

Kursstart alle 4 Wochen

CCNA und IT-Security-Beauftragte:r

Der Kurs vermittelt die Konfiguration von Cisco-Netzwerken, die Umsetzung von LAN-Konzepten und Routingtechnologien, Sicherheits- und Schutzmaßnahmen sowie psychologische Aspekte zur Sensibilisierung der Mitarbeitenden. Du erfährst, wie Künstliche Intelligenz (KI) im Beruf eingesetzt wird.



Abschlussart

Cisco Certified Network Associate-Zertifikat (CCNA)
Zertifikat „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation“



Abschlussprüfung

Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
Cisco-Zertifizierungsprüfung CCNA 200-301 (in englischer Sprache)
IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation



Dauer

12 Wochen



Unterrichtszeiten

Montag bis Freitag von 08:30 bis 15:35 Uhr
(in Wochen mit Feiertagen von 8:30 bis 17:10 Uhr)



Nächste Kursstarts

27.05.2024
24.06.2024
22.07.2024

LEHRGANGSZIEL

Nach dem Lehrgang kannst du Cisco-Netzwerke in Unternehmen konfigurieren und verwalten. Du kennst die wichtigsten LAN-Konzepte, aber auch gängige Sicherheitslücken, bist mit Netzwerkinfrastrukturen und Automatisierungen in Netzwerken vertraut und beherrscht Routingtechnologien wie WAN, IPv4 und IPv6.

Des Weiteren kennst du als IT-Sicherheitsbeauftragte:r die wesentlichen Aspekte und Anforderungen der IT-Sicherheit: Datensicherheit und -schutz, physische IT-Sicherheit, Kryptographie, Netzsicherheit, PKI, Computersicherheit und organisatorische Sicherheit. Du weißt, die relevanten Standards nach ISO/IEC 27001 und des IT-Grundschutzes nach BSI in der Praxis umzusetzen.

ZIELGRUPPE

Personen mit praktischer Erfahrung und guten Kenntnissen im IT-Bereich und in der Netzwerktechnik (auch Quereinsteiger:innen und Studienabbrecher:innen) sowie IT-Fachkräfte.

Zusätzlich richtet sich dieser Kurs an verantwortliche Personen aus den Bereichen IT-Sicherheit, Netz- und Systemadministration, IT-Organisation, IT-Beratung, Revision und Risikomanagement.

BERUFSAUSSICHTEN

In allen Branchen wächst der Bedarf an qualifizierten Netzwerk-Fachkräften - die Zertifikate von Cisco gehören dabei zu den begehrtesten Qualifikationsnachweisen. Mit dem neuen CCNA-Zertifikat kannst du dich als Netzwerktechniker:in, im Help-Desk-Bereich oder im Bereich der IT-Security bewerben.

Zudem werden IT-Security-Beauftragte werden in Unternehmen aller

Branchen eingesetzt, um einen sicheren und zuverlässigen IT-Betrieb zu gewährleisten.

VORAUSSETZUNGEN

Dieser Lehrgang setzt Netzwerkgrundkenntnisse sowie gute Englisch-Kenntnisse für die Zertifizierungsprüfung voraus.

LEHRGANGSINHALTE

CCNA – CISCO CERTIFIED NETWORK ASSOCIATE

Network Fundamentals (ca. 8 Tage)

Gegenstand und Definitionen der Netzwerktechnik
Gegenüberstellung OSI- und TCP/IP-Referenzmodell
Ethernet-Standards, Ethernetframe-Formate gemäß 802.3 und Änderungsgründe
Aufgaben und Funktionen TCP/IP
Ethernet und IP als paketvermittelnde Netzwerktechnik
Netzwerktopologien und Designs: Three Tier- und Collapsed Core-Architecture
Wirelessinfrastruktur, AccessPoints, Security-Devices (IDS/IPS, Firewalls), End Points
Klassisches Netzwerkkonzept vs. Kontroller-basiertes Konzept
IPv4 Grundlagen, Konfiguration und Troubleshooting
Subnetting und Supernetting (Zusammenfassung von Netzwerkroutern)
ICMP, IGMP und MTU Discovery
IP-Parameter für Client-Betriebssysteme
Router als Broadcast-Barriere und Cisco extended Ping
IPv6 Grundlagen, Konfiguration und Troubleshooting
Adressformat, IPv6- und Extension-Header
Unicast-, Multicast- und Anycast-Adressen
Stateless Address Autoconfiguration (SLAAC)
Wireless Infrastruktur, 802.11-Standards, Prinzipien und Terminologie
Non-Overlapping Wifi-Channels und Optimierung
Komponenten Wireless LANs

