalte ein Querschnittsthema dar, das in allen inhaltlichen Bereichen – Informatik, Wirtschaft/Management, Cybersicherheit – einen massiven Einfluss auf die heutige und zukünftige Entwicklung hat. Beispielhaft lässt sich dies in der Cybersicherheit strukturieren, in die Auswirkungen von KI erstens in der Nutzung von KI für Cyberangriffe (z. B. Nutzung von generativer KI für zielgerichtetere, personalisierte Phishing-Angriffe), zweitens der Nutzung von KI zur Verteidigung oder Erhöhung der Resilienz (z. B. Nutzung von KI oder ML in der Mustererkennung in Log-Daten), drittens in der Absicherung von KI-Systemen (z. B. gegen Prompt Injection) und viertens in der übergreifenden Veränderung der Gesamtlandschaft durch KI (z. B. erhöhte Angriffsfläche durch massive Zunahme von KI-generiertem Code oder Ausnutzung von spezifischen, durch KI-Nutzung hervorgerufenen Sicherheitslücken). Diese Art von KI-/ML-Themen werden daher in den jeweiligen Modulen integrativ behandelt bzw. perspektivisch in einem Wahlpflichtmodul „Cybersicherheit aktuell" vertieft.

Methodisch in der Lehre werden KI und ML damit in den jeweiligen Modulen repräsentiert sein, die Ausgestaltung ist abhängig von den jeweiligen Inhalten des Moduls. So wird z. B. in Programmierungsmodulen die Codegenerierung mittels generativer KI thematisiert bzw. geübt, während in anderen Modulen beispielsweise Texte mit Hilfe von KI analysiert und erstellt werden.
Studierende werden aktiv in den Lernprozess einbezogen. Durch kleine Gruppengrößen und durch spezifisch für den Studiengang Cybersicherheit entwickelte Module ist sichergestellt, dass Interessen und Präferenzen der Studierenden bei der Gestaltung der Lehre im Sinne des **studierendenzentrierten Lehrens und Lernens** mitberücksichtigt werden können. Freiräume für ein selbstgestaltetes Studium werden insbesondere durch die zwei Module der interdisziplinären Lehre sowie die vier Wahlmodule eröffnet, die eine individuelle Vertiefung ermöglichen. Die Studierenden können bei den Wahlmodulen aus einem breiten Studienangebot wählen, welches sowohl technische Themen (z. B. Digitale Forensik) als auch Management-Themen (z. B. Risiko- und Krisenmanagement) vorsieht. Zudem kann sowohl im Praxisprojekt Cybersicherheit als auch im Praxissemester die Aufgabenstellung aus einem breiten Spektrum gewählt werden.

Bewertung

Die Gutachter*innen konnten sich auch durch die Gespräche mit den Studiengangsverantwortlichen und Lehrenden davon überzeugen, dass Qualifikationsziele auf Ebene des Studiengangs, Studiengangbezeichnung, Abschlussgrad und -bezeichnung sowie Modulkonzepte stimmig aufeinander bezogen sind. Das Studiengangskonzept des Bachelorstudiengangs Cybersicherheit wird insgesamt als sehr schlüssig und gut durchdacht bewertet. Die Gutachter heben insbesondere hervor, dass der Studiengang eine ausgewogene Mischung aus praxisorientierten Inhalten und fundierten theoretischen Grundlagen bietet. Die konsequente Ausrichtung auf die Bedürfnisse der Praxis sowie die enge Zusammenarbeit der Lehrenden mit der regionalen Wirtschaft stellen sicher, dass die Studierenden auf die realen Anforderungen des Arbeitsmarktes vorbereitet werden.
Ein weiteres starkes Merkmal des Konzepts ist die interdisziplinäre Herangehensweise. Die Verbindung von Informatik und Betriebswirtschaftslehre wird von den Gutachtern als gelungen angesehen, da sie den Studierenden ein breites Kompetenzprofil vermittelt und ihnen ermöglicht, die vielschichtigen Herausforderungen der Cybersicherheit aus verschiedenen Perspektiven zu verstehen. Darüber hinaus wird die Möglichkeit, verschiedene praxisorientierte Module und Laborübungen zu absolvieren, als besonders vorteilhaft betrachtet. Dies stellt sicher, dass die Studierenden nicht nur theoretische Kenntnisse erwerben, sondern diese auch praktisch anwenden können. Die Gutachter stellen jedoch fest, dass in den praktischen Laborübungen noch stärker auf spezifische Cybersicherheitsthemen eingegangen werden könnte, wie etwa Ethical Hacking, Penetration Testing oder Incident Response. Durch eine verstärkte Integration dieser praxisnahen Szenarien würde der Studiengang noch näher an den aktuellen Herausforderungen der Cybersicherheit ausgerichtet werden. Die Einbindung hochaktueller Themen wie Post-Quantum-Kryptographie und aktuelle technische Sicherheitslücken, einschließlich der Ausnutzung von Schwachstellen, wird als besonders sinnvoll erachtet, um den Studierenden ein noch breiteres und zukunftsorientiertes Kompetenzspektrum zu vermitteln. Der Studiengang scheint gut organisiert, und die beiden beteiligten Fachbereiche arbeiten eng zusammen, was sich positiv auf die Qualität und Kohärenz der Lehre auswirken wird.

Zusammenfassend lässt sich sagen, dass das Studiengangskonzept in seiner Gesamtheit als sehr gut durchdacht und praktikabel bewertet wird. Durch die Umsetzung der genannten Impulse und der Empfehlung zur Weiterentwicklung kann der Studiengang weiter optimiert und zukunftsfähig gestaltet werden.

Das Kriterium ist erfüllt.

Internationale Kooperationen und Mobilität

Cybersicherheit ist ein in hohem Maße internationales Thema: So ist Cyberkriminalität beispielsweise ein globales Phänomen, Bedrohungen sind oft unabhängig von der regionalen

Verortung gegeben, und die Community der Sicherheitsexperten ist international stark vernetzt und in aktivem Austausch. Dadurch eignet sich das Themenfeld besonders stark für Internationalität und Mobilität.

Das Curriculum ist bewusst so gestaltet, dass es den Studierenden einen Auslandsaufenthalt ohne Studienzeitverlängerung ermöglicht. Das 5. Semester ist als Mobilitätsfenster vorgesehen. Studierende werden ermutigt, dieses Semester an einer der zahlreichen Partnerhochschulen der HAW Kiel im Ausland zu verbringen.

Zudem bzw. alternativ kann das sechsmonatige berufspraktische Studiensemester im 6. Semester auch in einem ausländischen Betrieb stattfinden.

Die Anerkennung von im Ausland erbrachten Studienleistungen wird durch das ECTS-System und die transparente Modulstruktur erleichtert. Eine Anerkennung der im Ausland studierten Module erfolgt gemäß der Anerkennung- und Anrechnungsordnung der HAW Kiel. Zur Beurteilung einer Anerkennung werden auch die übergreifenden Qualifikationsziele des Studiengangs herangezogen. Sollten insbesondere die studiengangsspezifischen Pflichtmodule des 5. Semesters („Cybersicherheit und -Resilienz von Organisationen", „IT-Recht und Datenschutz") im Ausland nicht äquivalent studiert bzw. anerkannt werden, sind diese z. B. im 7. Semester nachzuholen.
Um eine reibungslose Anerkennung zu gewährleisten, wird eine frühzeitige Beratung durch die Studiengangsleitung und das International Office und die Einreichung eines Learning Agreement vor Beginn des Auslandssemesters beim Auslandsbeauftragten des Fachbereichs dringend empfohlen.

Die Kurse an den Partnerhochschulen werden in der Regel in der jeweiligen Landessprache oder auf Englisch unterrichtet. Das erforderliche Sprachniveau liegt dabei meist auf B2. Studierende haben über das Zentrum für Sprachen und Interkulturelle Kompetenz (ZSIK) der HAW Kiel Zugang zu einem breiten Angebot an Sprachkursen, um sich auf einen Auslandsaufenthalt vorzubereiten. Dies kann auch bereits ab dem 1. Semester geschehen und im Rahmen der Module „Interdisziplinäre Lehre" angerechnet werden.

Für ausländische Gaststudierende (Incomings) ist insbesondere hilfreich, dass ein hoher Anteil internationaler (meist englischsprachiger) Literatur bzw. Quellen vorliegt, sodass das Studium der Module mit Lehrsprache Deutsch meist auch durch Lernmaterialien in anderen Sprachen ergänzt werden kann.

