Cloud Security

Risk and Security when Using the Cloud

The introduction of the cloud into the daily work environment not only brings many benefits, but also some risks. One of these risks relates to cloud security. Security in cloud computing encompasses both technical and organizational aspects. Conventional protective measures quickly reach their limits in this environment.

The scalability and flexibility of the cloud in particular demand more modern methods for effective protection. It is also necessary to take a look at responsibilities. In the cloud, a shared responsibility model is used, the design and limits of which should be known. The course provides a holistic picture and a solid foundation of knowledge on the topic of cloud security and provides an overview of current threats and solutions from various providers.

Course Contents

- Identification of security risks in the cloud architecture
- Organizational aspects of cloud security
- Shared responsibility and compliance programs of cloud providers (ISO 27001, C5, ...)
- The concept of the landing zone and compliance policies
- Securing IaaS
- Design examples with Azure, AWS and OpenStack
- Workplace security
- Identity and access management
- Danger from the user: Bring Your Own Device, shadow IT, CASB
- Secure WAN connection: SD-WAN and SASE

E-Book The detailed digital documentation package, consisting of an e-book and PDF, is included in the price of the course.

Target Group

This course is aimed at technicians and presales staff who are involved in setting up cloud security.

Prerequisites

You should have basic network and IT knowledge. You should also be able to define basic cloud and cloud infrastructure terms.

This Course in the Web

You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/**CLSE**

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training		Prices, excl. of V.A.T.
Classes in Germany	**2 Days**	**€ 1,795**
Online Training	**2 Days**	**€ 1,795**
Date/course venue		Course language German
26/06-27/06/25 HYFrankfurt		23/10-24/10/25 HYFrankfurt
26/06-27/06/25 HYOnline		23/10-24/10/25 HYOnline

Status 04/30/2025

Table of Contents

Cloud Security – Risk and Security when Using the Cloud

1 Introduction to Cloud Security

1.1 Cloud Security Basics

1.2 Cloud Security - Organizational Aspects

1.2.1 Data protection and compliance

1.2.2 Multi-Cloud

1.2.3 Responsibilities in Cloud Security

1.2.4 Public cloud: What should be considered?

1.2.5 Overview of compliance programs

1.3 Application security in cloud environments

1.3.1 OWASP Top 10

2 Private Cloud and Virtualization Security

2.1 Physical access

2.2 Network Security in Virtualized Environments

2.3 Data Center Edge Security

2.4 Data Center Core Security

2.5 Security in the Aggregation Layer

2.5.1 IP access lists

2.5.2 Quality of Service

2.6 Security in the Access Layer

2.7 Virtualization

2.8 Introduction to SAN Security

2.9 Server security in virtualized environments

2.10 Hypervisor Security

2.10.1 VMware

2.10.2 KVM

2.10.3 Hyper-V

2.10.4 Container virtualization (Docker)

2.11 Example based on OpenStack

2.12 Example based on VMware NSX

2.12.1 NSX Distributed Firewall

2.12.2 Edge Devices

2.12.3 Check Point vSec

3 Public Cloud: IaaS protection etc.

3.1 Service Virtualization

3.1.1 Local Server Load Balancing

3.1.2 Virtual Firewalls - Contexts

3.2 Next Generation Firewalls

3.2.1 Stateful Inspection

3.2.2 Content Awareness and URL Filtering

3.2.3 Bot detection

3.2.4 IDS and IPS

3.2.5 Malware Protection

3.2.6 Identity Based Firewalling

3.2.7 Market and functional overview

3.2.8 Palo Alto

3.2.9 Fortinet

3.2.10 Cisco

3.3 Security and Network Function Virtualization

3.3.1 Security vulnerabilities of NFV

3.3.2 Protective measures

3.3.3 NFV Security Management Lifecycle

3.3.4 NFV Security Framework

3.4 Concepts with SDN

3.4.1 Realization of the VNF FG

3.4.2 Advantages of the VNF FG

3.5 Example based on ACI from Cisco

3.5.1 Use of device packages

3.5.2 Service Graphs Templates

3.5.3 Virtual router (CSR1000v)

3.5.4 Example of virtual edge router: Juniper vMX

3.6 Example: Deploying Networks in Azure

3.6.1 Subnets

3.6.2 Routing

3.6.3 DNS

3.7 Security features

3.7.1 User-defined routes (UDR)

3.7.2 Network Security Groups (NSG)

3.7.3 DDoS protection

3.7.4 Firewall

3.8 Coupling of networks

3.8.1 Peerings

3.8.2 Gateways (for VPN etc.)

3.8.3 Hybrid vs. cloud-only

4 Access permissions and management

4.1 User accounts and passwords

4.1.1 Access via CLI

4.1.2 Default parameters

4.2 Identity management

4.2.1 Central user management

4.2.2 Market and function overview

4.2.3 What is a directory service?

4.2.4 Active Directory

4.3 Authentication in the network (SSO)

4.3.1 Single sign-on

4.3.2 Security Assertion Markup Language (SAML)

4.3.3 Open Authentication 2 (OAuth2)

4.4 Information about user activity

4.5 Example: Microsoft Azure Active Directory

4.6 Security and identity management

4.7 Example: Keystone from OpenStack

5 Access to the cloud

5.1 Setting up cloud infrastructures

5.1.1 Hybrid Cloud: Impact on all layers

5.2 VPNs at a glance

5.2.1 MPLS VPNs

5.2.2 IP VPNs

5.3 VPN gateways for cloud connectivity

5.3.1 Cloud-based VPN

5.4 Example: MS Express Route

5.5 vCloud Air Hybrid Cloud Manager

5.6 Cisco CloudCenter

6 Danger from the user

6.1 Security measures for clients

6.1.1 Anti-virus programs

6.1.2 Personal firewalls

6.1.3 Patch management

6.1.4 Hard disk encryption

6.2 Security awareness measures

6.2.1 Involving users

6.2.2 Reveal reasons

6.2.3 Making restrictions understandable

6.3 Cisco AMP

6.4 The concept of proxies

6.4.1 Transparent proxies

6.4.2 Reverse proxies

6.4.3 Generic proxies

6.4.4 Application Layer Gateways

6.4.5 Mode of operation

6.4.6 Limitations

6.4.7 Web proxies

ExperTeach Benelux B.V.

Ceresstraat 1· 4811 CA Breda· Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com