Künstliche Intelligenz (KI) im Arbeitsprozess

Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Network Access (ca. 8 Tage)

Access-Switches, Switchingverfahren, -logik, -konfigurationen und -konzepte
Interface-Konfiguration und -Troubleshooting, administrativer und operationaler Mode
VLAN-Konfiguration und -Troubleshooting, Switchübergreifende VLANs
Virtual Trunking Protocol (VTP)
Varianten Inter-VLAN-Routing für IPv4
Inter-VLAN-Routing mit Router on a Stick (ROAS), Multilayer-Switches und Switch Virtual Interfaces (SVIs)
Spanning Tree-Protocol (STP), RootGuard, LoopGuard und EtherchannelGuard
Unterschiede: BPDU-Handling und -Formate, Port-Rollen, -Typen und -Prioritäten, Konvergenzverhalten
Dynamische und statische Etherchannel (Port-Channel) auf Basis LACP und PAgP
Wireless Architektur und Funktionsweise autonomer Access Points
Aufbau und Funktionsweise Wireless LAN-Controller (physikalische und logische Interfaces)

IP Connectivity (ca. 8,5 Tage)

Internetworking und Netzwerktypen
Zuordnung interior und exterior Gateways
Routing Logik, symmetrisches und asymmetrisches Routing
Typen von Routen bei IOS: Ultimate, Level 1 und Level 2 Routen
Bedeutung der Administrativen Distance
Die Metrik bei dynamischen Routingprotokollen, Bedeutung des Longest Prefix Match
Statische Routen und Default Routen
Gateway of Last Resort
Static Floating Routing
OSPF: Area-Konzept, Netzwerktypen und Typen von Routern
Aufbau der LSDB und Typen von Link State Advertisements (Type 1 bis 5)
Dynamisches Routing mit EIGRP
Cisco HSRP: Konfiguration, Troubleshooting, Versionsumstellung und Debugging
VRRP und Cisco GLBP

Network Services (ca. 3,5 Tage)

Device Hardening, Remote Zugriff via Telnet und SSH
SYSLOG-Funktion
Debugging und Filesysteme unter IOS
Backup und Wiederherstellung der Konfiguration sowie IPOS-Images auf TFTP- und FTP-Server
Remoteauthentifizierung mit AAA (TACACS+ und RADIUS)
Cisco Intent Based Networking
DHCP-Server und -Relay-Agents
SNMP Eigenschaften und Versionsunterschiede
NetFlow

Network Security (ca. 4 Tage)

Varianten möglicher Angriffe auf Netzwerke
Mögliche Gegenmaßnahmen (User Awareness, Access Control, SSL, TLS und DTLS)
Layer 2-Security (DHCP-Snooping, Dynamic ARP Inspection, Port-Security)
Access Control Lists (ACL, numbered, named)
Funktionen und Eigenschaften von IDS und IPS
Virtual Private Networks basierend auf IPSec und SSL/TLS
Sicherheitsprotokolle für Wireless-LAN-Zugriff (WPA, WPA2 und WPA3)

Software Defined Networking (SDN) (ca. 3 Tage)

Vergleich klassisches Networking und Software Defined Networking
Virtualisierung und Cloud Ressourcen
Architekturprinzipien SDN: Infrastructure, Control und Application Layer
Cisco SDA: Strukturprinzipien und Zielsetzung
Vergleich traditionelles Netzwerkmanagement (Campus) vs. Cisco DNA Center
Application Programming Interface (RESTFull-API)
Python als Scriptsprache
JSON
Konfigurationsmanagement mit Red Hat Ansible, Puppet und Chef

Projektarbeit, Zertifizierungsvorbereitung und Zertifizierungsprüfung (ca. 5 Tage)

Cisco Certified Network Associate – 200-301 CCNA (in englischer Sprache)

IT-SECURITY-BEAUFTRAGTE:R MIT TÜV RHEINLAND GEPRÜFTER QUALIFIKATION

Aufbau und Kernprozesse der IT-Sicherheit (ca. 2 Tage)

Struktur der IT-Sicherheit in Unternehmen und deren wirtschaftliche Bedeutung
Beteiligte Personen, Funktionen und Kommunikationswege innerhalb des IT-Netzwerks
Grundlegende Vorschriften, rechtliche Grundsätze, Normen

Physische Sicherheit im IT-Umfeld (ca. 2 Tage)

Klassifizierung der physikalischen Sicherheit
Einführung in die physischen Gefahrennormen
Sicherheitsmaßnahmen für die IT-Infrastruktur
Kontroll- und Alarmierungsmechanismen