Der Studiengang verfolgt das Ziel, die Studierenden auf eine globalisierte Arbeitswelt im Bereich der Cybersicherheit aktiv vorzubereiten – auch unter Berücksichtigung der Internationalisierungsstrategie der HAW Kiel.
Konkrete Maßnahmen zur Förderung der Internationalisierung umfassen unter anderem:
(i) Internationalität im Curriculum („Internationalization at Home"): Internationale Inhalte, Entwicklungen und Forschungserkenntnisse fließen kontinuierlich in die Lehre ein. Ein Großteil der relevanten Fachliteratur und der Veröffentlichungen von Sicherheitsforschern und unternehmen ist global ausgerichtet bzw. nicht länderspezifisch.

(ii) Förderung der Studierendenmobilität: Wie unter „Mobilität" beschrieben, wird das 5. Semester als Mobilitätsfenster angesehen. Auf die zahlreiche Partnerhochschulen, Kooperationen und Fördermöglichkeiten (z. B. ERASMUS), wird im Laufe des Studiums aktiv hingewiesen und beworben. Prof. Aßmuth hatte an seiner vorigen Hochschule Kontakte mit mehreren schottischen und finnischen Hochschulen aufgebaut und steht auch weiterhin mit den betreffenden Kolleg*innen in Kontakt. Diese Kontakte können direkt genutzt werden, z.B. Teilnahme an der jährlichen Ethical-Hacking-Konferenz „Securi-Tay" an der Abertay University in Dundee oder eine Teilnahme an der jährlichen Summer School „International Perspectives on Cybercrime and Cybersecurity" an der University of Strathclyde in Glasgow. Die Kontakte zur Arcada University of Applied Sciences in Helsinki können für Austausche in Verbindung mit den Themenbereichen Cybersicherheit und Künstliche Intelligenz sowohl von Studierenden als auch Dozierenden genutzt werden.
(iii) Perspektivische fremdsprachige Angebote: Es ist angedacht, ausgewählte Wahlmodule ggf. in englischer Sprache anzubieten, um sowohl die Attraktivität für internationale Gaststudierende (Incomings) zu erhöhen als auch den eigenen Studierenden die Möglichkeit zu geben, ihre Fachsprachenkompetenz zu vertiefen.

(iv) Integration von Incomings: Auch wenn das Curriculum auf Deutsch als Lehrsprache ausgerichtet ist, erleichtern die Verfügbarkeit vergleichbarer Lehr- und Lernmaterialien in anderen Sprachen sowie der modulare Aufbau die Integration von Gaststudierenden.

Bewertung/Entscheidungsvorschlag

Die Gutachter*innen bewerten das Kriterium „Internationale Kooperationen und Mobilität" insgesamt positiv. Sie sind der Meinung, dass für den Bachelorstudiengang Cybersicherheit geeignete Rahmenbedingungen geschaffen wurden, um die Mobilität der Studierenden zu fördern. Insbesondere das im Studiengang integrierte Mobilitätsfenster im 5. Semester ermöglicht es den Studierenden, auch ohne Zeitverlust an Partnerhochschulen im Ausland zu studieren. Diese Mobilität wird durch umfassende Kooperationen mit anderen Hochschulen sowie durch gut etablierte Beratungsstrukturen im Fachbereich wirksam unterstützt. Die Anerkennung von im Ausland erbrachten Studienleistungen ist für die Studierenden klar nachvollziehbar und gut umsetzbar, wobei ein im Vorfeld abgeschlossenes Learning Agreement erforderlich ist. Perspektivisch ließe sich die Mobilität des Studiengangs auch durch englischsprachige Wahlmodule weiter stärken, da diese die Attraktivität des Studiengangs für Austauschstudierende von Partneruniversitäten erhöhen würden.

Das Kriterium ist erfüllt.

Der Studiengang entspricht den Anforderungen gemäß § 12 Abs. 1 Satz 4 der Studienakkreditierungsverordnung SH.

Personelle Ausstattung

Dokumentation

Die Lehre und Betreuung der Studierenden im Studiengang „Cybersicherheit" wird hauptsächlich getragen von Professoren und Lehrkräften für besondere Aufgaben der Fachbereiche Wirtschaft (insbesondere Institut für Wirtschaftsinformatik) und Informatik und Elektrotechnik (insbesondere Institut für Informatik). Die genaue Aufteilung der Lehraufgaben ist im Studienverlaufsplan im Anhang I und der Curricularnormwert-Berechnung detailliert ausgewiesen.
Dabei sind von der HAW Kiel zum Winter 2024/2025 Professuren neu besetzt bzw. neu eingerichtet worden, die strategisch zur Stärkung des Themenfeldes dienen:

- Professur für „IT-Sicherheit" am Fachbereich Informatik und Elektrotechnik
- Professur für „Wirtschaftsinformatik, insb. Cybersicherheit" am Fachbereich Wirtschaft

Darüber hinaus besteht sowohl Expertise im Bereich Cybersicherheit bei weiteren bestehenden Professoren der HAW Kiel (z. B. in den Bereichen Wirtschaftsinformatik, Informatik und Medieninformatik) sowie interdisziplinäre Anknüpfungspunkte zu Professores in den Fachbereichen Soziale Arbeit (im Kontext der Delinquenz zu Cyberkriminalität) oder Medien (beispielsweise im Kontext Krisenkommunikation bei Cyberangriffen auf Unternehmen), welche perspektivisch entsprechende Wahlmodule anbieten könnten (siehe Kapitel 14 Fachlich-Inhaltliche Gestaltung des Studiengangs).
Der Studiengang wird aus den bestehenden Lehrkapazitäten der Fachbereiche betreut. Durch eine Kooperationsvereinbarung der beteiligten Fachbereiche Wirtschaft sowie Informatik und Elektrotechnik wird geregelt, dass eine Aufteilung des Curricularnormwertes entsprechend der eingebrachten Lehrkapazitäten (im geplanten Curriculum paritätisch) erfolgt. Zeitgleich mit der Einführung des Studiengangs Cybersicherheit sind Anpassungen der Studienplatzkapazitäten in bestehenden Bachelor-Studiengängen beider Fachbereiche vorgesehen, insbesondere BWL sowie Informatik, um Studienplatzkapazitäten für den neuen Studiengang zu schaffen.
Gleichzeitig werden durch die Nutzung bestehender Module insbesondere aus den Studiengängen Informatik, Wirtschaftsinformatik und BWL Synergien gehoben, um die vorhandenen personellen Ressourcen effizient einzusetzen und Austausch auch mit Studierenden angrenzender Disziplinen zu ermöglichen. Eine detaillierte Übersicht der beteiligten Lehrpersonen findet sich in Anlage G.

Bewertung/Entscheidungsvorschlag

Die Gutachter heben hervor, dass der Studiengang Cybersicherheit in Bezug auf die personelle Ausstattung gut aufgestellt scheint. Die Liste der Lehrenden zeigt eine ausreichende Beteiligung hauptberuflich tätiger Professor*innen, die für die erfolgreiche Umsetzung des Curriculums erforderlich ist. Insbesondere die Besetzung der neu geschaffenen Professuren, die sich bereits in den ersten Semestern im Modulplan widerspiegeln, wird als besonders positiv hervorgehoben. Diese Besetzung gewährleistet, dass den Studierenden ein fundiertes und aktuelles Fachwissen vermittelt wird, das sie optimal auf die Anforderungen vorbereitet.

Darüber hinaus wird die Betreuungsrelation zwischen Lehrenden und Studierenden als sehr gut bewertet. Dies ermöglicht eine persönliche Beratung und Unterstützung der Studierenden, was gerade bei einem komplexen und praxisintensiven Studiengang wie Cybersicherheit von großer Bedeutung ist. In den Gesprächen mit den Studierenden wurde betont, dass die Dozenten als verlässliche Ansprechpartner*innen zur Verfügung stehen und sich regelmäßig ausreichend Zeit für individuelle Anliegen und Fragen nehmen.

Der Studiengang entspricht den Anforderungen gemäß § 12 Abs. 1 Studienakkreditierungsverordnung SH.

Ressourcenausstattung

Dokumentation

Für die erfolgreiche Durchführung des Studiengangs steht eine angemessene sächliche und räumliche Ausstattung zur Verfügung. Da im Zuge der Einführung dieses Studiengangs Kapazitäten in gleicher Höhe in anderen Studiengängen in beiden beteiligten Fachbereichen abgebaut werden, ist die Ressourcenausstattung gewährleistet.

