Certificate of Advanced Studies

Networking and Security

Funktionalität und Sicherheit sind die zentralen Anforderungen an Netzwerke. Das CAS Networking & Security richtet sich an Personen, die für Konzeption, Aufbau und Betrieb von internetbasierten Kommunikationsnetzwerken verantwortlich sind.

Berner
Fachhochschule

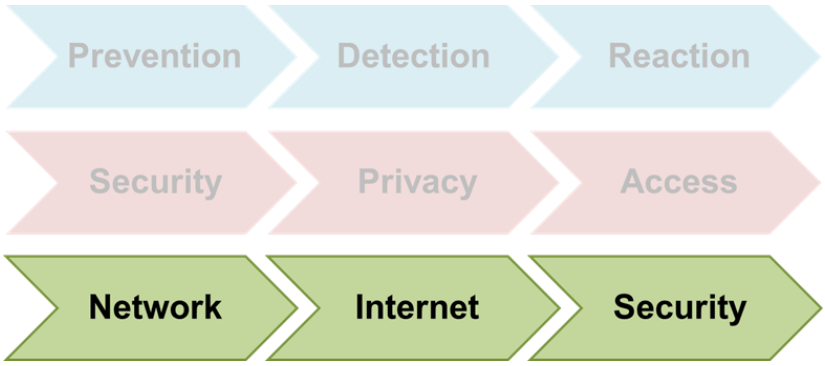
Inhaltsverzeichnis

Stand: 18.09.2023

1 Umfeld

In einer sich schnell ändernden IT-Landschaft erlauben die wachsenden Angebote des Cloud-Computing vollkommen neue Arbeits- und Problemlösungsmethoden. Um die neuen Technologien nutzbringend einzusetzen, werden stabile, sichere und schnelle Netzwerke und Netzwerkdienste benötigt. Mit Homeoffice, dem Internet of Things (IoT) und Industrie 4.0 steigen die Anforderungen an den Datenschutz markant. Dies erfordert neue zusätzliche Sicherheitsmassnahmen. Das CAS NS liefert einen Überblick über aktuelle Entwicklungen wie NFV (Network Function Virtualisation) und SDN (Software Defined Networking). Es vermittelt die Grundlagen und Methoden, um sichere Netzwerke aufzubauen. Das CAS NS ist Teil des MAS Cyber Security und bildet das Fundament für einen erfolgreichen MAS-Abschluss.

Cyber Security



2 Zielpublikum

- Das CAS NS richtet sich an Personen, die für gesicherte, internetbasierte Kommunikations-Netzwerke zuständig oder daran interessiert sind.
- Speziell werden Ingenieurinnen und Ingenieure angesprochen, die sich fundiert mit der Internet-Technologie und der dazugehörenden Netzwerksicherheit auseinandersetzen wollen.

3 Ausbildungsziele

- Sie sind befähigt, sichere Netzwerke für den Einsatz in Industrie und Verwaltung zu konzipieren, zu realisieren und zu beurteilen.
- Sie kennen sich in den Bereichen Virtualisierung, Cloud-Dienste, Outsourcing und neue Internet-Technologien wie LoRaWAN, IPv6, NFV und SDN aus.

4 Voraussetzungen

- Die Teilnehmenden bringen IT-Vorkenntnisse im Rahmen einer Informatik- oder Wirtschaftsinformatik-Ausbildung mit. Insbesondere sind Erfahrungen in der Mitarbeit und Umsetzung von Informatikprojekten erforderlich.
- Erfahrungen in der Systemadministration von Windows- und Linux-Servern sowie der Datenkommunikation sind von Vorteil und erleichtern den Einstieg in diesen Lehrgang.
- Für das Studium der Fachliteratur und der Kursunterlagen werden Englisch-Kenntnisse vorausgesetzt.

