Grundlage – Anlage 1, BGBl. II Nr. 262/2015 idgF

Anlage 1.xx

LEHRPLAN DER HÖHEREN LEHRANSTALT FÜR CYBERSECURITY

I. STUNDENTAFEL[1]

(Gesamtstundenzahl und Stundenausmaß der einzelnen Unterrichtsgegenstände)

	Pflichtgegenstände, Verbindliche Übung	Wochenstunden Jahrgang I.	II.	III.	IV.	V.	Summe	Lehrverpflichtungsgruppe
A.	**Allgemeinbildende Pflichtgegenstände**							
1.	Religion/Ethik[2]	2	2	2	2	2	10	(III)
2.	Deutsch	3	2	2	2	2	11	(I)
3.	Englisch	2	2	2	2	2	10	(I)
4.	Geografie, Geschichte und Politische Bildung[3]	2	2	2	2	-	8	III
5.	Wirtschaft und Recht[4]	-	-	-	3	2	5	II bzw. III
6.	Bewegung und Sport	2	2	2	1	1	8	(IVa)
7.	Angewandte Mathematik	4	3	3	2	2	14	(I)
8.	Naturwissenschaften	3	2	2	2	-	9	II
B.	**Fachtheorie und Fachpraxis**							
1.	Software Technologies[5]	3	3	3	3	3	15	I
2.	Compliance und Ethics	-	2	2	2	2	8	II
3.	IT Infrastructure[5]	6	6	4	2	2	20	I
4.	Cyber Defense[5]	-	2	4	4	6	16	I
5.	Ethical Hacking[5]	-	2	4	4	5	15	I
6.	Security Lab[5]	4	4	4	6	6	24	II
C.	**Verbindliche Übung**							
	Soziale und personale Kompetenz[6]	1	1	-	-	-	2	III
	Gesamtwochenstundenzahl	32	35	36	37	35	175	
D.	**Pflichtpraktikum**	mindestens 8 Wochen in der unterrichtsfreien Zeit vor Eintritt in den V. Jahrgang						

	Freigegenstände, Unverbindliche Übung, Förderunterricht	Wochenstunden Jahrgang I.	II.	III.	IV.	V.	Lehrverpflichtungsgruppe
E.	**Freigegenstände**						
1.	Zweite lebende Fremdsprache[7]	2	2	2	2	2	(I)
2.	Kommunikation und Präsentationstechnik	–	–	2	2	–	III
3.	Naturwissenschaftliches Laboratorium	–	2	–	–	–	III

1 Durch schulautonome Lehrplanbestimmungen kann von der Stundentafel im Rahmen des IV. Abschnittes abgewichen werden.

2 Pflichtgegenstand für Schülerinnen und Schüler, die am Religionsunterricht nicht teilnehmen. Das Stundenausmaß des Pflichtgegenstandes Ethik ist nicht veränderbar.

3 Einschließlich volkswirtschaftlicher Grundlagen.

4 Die Lehrverpflichtungsgruppe III bezieht sich im Ausmaß von drei Wochenstunden auf den Bereich „Recht“.

5 Mit Übungen.

6 Mit Übungen sowie in Verbindung und inhaltlicher Abstimmung mit einem oder mehreren Pflichtgegenständen.

7 In Amtsschriften ist die Bezeichnung der Fremdsprache anzuführen.

4. Forschen und Experimentieren	2	–	–	–	–	III
5. Entrepreneurship und Innovation	–	–	–	2	–	III
F. Unverbindliche Übung						
Bewegung und Sport	2	2	2	2	2	(IVa)

G. Förderunterricht[8]

1. Deutsch
2. Englisch
3. Angewandte Mathematik
4. Fachtheoretische Pflichtgegenstände

8 Bei Bedarf parallel zum jeweiligen Pflichtgegenstand bis zu 16 Unterrichtseinheiten pro Schuljahr; Einstufung wie der entsprechende Pflichtgegenstand.

Stundentafel der Deutschförderklasse

Pflichtgegenstände, Verbindliche Übung	Wochenstunden pro Semester	Lehrverpflichtungsgruppen
1. Deutsch in der Deutschförderklasse	20	(I)
2. Religion	2	(III)
3. Weitere Pflichtgegenstände, Verbindliche Übung[1]	x[2]	Einstufung wie entsprechende/r Pflichtgegenstand, Verbindliche Übung
Gesamtwochenstundenzahl	x[3]	
Freigegenstände und Unverbindliche Übung[4]		

1 Einzelne oder mehrere Pflichtgegenstände (ausgenommen den Pflichtgegenstand Religion) sowie die verbindliche Übung gemäß der Stundentafel der Höheren Lehranstalt für Cybersecurity; die Festlegung der weiteren Pflichtgegenstände sowie der verbindlichen Übung erfolgt durch die Schulleitung.

2 Die Festlegung der Anzahl der Wochenstunden, die auf die einzelnen weiteren Pflichtgegenstände sowie die verbindliche Übung entfallen, erfolgt durch die Schulleitung; die Gesamtwochenstundenzahl der weiteren Pflichtgegenstände sowie der verbindlichen Übung ergibt sich aus der Differenz zur Gesamtwochenstundenzahl.

3 Die Gesamtwochenstundenzahl entspricht jener des jeweiligen Jahrganges gemäß der Stundentafel der Höheren Lehranstalt für Cybersecurity.

4 Wie Stundentafel der Höheren Lehranstalt für Cybersecurity.

II. ALLGEMEINES BILDUNGSZIEL

Siehe Anlage 1.

III. FACHBEZOGENES QUALIFIKATIONSPROFIL

1. Einsatzgebiete und Tätigkeitsfelder:

Die Absolventinnen und Absolventen der Höheren Lehranstalt für Cybersecurity sind befähigt, ingenieurmäßige Tätigkeiten im Bereich des Themengebietes selbstständig auszuführen. Sie sind in der Lage, sicherheitsrelevante Aufgaben entlang des gesamten Lebenszyklus von IT-Systemen zu übernehmen. Sie analysieren Bedrohungen, identifizieren Schwachstellen und wirken bei der Planung sowie Umsetzung geeigneter Schutzmaßnahmen mit.

Im Sinne des European Cybersecurity Skills Framework (ECSF) arbeiten sie in Rollen wie Security Analyst, Incident Responder oder System Hardening Specialist. Sie überwachen IT-Systeme und Netzwerke, erkennen Sicherheitsvorfälle und reagieren strukturiert darauf.

Darüber hinaus unterstützen sie beim Aufbau und Betrieb sicherer Infrastrukturen sowie bei der Umsetzung von Sicherheitsrichtlinien und Compliance-Vorgaben. Sie wirken bei Risikoanalysen mit und dokumentieren sicherheitsrelevante Prozesse nachvollziehbar. Durch die Anwendung aktueller Tools und Methoden tragen sie zur Prävention, Detektion und Reaktion auf Cyberangriffe bei. Sie kommunizieren sicherheitsrelevante Sachverhalte verständlich an technische und nicht-technische Zielgruppen. Teamarbeit, Verantwortungsbewusstsein und kontinuierliche Weiterbildung sind zentrale Bestandteile ihres beruflichen Handelns

2. Berufsbezogene Lernergebnisse des Abschnittes B:

Software Technologies:

Im **Bereich Softwareentwicklung und Architektur** können die Absolventinnen und Absolventen softwaretechnische Problemstellungen analysieren, in Modelle überführen und Anwendungen planen, entwerfen und implementieren; sie können moderne Architekturmuster, Schnittstellen und Entwicklungswerkzeuge fachgerecht anwenden.

Im **Bereich Datenmanagement** können die Absolventinnen und Absolventen Daten strukturieren, modellieren, speichern und abfragen; sie können geeignete Datenhaltungssysteme auswählen und Anwendungen entwickeln, die externe Datenquellen verarbeiten.

Im **Bereich Softwarequalität, Sicherheit und Betrieb** können die Absolventinnen und Absolventen Software testen, Schwachstellen analysieren und Sicherheitsmaßnahmen umsetzen; sie können automatisierte Build-, Test- und Deploymentprozesse anwenden und Software sicher in den Betrieb überführen.

Compliance und Ethics:

Im **Bereich Projekt- und Prozessmanagement** können die Absolventinnen und Absolventen Prozesse darstellen, analysieren und bewerten; sie können Projektmethoden anwenden und Kennzahlen zur Prozesssteuerung nutzen.

Im **Bereich Risikomanagement** können die Absolventinnen und Absolventen Risiken identifizieren, analysieren und bewerten; sie können risikobasierte Maßnahmen entwickeln und den Aufbau eines Risikomanagements unterstützen.

Im **Bereich Datenschutz und rechtliche Grundlagen** können die Absolventinnen und Absolventen gesetzliche Vorgaben aus Datenschutz und IT-Recht anwenden; sie können technische und organisatorische Maßnahmen daraus ableiten.