- Räumlichkeiten: Es werden die vorhandenen und bereits ausgestatteten Hörsäle, Seminar- und PC-Räume der Fachbereiche Wirtschaft und Informatik und Elektrotechnik genutzt.
- Labore: Für die praxisorientierten Module stehen die ausgestatteten PC-Labore insbesondere des Fachbereichs Informatik und Elektrotechnik zur Verfügung. In diesen Laboren und virtualisierten Umgebungen lassen sich umfangreiche realistische Aufgabenstellungen der Cybersicherheit nachstellen.
- Bibliothek: Die zentrale Hochschulbibliothek bietet Zugang zu einer umfassenden Sammlung von Fachbüchern, E-Books und wissenschaftlichen Datenbanken aus den Bereichen Informatik, Wirtschaft und Cybersicherheit. Der Bestand ist durch die vorhandenen Studiengänge Informatik und Wirtschaftsinformatik, die jeweils bereits Module zu IT-Sicherheit beinhalten, bereits gut ausgestattet – zudem eignet sich das Themenfeld Cybersicherheit oft auch für die Nutzung von frei verfügbaren Quellen (z. B. kostenlose Online-Veröffentlichungen von Sicherheitsexperten), sodass eine Anpassung der Bibliotheksausstattung an die Bedürfnisse des neuen Studiengangs keine Hürde darstellt.
- IT-Infrastruktur: Die Studierenden haben Zugang zur gesamten IT-Infrastruktur der Hochschule, inklusive WLAN, Lernplattformen (z. B. Moodle) und Softwarelizenzen.

Bewertung/Entscheidungsvorschlag

Die Ressourcenausstattung des Bachelorstudiengangs Cybersicherheit ist gut auf die Anforderungen des Studiengangs abgestimmt und ermöglicht eine praxisorientierte

Ausbildung der Studierenden. Der Studiengang verfügt über alle notwendigen materiellen und technischen Ressourcen, um eine qualitativ hochwertige Lehre sicherzustellen. Die Fachbereiche sind mit moderner IT-Infrastruktur und spezialisierten Labors ausgestattet, die für die praxisnahe Ausbildung in Cybersicherheit erforderlich sind. Dazu gehören unter anderem fortschrittliche Tools und Software, die den Studierenden ermöglichen, praxisorientierte Erfahrungen zu sammeln und sich intensiv mit aktuellen Technologien sowie Sicherheitspraktiken auseinanderzusetzen. Zudem wird bei Bedarf kontinuierlich in Studienmaterialien, Lizenzen und weitere technische Ausstattungen investiert, um den Studierenden eine adäquate Ausbildung zu bieten.

Der Studiengang entspricht den Anforderungen gemäß § 12 Abs. 1 Studienakkreditierungsverordnung SH.

Prüfungssystem

Dokumentation

Das Prüfungssystem des Studiengangs ist konsequent kompetenzorientiert gestaltet. Die Auswahl der Prüfungsformen ist spezifisch auf die in den jeweiligen Modulen zu erwerbenden Lernergebnisse und Kompetenzen abgestimmt. Ziel ist es nicht nur, Faktenwissen abzufragen, sondern die Fähigkeit zur Analyse, Anwendung und Problemlösung zu überprüfen.
Es kommt ein breites Spektrum an Prüfungsformen zum Einsatz, um den unterschiedlichen Kompetenzdimensionen gerecht zu werden und sicherzustellen, dass Studierende im Studienverlauf vielfältige Prüfungserfahrungen sammeln:

- Klausuren (z. B. „Einführung in die Programmierung", „Datenbanken"): Zur Überprüfung von grundlegendem Fach- und Methodenwissen in den Basismodulen.
- Projektarbeiten und Hausarbeiten (z. B. „Fortgeschrittene Programmierung"): Zur Bewertung der Fähigkeit, komplexe Problemstellungen über einen längeren Zeitraum selbstständig und/oder im Team zu bearbeiten.
- Präsentationen und Referate (z. B. in Seminaren oder als Teil von Projektarbeiten): Zur Überprüfung der Kommunikations- und Präsentationskompetenz.
- Kolloquium: Zur Verteidigung der wissenschaftlichen Arbeit und zur Überprüfung des tiefgehenden Verständnisses des bearbeiteten Themas.

Um die vielfältigen, anwendungsorientierten Kompetenzen adäquat zu erfassen, setzt das Prüfungskonzept des Studiengangs auch auf Portfolioprüfungen und die Kombination aus verschiedenen Teilleistungen vor (z. B. Klausur, Ausarbeitung und Präsentation). Diese didaktische Entscheidung gründet sich auf die spezifischen Anforderungen der unterschiedlichen Modultypen:

- In Modulen mit Programmieranteil (Web-Anwendungen, Fortgeschrittene Programmierung, Cloud Computing) ermöglicht dies die Bewertung der

unterschiedlichen Facetten einer Programmierleistung (Code-Funktionalität, Aspekte des
Softwaredesigns, Qualität der Dokumentation) zu kombinieren mit kritischer Reflexion über den Einsatz von KI bei der Code-Generierung, was durch eine einzelne Prüfung oder Abgabe kaum abgebildet werden kann, durch ein Portfolio aus praktischen Aufgaben und reflektierenden Berichten jedoch sehr gut.

- Module mit projektartigem Charakter im Unternehmenskontext (Einführung in die ABWL, Geschäftsprozessmanagement, IT-Management), profitieren von dynamischen Mischformen der Prüfung. Hier können Teilleistungen wie die Ausarbeitung eines Konzepts, eine überzeugende Präsentation vor einem fiktiven Managementgremium und die aktive Teilnahme an Fachdiskussionen kombiniert werden. Dies simuliert die realen Anforderungen des Berufslebens, wo Fachwissen, Überzeugungskraft und Kommunikationsstärke gleichermaßen zum Erfolg beitragen.
- In Modulen, die verhaltensbezogene Elemente beinhalten (Cybersicherheit und menschliches Verhalten – auch mit Elementen des digitalen und psychologischen Selbstschutzes) ist ein Portfolio mit Elementen der Reflektion bzw. interaktiven Elementen unerlässlich.

Dies ermöglicht gleichzeitig eine flexiblere Anpassung an die Herausforderung des sich aktuell sehr dynamisch entwickelnden Einflusses von generativer KI auf die Wahl einer didaktisch sinnvollen Prüfungsform.
Die grundsätzlichen Fragen der Organisation der Prüfungen obliegt dem Prüfungsamt des federführenden Fachbereichs Wirtschaft in enger Abstimmung mit den Prüfenden beider Fachbereiche. Die Regelungen sind in der studiengangsspezifischen Prüfungsordnung (siehe Anhang D) verbindlich festgelegt und werden den Studierenden transparent kommuniziert.
Dies stellt einen geordneten und verlässlichen Prüfungsablauf sicher.

Bewertung

Die Prüfungsmodalitäten für jedes Modul sind verbindlich im Modulhandbuch festgelegt, was den Studierenden eine transparente und gut planbare Struktur bietet. Die Voraussetzungen für die Teilnahme an Prüfungen sind für ein Modul gemäß § 4 der Prüfungsordnung aufgeführt. Die Verantwortlichkeit für die Sicherstellung der Angemessenheit der Prüfungsbelastungen liegt gemäß der Qualitätssatzung der HAW Kiel primär bei den Modulverantwortlichen und der Studiengangsleitung. Diese Struktur garantiert eine kontinuierliche Überprüfung und Anpassung des Prüfungskonzepts, um sicherzustellen, dass diese den Qualifikationszielen des Studiengangs entsprechen. Die Auswahl der Prüfungsformen steht im Einklang mit den Kompetenzen der jeweiligen Module (u.a. schriftliche Prüfungen, Präsentation, Portfolio, Projektarbeit). Auch in den Gesprächen mit den Studierenden wurde das Prüfungssystem als fair und überwiegend gut organisiert wahrgenommen, was zu einer insgesamt positiven Einschätzung führt.

Das Kriterium ist erfüllt.

Der Studiengang entspricht den Anforderungen gemäß § 12 Abs. 4 Studienakkreditierungsverordnung SH.

