

Drehbuch K0: Kick-off & Organisation

Christopher Scherb

17. September 2025

Rahmenbedingungen

Die Lehrveranstaltung umfasst 14 Termine, jeweils donnerstags von 16:15 bis 18:50 Uhr. Die Wochen wechseln zwischen Vorlesungen, Laborphasen und betreuter Projektarbeit. Das Dozierendenteam besteht aus Christopher Scherb (Professor für Cybersecurity, PhD Universität Basel; Schwerpunkte Software-Exploits, Vulnerability Detection, Netzwerksicherheit) und Linus Espach (B.Sc. Nautik und IT Security, CEO Rheintec Solutions; Fokus moderne Netzwerk- und Cloud-Security-Lösungen wie ZTNA, SASE, Hybrid-Clouds).

Lernziele

Die Lehrveranstaltung vermittelt ein belastbares Fundament für Campus-, Rechenzentrums- und Cloud-Netze. Klassische Kontrollen (802.1X, Firewalls, AAA, LAN-Härtung) werden mit modernen Architekturmustern (SD-WAN, SSE/SASE, Zero Trust) verbunden. Praktische Labs und das Semesterprojekt dienen dazu, Betriebskonzepte und Automatisierungsschritte nachvollziehbar umzusetzen.

Wochenübersicht

Woche	Format / Schwerpunkt
1	Lecture: Kick-off, Projektbriefing, Überblick Netzwerksicherheit
2	Lab: NAC-Starter, Toolchain-Setup, Projektboard
3	Lecture: K2 – Härtung von Netzwerkelementen
4	Lecture: K3 – Firewalls der ersten Generation
5	Lab 2: Firewall-Zonen (DMZ, DC, User); Start Site-to-Site VPN
6	Lecture: K5 – LAN-Segmentierung; Site-to-Site VPN Abschluss
7	Prüfung 1 – Klassische Netzsicherheit
8	Lecture: K5 – Standortanbindungen, WAN-Edge, SSE/SASE
9	Lab: L4 – Migration VPN zu SD-WAN, Policy Based Routing
10	Lecture: L5 – Implementierung von SSE
11	Lecture: K6 – Web Application Firewall, Mail Security, DNSSEC
12	Lab: L6 – WAF-, Mail- und DNSSEC-Implementierung
13	Lecture/Workshop: K7 – Security Operations Stack; Modernisierungs-Review
14	Lecture: K8 – Cloud-/SDN-Architekturen
TBD	Prüfung 2 – Moderne Netzsicherheit (Termin wird kommuniziert)

*Hinweis: Nach dem umfassenden Redesign lernen wir den Zeitplan noch kennen
– kleinere Verschiebungen sind möglich und werden frühzeitig kommuniziert.*

Projekt-Checkpoints & Abnahmen

Für den klassischen Teil ist ein Projekt-Zwischenstand vorzulegen, für den modernen Teil eine Modernisierungs-Roadmap. Beide Checkpoints sind Testatbedingungen. Projektabnahmeterminen werden separat vereinbart und ausserhalb des Standardzeitplans durchgeführt.

Bewertung & Verpflichtungen

Zur Bewertung zählen zwei schriftliche Prüfungen (Woche 7 und Termin TBD für moderne Netzsicherheit) sowie die erfolgreichen Projekt-Checkpoints. Labs liefern die technische Basis (OpnSense, SD-WAN, Cloudflare). Eine fortlaufende Dokumentation und fristgerechte Abgaben sind Voraussetzung für die Modulzulassung.