Künstliche Intelligenz (KI) im Arbeitsprozess

Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Identity- und Access-Management (ca. 2 Tage)

Grundlagen des Access-Managements
Unterscheidung und Spezifizierung der Zutritts-, Zugangs- und Zugriffskontrollen in einem Unternehmen sowie deren Umsetzung
Konzeption und Kontrolle im Accessmanagement
Revisions sichere Archivierung
Identitätsprüfung und Rechtezuweisung
Schutzmechanismen für die IT-Infrastruktur

Bedrohungsszenarien und Konsequenzen für die Umsetzung im Unternehmen (ca. 3 Tage)

DLP – die Bedeutung von Data Loss Prevention und Data Leakage Prevention in der IT-Security
Maßnahmen der Data Loss Prevention und Data Leakage Prevention
Klassifizierung und Schutz vor Schadprogrammen
IOT (Internet Of Things) und Industrie 4.0 – mögliche Bedrohungsszenarien

Network-Security (ca. 2 Tage)

Besondere Maßnahmen für den Schutz des Netzwerkes
Datenschutzanforderungen an Mailserver
Verwaltung und Sicherheit bei Cloud-Nutzung
Prüfung der Systembestandteile und -anwendungen gegenüber unautorisierten Personen/Programmen/Fernzugriffen

Analyse und Realisierung eines IT-Sicherheitssystems für Unternehmen (ca. 2 Tage)

Grundlagen des Informationssicherheitsstandards nach ISO/IEC 27001:2022 sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI) (ca. 2 Tage)

Struktur und Umsetzung des Notfallmanagements nach BSI-Standard 100-4 und 200-4 (BCM) (ca. 1 Tag)

IT-Sicherheit im Unternehmen – Trainings und Sensibilisierung für Mitarbeiter:innen (ca. 1 Tag)

Projektarbeit, Zertifizierungsvorbereitung und Zertifizierungsprüfung „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation“ (ca. 3 Tage)

UNTERRICHTSKONZEPT

Didaktisches Konzept

Deine Dozierenden sind sowohl fachlich als auch didaktisch hoch qualifiziert und werden dich vom ersten bis zum letzten Tag unterrichten (kein Selbstlernsystem).

Du lernst in effektiven Kleingruppen. Die Kurse bestehen in der Regel aus 6 bis 25 Teilnehmenden. Der allgemeine Unterricht wird in allen Kursmodulen

durch zahlreiche praxisbezogene Übungen ergänzt. Die Übungsphase ist ein wichtiger Bestandteil des Unterrichts, denn in dieser Zeit verarbeitest du das neu Erlernte und erlangst Sicherheit und Routine in der Anwendung. Im letzten Abschnitt des Lehrgangs findet eine Projektarbeit, eine Fallstudie oder eine Abschlussprüfung statt.

Virtueller Klassenraum alfaview®

Der Unterricht findet über die moderne Videotechnik alfaview® statt - entweder bequem von zu Hause oder bei uns im Bildungszentrum. Über alfaview® kann sich der gesamte Kurs face-to-face sehen, in lippensynchroner Sprachqualität miteinander kommunizieren und an gemeinsamen Projekten arbeiten. Du kannst selbstverständlich auch deine zugeschalteten Trainer:innen jederzeit live sehen, mit diesen sprechen und du wirst während der gesamten Kursdauer von deinen Dozierenden in Echtzeit unterrichtet. Der Unterricht ist kein E-Learning, sondern echter Live-Präsenzunterricht über Videotechnik.

FÖRDERMÖGLICHKEITEN

Die Lehrgänge bei alfatraining werden von der Agentur für Arbeit gefördert und sind nach der Zulassungsverordnung AZAV zertifiziert. Bei der Einreichung eines Bildungsgutscheines oder eines Aktivierungs- und Vermittlungsgutscheines werden in der Regel die gesamten Lehrgangskosten von deiner Förderstelle übernommen. Eine Förderung ist auch über den Europäischen Sozialfonds (ESF), die Deutsche Rentenversicherung (DRV) oder über regionale Förderprogramme möglich. Als Zeitsoldat:in besteht die Möglichkeit, Weiterbildungen über den Berufsförderungsdienst (BFD) zu besuchen. Auch Firmen können ihre Mitarbeiter:innen über eine Förderung der Agentur für Arbeit (Qualifizierungschancengesetz) qualifizieren lassen.

- ① Änderungen möglich. Die Lehrgangsinhalte werden regelmäßig aktualisiert. Die aktuellen Lehrgangsinhalte findest Du immer unter www.alfatraining.de.