Im **Bereich Informationssicherheitsmanagement** können die Absolventinnen und Absolventen Bedrohungsanalysen durchführen, Sicherheitsrichtlinien entwickeln und ISMS-Prozesse nach Standards wie ISO 27001 oder NIS2 begleiten.

Im **Bereich Ethik in der Informationstechnologie** können die Absolventinnen und Absolventen gesellschaftliche und ethische Auswirkungen digitaler Technologien reflektieren; sie können kontrovers diskutieren, argumentieren und technologische Spannungsfelder beurteilen.

Im **Bereich IT-Compliance** können die Absolventinnen und Absolventen regulatorische Anforderungen interpretieren; sie können Rollen, Verantwortlichkeiten und Audit- bzw. Zertifizierungsprozesse anwenden.

Im **Bereich rechtliche Grundlagen zu Artificial Intelligence** können die Absolventinnen und Absolventen rechtliche Rahmenbedingungen für KI-Systeme beurteilen und deren Einsatz im Unternehmen verantwortungsvoll begleiten.

IT Infrastructure:

Im **Bereich PC- und Betriebssystemgrundlagen** können die Absolventinnen und Absolventen Betriebssysteme installieren, konfigurieren und absichern; sie können Fehler systematisch analysieren und beheben.

Im **Bereich Netzwerktechnik** können die Absolventinnen und Absolventen Netzwerke planen, konfigurieren und segmentieren; sie können Protokolle verschiedener Schichten anwenden und Netzwerkverkehr analysieren.

Im **Bereich Virtualisierung und Containerisierung** können die Absolventinnen und Absolventen virtuelle Maschinen, Container und Cloud-Umgebungen bereitstellen und verwalten; sie können deren Einsatzgebiete beurteilen.

Im **Bereich Serverdienste und Administration** können die Absolventinnen und Absolventen zentrale Serverdienste konfigurieren, administrieren, sowie Richtlinien- und Namensdienste anwenden.

Im **Bereich Kryptografie und sichere Kommunikation** können die Absolventinnen und Absolventen kryptografische Verfahren anwenden, PKI-Konzepte umsetzen und sichere Kommunikationsprotokolle betreiben.

Im **Bereich moderne Infrastrukturtechnologien** können die Absolventinnen und Absolventen SDN-, IaaS-, Cloud- und Automatisierungswerkzeuge anwenden; sie können Blockchain- und quantensichere Technologien einordnen.

Cyber-Defense:

Im **Bereich Firewalls** können die Absolventinnen und Absolventen Host-based-, stateless- und stateful-Firewalls konfigurieren; sie können zonenbasierte Regeln erstellen und Netzwerkverkehr kontrollieren.

Im **Bereich Layer-2-Security** können die Absolventinnen und Absolventen Sicherheitsrisiken auf Layer 2 erkennen und geeignete Härtungsmaßnahmen umsetzen.

Im **Bereich Security im Netzwerk** können die Absolventinnen und Absolventen VPN-, IDS- und IPS-Systeme anwenden; sie können Sicherheitsereignisse im Netzwerk identifizieren und bewerten.

Im **Bereich Device Hardening** können die Absolventinnen und Absolventen Härtungsmaßnahmen auf Endgeräten und Netzwerkkomponenten anwenden; sie können Angriffsflächen systematisch reduzieren.

Im **Bereich DevSecOps** können die Absolventinnen und Absolventen Automatisierungs- und Konfigurationsprotokolle nutzen, APIs anwenden und Sicherheit in DevOps-Prozesse integrieren.

Im **Bereich moderne Sicherheitsarchitekturen** können die Absolventinnen und Absolventen IAM-Systeme, AAA-Konzepte, Zero-Trust- und SASE-Modelle sowie NGFW-Systeme umsetzen und bewerten.

Im **Bereich Threat Intelligence und Endpoint Security** können die Absolventinnen und Absolventen sicherheitsrelevante Informationen interpretieren, EDR-Systeme anwenden und Zusammenhänge im SOC verstehen.

Im **Bereich Security Data Analysis** können die Absolventinnen und Absolventen sicherheitsrelevante Datenquellen sammeln, normalisieren und zur Angriffserkennung interpretieren.

Im **Bereich Forensik und Anti-Forensik** können die Absolventinnen und Absolventen digitale Spuren sichern, analysieren und dokumentieren; sie können Grenzen forensischer Methoden beurteilen.

Im **Bereich SIEM und Threat Hunting** können die Absolventinnen und Absolventen SIEM-Systeme einsetzen, Ereignisdaten korrelieren und Hypothesen für proaktive Angriffssuche anwenden.

Ethical Hacking:

Im **Bereich Grundlagen von Angriffsmodellen** können die Absolventinnen und Absolventen typische Angriffswege erklären, Schwachstellen erkennen und Angriffsphasen einordnen.

Im **Bereich Netzwerkanalyse und Protokollverständnis** können die Absolventinnen und Absolventen Netzwerkanalysetools anwenden und Angriffe anhand des Netzwerkverkehrs interpretieren.

Im **Bereich Scanning und Enumeration** können die Absolventinnen und Absolventen Systeme identifizieren, Dienste klassifizieren und potenzielle Schwachstellen modellieren.

Im **Bereich Initial Access und Passwortangriffe** können die Absolventinnen und Absolventen Erstzugriffe durchführen, Exploits anwenden und Authentifizierungsangriffe analysieren.

Im **Bereich Privilege Escalation und Lateral Movement** können die Absolventinnen und Absolventen Berechtigungen erweitern und sich über mehrere Systeme hinwegbewegen.

Im **Bereich Persistenz und Post-Exploitation** können die Absolventinnen und Absolventen dauerhafte Zugänge einrichten und interne Daten aus kompromittierten Systemen nutzen.

Im **Bereich Exfiltration, Command-and-Control und Tarnung** können die Absolventinnen und Absolventen Daten exfiltrieren, Steuerkanäle aufbauen und Tarnmechanismen anwenden.

Im **Bereich Angriffe gegen KI-basierte Systeme** können die Absolventinnen und Absolventen KI-Modelle analysieren, manipulieren und sicherheitskritische Auswirkungen beurteilen.

Im **Bereich offensive Operationen** können die Absolventinnen und Absolventen komplexe Angriffsketten planen, durchführen und sicherheitstechnisch bewerten.

Security Lab:

Im **Bereich Laborgrundlagen und Methodik** können die Absolventinnen und Absolventen Laborumgebungen bedienen, Aufgaben systematisch lösen und Ergebnisse dokumentieren.

Im **Bereich Red- und Blue-Teamübungen** können die Absolventinnen und Absolventen offensive und defensive Techniken praktisch anwenden und analysieren.

Im **Bereich Red-/Blue-Team-Szenarien** können die Absolventinnen und Absolventen realitätsnahe Angriff- und Verteidigungsabläufe durchführen und bewerten.

Im **Bereich Purple Team** können die Absolventinnen und Absolventen Erkenntnisse aus Angriff und Verteidigung vergleichen, kombinieren und daraus sicherheitsrelevante Verbesserungen ableiten.

Im **Bereich CTF und Wettbewerbe** können die Absolventinnen und Absolventen sicherheitsrelevante Challenges lösen, Strategien anwenden und an Wettbewerben teilnehmen.

Im **Bereich Full-Scope-Simulation** können die Absolventinnen und Absolventen komplexe operative Szenarien planen, durchführen, analysieren und professionell präsentieren.

IV. SCHULAUTONOME LEHRPLANBESTIMMUNGEN

Siehe Anlage 1.

V. DIDAKTISCHE GRUNDSÄTZE

Siehe Anlage 1.

VI. LEHRPLÄNE FÜR DEN RELIGIONSUNTERRICHT

Siehe Anlage 1.

VII. BILDUNGS- UND LEHRAUFGABEN UND LEHRSTOFFE DER UNTERRICHTSGEGENSTÄNDE

Pflichtgegenstände, Verbindliche Übung

A. Allgemeinbildende Pflichtgegenstände

„Deutsch“, „Englisch“, „Geografie, Geschichte und Politische Bildung“, „Wirtschaft und Recht“, „Naturwissenschaften“ und „Ethik“.

Siehe Anlage 1.

6. BEWEGUNG UND SPORT

Siehe BGBl. Nr. 37/1989 idgF.

7. ANGEWANDTE MATHEMATIK

Siehe Anlage 1 mit folgenden Ergänzungen:

I. Jahrgang (1. und 2. Semester):

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Zahlen und Maße

- mathematische Sachverhalte durch Aussagen präzise formulieren und die Booleschen Verknüpfungen anwenden;
- Dezimalzahlen in Dualzahlen (und umgekehrt) konvertieren sowie mit Dualzahlen rechnen.

Lehrstoff:

Bereich Grundlagen der Mathematik:

Aussagen, Verknüpfungen von Aussagen, Wahrheitstabellen.