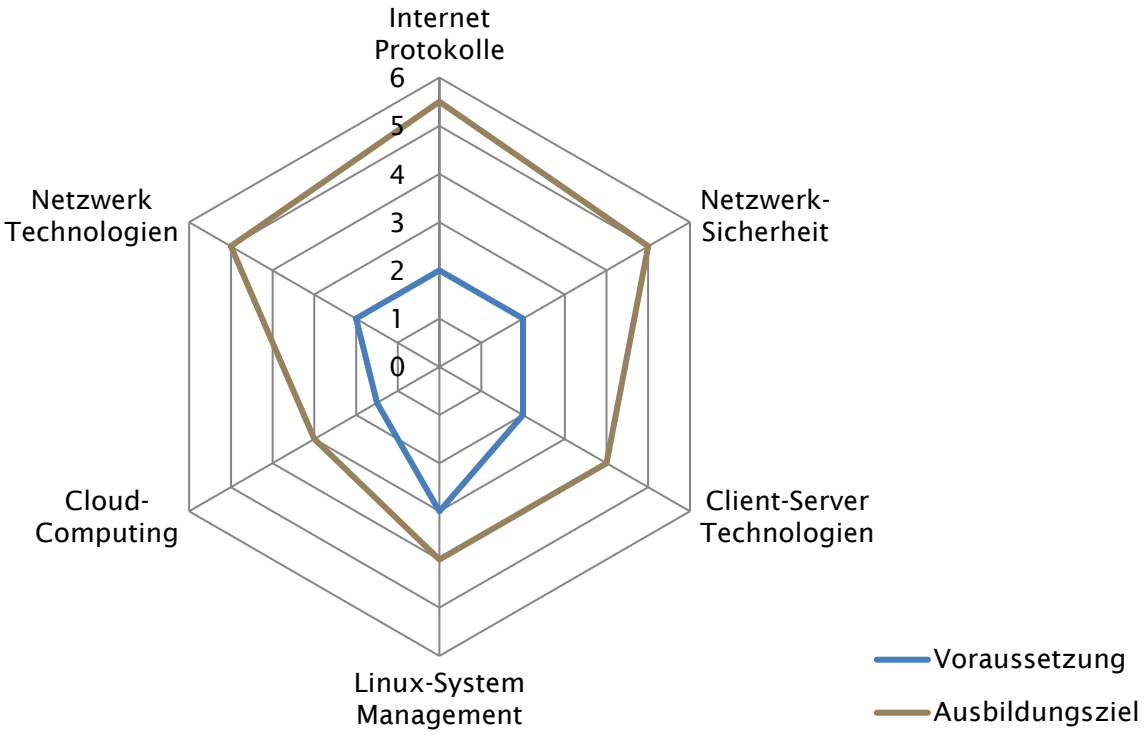
5 Unterrichtssprache

Die Unterrichtssprache ist Deutsch, die Unterlagen sind teilweise in Englisch.

6 Durchführungsort

Berner Fachhochschule, Weiterbildung, Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne), 2503 Biel,
Telefon +41 31 848 31 11, E-Mail weiterbildung.ti@bfh.ch.

7 Kompetenzprofil



Kompetenzstufen

1. Kenntnisse/Wissen
2. Verstehen
3. Anwenden
4. Analyse
5. Synthese
6. Beurteilung

8 Kursübersicht

Kurs / Lehreinheit	Lektionen	Stunden	Dozierende
Netzwerk-Technologien	52		Rolf Lanz Emiliano Contaldi
Sichere Netzwerke	60		Jean-Claude Kiener
Internet-Technologien	72		Hansjürg Wenger Marcel Ritschard
Labor / Praktika		~ 100	Div.
Total	**184**	**~ 100**	

Das CAS umfasst insgesamt 12 ECTS-Punkte. Für die einzelnen Kurse ist entsprechend Zeit für Selbststudium, Prüfungsvorbereitung, erweiterte Laborversuche etc. einzurechnen.

Das CAS ist Teil des «Master of Advanced Studies in Cyber Security» der Berner Fachhochschule.

9 Didaktik, Präsenz, Distance Learning

Didaktisch ist das CAS geprägt von einer hohen Interaktion zwischen Dozierenden und den Studierenden. Der Theorieteil des Unterrichts wird mit kleinen Aufgaben, Übungen und Diskussionen ergänzt. In verschiedenen kleinen bis mittleren Gruppenarbeiten wird das im CAS erworbene Wissen an konkreten Beispielen aus der Schule oder aus dem Umfeld der Studierenden angewendet.

