AW410 Security Engineering on AWS

Kurzbeschreibung:

Security Engineering on AWS ist ein dreitätiger Kurs, der den Teilnehmern die AWS-Sicherheitsdienste vorstellt und deren Nutzen in Bezug auf Sicherheit und Compliance erläutert.

Zielgruppe:

- Sicherheitsfachleute
- Sicherheitsarchitekten
- Sicherheitsanalysten
- Sicherheitsprüfer
- Für die Leitung, Überwachung und das Testen der IT-Infrastruktur einer Organisation sowie die Sicherstellung von deren Konformität mit Sicherheits-, Risiko- und Compliance-Richtlinien zuständige Personen

Voraussetzungen:

Die Teilnehmer sollten folgende Voraussetzungen erfüllen:

- Teilnahme am Kurs Grundlagen der AWS-Sicherheit
- Erfahrung im Umgang mit Governance-, Risiko- und Compliance-Vorschriften sowie Kontrollzielen
- Praxiserfahrung im Umgang mit IT-Sicherheitsverfahren
- Praxiserfahrung im Umgang mit IT- Infrastrukturkonzepten
- Verständnis von Cloud Computing-Konzepten

Sonstiges:

Dauer: 3 Tage

Preis: 2685 Euro plus Mwst.

Ziele:

- Shared Security Responsibility durch Anpassung und Nutzung des AWS-Modells
- Verwaltung von Benutzeridentitäten und Zugriffsrechten in der AWS-Cloud
- Einsatz diverser Sicherheitsservices von AWS, wie z.B.: AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS CloudTrail, AWS Key Management Service, AWS CloudHSM und AWS Trusted Advisor
- Implementierung von Sicherheitskontrollen für Ressourcen in der AWS-Cloud
- Verwendung der Sicherheitsperspektive für die Verwaltung und Überwachung von AWS-Ressourcen
- Zugriff und Nutzung von Datenverarbeitungs-, Speicherungs-, Netzwerk- und Datenbankservices in AWS überwachen und protokollieren
- Shared Compliance Responsibility durch Anpassung und Nutzung des AWS-Modells
- Automatisierung durch AWS-Services und Tools
- Sicherheitsvorgänge in der AWS Cloud überwachen und verwalten
- Sicherheitsvorfälle in der AWS-Cloud verwalten

Inhalte/Agenda:

- Dabei werden vor allem die, von AWS empfohlenen, Sicherheitsmethoden behandelt, mit denen eine erhöhte Sicherheit von Daten und Systemen in der Cloud erreicht werden kann.
  Sicherheitsfunktionen wichtiger Services aus dem Bereich Datenverarbeitung, Speicher, Netzwerk und Datenbanken, die von AWS angeboten werden, werden ebenso vorgestellt, wie der Umgang mit Sicherheitskontrollzielen und Standards zur Einhaltung gesetzlicher Vorschriften. Anwendungsfälle aus verschiedenen Branchen geben einen Einblick in die kontinuierlich regulierten Verarbeitungslasten auf AWS.
  Die Vorstellung verschiedener AWS-Tools und -Services, die zur Automatisierung, Überwachung und Protokollierung sowie zur Reaktion auf Sicherheitsvorfälle genutzt werden können, rundet diesen Kurs ab.

  Dieser Kurs setzt sich aus einer Präsentation und Übungen zusammen, um das Erlernte praktisch anzuwenden.

  Die Kursunterlagen (E-Book) sind in englischer Sprache, die Kurssprache ist deutsch.

- Der Kurs Security Engineering on AWS unterstützt Sie bei der Vorbereitung auf folgende Prüfung:
  - AWS Certified Security Specialty
- **Tag 1**
  - Sicherheit in der Cloud Einführung
  - Sicherheit in der AWS-Cloud
  - Governance und Compliance
  - Verwaltung von Zugriffsrechten und Benutzern
  - Lab 1: Einsatz von AWS-IAM
  - Sicherheit für AWS Infrastructure Services 1. Teil
  - Lab 2: Erstellung einer virtuellen privaten Cloud
- **Tag 2**
  - Sicherheit für AWS Infrastructure Services 2. Teil
  - Sicherheit für AWS Container Services 1. Teil
  - Sicherheit für AWS Container Services 2. Teil
  - Lab 3: Einsatz von RDS-Sicherheitsgruppen
  - Sicherheit für abstrahierte AWS-Services
  - Lab 4: Amazon S3-Buckets sichern
  - Einsatz von AWS Security Services 1. Teil
  - Lab 5: Erfassung von Protokollen
- **Tag 3**
  - Einsatz von AWS Security Services 2. Teil
  - Lab 6: Einsatz von AWS Config
  - Lab 7: Einsatz von AWS Service Catalogs
  - Datenschutz in der AWS-Cloud
  - Fallstudien: Compliant-Workloads in AWS erstellen
  - Sicherheitsvorfälle in der Cloud managen