Bereich Reelle Zahlen:

Zahlensysteme; Konversion von Zahlen unterschiedlicher Zahlensysteme.

Bereich Boolesche Algebra:

Schaltfunktionen und Boolesche Ausdrücke.

II. Jahrgang:

4. Semester – Kompetenzmodul 4:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Zahlen und Funktionen

- Polynomfunktionen, Exponentialfunktionen, Logarithmusfunktionen und trigonometrische Funktionen auf Aufgabenstellungen des Fachgebietes anwenden;
- logarithmische Skalierungen interpretieren und anwenden.

Lehrstoff:

Bereich Funktionen:

Aufgabenstellungen des Fachgebiets, logarithmische Skalierung.

IV. Jahrgang:

7. Semester – Kompetenzmodul 7:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Integralrechnung

- Begriffe der Differential- und Integralrechnung benennen sowie facheinschlägige Anwendungen berechnen und interpretieren;
- Anfangswertprobleme mit linearen Differentialgleichungen erster und zweiter Ordnung mit konstanten Koeffizienten lösen und im Besonderen die Lösungsfälle der linearen Schwingungsgleichung mit konstanten Koeffizienten interpretieren;
- Funktionen in zwei Variablen geometrisch als Flächen im Raum interpretieren und anhand von Beispielen veranschaulichen;
- partielle Ableitungen berechnen und mit Hilfe des Differentials Fehler abschätzen;
- Funktionen in Taylorreihen entwickeln und damit näherungsweise Funktionswerte berechnen;
- periodische Funktionen durch trigonometrische Polynome approximieren und die Fourierkoeffizienten interpretieren;
- zu vorgegebenen Stützstellen und Stützwerten Interpolationspolynome n-ten Grades berechnen.

Lehrstoff:

Bereich Differential- und Integralrechnung:

Fachbezogene Anwendungen der Differential- und Integralrechnung.

Bereich Lineare Differentialgleichungen:

Trennung der Variablen; lineare Differentialgleichungen erster und zweiter Ordnung mit konstanten Koeffizienten; elementare Lösungsmethoden.

Bereich Funktionen mehrerer Variablen:

Darstellung von Funktionen von zwei Variablen; partielle Ableitungen; totales Differential, lineare Fehlerfortpflanzung und maximaler Fehler.

Funktionenreihen:

Taylorpolynome, Taylorreihen, Konvergenzradius; Approximation von Funktionen durch trigonometrische Polynome; Fourierreihen.

Bereich Interpolation:

Interpolationspolynome.

8. Semester – Kompetenzmodul 8:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Algebra und Geometrie

- die Begriffe „Gruppe“ und „Körper“ interpretieren sowie mit Restklassen rechnen;
- die algebraischen und zahlentheoretischen Grundlagen der Codierung und Chiffrierung zur Lösung von fachrelevanten Beispielen der symmetrischen und asymmetrischen Verschlüsselungsmethoden anwenden.

Bereich Matrizen und Stochastik

- Matrizen als Operatoren von Abbildungen im zwei- und dreidimensionalen Raum interpretieren sowie mit diesen anwendungsbezogen modellieren und operieren;
- die Anzahl möglicher Anordnungen von unterscheidbaren und nicht unterscheidbaren Objekten mit und ohne Berücksichtigung der Reihenfolge bestimmen.

Lehrstoff:

Bereich Algebra und Geometrie

Rechnen in algebraischen Strukturen:

Menge, Gruppe, Ring, Körper, Restklassen.

Bereich Codierung und Chiffrierung:

Algebraische und zahlentheoretische Grundlagen der Codierung und Chiffrierung; symmetrische und asymmetrische Verschlüsselung.

Bereich Matrizen und Stochastik:

Inverse Matrix, Matrizen als Operatoren von Abbildungen, homogene Koordinaten, Anwendungen aus der Fachtheorie.

Bereich Kombinatorik:

Permutationen, Kombinationen, Variationen.

V. Jahrgang – Kompetenzmodul 9:

9. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Stochastik

- die Entscheidungsalternativen und das Prinzip des Alternativtests wiedergeben, signifikante und nicht signifikante Testergebnisse interpretieren und eine signifikante Abweichung eines Mittelwertes von einem vorgegebenen Wert feststellen;
- die für das Fachgebiet relevanten mathematischen Methoden anwenden.

Lehrstoff:

Bereich Beurteilende Statistik:

Verteilung des Stichprobenmittels, zentraler Grenzwertsatz, Intervallschätzung; Prinzip des Alternativtests, Einstichproben t-Test.

Bereich Relevante mathematische Methoden:

Fachbezogene Anwendungen.

10. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können die für das Fachgebiet relevanten mathematischen Methoden anwenden.

Lehrstoff:

Bereich Relevante mathematische Methoden:

Fachbezogene Anwendungen.

B. Fachtheorie und Fachpraxis

1. SOFTWARE TECHNOLOGIES

I. Jahrgang (1. und 2. Semester):

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwareentwicklung und Architektur

- einfache Problemstellungen sprachlich beschreiben und in Modelle überführen;
- einfache Programme entwickeln und systematisch testen;
- grundlegende Funktionen von Entwicklungsumgebungen verwenden und Sourcecode-Verwaltung anwenden.

Lehrstoff:

Bereich Softwareentwicklung und Architektur:

Pseudocode, Algorithmus, graphische Darstellung der Ablauflogik, Syntax, Anweisungen, Operatoren, Ausdrücke, Datentypen, Kontrollstrukturen, Zugriffe auf externe Datenquellen, grundlegende Fehlersuche, Grundlagen der Sourcecode-Verwaltung, Grundlagen einer IDE.

II. Jahrgang:

3. Semester – Kompetenzmodul 3:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwareentwicklung und Architektur

– den Aufbau moderner Benutzeroberflächen und serverseitiger Anwendungen erläutern;
– aktuelle Technologien der Frontend- und Backendentwicklung anwenden;
– grundlegende Elemente von User Interfaces verstehen.

Lehrstoff:

Bereich Softwareentwicklung und Architektur:

Architekturmuster für einfache Systeme, Schnittstellen zwischen Frontend und Backend; implementieren einer Anwendung mit Frontend und Backend; Grundlagen UI-Design.

4. Semester – Kompetenzmodul 4:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwareentwicklung und Architektur

– technologiespezifische Sprachkonzepte fachgerecht anwenden;
– einfache Anwendungen mit Frontend und Backend entwickeln.

Bereich Datenmanagement

– auf externe Datenquellen zugreifen.

Lehrstoff:

Bereich Softwareentwicklung und Architektur:

Syntax, Kontrollstrukturen, Module, Klassen, Funktionen; planen, entwerfen und implementieren einer Anwendung mit Frontend und Backend.

Bereich Datenmanagement:

grundlegende Protokolle und Datenformate für den Austausch und die Speicherung von Daten.

III. Jahrgang:

5. Semester – Kompetenzmodul 5:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Datenmanagement

– Abfragen zur Datenanalyse und -manipulation in Datenhaltungssystemen entwerfen;
– ein geeignetes Datenbankmanagementsystem auswählen.

Bereich Softwareentwicklung und Architektur

– Softwarekomponenten entwickeln und Kommunikationsprotokolle anwenden.

Lehrstoff:

Bereich Datenmanagement:

Abfrage und Bearbeitung von Daten in Datenhaltungssystemen; aktuelle logische Datenmodelle.

Bereich Softwareentwicklung und Architektur:

zeitgemäße Tools und Protokolle für Frontend- und Backendentwicklung.

6. Semester – Kompetenzmodul 6:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwareentwicklung und Architektur

– verteilte Systeme entwickeln und optimieren.

Bereich Softwarequalität, Sicherheit und Betrieb

– verteilte Systeme strukturiert testen;
– sichere Kommunikation in verteilten Systemen implementieren.

Lehrstoff:

Bereich Softwareentwicklung und Architektur:

vollständiger Technologie-Stack aus Frontend- und Backendkomponenten.

Bereich Softwarequalität, Sicherheit und Betrieb:

Testframeworks für Frontends und Backends; sichere Kommunikationsprotokolle, Authentifizierung, Autorisierung.

IV. Jahrgang:

7. Semester – Kompetenzmodul 7:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwareentwicklung und Architektur

– Secure Coding Practices verstehen und anwenden;
– Zugriff auf Daten steuern;
– Bereich Softwarequalität, Sicherheit und Betrieb;
– Softwarefehler protokollieren, finden und beheben.

Lehrstoff:

Bereich Softwareentwicklung und Architektur:

Input Validation, Output encoding; Identity Access Management.

Bereich Softwarequalität, Sicherheit und Betrieb:

Logging, Tracing, Error Handling.

8. Semester – Kompetenzmodul 8:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwareentwicklung und Architektur

– komplexe verteilte Systeme entwickeln.

Bereich Softwarequalität, Sicherheit und Betrieb

– Security-Konzepte in Softwaretechnologien anwenden.

