alfatraining Beratung
beratung@alfatraining.de
0800 3456-500
Mo. - Fr. von 8 bis 17 Uhr kostenfrei aus allen Netzen.

Kursstart alle 4 Wochen

Linux Administrator (LPIC-1) und IT-Security-Beauftragte:r

Der Lehrgang vermittelt organisatorische und technische Sicherheitsmaßnahmen, physische Schutzmaßnahmen, den Einsatz von Künstlicher Intelligenz (KI) in diesem Bereich, psychologische Aspekte zur Sensibilisierung der Mitarbeitenden sowie Kenntnisse im sicheren Umgang mit Linux-Systemen.

Abschlussart
Zertifikat „Linux Administrator" (LPIC-1)
Zertifikat „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation"

Abschlussprüfung
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
Linux-Zertifizierungsprüfungen LPI-101 und LPI-102
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 Kurs gehst du sicher mit Linux-Systemen um. Du kannst Installationen durchführen, Kommandos eingeben, Dateien verwalten und einfache Skripte erstellen. Damit beherrschst du den sicheren Umgang mit kleinen Netzwerken und kannst diese fachgerecht verwalten.

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 ersten praktischen Erfahrungen im IT-Bereich (auch Quereinsteiger:innen), IT-Fachkräfte, (Fach-)Informatiker:innen (auch Studienabbrecher:innen), Programmierer:innen, Datenbank- und Netzwerkfachkräfte.

BERUFSAUSSICHTEN

Mit dem weltweit einheitlichen und anerkannten LPIC-1-Zertifikat verbesserst du deine beruflichen Perspektiven auf dem Arbeitsmarkt branchenübergreifend. Linux-Fachkräfte sind sowohl bei großen als auch mittelständischen Unternehmen nachgefragt.

Zudem werden IT-Security-Beauftragte werden in Unternehmen aller Branchen eingesetzt, um einen sicheren und zuverlässigen IT-Betrieb zu gewährleisten.

VORAUSSETZUNGEN

Grundkenntnisse über Betriebssysteme oder Computernetzwerke sind vorteilhaft.

LEHRGANGSINHALTE

LINUX ADMINISTRATOR (LPIC-1)

Systemarchitektur (ca. 2 Tage)
Bestimmen und Konfigurieren der Hardwareeinstellungen
Startvorgang des Systems begleiten
Anhalten oder Neustart des Systems sowie Wechsel des Runlevels/Boot-Targets

Künstliche Intelligenz (KI) im Arbeitsprozess
Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Linux-Installation und Linux-Paketverwaltung (ca. 5 Tage)
Entwurf eines Platten-Partitionierungsschemas für ein Linux-System/Planung einer Festplattenaufteilung
Auswahl, Installation und Konfiguration eines Boot-Managers
Verwaltung, Bestimmung sowie Installation von Shared Libraries
Debian-Paketverwaltung
RPM- und YUM-Paketverwaltung
Linux Virtualisierung und Cloud Konzepte

Einsetzen von GNU- und Unix-Kommandos (ca. 8 Tage)
Arbeiten mit Shells und Kommandos über die Kommandozeile
Verarbeiten von Textströmen mit Filtern
Verwendung von grundlegenden Linux-Kommandos zur Dateiverwaltung
Nutzung von Strömen, Pipes und Umleitungen zur effizienten Verarbeitung von Textdaten
Prozessverwaltung
Verwaltung der Ausführungsprioritäten von Prozessen
Durchsuchen von Textdateien mit regulären Ausdrücken
Editieren von Dateien mit „vi"

Geräte, Linux-Dateisysteme, Filesystem Hierarchy Standard (ca. 5 Tage)
Konfiguration von Plattenpartitionen, Anlegen von Dateisystemen
Verwaltung eines Standarddateisystems, Integrität von Dateisystemen sichern
Konfiguration des Ein- und Aushängens eines Dateisystems
Steuerung von Dateizugriffen durch den Einsatz von Rechten und Eigentümerschaften
Anlegen und Verwalten von harten und symbolischen Links
Filesystem Hierarchy Standard (FHS), typische Dateiorte und Verzeichnisklassifizierungen
Zertifizierung LPI-101

Shells und Shell-Skripte (ca. 3 Tage)
Die Shell-Umgebungen anpassen und verwenden
Einfache Skripte anpassen oder schreiben

Benutzerschnittstellen und Desktops (ca. 2 Tage)
X11 installieren und konfigurieren
Grafische Desktops
Barrierefreiheit

Administrative Aufgaben (ca. 3 Tage)
Benutzer- und Gruppenkonten und dazugehörige Systemdateien verwalten
Systemadministrationsaufgaben durch Einplanen von Jobs automatisieren
Lokalisierung und Internationalisierung

Grundlegende Systemdienste (ca. 3 Tage)
Die Systemzeit verwalten
Systemprotokollierung
Grundlagen von Mail Transfer Agents (MTA)
Drucker und Druckvorgänge verwalten

Netzwerkgrundlagen (ca. 3 Tage)
Grundlagen von Internetprotokollen
Persistente Netzwerkkonfiguration
Grundlegende Netzwerkfehlerbehebung
Clientseitiges DNS konfigurieren

Sicherheit (ca. 3 Tage)
Administrationsaufgaben für Sicherheit durchführen
Einen Rechner absichern
Daten durch Verschlüsselung schützen

Projektarbeit (ca. 3 Tage)
Zur Vertiefung der gelernten Inhalte
Präsentation der Projektergebnisse
Zertifizierung LPI-102

Nach Bestehen der Prüfungen LPI-101 und LPI-102 bist du Linux Administrator

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

Aufbau und Kernprozesse der IT-Sicherheit (ca. 2 Tage)
Struktur der IT-Security 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 Zugriffkontrollen in einem Unternehmen sowie deren Umsetzung
Konzeption und Kontrolle im Accessmanagement
Revisionssichere 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.

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