Studierbarkeit

Dokumentation

Die Gewährleistung der Studierbarkeit des Curriculums in der Regelstudienzeit von sieben Semestern hat bei der Konzeption des Studiengangs höchste Priorität. Hierfür werden strukturelle und organisatorische Maßnahmen getroffen:

Verantwortlichkeiten und Organisation: Die Verantwortlichkeiten sind durch eine Kooperationsvereinbarung zwischen den Fachbereichen klar geregelt. Der Studiengang wird administrativ klar von einem einzelnen Fachbereich geführt, was den Studierenden eine zentrale Anlaufstelle für alle organisatorischen Belange (Einschreibung, Prüfungsamt etc.) bietet. Die akademische Leitung des Studiengangs wird von zwei Studiengangsverantwortlichen wahrgenommen, d. h. einer Professorin oder einem Professor aus jedem der beiden Fachbereiche, um eine enge Abstimmung und Einbeziehung beider Fachbereiche jederzeit zu gewährleisten. Die formale Studiengangsleitung alterniert regelmäßig zwischen beiden Studiengangsverantwortlichen. Ein verlässlicher Studienbetrieb ist durch eine langfristige Lehrplanung und die feste Verankerung der Module in den Deputaten der Lehrenden sichergestellt.

Transparente Information: Die Studierenden werden durch verschiedene Kanäle regelmäßig und transparent über alle Belange des Studiums informiert. Dazu gehören die offizielle Hochschulwebsite, die Lernplattform Moodle, regelmäßige Informationsveranstaltungen durch die Studiengangsleitung sowie die direkte Kommunikation mit den Lehrenden und der Fachschaft. Das Modulhandbuch und die Prüfungsordnung sind jederzeit online einsehbar.

Workload und Belastung: Die Zuordnung der Leistungspunkte zu den Modulen erfolgt auf Basis bestehender Module bzw. für neue Module auf Basis von Erfahrungswerten aus vergleichbaren Modulen, wobei der gesamte studentische Arbeitsaufwand (Präsenzzeit, Vor- und Nachbereitung, Prüfungsvorbereitung) berücksichtigt wird. Die Kombination unterschiedlicher Prüfungsformen je Semester vermeidet beispielsweise Häufungen von Klausuren im Prüfungszeitraum und trägt somit zu einer angemessenen Workload-Dichte bei. Eine regelmäßige Überprüfung des tatsächlichen Workloads erfolgt sowohl im Rahmen der Lehrevaluationen als auch im Rahmen der Student Lifecycle Evaluation (SLE). Die Ergebnisse werden, zusammen mit den entsprechenden regelmäßigen Studiengangssnapshots der HAW, von den Studiengangsverantwortlichen beider Fachbereiche analysiert, um bei Bedarf Anpassungen im Curriculum oder den Modulen vorzunehmen.

Betreuung und Beratung: Den Studierenden steht ein umfassendes Betreuungs- und Beratungsangebot zur Verfügung. Die Studiengangsleitung bzw. die Studiengangsverantwortlichen sind die ersten Ansprechpartner*innen für die fachliche Studienberatung. Darüber hinaus bieten alle Lehrenden regelmäßige Sprechstunden an. Für

überfachliche Fragen und bei persönlichen Herausforderungen stehen u. a. die Zentrale Studienberatung (ZSB), das International Office und die psychosoziale Beratung der Hochschule zur Verfügung. Die zuständige Fachschaft ist primär die des federführenden Fachbereichs Wirtschaft. Angedacht ist zudem nach Etablierung des Studiums die Einrichtung eines Mentoring-Programms, um Studierende höherer Semester mit Erstsemester-Studierenden in Kontakt zu bringen, was angesichts der kleinen Kohortengröße einen nahen und direkten Austausch ermöglicht.

Überwachung Studierbarkeit und Aktualität: Für die Überwachung der Qualität von Studium und Lehre am Fachbereich Wirtschaft ist der vom Konvent gewählte Studiengangsausschuss zuständig, der mindestens einmal pro Semester tagt und vom Prodekan für Studium und Lehre geleitet wird. Er überwacht insbesondere die strategische Studiengangsqualität (Angemessenheit der Qualifikationsziele, Eignung des Curriculums und seiner grundsätzlichen Umsetzung im Studienprogramm) sowie die operative Qualität der Durchführung von Studium und Lehre. Der Studiengangsausschuss entwickelt wo nötig auf der Grundlage von Evaluationen, Qualitätsberichten, Statistiken und/oder anderen Analysen Maßnahmenvorschläge zur Verbesserung der Qualität. Die Modulverantwortung (inkl. Pflege bzw. Aktualisierung der Modulinhalte und Modulbeschreibungen, Ansprechpartner für Lehrende und für Studierende des Moduls) liegt bei den Modulverantwortlichen; diese Aufgabe wird von hauptamtlich Lehrenden wahrgenommen.

Bewertung

Die Studierbarkeit des Bachelorstudiengangs Cybersicherheit wird von den Gutachtern als gut eingeschätzt. Die strukturierte Studienorganisation und die klare Gliederung des Studienverlaufs tragen maßgeblich dazu bei, dass die Studierenden in der Regelstudienzeit erfolgreich durch das Studium geführt werden können. Die im Studienplan integrierten Mobilitätsfenster ermöglichen es den Studierenden, während des Studiums wertvolle Erfahrungen im Ausland zu sammeln, ohne dass dies zu einem Verzögerung im Studienverlauf führt. Die Gespräche mit den Studierenden und Lehrenden belegen, dass diese Fenster auch in anderen studiengängen durch eine enge Abstimmung mit den Partnerhochschulen gut in die Studienstruktur eingebunden werden können.

Ein weiterer wichtiger Punkt für die gute Studierbarkeit sind die klaren Prüfungsmodalitäten, die im Modulhandbuch festgelegt sind und eine frühzeitige und nachvollziehbare Planung ermöglichen. Aus dem Modulhandbuch geht hervor, dass Module in der Regel mindestens fünf Leistungspunkte umfassen und mit einer Prüfung abgeschlossen werden, die gelegentlich aus zwei Teilen besteht. Die Studiengangsleitungen erhalten rechtzeitig vor Beginn des Semesters Informationen über die geplanten Modulprüfungen, und es wird darauf geachtet, dass die Prüfungsdichte den Belastungen der Studierenden entspricht. Die Studierenden berichten, dass sie bei Bedarf jederzeit auf die Dozenten zugehen können, was die Studienorganisation erheblich vereinfacht und das Gefühl der Nähe zu den Lehrenden stärkt. Die Studierenden erhalten ausreichend Unterstützung, um ihr Studium erfolgreich und in der Regelstudienzeit zu absolvieren.

Die Arbeitsbelastung der Studierenden und die Anforderungen an sie werden regelmäßig durch Evaluationen der Lehrveranstaltungen sowie ergänzende Befragungen im Studendierendenlebenszyklus überprüft und gegebenenfalls angepasst.

Das Kriterium ist erfüllt.