Lehrstoff:

Bereich Softwareentwicklung und Architektur:

Fullstack-Entwicklung mit Frontend- und Backendtechnologien.

Bereich Softwarequalität, Sicherheit und Betrieb:

Sichere Einbindung von Drittanwendungen, Software härten.

V. Jahrgang- Kompetenzmodul 9:

9. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwarequalität, Sicherheit und Betrieb

– Deployment und kontinuierliche Integration durchführen;
– Softwareprojekte automatisiert in einen sicheren Betrieb überführen;
– automatisierte Tests für Softwareprojekte anwenden.

Lehrstoff:

Bereich Softwarequalität, Sicherheit und Betrieb:

Einführung in Deployment-Strategien, Grundlagen der kontinuierlichen Integration (CI); Pipelines für CI/CD; Testframeworks.

10. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Softwarequalität, Sicherheit und Betrieb

– sichere verteilte Anwendungen deployen;
– verteilte Systeme strukturiert und automatisiert testen und bewerten.

Lehrstoff:

Bereich Softwarequalität, Sicherheit und Betrieb:

Angriffsvektoren analysieren und Softwaresysteme härten; Testspezifikation, Dokumentation, Bereich Testprotokolle.

2. COMPLIANCE UND ETHICS

II. Jahrgang:

3. Semester – Kompetenzmodul 3:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Grundlagen des Projekt- und Prozessmanagement

– die Grundlagen des Projektmanagements benennen;
– grundlegende Darstellungsmethoden von Prozessen erläutern.

Bereich Grundlagen des Risikomanagements

– Risiken identifizieren und hinsichtlich ihrer Eintrittswahrscheinlichkeit und Auswirkungen analysieren;
– Methoden und Werkzeuge des Risikomanagements anwenden.

Lehrstoff:

Bereich Grundlagen des Projekt- und Prozessmanagements:

Prozessbeschreibung und –darstellung, Kennzahlen von Prozessen.

Bereich Grundlagen des Risikomanagements:

Risikoanalyse, Methoden des Risikomanagements.

4. Semester – Kompetenzmodul 4:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich rechtliche Grundlagen

– rechtliche Grundlagen des Datenschutzes und Urheberrechts grundlegend anwenden;
– die strafrechtliche Relevanz von Handlungen im Bereich IT-Sicherheit einschätzen.

Bereich Ethik in der Informationstechnologie

– die Wechselwirkungen zwischen (Informations-)Technologie und Gesellschaft kritisch hinterfragen;
– Probleme und Herausforderungen von Internetinhalten beleuchten, kontroversiell diskutieren und argumentieren.

Lehrstoff:

Bereich rechtliche Grundlagen:

Rechtliche Grundlagen des Datenschutzes, Urheberrecht, Strafrecht.

Bereich Ethik in der Informationstechnologie:

Aufgabe und Funktion von Technologie in der Gesellschaft, soziale Auswirkungen von Technologie.

III. Jahrgang:

5. Semester – Kompetenzmodul 5:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich rechtliche Grundlagen

– einschlägige Rechtsnormen für den IT-Betrieb verstehen;
– die Notwendigkeit von Standards und Normen beurteilen.

Bereich Risikomanagement

– die Bedeutung der Risikoanalyse in einem ISM begründen;
– Risiken mittels Katalogbausteinen erarbeiten und evaluieren.

Lehrstoff:

Bereich rechtliche Grundlagen:

ISMS nach ISO27001, ITIL, COBIT, NIS2.

Bereich Risikomanagement:

Ablauf einer Risikoanalyse; Risikobausteine.

6. Semester – Kompetenzmodul 6:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Informationssicherheitsmanagement

– Bedrohungsanalysen anhand von Guidelines durchführen;
– ein IT-Sicherheitshandbuch in einfacher Form erstellen;
– ein Notfallhandbuch erstellen.

Bereich Ethik in der Informationstechnologie

– die Wechselwirkungen zwischen (Informations-)Technologie und Gesellschaft kritisch hinterfragen.

Lehrstoff:

Bereich Informationssicherheitsmanagement:

Sicherheitshandbuch, Bedrohungsanalysen

Bereich Ethik in der Informationstechnologie:

IT und Gender, IT und Ökologie, Medienkonsum, Demokratisierung vs. Zentralisierung von Information.

IV. Jahrgang:

7. Semester – Kompetenzmodul 7:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich IT-Compliance

– Rollenbeschreibungen in der IT-Sicherheit;
– sicherheitsrelevante Kennzahlen und Metriken anwenden;
– Zertifizierungen und Normierungen anwenden.

Lehrstoff:

Bereich IT-Compliance:

Zertifizierungsablauf, Audit, Aufgaben und Funktionen, CISO, branchenspezifische Regulierungen.

8. Semester – Kompetenzmodul 8:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Artificial Intelligence

– rechtliche Grundlagen zur Nutzung von Artifical Intelligence erörtern;
– rechtliche Grundlagen für den Einsatz digitaler Dienste anwenden.

Bereich Ethik in der Informationstechnologie

– ethische Fragen zu Artifical Intelligence und Informationssicherheit verstehen und diskutieren;
– ethische Fragen autonomer Maschinen kritisch beleuchten.

Lehrstoff:

Bereich Artifical Intelligence:

Rechtsgrundlagen für Artifical Intelligenceund digitale Dienste.

Bereich Ethik in der Informationstechnologie:

Autonome Fahrzeuge, autonome Waffensysteme, Diagnosesysteme, soziale Bewertungssysteme, Robotersysteme für soziale Aufgaben.

V. Jahrgang – Kompetenzmodul 9:

9. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich IT-Compliance

– einen Überblick über rechtliche Grundlagen für kritische Infrastruktur geben

Bereich Ethik in der Informationstechnologie

– das Spannungsfeld von Informationssicherheit, Überwachung und Zensur kritisch hinterfragen und bewerten.

Lehrstoff:

Bereich IT-Compliance:

Rechtliche Vorgaben für kritische Infrastrukturen.

Bereich Ethik in der Informationstechnologie:

Überwachung als Sicherheitsdogma; Sicherheit vs. Freiheit; Zensur; offensive und aktive Überwachungsmaßnahmen; biometrische Identifikation.

10. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich IT-Compliance:

– rechtliche Grundlagen für kritische Infrastruktur anwenden.

Bereich Ethik in der Informationstechnologie

– technische und ethische Fragen in Bezug auf Cyberkrieg kritisch erörtern.

Lehrstoff:

Bereich IT-Compliance:

Rechtliche Vorgaben für kritische Infrastruktur.

Bereich Ethik in der Informationstechnologie:

Offensive und defensive Maßnahmen; Attribuierung; Auswirkungen eines Cyberkriegs.

3. IT INFRASTRUCTURE

I. Jahrgang (1. und 2. Semester):

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich PC- und Betriebssystemgrundlagen

– den Aufbau eines PCs und mobiler Endgeräte erklären;
– grundlegende Aufgaben eines Betriebssystems beschreiben;
– Betriebssysteme, Softwarepakete, Sicherheitssoftware installieren und konfigurieren.

Bereich Netzwerktechnik und Heimnetzwerk

– ein Heimnetzwerk einrichten und absichern sowie den Internetzugang einrichten;
– Netzwerkgeräte grundlegend konfigurieren;
– Providertechnologien und Wireless-Technologien;
– Modelle und Adresskonzepte zur Rechnerkommunikation beschreiben und anwenden.

Bereich Virtualisierung und Anwendungsprogramme

– eine virtuelle Maschine erstellen und mit einem Netzwerk verbinden;
– Anwendungsprogramme nutzen.

Lehrstoff:

Bereich PC- und Betriebssystemgrundlagen:

Funktionsweise von CPU, RAM, Massenspeicher, Busse; Installation und Konfiguration von Betriebssystem und Softwarepaketen sowie Konfiguration einer persönlichen Firewall und Antivirus; Backup-Strategien.

Bereich Netzwerktechnik und Heimnetzwerk:

Einrichtung und Absicherung von Heimnetzwerken; grundlegende Konfiguration von Netzwerkgeräten.

Grundlagen von Kommunikationsmodellen (OSI, TCP/IP); grundlegende Adresskonzepte und Protokolle zur Adressvergabe.

Bereich Virtualisierung und Anwendungsprogramme:

Betriebssysteme virtualisieren; Nutzung von Anwendungsprogrammen, Collaboration-Tools, KI-prompting.

II. Jahrgang:

3. Semester – Kompetenzmodul 3:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Betriebssysteme und Serverdienste

– Serversoftware installieren und konfigurieren;
– Benutzer, Gruppen und Berechtigungen verwalten;
– Netzwerkdienste einrichten und administrieren;
– Skriptsprachen für administrative Aufgaben einsetzen.