Neben dem klassischen Präsenzunterricht im Klassenzimmer werden einzelne Kursteile auch im Fernunterricht per MS-Teams gehalten oder in hybrider Form (Unterricht im Klassenzimmer mit Live-Übertragung per MS-Teams) angeboten. Die gewählte Unterrichtsform orientiert sich dabei an den zu behandelnden Themen und den jeweils aktuellen Vorgaben des BAG.

10 Kursbeschreibungen

Nachfolgend sind die einzelnen Kurse dieses Studienganges beschrieben.

Der Begriff Kurs schliesst alle Veranstaltungstypen ein. Kurs ist ein zusammenfassender Begriff für verschiedene Veranstaltungstypen wie Vorlesung, Lehrveranstaltung, Fallstudie, Living Case, Fach, Studienreise, Semesterarbeiten, usw.

10.1 Netzwerk-Technologien

Lernziele	Die Teilnehmenden lernen in diesem Kurs zu beurteilen, welche Netzwerk-Technologien und Konfigurationen für die Datenkommunikation bezüglich Performance, Verfügbarkeit und Sicherheit in einer Firma am besten geeignet sind. Sie kennen die dazu passenden Konfigurationsmöglichkeiten der aktiven Netzwerkkomponenten und sind in der Lage, ihre Netzwerk-Infrastruktur selbständig oder zusammen mit externen Partnern zu planen, in Betrieb zu nehmen und sicher zu betreiben.

Themen und Inhalte	– Grundlagen der Netzwerk-Technologien
	  – aktuelle LAN-Technologien im ISO/OSI-Modell
	  – vom Megabit-Ethernet zum Terabit-Ethernet
	  – sichere WLANs und deren Weiterentwicklungen bis WiFi-7
	  – Technologie und Anbindung von IoT-Devices
	  – Praktika zur Vertiefung
	– Lichtwellenleiter
	  – Vorteile und Funktion von Glasfaserkabeln
	  – FTTx auf allen Ebenen einer aktuellen Kommunikationsinfrastruktur
	  – Fallstudie: LWL-Verkabelung
	– aktive Netzwerkkomponenten
	  – vom Repeater über Bridges, Switch, Router, Multilayer-Switch bis zum Application-Layer Gateway
	  – redundante, sichere, virtuelle LANs mit Link-Aggregation
	  – ausführliche Praktika zur Vertiefung der behandelten Theorie
	– Netzarchitekturen anhand einer Fallstudie
	– Projektarbeiten im Informatiklabor
	  – Planung, Aufbau, Konfiguration und Härtung eines sicheren und redundanten Firmennetzes
	  – zur fächerübergreifenden Integration des erworbenen Wissens und als Basis für weiterführende Übungen in den nachfolgenden Kursteilen
	– Software-Defined Networking (SDN) mit Praktikum
	  – SDN- und NFV-Grundlagen
	  – Konzepte und Architekturen für SDN
	  – typische Anwendungsfälle
	  – virtuelles Netzwerk-Labor

Lehrmittel	– kommentierte Foliensets, die alle wesentlichen Lerninhalte umfassen – Literaturempfehlungen Nr. 1, 2, 3 oder 4

10.2 Internet-Technologien

Lernziele	Die Teilnehmenden verstehen die Mechanismen der Internettechnologie. Sie sind am Ende des Kurses in der Lage, eine Internetprotokoll-basierte Infrastruktur mit allen wesentlichen Netzwerk-Services für den eigenen Betrieb oder für externe Auftraggeber zu konzipieren, aufzubauen und weiterzuentwickeln.

