

K0: Kick-off & Organisation

Christopher Scherb <christopher.scherb@fhnw.ch>

FHNW Hochschule für Technik

17. September 2025

Einführung

- ▶ 14 Termine Donnerstags 16:15–18:50: Kombi aus Vorlesungen, Labs und Projektarbeit.
- ▶ Zwei Lehrende: Christopher Scherb (Klassik-Fokus) und Linus Espach (Modernisierung).
- ▶ Projekte, Labs und Checkpoints bilden die Grundlage für die beiden Modulprüfungen.
- ▶ Erwartung: aktive Teilnahme, pünktliche Abgaben, kontinuierliche Dokumentation.

Ziele der Vorlesung

- ▶ Fundament für den Schutz von Campus-, Rechenzentrums- und Cloud-Netzen legen.
- ▶ Klassische Netzsicherheit (802.1X, Firewalls, AAA, LAN-Härtung) hands-on erlernen.
- ▶ Moderne Ansätze (SD-WAN, SSE/SASE, Zero Trust) beurteilen und implementieren.
- ▶ Projekte und Labs nutzen, um Betriebskonzepte und Automatisierung praxisnah zu vertiefen.

Christopher Scherb

- ▶ Professor für Cybersecurity, PhD (Universität Basel).
- ▶ Spezialisiert auf Software-Exploits, Vulnerability Detection und Netzwerksicherheit.
- ▶ Kontakt: christopher.scherb@fhnw.ch.



Linus Espach

- ▶ B.Sc. Nautik.
- ▶ B.Sc. IT Security.
- ▶ Fokus auf moderne Netzwerk- und Cloud-Security-Lösungen (ZTNA, SASE, Hybrid-Clouds).
- ▶ Tätigkeit: CEO Rheintec Solutions.



Zeitplan Phase Klassik (Wochen 1–7)

Woche	Schwerpunkte / Deliverables
1	Lecture: Kick-off, Projektbriefing, Überblick Netzwerksicherheit
2	Lab: NAC-Starter, Toolchain-Setup, Projektboard
3	Lecture: K2 – Härtung von Netzwerkelementen (Konsole, Rollen, Logging)
4	Lecture: K3 – Firewalls der ersten Generation, Betrieb & Change-Prozesse
5	Lab 2: Netzwerkumgebung mit Firewall und Zonen (DMZ, DC, User); Start Site-to-Site VPN
6	Lecture: K5 – LAN-Segmentierung, Layer-2-Abwehr; Site-to-Site VPN abschliessen
7	Prüfung 1 (Klassische Netzsicherheit) & Auswertung

Zeitplan Phase Modern (Wochen 8–15)

Woche	Schwerpunkte / Deliverables
8	Lecture: K5 – Standortanbindungen, WAN-Edge, SSE/SASE-Grundlagen
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 (NDR, API-GW, CNAPP, XDR, SIEM, usw.); Modernisierungs-Review
14	Lecture: K8 – Cloud-/SDN-Architekturen
TBD	Prüfung (Moderne Netzsicherheit)

Projekt-Checkpoints

- ▶ Klassik: Projekt-Zwischenstand präsentieren, Testatpflicht für weitere Teilnahme.
- ▶ Modern: Modernisierungs-Roadmap präsentieren, Testatpflicht für Modulabschluss.

Bewertung & Verpflichtungen

- ▶ Zwei schriftliche Prüfungen: Woche 7 (Klassische Verteidigung) und Termin TBD (Moderne Netzsicherheit).
- ▶ Projektarbeit mit zwei Testat-Checkpoints: Klassik (Woche 6) und Modern (Woche 13) – **müssen präsentiert und bestanden werden.**
- ▶ Labs liefern die technische Basis (OpnSense, SD-WAN, Cloudflare) für die Zwischenstände.
- ▶ Laufende Dokumentation und termingerechte Abgaben sind Voraussetzung für die Modulzulassung.