Bereich Netzwerktechnik

– die Funktionsweise von Protokollen zum verbindungslosen und verbindungsorientierten Transport von Paketdaten sowie zur Namensauflösung, zur Adresszuweisung und zur Anwendungskommunikation erklären;
– Netzwerksegmentierung und statisches Routing umsetzen.

Bereich Virtualisierung

– Virtuelle Maschinen erstellen und konfigurieren;
– Netzwerkkonfigurationen in virtuellen Umgebungen anwenden;
– Externe Hardware in virtuelle Systeme einbinden.

Lehrstoff:

Bereich Betriebssysteme und Serverdienste:

Installation und Grundkonfiguration von Windows Server, Verzeichnisdienste, Namensauflösung und Adresszuweisungsdienste auf Windows Server, Benutzer- und Gruppenverwaltung, NTFS-Berechtigungen, Netzwerkfreigaben (inkl. Rechteverwaltung und Zugriffskontrolle), Funktionen und Module für Systemadministration, einfache Automatisierungsskripte.

Bereich Netzwerktechnik:

Protokolle der Transportschichte (z.B.: TCP, UDP, Adressierung, Paketaufbau), Protokolle der Anwendungsschicht (z.B.: DNS, HTTP, DHCP), VLANs und statisches Routing.

Bereich Virtualisierung:

Virtualisierungsplattformen, Netzwerkkonfiguration (z.B.: NAT, Bridging, Host-only), externe Hardware einbinden.

4. Semester – Kompetenzmodul 4:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Betriebssysteme und Serverdienste

– Unix artige Betriebssystemumgebungen einrichten und Grundkonfigurationen durchführen;
– Fehler systematisch und strukturiert analysieren, eingrenzen und beheben;
– Skripte für die Automatisierung von Systemabläufen entwickeln.

Bereich Netzwerktechnik

– Netzwerkdienste und Anwendungsprotokolle beschreiben und einrichten;
– Redundante Netzwerk-Konzepte bewerten und umsetzen;
– Sichere Zugriffe auf entfernte IT-Systeme einrichten.

Bereich Virtualisierung

– Virtualisierung- und Containerkonzepte anwendungsgerecht einsetzen;
– Unterschiede zwischen virtuellen Maschinen und Container beschreiben.

Lehrstoff:

Bereich Betriebssysteme:

Standardinstallation von Betriebssystemen und Anwendungssoftware, Fehlersuche und Fehlerbehebung, Skriptsprachen in Betriebssystemen.

Bereich Netzwerktechnik

Adressierungs- und Namensdienste, Dynamische Routingprotokolle, Redundanz, Remotezugriff, Anwendungsprotokolle.

Bereich Virtualisierung

Grundlagen der Containervirtualisierung.

III. Jahrgang:

5. Semester – Kompetenzmodul 5:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Verzeichnisdienste und Richtlinienverwaltung

– zentrale Verzeichnisdienste einrichten und administrieren;
– Richtlinien zur zentralen Konfiguration, Standardisierung und Absicherung von Benutzer- und Endgeräteeinstellungen erstellen, zuweisen und deren Wirkung verifizieren.

Bereich Sicherheits- und Betriebsgrundlagen

– grundlegende Verfahren der Verschlüsselung sowie der Authentifizierung/Autorisierung im Infrastrukturbetrieb erläutern und für typische Einsatzfälle begründet auswählen;
– – Grundlagen des Netzwerkmanagements und des Netzwerkmonitorings anwenden sowie Betriebs- und Protokolldaten strukturiert erfassen und zur Fehleranalyse heranziehen.

Lehrstoff:

Bereich Verzeichnisdienste und Richtlinienverwaltung:

Zentrale Verzeichnisdienste, Namensräume und Verzeichnisstrukturen, Objektverwaltung, Berechtigungs- und Delegationskonzepte, Einbindung von Clients und Diensten in Verzeichnisdienste, Richtlinienverwaltung.

Bereich Sicherheits- und Betriebsgrundlagen:

Verschlüsselung im Infrastrukturkontext, Authentifizierung und Autorisierung, Netzwerkmanagement, Netzwerkmonitoring, Protokollierung und Log-Sammlung, Basisauswertung zur Fehler- und Ursachenanalyse.

6. Semester – Kompetenzmodul 6:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Virtualisierung, Containerisierung und Cloud-Konzepte

– Bereitstellungsformen beschreiben, vergleichen und für infrastrukturelle Aufgabenstellungen sachgerecht einsetzen.

Bereich Bereitstellung und Administration von Serverdiensten

– Dienste konfigurieren und betreiben;
– Serverdienste administrieren und typische Betriebsaufgaben durchführen und dokumentieren.

Lehrstoff:

Bereich Virtualisierung, Containerisierung und Cloud-Konzepte:

Virtualisierung, Containerisierung, Netz- und Speicheranbindung, Konfigurationsprinzipien, Lebenszyklus, Zusammenspiel mehrerer Dienste; Persistenzkonzepte, Cloud-Konzepte.

Bereich Bereitstellung und Administration von Serverdiensten:

Dienste bereitstellen, Administration von Serverdiensten, Datensicherung und Wiederherstellung, grundlegende Verfügbarkeits- und Performanceaspekte, Störungsbehebung.

IV. Jahrgang:

7. Semester – Kompetenzmodul 7:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Netzwerktechnik

– Software Defined Networking (SDN) verstehen und anwenden;
– Infrastructure as a Service (IaaS) mit Automatisierungstools verstehen und anwenden.

Bereich Management und Sicherheit

– Best Practices für Skalierbarkeit, Ausfallsicherheit und Sicherheit anwenden;
– Identity Provider konfigurieren und integrieren.

Lehrstoff:

Die Schülerinnen und Schüler können im

Bereich Netzwerktechnik:

Motivation und Vorteile von SDN, Architektur von SDN, Virtualisierte Infrastrukturen (Server und Netzwerke) mit Infrastructure as a Service (IaaS) Werkzeugen implementieren.

Bereich Management und Sicherheit:

Public, Private und Hybrid-Cloud, Skalierbarkeit und Hochverfügbarkeit, Sicherheitsaspekte, Identity Provider, Monitoring und Logging in Cloud-Umgebungen.

8. Semester – Kompetenzmodul 8:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Kryptografische Grundlagen und Verfahren

– Mathematische Grundlagen für die Kryptografie erläutern und auf einfache Problemstellungen anwenden;
– Symmetrische, asymmetrische und hybride Verfahren sowie Klassen von Chiffren vergleichen.

Bereich Integrität, Schlüsselmanagement und sichere Kommunikation

– kryptografische Hashfunktionen zur Integritätssicherung einordnen und deren Schwachstellen erklären;
– digitale Signaturen, Zertifikate und grundlegende PKI-Konzepte beschreiben sowie den Ablauf sicherer Kommunikationsaufbauten nachvollziehen;
– Schlüsselaustauschverfahren vergleichen, anwendungsgerecht auswählen und den Unterschied zu Ticket-basierten Systemen beschreiben.

Lehrstoff:

Bereich Kryptografische Grundlagen und Verfahren:

Primzahlen, Faktorisierung, symmetrische und asymmetrische Kryptografie, Chiffrenklassen, Grundprinzipien und typische Einsatzszenarien, mathematische Prinzipien und Performanceabschätzungen: Rechenaufwand, Einfluss von Parametern, Ressourcenbedarf, Padding.

Bereich Integrität, Schlüsselmanagement und sichere Kommunikation:

Schlüsselmanagement, organisatorische und technische Maßnahmen, Hashing, MAC, Digitale Signaturen, Zertifikate und PKI, sichere Kommunikationsprotokolle, Grundzüge TLS, authenticated encryption.

V. Jahrgang - Kompetenzmodul 9:

9. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Quantenkryptografie und Quantensicherheit

– Grundkonzepte der Quantenkryptografie beschreiben und deren Zielsetzung sowie Rahmenbedingungen erläutern;
– Auswirkungen quantentechnologischer Entwicklungen auf etablierte kryptografische Verfahren beurteilen und grundlegende Strategien zur Quantensicherheit ableiten.

Bereich Blockchain und aktuelle Technologien im Infrastrukturkontext

– Grundprinzipien der Blockchain-Technologie erklären sowie Sicherheitsannahmen, Skalierungs- und Betriebsaspekte darstellen.

Lehrstoff:

Bereich Quantenkryptografie und Quantensicherheit:

Quantenkryptografie, Quantenbedrohungsmodell, Quantensicherheit, Risikobetrachtung.

Bereich Blockchain und aktuelle Technologien im Infrastrukturkontext:

Blockchain-Grundlagen, Datenstrukturen, Konsensprinzipien.

10. Semester:

Bildungs- und Lehraufgabe:

Bereich aktuelle Technologien im Infrastrukturkontext

– aktuelle Technologien und Entwicklungen im Umfeld kryptografischer Verfahren und IT-Infrastruktur recherchieren, einordnen und anhand fachlicher Kriterien bewerten.