Themen und Inhalte	– Internet-Protokolle
	  – Gremien und Standardisierungsverfahren der Internet-Protokoll-Familie
	  – Architektur und Basisprotokolle des Internets
	  – aktuelle und zukünftige Technologien und Protokolle
	  – (IPv4, IPv6, 6LoWPAN, IPsec, DNSSEC, OSPF, usw.)
	– Systeme, Netzwerke und Routing
	  – Konfiguration und Adressierung von Internet-Systemen
	  – Routing-Architektur und Protokolle im Firmennetz und im Internet
	  – Migrationsszenarien von IPv4 auf IPv6
	– Standard- und Cloud-Dienste
	  – Internet-Standard-Dienste und -Anwendungen, Protokolle, Funktionsweise und Konfiguration
	  – die Möglichkeit, diese Dienste als Cloud-Services zu beziehen oder zu betreiben
	  – Vergleich der Cloud-Services mit selbst erbrachten Services
	– praktische Umsetzung
	  – Aufbau eines Netzwerks mit Systemen und Routern
	  – Realisierung von Services und Anwendungen, konventionell oder als Cloud-Service mit Hilfe einer virtuellen Infrastruktur
	  – Kopplung des virtuellen Labors mit dem Internet der realen Welt

Lehrmittel	– Folien-Skript, das alle wesentlichen Lerninhalte umfasst – Literaturempfehlungen Nr. 3 oder 4 und 5 oder 6

10.3 Sichere Netzwerke

Lernziele	Die Teilnehmenden sind am Ende dieses Kurses in der Lage, Gefahren in ICT-Netzwerken zu erkennen, Risiken korrekt einzuschätzen und erforderliche Gegenmassnahmen vorzuschlagen und umzusetzen.

Themen und Inhalte	– Grundlagen zum Begriff Sicherheit
	  – Definitionen und Abgrenzungen
	  – Gefahren und deren Auswirkungen, Risikoeinschätzung
	  – Grundsätze und Prinzipien der Informationssicherheit
	  – warum Netzwerksicherheit, Angriffe auf und über das Netzwerk
	– Elemente der Netzwerksicherheit
	  – physische Sicherheit
	  – Verfügbarkeitsmassnahmen, Zugangsschutz
	  – sichere Netzwerkkomponenten und Netzwerkdienste
	  – gezielter Datenfluss, Netzsegmentierung
	  – Proxies, Remote Access, Virtual Private Networks
	– Sicherheitsrisiken von Netzwerkprotokollen
	  – IP-Stack und dessen Angriffsflächen (IPv4 und IPv6)
	  – Distributed Denial of Service (DDOS)
	  – Sniffing, Spoofing, man-in-the-middle, …
	  – Protokollattacken und effiziente Gegenmassnahmen
	  – Sicherheitsaspekte bei Voice over IP (VoIP)
	– Steuern und Kontrollieren der Datenflüsse
	  – Packet Filter, Stateful Inspection, Web Application Firewall
	  – die Firewalls heute, Lösungsarchitekturen und Produkte
	  – Implementation und Betrieb von Firewalls
	  – Intrusion Detection und Intrusion Prevention
	  – Herausforderungen Cloud-Sicherheit
	– sichere Datenübertragung, Schutz vor Angriffen
	  – Verschlüsselung, Zertifikate, MACsec
	  – VPNs, IPsec, OpenVPN, Toor
	  – sichere Übertragung in WLANs
	  – DNS-Sicherheit
	– Operational Technology (OT) Sicherheit in Netzwerken
	  – OT vs. IT: Verständnis der unterschiedlichen Schwerpunkte und Bedürfnisse
	  – historische und aktuelle Bedrohungen
	  – Besonderheiten von OT-Systemen in Netzwerkumgebungen
	– Erkennen von Angriffen
	  – Hacking, Cracking, Malware, Social Engineering, …
	  – die Angreifer, deren Motivationen und Werkzeuge
	  – die Frage des «von wo»
	  – Intrusion Prevention / Detection
	  – Ablauf einer typischen Netzwerk-Attacke
	  – Erkennen und Behandeln von Sicherheitsvorfällen
	  – Grundlagen der ICT-Forensik
	– Gastreferat
	Spezialthema oder ein Beispiel aus der Praxis

Lehrmittel	– Folienskript, das alle wesentlichen Lerninhalte umfasst Aktualisierte Literaturempfehlungen folgen im Unterricht.

