Cloud Security

Risiko und Sicherheit beim Cloud-Einsatz

Der Einzug der Cloud in das tägliche Arbeitsfeld bringt nicht nur viele Vorteile mit sich, sondern auch einige Risiken. Eines dieser Risiken betrifft das Thema Cloud Security. Die Sicherheit beim Cloud Computing umfasst sowohl technische als auch organisatorische Aspekte. Herkömmliche Schutzmaßnahmen geraten in diesem Umfeld schnell an ihre Grenzen.

Vor allem die Skalierbarkeit und die Flexibilität der Cloud fordern modernere Methoden für einen effektiven Schutz. Dabei ist auch ein Blick auf die Verantwortlichkeiten notwendig. In der Cloud wird mit einem Shared-Responsibility-Modell gearbeitet, dessen Ausgestaltung und Grenzen man kennen sollte. Der Kurs vermittelt ein ganzheitliches Bild sowie ein solides Know-how-Fundament zum Thema Cloud Security und liefert einen Überblick über die aktuellen Bedrohungen sowie Lösungsansätze verschiedener Anbieter.

Kursinhalt

- Identifikation von Sicherheitsrisiken in der Cloud-Architektur
- Organisatorische Aspekte der Cloud Security
- Shared Responsibility und Compliance-Programme der Cloud-Provider (ISO 27001, C5, …)
- Das Konzept der Landing Zone und Compliance-Policies
- Absichern von IaaS
- Design-Beispiele mit Azure, AWS und OpenStack
- Workplace Security
- Identity und Access Management
- Gefahr durch den User: Bring Your Own Device, Schatten-IT, CASB
- Sichere WAN-Anbindung: SD-WAN und SASE

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Dieser Kurs richtet sich an Technikerinnen und Techniker sowie Mitarbeitende aus dem Bereich Presales, die sich mit dem Aufbau von Cloud Security beschäftigen.

Voraussetzungen

Grundlegende Netzwerk- und IT-Kenntnisse sollten vorhanden sein. Darüber hinaus sollten Sie Grundbegriffe der Cloud und Cloud-Infrastruktur definieren können. Idealerweise verfügen Sie über das Wissen, welches im Kurs Die Cloud im Einsatz – Konzepte, Entwicklung, Migration vermittelt wird.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**CLSE**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Deutschland	**2 TageCHF 1.975,-**
Online Training	**2 TageCHF 1.975,-**
Termin/Kursort	Kurssprache Deutsch
26.06.-27.06.25 HYFrankfurt	23.10.-24.10.25 HYFrankfurt
26.06.-27.06.25 HYOnline	23.10.-24.10.25 HYOnline

Stand 22.03.2025

Cloud Security

Inhaltsverzeichnis

Cloud Security – Risiko und Sicherheit beim Cloud-Einsatz

1 Einführung in die Cloud-Security
1.1 Angriffe und Bedrohungen
1.1.1 Public Cloud vs. interne IT
1.1.2 Die größten Bedrohungen laut Cloud Security Alliance (CSA)
1.1.3 Security „in" the Cloud vs. Security „of" the Cloud
1.2 Verantwortlichkeiten bei der Cloud Security
1.2.1 Multi-Cloud
1.3 Cloud-Angebot bestimmt Kontrollmöglichkeit
1.3.1 Verantwortlichkeiten im Vergleich
1.4 Applikationssicherheit in Cloud-Umgebungen
1.4.1 OWASP Top 10

2 Compliance, Landing Zones und Verfügbarkeitskonzepte
2.1 Cloud Security - Organisatorische Aspekte
2.1.1 Welche Compliance-Anforderungen gelten für mich?
2.2 Übersicht der Compliance-Programme
2.2.1 ISO/IEC 27001 und 27002
2.2.2 IT-Grundschutz-Standards
2.2.3 BSI Grundschutz nach BSI-Standard 200-4
2.2.4 Cloud Controls Matrix (CSA-CCM)
2.2.5 C5 Testat – Audits für die Cloud
2.2.6 SOC 2 Type 2
2.3 Landing Zone
2.3.1 Cloud-Strategie
2.3.2 Weiterentwicklung: Landing Zone Lifecycle
2.3.3 Best Practices
2.3.4 Beispiel AWS Landing Zone
2.3.5 Beispiel Azure Landing Zone
2.4 Hochverfügbarkeit von VMs
2.4.1 Verfügbarkeitsgruppen
2.4.2 Verfügbarkeitszonen
2.5 Lastausgleich
2.5.1 Azure Backup
2.5.2 Site Recovery
2.6 Object Storage bei Azure
2.6.1 Replikationen
2.6.2 Berechtigungen und Sicherheit