Lehrstoff:

Bereich Technologien im Infrastrukturkontext:

Aktuelle Technologien: Beobachtung von Standards/Trends; Kriteriengeleitete Bewertung.

4. CYBER DEFENSE

II. Jahrgang:

3. Semester – Kompetenzmodul 3:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Host Based Firewalls

– Aufgaben und Funktionsweise von Host-based Firewalls erklären;
– regelbasierte Filterung von Netzwerkverkehr anwenden;
– linux- und windows basierende Firewalls einrichten.

Bereich Layer-2-Security

– Sicherheitsrisiken auf Layer 2 benennen;
– Grundlegende Schutzmechanismen auf Layer 2 erklären und anwenden.

Lehrstoff:

Bereich Host Based Firewalls:

Aufgaben und Funktionsweise von Host-based Firewalls, Abgrenzung zu Netzwerk- und Perimeter-Firewalls, regelbasierte Filterung von Netzwerkverkehr, NAT/PAT.

Layer-2-Security:

Umsetzung einfacher Angriffe mit Erkennung durch Syslog.

4. Semester – Kompetenzmodul 4:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Host Based Firewalls

– typische Einsatzszenarien erklären;
– das Konzept von stateful Firewalls fallbeispielhaft umsetzen.

Bereich Layer-2-Security

– Erweiterte Schutzmechanismen auf Layer 2 erklären und anwenden;
– Sensibilisierung für interne Angriffsvektoren in lokalen Netzen.

Bereich Netzwerkanalyse und Protokollverständnis

– tools zur Netzwerkanalyse anwenden – und den output interpretieren.

Lehrstoff:

Bereich Host Based Firewalls:

Logging, Monitoring und Fehleranalyse, Typische Einsatzszenarien in Client- und Serverumgebungen fallbeispielhaft umsetzen.

Bereich Layer-2-Security:

Umsetzung erweiterter Angriffe mit Erkennung durch Syslog.

Bereich Netzwerkanalyse und Protokollverständnis:

Grundlagen der Netzwerkanalyse, Zusammenhang zwischen Netzwerkverkehr und Angriffen, Portscans, Einsatz von Portscan-Werkzeugen, Informationsgewinn durch offene Dienste, Risiken und Erkennungsmerkmale.

III. Jahrgang:

5. Semester – Kompetenzmodul 5:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Security im Netzwerk

– zonenbasierende Firewallkonzepte umsetzen;
– Einsatzszenarien von VPN-basierenden Verbindungen erklären;
– Anomaliebasierende Erkennung erklären;
– die Funktionen und Aufgaben von IDS erklären.

Bereich Devicehardening und Sicherheitskonzepte

– Ziele und Prinzipien der Gerätehärtung benennen und fallbeispielhaft anwenden;
– Konzepte zur Reduktion von Angriffsoberflächen erklären;
– Sandboxingsysteme erklären;
– Bereich DevSecOPs;
– das Konzept von DevOPs erklären und anwenden.

Lehrstoff:

Bereich Security im Netzwerk:

Zonenkonzepte in modernen Firewall-Architekturen umsetzen, Kommunikationsregeln zwischen Zonen.

Absicherung verschlüsselter Verbindungen, Site-to-Site-VPNs, Fehlkonfigurationen und Sicherheitsrisiken, einfache IDS-Systeme fallbeispielhaft umsetzen.

Bedrohungen auf Client- und Server-Systeme, Endpoint-Schutzmechanismen, Zusammenspiel von Host-Netzwerk- und Endpoint-Security, Bedeutung von Updates, Patches und Monitoring, Bewertung von Endpoint-Sicherheitsstrategien.

Bereich Devicehardening und Sicherheitskonzepte:

Hardening-Maßnahmen auf Betriebssystemebene umsetzen, Hardening-Maßnahmen auf aktiven Netzwerkkomponenten umsetzen, IKT-Grundschutz, Asset-Management, containerbasierte Systeme einrichten.

Bereich DevSecOPs:

DevOPS-Konzepte, einfache Automatisierungsaufgaben., Restconf,, Netconf, notwendige Datenstrukturen, API.

6. Semester – Kompetenzmodul 6:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Security im Netzwerk

– die Funktionen und Aufgaben von IPS erklären;
– die Notwendigkeit und Bedeutung von Endpoint-Security erklären;
– Anforderungen an Managementsysteme für Endpoint-Security darstellen.

Bereich Devicehardening und Sicherheitskonzepte

– ein Assetmanagement fallbeispielhaft umsetzen;
– Containerisierungslösungen fallbeispielhaft umsetzen;
– Sandboxingsysteme fallbeispielhaft anwenden;
– Bereich DevSecOPs;
– einfache Automatisierungsumgebungen einrichten und anwenden.

Lehrstoff:

Bereich Security im Netzwerk:

Zusammenspiel von VPN und Firewall-Regelwerken, einfache IPS Systeme, anomalie-basierte Erkennung, IPS im Netzwerk, Grenzen automatisierter Angriffserkennung.

Devicehardening und Sicherheitskonzepte:

Erweiterte Hardening-Maßnahmen auf Betriebssystemebene umsetzen, erweiterte Hardening-Maßnahmen auf aktiven Netzwerkkomponenten umsetzen.

Sicherheitsaspekte containerbasierter Systeme, Isolierung und Ressourcenbeschränkung, Sandboxing-Konzepte.

Bereich DevOPS:

DevOPS-Konzepte, Automatisierungsaufgaben.

IV. Jahrgang:

7. Semester – Kompetenzmodul 7:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich moderne Sicherheitsarchitekturen

– Anforderungen an Identity- und Access- Managements erklären;
– AAA Konzepte fallbeispielhaft umsetzen;
– das Grundkonzept von Secure Access Service Edge erklären;
– das Konzept von Zero Trust Ansätzen darstellen.

Bereich Threat intelligence services:

– Anforderungen Endpoint Detection und Response Systeme darstellen;
– das Zusammenwirken von SOC, NOC und Siem-Systemen erklären;
– Funktionsabläufe in Siem-Systemen erklären.

Bereich Security Data Analysis

– Datenquellen für die Analyse von Incidents benennen.

Lehrstoff:

Bereich Moderne Sicherheitsarchitekturen:

Grundlagen des Identity- und Access-Managements (IAM), AAA-Konzepte, Zentrale Authentifizierungsdienste, Föderierte Identitäten und moderne Autorisierungsansätze, Verwaltung digitaler Identitäten in lokalen und cloudbasierten Umgebungen, Authentifikationsfaktoren, Biometrische Verfahren und deren Einsatzgebiete, Sicherheitsrisiken, Datenschutz und Akzeptanz, Bewertung moderner Authentifikationslösungen.Grundprinzipien von Secure Access Service Edge (SASE),

Verschmelzung von Netzwerk- und Sicherheitsdiensten, Zero-Trust-Ansätze, Vergleich klassischer Perimeter-Modelle mit SASE, Auswirkungen auf Unternehmensnetzwerke.

Bereich Threat intelligence services:

Endpoint Detection and Response (EDR), Vulnerability Assessment und Schwachstellenmanagement, Aufgaben und Zusammenspiel von SOC, NOC und Threat Intelligence Services (TIS).

Bereich Security Data Analysis:

Bedeutung von Datenanalyse in der Cybersicherheit, Logquellen und Ereignisdaten, Korrelation und Interpretation sicherheitsrelevanter Informationen, Grundlagen der Angriffserkennung durch Analyse, Grenzen automatisierter Auswertung.

8. Semester – Kompetenzmodul 8:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich moderne Sicherheitsarchitekturen

– Next Generation Firewalls fallbeispielhaft implementieren;
– MFA basierende Systeme erklären und anwenden;
– eine PKI fallbeispielhaft implementieren.

Bereich Threat intelligence services:

– Plattformen für Incident-response-Systeme benutzen;
– ein einfaches Siem-System implementieren;

Bereich Security Data Analysis

– fallbeispielhafte Implementierungen zur Analyse von security-relevantem Traffic umsetzen.

Lehrstoff:

Bereich Moderne Sicherheitsarchitekturen:

Next-Generation Firewalls (NGFW) und Proxy-Funktionalitäten, Applikations- und Benutzerkontext in Firewall-Entscheidungen.

Grundlagen kryptografischer Identitäten, Aufbau und Funktion einer PKI, Zertifikate.

Bereich Threat intelligence services:

Ereignisbewertung, Eskalation und Incident Handling, Rollen, Prozesse und Verantwortlichkeiten im Sicherheitsbetrieb, VERIS.

Bereich Security Data Analysis:

Analyse großer Mengen sicherheitsrelevanter Daten.

V. Jahrgang - Kompetenzmodul 9:

9. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Forensik

– Ziele und Aufgaben der digitalen Forensik benennen;
– einfache forensische Analysen durchführen und Berichte erstellen;
– die Grenzen forensischer Analysen beschreiben.

Bereich Security Information and Event Management

– ein SIEM-System implementieren.

