Technology
Arts Sciences
TH Köln

Lehrveranstaltung
NSA - Netzsicherheit und Automation

Version: 7 | Letzte Änderung: 09.12.2022 13:03 | Entwurf: 0 | Status: vom verantwortlichen Dozent freigegeben

Allgemeine Informationen

Langname	Netzsicherheit und Automation
Anerkennende LModule	NSA_BaTIN, NSA_BaET
Verantwortlich	Prof. Dr. Andreas Grebe Professor Fakultät IME
Niveau	Bachelor
Semester im Jahr	Sommersemester
Dauer	Semester
Stunden im Selbststudium	60
ECTS	5
Dozenten	Prof. Dr. Andreas Grebe Professor Fakultät IME
Voraussetzungen	Kenntnisse und Kompetenzen des Moduls "Netze und Protokolle (NP)" alternativ: Kenntnisse und Anwendung von grundlegenden Internetworking Techniken Grundlegende Vernetzungstechniken TCP/IP Protokollfamilie ISO/OSI Schichtenmodellierung IPv4/IPv6 Routing Switchingtechniken TCP/UDP Transporttechniken Anwendungsprotokolle Umgang mit Netzelementen (Client, Server, Switch, Router)
Unterrichtssprache	deutsch
separate Abschlussprüfung	Ja

Abschlussprüfung

Details

Die Studierenden weisen in einer abschließenden Prüfung (schriftlich, optional mündlich) summarisch ihre Kompetenzen nach. Die Prüfung umfasst folgende Teilbereiche, in denen sechs Taxonimiestufen (Wiedergeben, Verstehen, Anwenden, Analysieren, Synthetisieren, und Bewerten) enthalten sind.
1.) Sichere Beherrschung grundlegender Begrifflichkeiten, Konzepte und Techniken. Typische Aufgabenformen sind Multiple-Choice-Fragen, offene Fragen, Bewertung von Aussagen hinsichtlich ihrer Korrektheit
2.) Anwendung von Planungs- und Bewertungstechniken. Typische Aufgabenformen sind Planungsaufgaben von Netzen oder Teilsystemen.
3.) Prüfung von Lösungsvorschlägen auf Korrektheit, Identifikation von Fehlern in Aussagen oder vorgegebenen Netzen. Typische Aufgabenformen enthalten die Analyse vorgegebener Netzarchitekturen und Sysetmaussagen.

Mindeststandard

Erreichen der individuellen Mindestpunktzahl je Klausur, typisch 50% der maximalen Punktzahl.

Prüfungstyp

Die Studierenden weisen in einer abschließenden Prüfung (schriftlich, optional mündlich) summarisch ihre Kompetenzen nach. Die Prüfung umfasst folgende Teilbereiche, in denen sechs Taxonimiestufen (Wiedergeben, Verstehen, Anwenden, Analysieren, Synthetisieren, und Bewerten) enthalten sind.
1.) Sichere Beherrschung grundlegender Begrifflichkeiten, Konzepte und Techniken. Typische Aufgabenformen sind Multiple-Choice-Fragen, offene Fragen, Bewertung von Aussagen hinsichtlich ihrer Korrektheit
2.) Anwendung von Planungs- und Bewertungstechniken. Typische Aufgabenformen sind Planungsaufgaben von Netzen oder Teilsystemen.
3.) Prüfung von Lösungsvorschlägen auf Korrektheit, Identifikation von Fehlern in Aussagen oder vorgegebenen Netzen. Typische Aufgabenformen enthalten die Analyse vorgegebener Netzarchitekturen und Sysetmaussagen.

Vorlesung / Übungen

Lernziele

Kenntnisse

Grundlagen zum Aufbau von hierarchisch strukturierten Netzen, Unternhemensnetzen mit Redunanztechniken, Wireless LAN (WLAN), standortübergreifende Kommunikation, WAN-Techniken. Einführung in die Netzsicherheit mit Vertiefungen zu Angriffen, Sicherheitszielen, kryptographischen Verfahren, Verschlüsselung, Paketfilter, sichere Infrastrukturen, virtuelle private Netze. Einführung in verteiltes Netzmanagement und Servicequalitätstechniken. Techniken zur Netzvirtuaisierung, Software-defined Networking und Netzautomatiisierung.