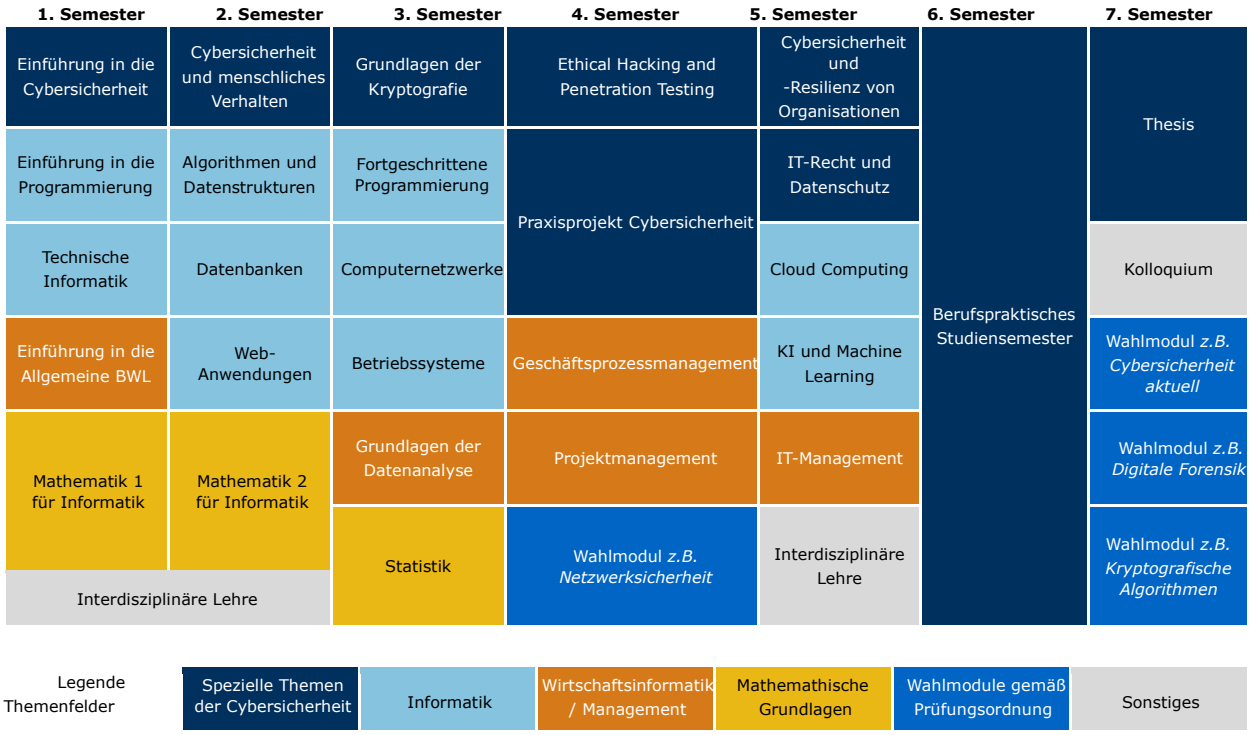
Der Studiengang entspricht den Anforderungen gemäß § 12 Abs. 5 Studienakkreditierungsverordnung SH.

2.2.3 Fachlich-Inhaltliche Gestaltung des Studiengangs

(§ 13 Studienakkreditierungsverordnung SH)

Dokumentation

Das Curriculum des Studiengangs „Cybersicherheit" ist als ein integratives und progressiv aufgebautes Programm konzipiert, das die Studierenden schrittweise von den Grundlagen zu breiten und vertieften sowie anwendungsorientierten Kompetenzen führt. Die wesentlichen curricularen Elemente sind die thematischen Säulen Cybersicherheit, Informatik, Wirtschaft/Management und mathematische Grundlagen, ergänzt durch Praxisphasen und Wahlmöglichkeiten.



Bei der Konzeption des Studiengangs wurden fachspezifische Referenzrahmen berücksichtigt, unter anderem die Empfehlungen des „Cybersecurity Curricula Guidelines" (CSEC 2017) von

ACM et al[2] mit acht „Knowledge Areas"[3] sowie die Anforderungen gängiger Industriestandards wie dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[4]. Aktuelle Empfehlungen der Gesellschaft für Informatik e.V. (GI) für

Cybersicherheit oder IT-Sicherheit liegen nicht vor, die letzte Empfehlung datiert auf Oktober 2006[5], daher wurde in Teilen auch auf Empfehlungen der Gesellschaft für Informatik e.V. (GI) für Informatik-Studiengänge (Typ 2)[6] sowie Wirtschaftsinformatik-Studiengänge[7] zurückgegriffen. Diese Kombination stellt sicher, dass das Curriculum sowohl wissenschaftlich fundiert als auch an den Bedarfen der Praxis ausgerichtet ist.

Das Curriculum folgt dabei einer klaren Logik aus drei aufeinander aufbauenden Phasen:

- Erste Phase, Semester 1-3: **Grundlagen**. In den ersten drei Semestern wird das Fundament gelegt. Die Module „Technische Informatik", „Betriebssysteme" und „Computernetzwerke" vermitteln die technische Grundlage aus der systemnahen Informatik. Die Module „Einführung in die Programmierung", „Algorithmen und Datenstrukturen", „Fortgeschrittene Programmierung", „Datenbanken" und „Web-Anwendungen" bilden einen Strang an Grundlagen zur Programmierung und Anwendungsentwicklung. Parallel dazu schaffen „Einführung in die allgemeine Betriebswirtschaftslehre" und „Geschäftsprozessmanagement" (im 4. Semester) das betriebswirtschaftliche Kontextverständnis, um Wertschöpfung und Prozesse in Unternehmen zu verstehen. Die Mathematik- und Statistik-Module liefern die notwendigen formalen Methoden, die vertiefend beispielsweise für die Kryptografie und Datenanalyse benötigt werden. Parallel dazu werden bereits in dieser ersten Phase des Studiums mit „Einführung in Cybersicherheit", „Cybersicherheit und menschliches Verhalten" und „Grundlagen der Kryptografie" Grundlagen gelegt, um die Inhalte alle Module im Kontext der Cybersicherheit verstehen zu können sowie inhaltliche Akzente zu setzen.

[2] Cybersecurity Curricular Guidelines, a joint effort of the ACM, IEEE Computer Society, AIS SIGSAC, and IFIP WG 11.8. https://cybered.hosting.acm.org/wp/

[3] Wie oben beschrieben, ist der Studiengang bewusst nicht primär darauf auszurichten, Entwickler*innen sicherer Software, Hardware oder Produkte auszubilden. Insofern sind die Knowledge Areas „Software Security" und „Component Security" nicht vollständig abgedeckt. Auch andere Knowledge Area wie insbesondere „Social Security" können in der Tiefe eines Bachelor-Studiengangs nicht vollständig abgedeckt, aber als Referenznahmen genutzt werden.

[4] IT-Grundschutz-Kompendium (Edition 2023). Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GSKompendium/IT_Grundschutz_Kompendium_Edition2023.pdf

[5] IT-Sicherheit in der Ausbildung (Oktober 2006). Bonn: Gesellschaft für Informatik e.V. https://dl.gi.de/items/2549ed9a-6c00-4d38-a390-1cc2c9ff75ac

[6] Empfehlungen für Bachelor- und Masterprogramme im Studienfach Informatik an Hochschulen (Juli 2016). Bonn: Gesellschaft für Informatik e.V. https://dl.gi.de/items/0986c100-a3b9-47c8-8173-54c16d16c24e

[7] Rahmenempfehlung für die Ausbildung in Wirtschaftsinformatik an Hochschulen (März 2017). Bonn: Gesellschaft für Informatik e.V. https://dl.gi.de/items/ef52ab08-2440-4120-bcd0-c46a5218066e sowie Rahmenempfehlung für Studiengänge in Wirtschaftsinformatik an Hochschulen (September 2024). Bonn: Gesellschaft für Informatik e.V. et al. https://wirtschaftsinformatik.de/termine-startseite/rahmenempfehlung-studiengang-2024

- Zweite Phase, Semester 4-5: **Integration und Vertiefung**. Diese Phase dient der Integration des Gelernten in größeren Kontexten und der damit verbundenen inhaltlichen Vertiefung. Kernmodule sind „Ethical Hacking and Penetration Testing", „Cybersicherheit und -Resilienz von Organisationen" sowie das „Praxisprojekt Cybersicherheit", die das Herzstück der Cybersicherheits-Ausbildung bilden und den Studierenden ermöglichen, ihr Wissen aus allen Bereichen auf integrierte, komplexe Problemstellungen anzuwenden. Module wie „IT-Management" und „Projektmanagement" runden das wirtschaftliche Profil ab, während Module zu „Cloud-Computing" und „KI und Machine Learning" die eher technischen Fähigkeiten vertiefen.
- Dritte Phase, Semester 6-7: **Praxis und Professionalisierung**. Das 6. Semester ist vollständig dem „berufspraktischen Studiensemester" gewidmet, in dem die Studierenden ihre Kompetenzen in einem Unternehmen oder einer Organisation anwenden und vertiefen. Das 7. Semester dient der weiteren individuellen Professionalisierung durch drei zusätzliche Wahlmodule und dem akademischen Abschluss durch die Anfertigung der Thesis und die Durchführung des Kolloquiums.