11 Kompetenznachweis

Für die Anrechnung der 12 ECTS-Punkte ist das erfolgreiche Bestehen der Qualifikationsnachweise (Prüfungen, Projektarbeiten) erforderlich, gemäss folgender Aufstellung:

Kompetenznachweis	Gewicht	Art der Qualifikation	Erfolgsquote Studierende
Netzwerk-Technologien	3.0	Gruppenarbeiten und Prüfung	0 – 100 %
Internet-Technologien	3.5	Gruppenarbeit und Prüfung	0 – 100 %
Sichere Netzwerke	3.5	Gruppenarbeiten und Prüfung	0 – 100 %
Gesamtgewicht/Erfolgsquote	10		0 – 100 %

Studierende können in einem Kompetenznachweis eine Erfolgsquote von 0 bis 100% erreichen. Die gewichtete Summe aus den Erfolgsquoten pro Thema und dem Gewicht des Themas ergibt eine Gesamterfolgsquote zwischen 0 und 100%. Der gewichtete Mittelwert der Erfolgsquoten der einzelnen Kompetenznachweise wird in eine Note zwischen 3 und 6 umgerechnet. Die Note 3 (gemittelte Erfolgsquote weniger als 50%) ist ungenügend, Die Noten 4, 4.5, 5, 5.5 und 6 (gemittelte Erfolgsquote zwischen 50% und 100%) sind genügend.

12 Lehrmittel

Für das Einlesen und als Begleitmaterial werden folgende Bücher oder E-Books empfohlen. Die Beschaffung liegt im Ermessen der Studierenden:

Nr.	Titel	Autoren	Verlag	Jahr	ISBN Nr.
1.	Computer Networks (Original in English)	David J. Wetherall Andrew S. Tanenbaum	Pearson Education	2021	978-1-292-37406-2
2.	Computernetzwerke (Deutsche Übersetzung)	David J. Wetherall Andrew S. Tanenbaum	Pearson Studium	2012	978-3-86894-137-1
3.	Computer Networking: A Top-Down Approach	Keith W. Ross James F. Kurose	Pearson Education	2021	978-1-292-40546-9
4.	Computernetzwerke: Der Top-Down-Ansatz	Keith W. Ross James F. Kurose	Pearson Studium	2014	978-3-86894-237-8
5.	LINUX – Das umfassende Handbuch	Johannes Plötner Steffen Wendzel	Rheinwerk «openbook»	2012	freier Download
6.	Ubuntu 20.04 Essentials A Guide to Ubuntu 20.04 Desktop and Server Editions	Neil Smyth	Payload Media	2020	978-1951442187

13 Dozierende

Vorname Name	Firma	E-Mail
Prof. Rolf Lanz	Berner Fachhochschule	rolf.lanz@bfh.ch
Prof. Hansjürg Wenger	Berner Fachhochschule	hansjuerg.wenger@bfh.ch
Emiliano Contaldi	Fedpol EJPD	emiliano.contaldi@bfh.ch
Jean-Claude Kiener	Stadt Thun	jean-claude.kiener@bfh.ch
Marcel Ritschard	Kommando Cyber	marcel.ritschard@bfh.ch

14 Organisation

CAS-Leitung:
Rolf Lanz
Tel: +41 31 848 32 73
E-Mail: rolf.lanz@bfh.ch

CAS-Administration:
Andrea Moser
Tel: +41 31 848 32 11
E-Mail: andrea.moser@bfh.ch

Während der Durchführung des CAS können sich Anpassungen bezüglich Inhalten, Lernzielen, Dozierenden und Kompetenznachweisen ergeben. Es liegt in der Kompetenz der Dozierenden und der Studienleitung, aufgrund der aktuellen Entwicklungen in einem Fachgebiet, der konkreten Vorkenntnisse und Interessenslage der Teilnehmenden, sowie aus didaktischen und organisatorischen Gründen Anpassungen im Ablauf eines CAS vorzunehmen.

Berner Fachhochschule
Weiterbildung
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel

Telefon +41 31 848 31 11
E-Mail: weiterbildung.ti@bfh.ch

bfh.ch/ti/weiterbildung
bfh.ch/ti/mas-cs
bfh.ch/ti/cas-ns