Auszug der Inhalte:
Hierarchische Netze, Redundanz, STP, EtherChannel, FHRP, Single-area und Multiarea OSPF, OSPF Sicherheitstechniken, WLAN, WAN-Anschluss, PPP, xDSL
Netzsicherheit mit Sicherheitszielen, kryptographische Verfahren, Algorithmen, Paketfilter, ACL, NAT, FireWall, DMZ, VPN, IPsec
SNMP, Syslog, QoS – Quality-of-Service
Sofware Defined Networking (SDN), SDN Controller, Cloud, Virtualisierung, Ansible, JSON, YAML, REST API

Fertigkeiten

Studierende erhalten die Kompetenzen, mittelgroße, standortübergreifende Unternehmensnetze Netze unter Einsatz geeigneter Tools analysieren, geeigente Architekturen auszuwählen und entsprechende Netze zu planen und zu implementieren. Sie benennen und identifizieren Gefährdungslagen

für Unternehmensnetze. Geeignete Sicherheitsmechansimen sind auszuwählen, zu designen und zu implementieren. Aufgaben und Methoden softwaregesteuerter Netze inklusive und Virtualisierungen werden benannt und Mechnismen zur Netzautomaitisierung geplant und umgesetzt.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Vorlesung	2
Übungen (ganzer Kurs)	2
Übungen (geteilter Kurs)	0
Tutorium (freiwillig)	0

Separate Prüfung

keine

Praktikum

Lernziele

Kenntnisse

Konzepte und Technologien für mittelgroße, standortübergreifende Unternehmensnetze benennen, strukturieren, einordnen. Netzanalysetechniken und Tools beherrschen, Netzdesignschritte kennen und Methoden zur Netzplanung kennen. Sicherheitsrelevante Netzapsekte identifizeiern und geeignete Massnahmen zur Netzsicherheit und deren Umsetzung kennen. Aufgaben der Netzautomatisierung und Virtualisierung kennen und für geeignete Netzbereiche deren Umsetzung beherrschen.

Fertigkeiten

Planung, Implementierung und Analyse von VLAN-Architekturen, WLAN.Netzen, standorübergreifende VPN und Paketfilter-Firewall.
Implementierung und Analyse von Netzmanagement mit SNMP und Syslog.
Implementierung und Analyse von Netzautomatisierung an Netzelementen (u.a. Router, Switch, Host, SDN-Controller) über REST API mit Phython-Scripting oder Ansible YAML Skripting.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Praktikum	1

Tutorium (freiwillig)	0

Separate Prüfung

Prüfungstyp

praxisnahes Szenario bearbeiten (z.B. im Praktikum)

Details

Es sind mehrer Praktikumstermine mit verschiedenen Aufgaben wahrzunehmen.
Für jeden Termin sind folgende Aufgaben zu bearbeiten:
Selbstständige Lösung der vorbereitenden Selbstlernaufgaben (Hausaufgabe).
Lösung der Netzdesign-, Implementierungs- und Analyseaufgaben im Kleinteam (typisch 2 Studierende), ggf. unter Inanspruchnahme von Hilfestellungen.
Optional ist die Teilnahme an Cisco Academy CCNA (Cisco Certified Network Associate) Moduln möglich. Der erfolgreiche Abschluss von ausgewählten Labs von CCNA 1 und CCNA 2 wird für das Praktikum anerkannt.

Mindeststandard

Erfolgreiche Teilnahme an allen Praktikumsterminen.
Jeweils korrekte Lösung aller Selbstlernaufgaben und jeweils Abschluss aller Aufgaben des Praktikumtermins.