3 Public Cloud: IaaS-Absicherung, Compiance-Policies und mehr
3.1 Service Virtualization
3.2 Next Generation Firewall
3.2.1 Der Begriff des Proxies
3.3 Beispiel anhand von OpenStack
3.3.1 Security Groups
3.4 Beispiel: Bereitstellen von Netzwerken in Azure
3.4.1 Subnetze
3.4.2 Peerings
3.4.3 Routing
3.4.4 Sicherheitsfunktionen bei Azure
3.4.5 Benutzerdefinierte Routen (UDR)
3.4.6 Network Security Groups (NSG)
3.4.7 DDoS-Schutz
3.4.8 Firewall
3.4.9 Beispiel: N-schichtige Windows-Anwendung in Azure
3.4.10 Hybrid vs. Cloud-only
3.5 Beispiel: Bereitstellen von Netzwerken in AWS
3.5.1 VPCs und Subnetze
3.5.2 Security Groups und Network ACLs
3.6 Zugriff auf VMs
3.7 Compliance und Policies
3.7.1 AWS Organizations und Policies
3.7.2 Azure Policies
3.8 Security-Frameworks der Cloud-Provider
3.8.1 Security bei AWS
3.8.2 Security bei Microsoft Azure

4 Gefahr durch den User
4.1 Sicherheitsmaßnahmen für Clients
4.1.1 Arten von Malware
4.1.2 Virenschutz, Personal Firewall und Co.
4.1.3 Patch Management
4.2 Datenklassifizierung und -verschlüsselung
4.2.1 Verschlüsselung
4.3 Die Mobility Story – BYOD
4.3.1 Mobile Endgeräte angreifen
4.3.2 Mobile Device Management
4.4 Security-Awareness-Maßnahmen
4.4.1 Einschränkungen begreifbar machen
4.5 Security Services Edge (SSE)
4.5.1 Firewall as a Service (FWaaS)
4.5.2 Secure Web Gateway (SWG)
4.5.3 DNS-Layer Security
4.6 SaaS-Einbindung
4.6.1 Schatten-IT
4.6.2 Schatten-IT-Risiko-Assessment
4.6.3 Cloud Access Security Broker (CASB)
4.7 Zero Trust Network Access – ZTNA
4.7.1 Weitergehende Leistungsmerkmale einer SSE-Lösung
4.8 Cloud Security Posture Management (CSPM)
4.9 Cloud Workload Protection Platform (CWPP)
4.10 Cloud Native Application Protection Platform (CNAPP)

5 Zugriffsberechtigungen und -Management
5.1 User-Accounts und Passwörter
5.1.1 Regeln für die Passwort-Vergabe
5.1.2 Metadata Service (Beispiel: OpenStack)
5.2 Identity Management
5.2.1 Multi-Factor Authentication (MFA)
5.2.2 Was ist ein Verzeichnisdienst?
5.2.3 Active Directory
5.2.4 Organisationseinheiten und Gruppenrichtlinien
5.2.5 Sites
5.2.6 Beispiel MS Azure: AD in VM in virtuellem Netz
5.3 Authentisierung im Netzwerk (SSO)
5.3.1 Single Sign-on
5.3.2 Modern Authentication with AD FS
5.3.3 Security Assertion Markup Language (SAML)
5.3.4 Open Authentication 2 (OAuth2)
5.4 Beispiel: Microsoft Entra ID
5.4.1 Authentisierung mit Entra ID
5.5 Beispiel: Keystone von OpenStack

6 Zugriff auf die Cloud
6.1 Aufbau von Cloud-Infrastrukturen
6.1.1 IP VPN
6.1.2 MPLS-VPNs
6.2 VPN Gateways zur Cloud-Anbindung
6.2.1 Gateways für VPNs am Beispiel Azure
6.3 Lösungen der Hyperscaler: Beispiel MS Express Route
6.3.1 Lösungen der Hyperscaler: Beispiel AWS Direct Connect
6.4 Aufbau und Limitierungen klassischer WANs
6.5 SD-WAN
6.5.1 SD-WAN Details
6.5.2 SD-WAN: Kundennutzen
6.5.3 Architekturebenen
6.6 Security-Konzepte bei SD-WAN
6.6.1 Lokale SD-WAN-Security
6.6.2 Secure Access Service Edge (SASE)

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch