



Kursstart alle 4 Wochen


IT-Security-Beauftragte:r mit Microsoft Endpoint und Information Protection Administration


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 den BSI Standard mit seinen IT-Grundschutzkatalogen. Du verstehst, wie du als Microsoft Endpoint Administrator das Windows Betriebssystem bereitstellen und aktualisieren kannst. Auch kannst du Steuerelemente für die Complianceanforderungen planen und implementieren.

 **Abschlussart**
Zertifikat „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation“
Original Microsoft-Zertifikat „Microsoft 365 Certified: Endpoint Administrator Associate“
Original Microsoft-Zertifikat „Microsoft Certified: Information Protection and Compliance Administrator Associate“

 **Abschlussprüfung**
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation
Microsoft-Zertifizierungsprüfung MD-102: Endpoint Administrator
Microsoft-Zertifizierungsprüfung SC-400: Microsoft Information Protection and Compliance Administrator

 **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**
24.06.2024
22.07.2024
19.08.2024

LEHRGANGSZIEL

Als IT-Sicherheitsbeauftragte:r kennst du 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.

Zusätzlich kannst du als Endpoint Administrator die Bereitstellung, Konfiguration, Sicherung, Verwaltung und Überwachung von Microsoft 365 Netzwerken und Anwendungen in deinem Unternehmen übernehmen.

Du bist in der Lage, die technische Implementierung und Definition von Anforderungen und Kontrollen für den Informationsschutz vorzunehmen, und kannst IT-Prozesse und -Vorgänge entsprechend bewerten. Des Weiteren hast du ein Verständnis für die Bereiche Inhaltsklassifizierung, Datenverlust und Governance.

ZIELGRUPPE

(Fach-)Informatiker:innen, IT- und Netzwerk-Fachkräfte, Personen mit praktischer Erfahrung und guten Kenntnissen im IT-Bereich (auch Quereinsteiger:innen).

BERUFSAUSSICHTEN

IT-Security-Beauftragte werden in Unternehmen aller Branchen eingesetzt, um einen sicheren und zuverlässigen IT-Betrieb zu gewährleisten. Die weltweit einheitlichen und anerkannten Microsoft-Zertifizierungen

zählen zu den wichtigsten Herstellerzertifizierungen, mit der Sie Ihre beruflichen Perspektiven auf dem Arbeitsmarkt branchenübergreifend verbessern. Fachkräfte mit entsprechenden Kenntnissen sind sowohl bei großen als auch mittelständischen Unternehmen nachgefragt.

VORAUSSETZUNGEN

Vorausgesetzt wird ein gutes Verständnis von Microsoft 365 Produkten und Diensten.

LEHRGANGSINHALTE

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 Zugriffskontrollen in einem Unternehmen sowie deren Umsetzung
Konzeption und Kontrolle im Accessmanagement
Revisionsichere 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-Beauftragter mit TÜV Rheinland geprüfter Qualifikation“ (ca. 3 Tage)

MICROSOFT ENDPOINT ADMINISTRATION

Windows Client Deployment (ca. 4 Tage)

Planung, Endpoint Analytics
Windows Autopilot
Microsoft Deployment Toolkit (MDT)
Remoteverwaltung, Konfiguration

Identity und Compliance Management (ca. 2,5 Tage)

Identität verwalten in Azure Active Directory
Compliancerichtlinien für Geräteplattformen

Künstliche Intelligenz (KI) im Arbeitsprozess

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

Management, Wartung und Schutz von Geräten (ca. 7 Tage)

Lebenszyklus von Geräten
Gerätekonfiguration
Geräteüberwachung
Geräte-Updates
Endpoint Protection

Management von Apps (ca. 1,5 Tage)

Apps bereitstellen und aktualisieren
App-Schutz und Konfigurations-Richtlinien für iOS und Android

Projektarbeit (ca. 5 Tage)

Zur Vertiefung der gelernten Inhalte
Präsentation der Ergebnisse
Zertifizierungsprüfung MD-102: Endpoint Administrator

MICROSOFT INFORMATION PROTECTION ADMINISTRATION

Implementieren von Informationsschutz (ca. 4,5 Tage)

Vertrauliche Informationstypen (Benutzerdefinierte Typen, EDM-Klassifizieren)
Trainierbare Klassifizierer
Vertraulichkeitsbezeichnungen
Verschlüsselung von E-Mail-Nachrichten

Künstliche Intelligenz (KI) im Arbeitsprozess

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

Implementieren von DLP (ca. 3 Tage)

DLP-Richtlinien
DLP-Einstellungen für Endpunkte
DLP-Aktivitäten (Berichte, Aktivitäten, Warnungen)

Implementieren der Datenlebenszyklus- und Datensatzverwaltung (ca. 2 Tage)

Aufbewahren und Löschen von Daten mithilfe von Aufbewahrungsbezeichnungen
Datenaufbewahrung in Microsoft 365-Workloads
Microsoft Purview-Datensatzverwaltung

Überwachen und Untersuchen von Daten und Aktivitäten mithilfe von Microsoft Purview (ca. 2,5 Tage)

Gesetzliche Anforderungen mithilfe des Compliance Managers
eDiscovery und Inhaltssuche
Überwachungsprotokolle und Berichte

Verwalten von Insider- und Datenschutzrisiken in Microsoft 365 (ca. 3 Tage)

Microsoft Purview-Kommunikationscompliance
Insider-Risikomanagement (IRM)
Microsoft Purview-Informationsbarrieren (IBs)
Datenschutzanforderungen

Projektarbeit (ca. 5 Tage)

Zur Vertiefung der gelernten Inhalte
Präsentation der Ergebnisse
Zertifizierungsprüfung SC-400: Microsoft Information Protection and Compliance Administration

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.