Eine regelmäßige Aktualisierung ist im Bereich Cybersicherheit erforderlich und erfolgt durch Anpassung der spezifischen Modulinhalte und Wahlmodule. Die Modulbeschreibungen, sowie alle Änderungen dieser werden jedes Semester von den Konventen der Fachbereiche freigegeben.
Das zum Zeitpunkt der Feinkonzeption angedachte Angebot an disziplinspezifischen Wahlmodulen umfasst die im Modulhandbuch dargestellten Wahlmodule „Netzwerksicherheit", „Cybersicherheit aktuell", „Digitale Forensik", sowie „Kryptografische Algorithmen". Darüber hinaus werden relevante Wahlmodule aus den Wahlmodulkatalogen der Informatik, Wirtschaftsinformatik und BWL angeboten, die zusammen mit Studierenden der entsprechenden Studiengänge besucht werden können. Im Sinne der interdisziplinären Ausrichtung des Studiengangs sind zudem perspektivisch Wahlmodule angedacht, die relevante Aspekte im Überlappungsbereich mit weiteren Fachbereichen der HAW Kiel aufnehmen, beispielsweise:

- Wahlmodul „Cybercrime" (Prof. Dr. Anna Isenhardt, Fachbereich Soziale Arbeit und Gesundheit): Im Wahlmodul wird zunächst ein Überblick über verschiedene Erscheinungsformen und die Verbreitung (im Hell- und Dunkelfeld) von Cybercrime mit einem Fokus auf Cybercrime im sogenannten engeren Sinne gegeben. Anschließend wird der Frage nachgegangen, wer die Täter*innen sind und Folgen für betroffene Unternehmen und Privatpersonen beleuchtet. Im zweiten Teil des Themenschwerpunkts liegt der Fokus auf der Strafverfolgung: Wie und wo kann Anzeige erstattet werden? Warum ist das sinnvoll? Welche Gründe sprechen dafür, welche dagegen? Wie laufen Strafverfahren ab? Was sind Schwierigkeiten bei der Strafverfolgung im Bereich Cybercrime?

- Wahlmodul „Cybersicherheit in der integrierten Unternehmenskommunikation“ (Prof. Dr. Holger Ihle, Fachbereich Medien): Das Wahlmodul fokussiert praxisorientiert auf die Zusammenarbeit zwischen Cybersicherheitsexperten und Unternehmenskommunikatoren, um Organisationen resilient gegen Cyberangriffe zu machen. Studierende lernen, wie interne Kommunikationsmaßnahmen entwickelt und umgesetzt werden, um Mitarbeitende für Sicherheitsrisiken zu sensibilisieren und präventives Verhalten zu fördern. Zudem wird vermittelt, wie Expertenteams und Kommunikationsabteilungen im Falle eines Cyberangriffs koordiniert Krisenkommunikation betreiben und gemeinsam Reputationsrisiken minimieren können. Praktische Übungen, wie die Entwicklung von Sicherheitskampagnen und die Simulation von Krisenszenarien, vertiefen die erworbenen Kenntnisse.

Bewertung

Die fachlich-inhaltliche Gestaltung des Bachelorstudiengangs Cybersicherheit an der HAW Kiel wird von den Gutachtern insgesamt sehr positiv bewertet. Die Struktur des Studiengangs sowie die Inhalte der einzelnen Module entsprechen den aktuellen Anforderungen des Fachgebiets und bieten eine solide Grundlage für die Ausbildung von Fachkräften im Bereich der Cybersicherheit. Es wird deutlich, dass der Studiengang eng mit der Praxis und den sich wandelnden Anforderungen der Praxis verzahnt ist.

Die regelmäßige Evaluation der Lehrveranstaltungen, zusammen mit Lifecycle-Erhebungen und Absolventenevaluationen, wird sicherstellen, dass der Studiengang kontinuierlich an die aktuellen Bedürfnisse und Entwicklungen im Bereich Cybersicherheit angepasst wird. Die enge Vernetzung mit Netzwerken wie der Digitalen Wirtschaft Schleswig-Holstein sowie die Kooperationen mit regionalen Unternehmen fördern die Integration praxisorientierter Erfahrungen und realer Sicherheitsfragen aus der Wirtschaft. Diese Nähe kann auch durch die Praxisprojekte, bei denen Unternehmen Themen anbieten und Studierende diese bearbeiten, weiter unterstützt werden.

Ein wesentlicher Aspekt, der von den Gutachtern besonders betont wurde, ist die Notwendigkeit eines starken Praxisbezugs in den Laboren. Die Studierenden lernen nicht nur theoretische Konzepte, sondern setzen diese auch in realitätsnahen Szenarien um. So kann beispielsweise der Bereich „Hacking“ durch Virtualisierungs- und Laborkonzepte effektiv in der Lehre eingebunden werden. Die Gutachter regen an, dass ein „Security Operations Center (SOC)“, Studierenden helfen kann, Sicherheitsvorfälle zu analysieren und zu bearbeiten. Auch ein Plan-Rollenspiel zur NIS2-Richtlinie könnte integriert werden, in dem Studierende verschiedene Rollen übernehmen, wie z.B. die eines IT-Sicherheitsbeauftragten, Krisenstabsmitglieds oder Behördenvertreters. In diesem Szenario könnten sie ein Cyberangriffsszenario durchspielen, bei dem sie Entscheidungen zur Incident Response und Risikomanagement treffen. Besonders in der NIS2-Richtlinie spielen Themen wie Governance,

Compliance und die operative Umsetzung eine zentrale Rolle, die auch in den Laboren praktisch geübt werden sollten.

Die Gutachter empfehlen weiterhin, dass der Wahlbereich des Studiengangs stärker auf spezialisierte Themen wie Ethical Hacking, Network Hacking, Penetration Testing, Proof-of-Concept-Analysen und Kosten-/Risikoanalysen (ROSI) ausgerichtet wird. Diese Themen sind zentral für die berufliche Praxis und sollten gezielt in den Modulen behandelt werden, um die Studierenden bestmöglich auf die Anforderungen der Cybersicherheitsbranche vorzubereiten. Auch die Post-Quantum-Kryptographie (PQC) sollte thematisch aufgenommen werden, da dieses Thema zunehmend an Bedeutung gewinnt.

Die Zusammenlegung von Lehrveranstaltungen und praktischen Übungen mit anderen Studiengängen ist grundsätzlich sinnvoll und ermöglicht die Nutzung von Synergien. Gleichzeitig sollte innerhalb dieser gemeinsamen Formate eine klare inhaltliche Differenzierung für die Studierenden des CS-Studiengangs erfolgen. So könnten CS-Studierende in ihren Kleingruppen spezifische, vertiefende Aufgaben bearbeiten, die über den allgemeinen Vorlesungsstoff hinausgehen. Im Web-Anwendungspraktikum sollten bestehende Anwendungen beispielsweise systematisch nach OWASP-Kriterien analysiert und abgesichert werden, anstatt ausschließlich funktionale Web-Anwendungen zu entwickeln. Entsprechende CS-spezifische Vertiefungen sind auch in Datenbankpraktika sowie in BWL-Modulen sinnvoll, etwa durch die Behandlung von Gefährdungs-, Risiko- und Kostenanalysen. Auf diese Weise wird sichergestellt, dass die Studierenden praxisrelevante und studiengangsspezifische Kompetenzen erwerben, die sie gezielt auf berufliche Anforderungen vorbereiten.

Ein weiterer Punkt, der aus Sicht der Gutachter von Bedeutung ist, ist die Einbindung von Themen wie IT-Recht, Datenschutz und Ethik, die eine Schnittstelle zur praktischen Cybersicherheit darstellen. Dabei wird die Bedeutung von Datenschutzgesetzen (wie DSGVO und NIS2) und ethischen Fragestellungen in der Cybersicherheit betont. Das Fach „Cybersicherheit und menschliches Verhalten" bietet hier bereits gute Ansätze, sollte jedoch weiter ausgebaut werden, insbesondere durch die Diskussion gesellschaftlicher und psychologischer Implikationen von Cybersicherheitsmaßnahmen.

Darüber hinaus wird das Modul „KI und Machine Learning" als besonders sinnvoll erachtet, jedoch wird angeregt, zu prüfen, wie das Modul „Statistik" diese Themen fundiert vorbereiten kann, um eine tiefere Vernetzung der Disziplinen zu gewährleisten. Zudem könnte ein eigenes Labor für Cybersicherheitsspezifische Themen wie KI-gestützte Angriffe und Penetration Testing eingeführt werden (s.o.).

Es wird angeregt, einige der oben genannten Themen und praktischen Elemente noch gezielter in den Studiengang zu integrieren, um die Studierenden auf die neuesten Entwicklungen in der Cybersicherheit vorzubereiten.

Das Kriterium ist erfüllt.

Der Studiengang entspricht den Anforderungen gemäß § 13 Studienakkreditierungsverordnung SH.