Bereich Threat Hunting und Threat Intelligence

– die Funktionsabläufe von Threat-Intelligence-Systemen darstellen.

Lehrstoff:

Bereich Identity Forensik:

Sicherung und Erhaltung digitaler Beweise, Integrität, Nachvollziehbarkeit und Dokumentation, Rechtliche und organisatorische Rahmenbedingungen, Chain of Custody, Rekonstruktion von Benutzeraktivitäten, Werkzeuge und Methoden zur Datenauswertung.

Bereich Security Information and Event Management:

Aufgaben und Architektur von SIEM-Systemen, Zentrale Logsammlung und Korrelation, Erkennung sicherheitsrelevanter Ereignisse, Alarmierung, Priorisierung und Eskalation.

Bereich Threat Hunting und Threat Intelligence:

Proaktives Threat Hunting vs. reaktive Erkennung, Nutzung von Threat-Intelligence-Informationen, Analyse von Indicators of Compromise (IoCs), Einbindung externer Threat-Intelligence-Quellen, Hypothesengetriebene Angriffssuche, Logaggregation, Visualisierung und Dashboards, Korrelation und Mustererkennung.

10. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Aktuelle Technologien

– Aktuelle Bedrohungslagen identifizieren und analysieren.

Lehrstoff:

Bereich Aktuelle Technologien:

Aktuelle Bedrohungslagen identifizieren und analysieren. Nutzung von Analyseplattformen im SOC-Umfeld, Bewertung der Aussagekraft von Analyseergebnissen.

5. ETHICAL HACKING

II. Jahrgang:

3. Semester – Kompetenzmodul 3:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Grundlagen von Angriffsmodellen

– grundlegende Angriffswege an Netzwerke und Systeme erklären;
– typische Schwachstellen in Systemen und Netzwerken beschreiben;
– Social-Engineering-Ansätze identifizieren.

Bereich Angriffsprinzipien

– Aufbau und Ablauf einfacher Angriffsketten darstellen;
– grundlegende Exploit-Konzepte erklären;
– Angriffsszenarien hinsichtlich Machbarkeit einordnen;
– die Grundlagen von spoofing basierten Techniken erklären.

Lehrstoff:

Bereich Grundlagen von Angriffsmodellen:

Grenzen einfacher Angriffe, Zusammenhang zwischen Angriff und Abwehrmaßnahmen.

Funktionsweise typischer Angriffs-Gadgets, Einsatzszenarien und Risiken, Sensibilisierung für physische Sicherheit.

Bereich Social Engineering, Begrifflichkeiten der Cybersecurity:

Angriffsprinzipien; Ziel von Angriffsmodellen, Phasen eines Cyberangriffs, Strukturierungsmodelle, Zuordnung konkreter Techniken zu Angriffsphasen, Nutzen von Angriffsmodellen für Analyse und Verteidigung, Exploit-Mechaniken, OSINT, Zusammenhang zwischen Informationsleck und Angriffserfolg.

4. Semester – Kompetenzmodul 4:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Zielanalyse

– Zielsysteme hinsichtlich Struktur beschreiben;
– Angriffsflächen identifizieren;
– Zielmerkmale kategorisieren.

Bereich Informationsgewinnung

– einfache OSINT-Techniken anwenden;
– Informationsquellen systematisch nutzen;
– Angriffspotential aus Daten ableiten.

Lehrstoff

Bereich Zielanalyse:

Infrastrukturerkennung, Modellierung einfacher Angriffsszenarien.

Bereich Informationsgewinnung:

Grundlegende OSINT-Methoden.

III. Jahrgang:

5. Semester – Kompetenzmodul 5:

Bildungs- und Lehraufgabe:

Bereich Scanning und Enumeration:

– den Ablauf von Angriffen gegen drahtlose Übertragungssysteme darstellen;
– strukturierte Netzwerkscans planen und durchführen;
– Dienste und Versionen enumerieren.

Bereich Schwachstellenanalyse

– gefundene Systeme und Dienste klassifizieren;
– potenzielle Schwachstellen ableiten;
– erste Angriffswege modellieren und ausnutzen.

Lehrstoff:

Bereich Scanning und Enumeration:

Schwachstellen drahtloser Systeme, Angriffsszenarien, Port-Scanning (TCP/UDP), Dienst-/Versionsbestimmung, Identifikation exponierter Dienste, Typische Fehlkonfigurationen und Default-Zugänge, physische Sicherheit, Grundlagen lokaler und netzwerkbasierter Authentifizierung, Angriffe auf Dienste, Bedeutung von Protokollsicherheit und Konfiguration.

Bereich Schwachstellenanalyse:

Grundlagen der Schwachstellenbewertung, Matching von Diensten zu bekannten Schwachstellen, Angriffspfad-Modellierung.

6. Semester – Kompetenzmodul 6:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Initial Access:

– gängige Erstzugriffsverfahren erklären;
– grundlegende Exploits zielgerichtet einsetzen;
– funktionale Zugangsketten nachvollziehen.

Bereich Passwort- und Authentifizierungsangriffe

– verschiedene Passwortangriffe durchführen;
– Hash- und Credential-Formate unterscheiden;
– Angriffsergebnisse interpretieren.

Bereich Angriffswerkzeuge und Analyseplattformen

– Systeme zur standardisierten Behandlung von Cyberincidents erklären und anwenden.

Lehrstoff:

Bereich Initial Access:

Basis-Exploits, Aufbau von Initial-Access-Ketten, Ziel und Aufbau der OWASP Top 10, Typische Schwachstellen in Webanwendungen.

Bereich Passwort- und Authentifizierungsangriffe:

Passwort-Cracking-Methoden (Brute Force, Dictionary usw.), Hash-Formate und Credential-Speicher, Auswertung von Cracking-Ergebnissen.

Angriffswerkzeuge und Analyseplattformen:

Nutzung von Wireshark zur Analyse von Angriffen, Arbeiten mit Sicherheitsdistributionen, Bewertung von Werkzeugen nach Zweck und Einsatzgebiet.

IV. Jahrgang:

7. Semester – Kompetenzmodul 7:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Privilege Escalation

– Mechanismen für Privilege Escalation erklären;
– Fehler in Berechtigungskonzepten nutzen;
– Privilegsteigerungen durchführen.

Bereich Lateral Movement

– Techniken für lateral movement Techniken anwenden;
– interne Angriffspfade darstellen.

Bereich Persistenz

– einfache Persistenzmechanismen anwenden;
– kontinuierlichen Zugriff sicherstellen.

Lehrstoff:

Bereich Privilege Escalation:

Lokale und Remote-Eskalation, Fehlkonfigurationen und Berechtigungsfehler, Token- und Handle-Missbrauch.

Bereich Lateral Movement:

Netzwerkpfadanalyse, Basis-Techniken: SMB-Movement, Remote-Execution, Interne Pfade und Verbindungsketten.

Bereich Persitenz:

Autostart-Mechanismen, Geplante Aufgaben / Dienste, Einfache Hintertüren.

8. Semester – Kompetenzmodul 8:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Post-Exploitation

– Informationen aus kompromittierten Systemen auswerten;
– interne Daten zur Angriffsplanung nutzen;
– erbeutete Credentials wiederverwenden.

Bereich Persistenz

– versteckte Persistenzmechanismen einsetzen;
– langfristigen Zugang sicherstellen;
– Strategien kombinieren.

Bereich OT Systeme

– Auswirkungen von Angriffen auf kritische Infrastrukturen bewerten;
– können das Purdue-Modell für OT-Systeme interpretieren.

Lehrstoff:

Bereich Post Exploitation:

Systeminformationserhebung, Interne Datenquellen, Credential Harvesting.

Bereich Persitenz:

Stealth-Persistenz, Modifikation tiefer Systemkomponenten, Kombination mehrerer Persistenzwege.

Bereich Angriffsvektoren:

Purdue-Modells, Trennung von IT- und OT, Angriffe entlang der Ebenen des Purdue-Modells, Bedeutung von Segmentierung und Monitoring.

V. Jahrgang – Kompetenzmodul 9:

9. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Exfiltration

– Exfiltrationstechniken erklären;
– Datenabflüsse durchführen;
– Tarnmechanismen anwenden.

Bereich Command und Control

– C&C-Konzepte erklären;
– einfache C&C-Kanäle einrichten;
– verdeckte Kommunikationspfade nutzen.

Bereich Tarnung und Obfuskation

– Obfuskationstechniken anwenden;
– Aktivitäten verschleiern;
– Zugänge verbergen.

Lehrstoff:

Bereich Exfiltration:

Übertragungswege (DNS-Tunnel, HTTPS-Tunneling, etc.), Automatisierte Abflüsse, Tarnmethoden.

Bereich Command und Control:

C2-Architekturen, Reverse-Shells / Beaconing, Verdeckte Kanäle.

Bereich Tarnung und Obfuskation

Code-Obfuskation, Log-Vermeidung, Tarnung aktiver Zugänge.

10. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Angriffsketten

– vollständige Angriffsketten planen;
– operative Ziele definieren;
– komplexe Übernahmeszenarien durchführen.

Bereich Angriffe gegen KI-basierte Systeme

– KI-Systeme als Bestandteil von Angriffsoberflächen bewerten;
– können Angriffe gegen KI-basierte Systeme durchführen.

Lehrstoff:

Bereich Angriffsketten:

Planung vollständiger operationeller Kampagnen, Zieldefinition und Priorisierung, Komplexe Angriffsszenarien, Tool stacks und Automatisierungsframeworks.

Bereich: Angriffe gegen KI-Systeme:

KI-Systeme als Angriffsoberfläche, Manipulation von Training, Modellmanipulation und -missbrauch, Prompt-basierte Angriffe, Auswirkungen fehlerhafter KI-Entscheidungen, Bedeutung von KI-Sicherheit in kritischen Systemen.

6. SECURITY LAB

I. Jahrgang (1. und 2. Semester):

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Laborgrundlagen und Arbeitsmethodik

– grundlegende Arbeitsweisen in Laborumgebungen anwenden;
– Aufgaben strukturiert und nachvollziehbar bearbeiten.

Bereich Einsteiger-Challenges und Dokumentation

– verschiedene Mini-CTF-Aufgaben methodisch bearbeiten;
– Vorgehensweisen und Ergebnisse verständlich dokumentieren.

Lehrstoff:

Bereich Laborgrundlagen und Arbeitsmethodik:

Virtuelle Umgebungen, Basis-Tools, Terminal, Dateiarbeit, grundlegende Bedienkonzepte, Einführung in LAB-Dokumentation.

Bereich Einsteiger-Challenges und Dokumentation:

Mini-Challenges, einfache CTF-Aufgaben, Teamrollen, Kommunikation, Ergebnisdarstellung, CTF-Basics (Crypto, Web, Forensics), Write-Up-Struktur, Dokumentationsprinzipien; Scanning-Basics, Hash-Tools, Log-Viewer, strukturiertes Troubleshooting, Analyseverfahren.

II. Jahrgang:

3. Semester – Kompetenzmodul 3:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Grundlagen Offensive Techniques

– grundlegende Analyseschritte in einfachen Angriffsszenarien nachvollziehen;
– typische Merkmale grundlegender Schwachstellen erkennen.

Bereich Grundlagen Defensive Techniques

– sicherheitsrelevante Informationen aus grundlegenden Datenquellen ableiten;
– einfache Auffälligkeiten oder Abweichungen erkennen.

Lehrstoff:

Bereich Grundlagen Offensive Techniques:

Recon (OSINT, Scans), einfache Vulnerability-Reproduktion, Aufbau einfacher Angriffsketten.

Bereich Grundlagen Defensive Techniques:

Logquellen und Basisindikatoren, grundlegende Anomalien, einfache Schutzmaßnahmen (konzeptionell).

4. Semester – Kompetenzmodul 4:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Red-Team-Übungen

– grundlegende offensive Laborübungen strukturiert durchführen;
– Ergebnisse und Zwischenschritte sinnvoll festhalten.

Bereich Blue-Team-Übungen

– grundlegende Spuren sicherheitsrelevanter Vorgänge erkennen;
– einfache Bewertungen zu sicherheitsrelevanten Ereignissen treffen.

Lehrstoff:

Bereich Red-Team-Übungen:

einfache Angriffsketten, Basis-Eskalationsübungen, technische Dokumentation.

Bereich Blue-Team-Übungen:

einfache IOCs und Log-Abweichungen, Detection-Basics, Grundreaktionen.

III. Jahrgang:

5. Semester – Kompetenzmodul 5:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Red-Team-Übungen

– strukturierte Analyseschritte in Recon- und Scan-Umgebungen anwenden;
– einfache Exploit-Übungen zielgerichtet durchführen;
– offensive CTFs durchführen.

Lehrstoff:

Bereich Red-Team-Übungen:

OSINT vertieft, Scans, Enumeration, Schwachstellenmatching, Einsteiger-Exploits, Web-, Crypto-, Forensics-Basics, CTF-Aufbau und Workflow, Write-Up-Techniken.

6. Semester – Kompetenzmodul 6:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Red-Team-Übungen

– grundlegende Schritte zum horizontalen und vertikalen Movement anwenden;
– einfache Methoden zur Einrichtung von Persistenz anwenden;
– mehrere Arbeitsschritte zu Abläufen verknüpfen.

Bereich Blue-Team-Übungen

– Zusammenhänge zwischen Rechten, Zugriffen und Bewegungen erkennen;
– Angriffe anhand von Logdatenanalyse erkennen.

Lehrstoff:

Bereich Read-Team-Übungen

Privilege Escalation, horizontales und vertikales Movement, Autostart, Dienste und Tasks, Backdoors.

Blue-Team-Übungen.

Logdaten auswerten.

IV. Jahrgang:

7. Semester – Kompetenzmodul 7:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Red-Team-Szenarien

– mehrere Laborarbeitsschritte zu mittleren Angriffsketten verbinden;
– verschiedene Kommunikations- und Übertragungstechniken praktisch erproben;
– komplexere Abläufe nachvollziehbar darstellen.

Bereich Blue-Team-Szenarien

– Mehrere Datenquellen zur Erkennung von Angriffen verbinden;
– auf Incidents reagieren.

Lehrstoff:

Bereich Red-Team-Szenarien:

Mid-Level-Red-Team-Scenarios, komplexere Chains (IN→THROUGH→OUT), technische Ergebnisberichte, DNS/HTTPS-Exfiltration, Reverse-Shells / C2-Basics, Verbindungsaufbau und Kommandoabläufe.

Bereich Blue-Team-Szenarien:

SIEM, SOC, Incident response.

8. Semester – Kompetenzmodul 8:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Purple-Team-Szenarien

– LAB-Projekte selbstständig planen und strukturieren;
– eigenständige Lösungen in hybriden Szenarien entwickeln;
– erweiterte Tools und Methoden situationsbezogen anwenden;
– für Wettbewerben trainieren.

Lehrstoff:

Bereich Purple-Team-Szenarien:

Hybride Red-Blue-Team-Szenarien, Wettbewerbsvorbereitung.

V. Jahrgang – Kompetenzmodul 9:

9. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Purple-Team-Szenarien

– LAB-Projekte selbstständig planen und strukturieren;
– eigenständige Lösungen in hybriden Szenarien entwickeln;
– erweiterte Tools und Methoden situationsbezogen anwenden;
– für Wettbewerben trainieren.

Lehrstoff:

Bereich Purple-Team-Szenarien:

Hybride Red-Blue-Team-Szenarien, Wettbewerbsvorbereitung.

10. Semester:

Bildungs- und Lehraufgabe:

Die Schülerinnen und Schüler können im

Bereich Full-Scope-Simulation

– umfassende Szenarien mit unterschiedlichen Rollen bearbeiten;
– komplexe Abläufe im Gesamtzusammenhang bewerten;
– Ergebnisse strukturiert und zielgruppenorientiert aufbereiten;
– eigene Vorgehensweisen reflektieren und präsentieren.

Lehrstoff:

Bereich Full-Scope-Simulation:

Full-Scope-Simulation, Red/Blue-Integration, Abschlussanalyse, Abschlussberichte, Präsentationsformen, Peer-Review und Reflexion.

C. Verbindliche Übung

SOZIALE UND PERSONALE KOMPETENZ

Siehe Anlage 1.

D. Pflichtpraktikum

Siehe Anlage 1.

Freigegenstände, Unverbindliche Übung, Förderunterricht

E. Freigegenstände

Siehe Anlage 1.

F. Unverbindliche Übung

BEWEGUNG UND SPORT

Siehe BGBl. Nr. 37/1989 idgF.

G. Förderunterricht

Siehe Anlage 1.

H. Deutschförderklasse

Pflichtgegenstände

1. Deutsch in der Deutschförderklasse

Siehe Anlage 1.

2. Religion

Siehe Anlage 1.

3. Weitere Pflichtgegenstände und Verbindliche Übung

Für die weiteren Pflichtgegenstände und die verbindliche Übung sind die Bildungs- und Lehraufgabe sowie der jeweilige Lehrstoff gemäß Abschnitt VII Unterabschnitt A bis C anzuwenden unter Berücksichtigung der sprachlichen Kompetenzen und individuellen Voraussetzungen der Schülerin bzw. des Schülers.

Freigegenstände und Unverbindliche Übung

Für die Freigegenstände und unverbindliche Übung sind die Bildungs- und Lehraufgabe sowie der jeweilige Lehrstoff gemäß Abschnitt VII Unterabschnitt E und F anzuwenden unter Berücksichtigung der sprachlichen Kompetenzen und individuellen Voraussetzungen der Schülerin bzw. des Schülers.