2.2.4 Studienerfolg

(§ 14 Studienakkreditierungsverordnung SH)

Dokumentation
Die Sicherung und kontinuierliche Verbesserung des Studienerfolgs ist ein zentrales Anliegen der beteiligten Fachbereiche und ein persönliches Anliegen der Initiatoren bzw. Studiengangsverantwortlichen beider Fachbereiche.
Für die Evaluation und Verbesserung des Erfolgs während des Studiums wird ein systematischer Regelkreis des Monitorings unter aktiver Beteiligung der Studierenden etabliert. Die primären Instrumente zur Erfassung von Daten sind die standardisierten Lehrevaluationen der HAW Kiel (Evasys), die im Laufe jedes Semesters durchgeführt werden, sowie die zentralen „Student Lifecycle Evaluation"-Befragungen der HAW Kiel.
Die Ergebnisse dieser Evaluationen und Befragungen werden von den Studiengangsverantwortlichen systematisch ausgewertet. Mindestens einmal pro Semester werden die zusammengefassten Ergebnisse mit den Studiengangsleitungen diskutiert und soweit möglich Studierendenvertreter z. B. aus der Fachschaft oder das Feedback von Externen (z. B. im Rahmen von Praktika oder Gastvorträgen) mit einbezogen. In diesem Rahmen werden Stärken und Schwächen analysiert und bei Bedarf konkrete Maßnahmen zur Verbesserung abgeleitet, beispielsweise kleinere Anpassungen in einzelnen Modulen bis hin zu größeren curricularen Änderungen reichen.
Dieser etablierte Regelkreis stellt eine fortlaufende Überprüfung der Ergebnisse und deren Nutzung für die Weiterentwicklung des Studiengangs sicher.
Zum Studienerfolg gehört zudem – sofern aus Sicht der Absolvent*innen gewünscht – der erfolgreiche Einstieg ins Berufsleben nach dem Bachelor-Abschluss. Hierzu eröffnet der eingangs erwähnte Fachkräftemangel breite Perspektiven, während gleichzeitig bereits im Studium Wert darauf gelegt wird, Kontakte und persönliche Netzwerke aufzubauen sowohl in den Praxisanteilen des Studiums (Praxisprojekt Cybersicherheit, berufspraktisches Studiensemester, mögliche Zusammenarbeit z. B. mit Unternehmen für die Bachelor-Thesis) als auch zu Vertreter*innen potentieller Arbeitergeber (beispielsweise im Rahmen von Gastvorträgen im Seminar „Cybersicherheit aktuell"). Perspektivisch ist eine Evaluation des erfolgreichen Studienabschlusses auch möglich durch eine Vernetzung und ggf. spätere systematische Befragung von Absolvent*innen.

Bewertung

Die Gutachter konnten sich durch die Unterlagen sowie durch die Gespräche mit der Vizepräsidentin für Studium und Lehre, der Leitung der Abteilung Hochschulentwicklung und

den Studiengangsverantwortlichen davon überzeugen, dass der Bachelorstudiengang Cybersicherheit einem kontinuierlichen Monitoring unterliegen wird, das durch ein effektives Qualitätsmanagementsystem für Studium und Lehre unterstützt wird. Dieses Monitoring umfasst regelmäßige Evaluationen der Lehrveranstaltungen inkl. systematische Rückmeldung an die Studierenden sowie Studiengangssnapshots. So wird eine kontinuierliche Verbesserung der Studienbedingungen, Lehrmethoden und -inhalte ermöglicht. Die Studierenden haben dabei die Möglichkeit, aktiv an der Weiterentwicklung des Studiengangs teilzunehmen, sowohl durch die regelmäßige studentische Lehrevaluation als auch durch weitere spezifische Befragungen, die den gesamten Student Life Cycle abdecken. Auf diese Weise wird sichergestellt, dass ihre Erfahrungen und Wünsche in den Verbesserungsprozess einfließen und dass die Qualität des Studiengangs regelmäßig überprüft und angepasst wird. Dank dieses transparenten und partizipativen Monitoringprozesses werden die Studiengangsverantwortlichen in der Lage sein, frühzeitig auf Herausforderungen zu reagieren und sicherzustellen, dass die Studierenden gute Voraussetzungen für ihren Studienerfolg haben. Die Studierenden berichten in den Gesprächen ergänzend von einem guten Verhältnis zu den Lehrenden und einer praxisorientierten Ausbildung, die sie gut auf den Arbeitsmarkt vorbereitet.

Das Kriterium ist erfüllt.

Der Studiengang entspricht den Anforderungen gemäß § 14 Studienakkreditierungsverordnung SH.

2.2.5 Geschlechtergerechtigkeit und Nachteilsausgleich

(§ 15 Studienakkreditierungsverordnung SH)

Dokumentation

Der Studiengang „Cybersicherheit" ist den Zielen der Geschlechtergerechtigkeit und der Chancengleichheit in vollem Umfang verpflichtet. Im 6. Leitsatz der HAW Kiel wird explizit Bezug genommen auf diesen Bereich: „Unsere Hochschule lebt Vielfalt. Sie gestaltet Bildungsprozesse gendergerecht, interkulturell und diskriminierungsfrei." Die Konzepte der HAW Kiel in diesen Bereichen bzw. die Angebote der entsprechenden Einrichtungen der HAW Kiel (z. B. die Gleichstellungsstelle sowie die Diversitätsbeauftragte der HAW Kiel) finden auf allen Ebenen des Studiengangs Anwendung.
Das Informatik-affine Feld der IT-Sicherheit ist traditionell männlich dominiert. Daher werden Maßnahmen ergriffen, um den Studiengang für Studieninteressierte aller Geschlechter attraktiv zu machen. Dies beginnt bereits bei der Namenswahl und Ausgestaltung von „Cybersicherheit" als breiteres Themenfeld, das nicht nur technische Belange, sondern organisatorische und sozio-technische Belange stärker als andere vergleichbare Studiengänge mit einbezieht. Zu den Maßnahmen gehören weiterhin eine gender- und diversitätssensible Darstellung in allen Informationsmaterialien, die Betonung der interdisziplinären und

kommunikativen Aspekte des Berufsfeldes, die über rein technische Tätigkeiten hinausgehen, und nach Möglichkeit die aktive Einbeziehung von Praktikerinnen oder Studentinnen als Rollenvorbilder.
Benachteiligte Studierende können auf Antrag individuelle Anpassungen der Studien- und Prüfungsbedingungen erhalten, um chancengerecht am Studium teilhaben zu können. Regelungen zum Nachteilsausgleich sind nicht dokumentiert, da diese an die individuelle Situation anzupassen und daher nicht zu verallgemeinern sind. Wer erstmalig einen Antrag auf Nachteilsausgleich stellt, soll in einem formlosen Schreiben an den Prüfungsausschuss-Vorsitzenden die Beeinträchtigungen, sowie die beantragten Maßnahmen des Nachteilsausgleichs aufführen, die für Prüfungen im Verlauf des Studiums relevant werden können. Dringend erforderlich ist, dass diesem Schreiben entsprechende Nachweise (z. B. fachärztliche Stellungnahmen) beigelegt werden. Hierbei braucht nicht die Behinderung oder chronische Erkrankung selbst benannt werden, doch muss aus dem Schreiben und den Nachweisen hervorgehen, welche Prüfungsbeeinträchtigungen aus der Behinderung oder chronischen Erkrankung resultieren, für die Nachteilsausgleiche beantragt werden. Auf diese Weise wird der Prüfungsausschuss dazu befähigt, über Erforderlichkeit und Angemessenheit der Nachteilsausgleiche zu entscheiden. Die Studiengangsleitung und die zentralen Beratungsstellen der Hochschule stehen für vertrauliche Beratungen zur Verfügung.

Bewertung

Die Hochschule verfolgt aktiv Konzepte zur Geschlechtergerechtigkeit und unterstützt Studierende in besonderen Lebenslagen. Sie setzt sich dafür ein, allen Studierenden unabhängig von persönlichen oder individuellen Voraussetzungen gleiche Chancen im Studium zu bieten. Für Studierende, die besondere Unterstützung benötigen – beispielsweise aufgrund familiäre Care Arbeit, einer Erkrankung oder einer Behinderung – stehen verschiedene Beratungs- und Unterstützungsangebote zur Verfügung, darunter das Familienservicebüro und die Beauftragte für Diversität. Zudem können Studierende einen Nachteilsausgleich beantragen.

Das Kriterium ist erfüllt.

Der Studiengang entspricht den Anforderungen gemäß § 15 Studienakkreditierungsverordnung SH.

Umsetzung des Qualitätsmanagements auf Ebene des Studiengangs

(§ 17 und § 18 Studienakkreditierungsverordnung SH)
Dokumentation

Hier wird von dem Arbeitsbereich Akkreditierung und Recht der Abteilung Hochschulentwicklung überprüft, wie das Qualitätsmanagementsystem der Hochschule im Fachbereich konkret

realisiert wird, um die Studienqualität kontinuierlich zu verbessern. Es wird geprüft, ob im Fachbereich Zuständigkeiten und Verantwortlichkeiten gemäß dem übergeordneten QM System für die Weiterentwicklung, Überprüfung sowie Einrichtung und Einstellung von Studiengängen festgelegt sind und ob dieses hochschulweit veröffentlicht ist. Auch wird geprüft, ob systematische Verfahren zum Umgang mit fachbereichsinternen Konflikten entwickelt sind und ob es ein fachbereichsinternes Beschwerdesystem gibt. Es wird überprüft, ob der Studiengang über Konzepte zur Umsetzung der notwendigen Prozesse und Maßnahmen im Rahmen des FH-Qualitätsmanagements verfügt und diese dokumentiert werden. Dabei wird u.a. geprüft, wie die Studierenden in die kontinuierliche Qualitätsentwicklung des Studiengangs innerhalb des Fachbereichs konkret eingebunden werden.

Das Qualitätsmanagement der HAW Kiel ist in einem engen, formalen Rahmen eingebettet und besteht aus den drei folgenden Elementen: - dem Prozessmanagement, - der internen Akkreditierung sowie - dem Qualitäts-Monitoring.
Der Aufbau, die Verantwortlichkeiten und der Ablauf der drei Instrumente sind in der Qualitätssatzung der HAW Kiel geregelt. Dabei gilt, dass alle Mitglieder der Hochschule im täglichen Handeln miteinander und in der individuellen Funktion dazu beitragen, die Qualität der Lehre für die Studierenden zu verbessern. Das Qualitäts-Monitoring dient der laufenden Prüfung der Studiengangsqualität als Grundlage für die Entwicklung von Maßnahmen zur Verbesserung von Studium und Lehre im laufenden Studiengang. Hierzu werden regelmäßig die Studiengänge überprüft und Gespräche zwischen Qualitätsbeauftragtem der Hochschule und den Studiengangsleitungen durchgeführt.

Das Qualitätsmanagement an den beteiligten Fachbereichen wird stets weiterentwickelt und auf allen Ebenen gelebt. Das Qualitätsmanagement ist sowohl für die gesamte HAW Kiel (Qualitätssatzung, s.o.) als auch für den federführenden Fachbereich Wirtschaft konzipiert. Letzteres wird in der Dokumentation unserer Bausteine detailliert festgelegt (siehe Anlage H). Bezogen auf den Studiengang ist unter anderem geplant, Teaching Analysis Polls (TAPs) durchzuführen in Zusammenarbeit mit dem Zentrum für Lernen und Lehrentwicklung der HAW Kiel. TAP ist eine partizipative Evaluationsmethode für qualitatives, dialogorientiertes, strukturiertes Feedback zur Lehrentwicklung. Es dient dazu, Lehrende und Studierende zu einer lehrebezogenen Fragestellung, z. B. zu einem neuen Lehrkonzept oder einem Studienabschnitt, gezielt in einen Austausch über die erlebten Lehr- und Lernprozesse zu bringen. Dabei werden von eine*r geschulte*n TAP-Moderator*in moderierte Kleingruppengespräche mit Studierenden in einer Lehrveranstaltung geführt, die zuvor mit der Lehrperson festgelegte Fragestellungen adressieren. Im Gegensatz zu klassischen, meist quantitativen Evaluationen steht beim TAP das gemeinsame Gespräch und die partizipative Mitgestaltung der Lehre im Mittelpunkt. Aufbauend z.B. auf Evaluations- und TAP-Ergebnissen ist ein jährliches Treffen der Studiengangsverantwortlichen sowie weiterer Lehrender beider Fachbereiche vorgesehen, um Herausforderungen und positive Aspekte zu diskutieren und ggf. Maßnahmen für die Weiterentwicklung des Studiengangs oder zur Verbesserung der Studierbarkeit ab- und einzuleiten. Sofern das angedachte Mentor*innenprogramm etabliert wurde, sollten die Erfahrungen der Mentor*innen hierzu mit einbezogen werden. Die

vereinbarten Maßnahmen sollten dokumentiert und der Fortschritt der Umsetzung dokumentiert und regelmäßig diskutiert werden, spätestens beim nächsten Treffen.

Bewertung

Das Qualitätsmanagementsystem der Hochschule gewährleistet, dass der Bachelorstudiengang Cybersicherheit kontinuierlich überwacht, bewertet und weiterentwickelt wird. Die HAW Kiel hat ein QM-System implementiert, das sowohl auf hochschulweiten als auch fachbereichsinternen Prozessen basiert. Das fachbereichsinterne Qualitätsmanagement konkretisiert die allgemeinen, in der Qualitätssatzung definierten QM-Prozesse und stellt sicher, dass der Studiengang in den Bereichen Lehre, Organisation und Studienbedingungen stetig verbessert wird.

Ein zentraler Bestandteil dieses Systems ist die regelmäßige Evaluation der Lehrveranstaltungen durch die Studierenden. Diese Feedbackprozesse ermöglichen es den Studierenden, ihre Perspektiven und Verbesserungsvorschläge aktiv einzubringen, wodurch die Lehrqualität kontinuierlich gesteigert werden kann. Die Ergebnisse dieser Evaluationen fließen in die Weiterentwicklung der Lehrinhalte und -methoden ein, die regelmäßig auf ihre Aktualität und Relevanz hin überprüft und angepasst werden.

Das Kriterium ist erfüllt.

Kooperationen mit nichthochschulischen Einrichtungen

(§ 19 Studienakkreditierungsverordnung SH)

Nicht relevant

Hochschulische Kooperationen

(§ 20 Studienakkreditierungsverordnung SH)

Nicht relevant

3 Begutachtungsverfahren

3.1 Allgemeine Hinweise

Der 7-semestrige Bachelorsudiengang Cybersicherheit ist ein neuer Studiengang (Erstakkreditierung)

3.2 Rechtliche Grundlagen

Staatsvertrag über die Organisation eines gemeinsamen Akkreditierungssystems zur Qualitätssicherung in Studium und Lehre an deutschen Hochschulen (Studienakkreditierungsvertrag)

Landesverordnung zur Regelung der Studienakkreditierung des Landes Schleswig-Holstein in der zuletzt geltenden Fassung.

3.3 Gutachter

Prof. Dr. Marian Margraf (FU Berlin)
Prof. Dr. Volker Skwarek (HAW Hamburg)
Prof. Dr. Jens Söldner (Hochschule Ansbach)
Thomas Holst (BT Nord)
Jakob Thöne (Universität Potsdam)

4 Datenblatt

4.1 Daten zum Studiengang zum Zeitpunkt der Begutachtung

Es liegen keine Daten vor (neuer Studiengang).

4.2 Daten zur Akkreditierung

Eingang der Selbstdokumentation:	10.07.2025
Zeitpunkt der Begehung:	24.11 und 25.11.2025
Akkreditierungszeitraum:	von 01.03.2026 bis 01.03.2034
Personengruppen, mit denen Gespräche geführt worden sind:	1. Vizepräsidentin für Studium und Lehre, Leitung Abteilung Hochschulentwicklung 2. Gesprächsgruppe mit Studiengangs- und Fachbereichsverantwortlichen (Dekan, Prodekan, Beauftragter für Studium und Lehre, Gleichstellungsbeauftragte, Auslandsbeauftragter, Studiengangsleitung) 3. Gesprächsgruppe mit Studierenden und Alumni 4. Gesprächsgruppe mit hauptamtlich Lehrenden des Studiengangs der CAU und der HAW

Beschluss des Präsidiums

Bachelor-Studiengang „Cybersicherheit“

Beschluss des Präsidiums

Das Präsidium der HAW Kiel beschließt am 28.01.2026 die Akkreditierung des Bachelorstudiengangs „Cybersicherheit“ ohne Auflagen bis zum 01.03.2034.