# CLOUD SECURITY ADVISORY: IN 5 SCHRITTEN ZUR CLOUD SECURITY

DIGITAL Trust.

**Konformität mit gesetzlichen Regeln und unternehmensspezifischen Sicherheits-Anforderungen ist ein Muss. Das gilt besonders für die Public Cloud. Das Vorgehensmodell von Computacenter sorgt für kontinuierliche IT-Governance und ein zuverlässiges Risikomanagement.**

## NACHHALTIGE SICHERHEIT: 5-STEP-MODELL FÜR CLOUD SECURITY

Für die Cloud können Unternehmen bestehende Sicherheitsrichtlinien übernehmen, müssen diese aber an die agile Charakteristik der Public Cloud anpassen.

## SCHRITT 1 – ERWEITERUNG BESTEHENDER POLICYS

Organisationen verfügen über erprobte Sicherheits-Policys. Deshalb müssen IT-Expert:innen und das Management für die Cloud das Governance-Rad nicht neu erfinden. Es geht um Erweiterungen der bestehenden Policys, etwa durch zusätzliche AWS oder Azure Guardrails, die Beurteilung operativer Risiken und daraus abgeleitete Handlungsrichtlinien.

Computacenter unterstützt mit seiner Expertise dabei, unternehmensspezifische Guardrails, Guidelines und Building Blocks für die sichere Entwicklung und den Betrieb moderner Cloud-Architekturen zu erstellen.

## SCHRITT 2 – IMPLEMENTIERUNG DER GUARDRAILS

Scale your Knowledge. Das Wissen um die Sicherheit in Public-Cloud-Plattformen ist rar gesät. Momentan kommen auf eine Person mit Cloud-Sicherheits-Expertise ca. 500 Entwickler:innen. Trainings und eine verbindliche Dokumentation sind die ersten Schritte, um die neuen Cloud Guardrails in den unterschiedlichen Fachabteilungen und unter den IT-Sicherheitsverantwortlichen zu verbreiten.

Externe Sicherheitsberater:innen helfen hier bei internen Hürden. Denn sie wissen, dass Entwickler:innen und Administrator:innen in modernen DevOps-Umgebungen oft nur auf Funktionalität und Agilität achten. Security muss deshalb integriert sein.

## SCHRITT 3 – CLOUD RISK ASSESSMENTS

Bei der Migration in die Cloud können Risikopotenziale beim Cloud-Nutzer (Consumer), beim Cloud Provider oder bei der Compliance entstehen. Bereits im Vorfeld schafft hier ein qualifiziertes Risk Assessment große Klarheit und verhindert teure und gefährliche Sicherheitslücken.

Eine Analyse der Cloud Security Advisory, Datenklassifizierung und internen Kontrolle (IKS) ist auch ein schlagkräftiges Argument, um Cloud-Skeptiker:innen zu überzeugen und Vor- sowie Nachteile für App-Migrationen in Cloud-Lösungen sachlich abzuwägen.

## SCHRITT 4 – THREAT MODELING IN AGILEN PROJEKTEN

Moderne Methoden drehen sich um die kontinuierliche Weiterentwicklung und sehr schnelle, frühzeitige Tests und Reaktionen auf Anforderungen durch Nutzer:innen, veränderte Märkte und Nachfragewellen. Informationssicherheit kann hier bremsen, wenn Security-Konzepte nicht mitlaufen. Computacenter sorgt durch Security Sprints an jeder Stelle der agilen Entwicklung und des Betriebs dafür, dass sich Ihre IT-Governance automatisiert anpasst.

Mit unserem bewährten Modell passen wir Ihre Unternehmensvorgaben an Cloud-Infrastrukturen an und fügen sie in bestehende Projektstrukturen ein – die Basis für moderne Konzepte. So können Sie Sicherheitskonzepte für Cloud-Strukturen auf Enterprise-Niveau realisieren.

**Hauke Moritz**
**Solution Manager Cloud Security**

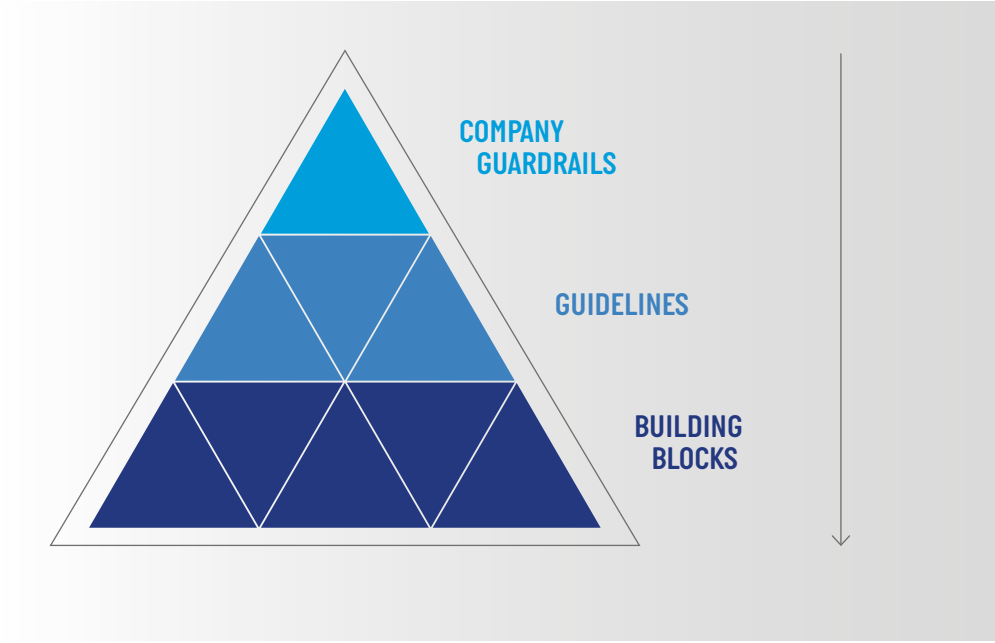

## SCHRITT 5 – CONTINUOUS CONTROL MONITORING

Agile Betriebsprozesse bedeuten permanente Änderungen der Umgebungen. Ein permanenter Konfigurationsdrift betrifft auch die Cloud-Provider-Einstellungen. Container, virtuelle Maschinen und Cloud-Instanzen verändern sich. Neue Funktionen und Features kommen hinzu.

## UMFASSENDE CLOUD-SICHERHEIT – POSTURE MANAGEMENT

Nahezu alle erfolgreichen Angriffe auf Cloud-Dienste entstehen durch Fehlkonfigurationen, Missmanagement oder menschliche Fehler. Verantwortliche für Sicherheit und Risikomanagement sollten in externes Know-how, Prozesse und Tools zur Überwachung ihrer Cloud-Sicherheitslage investieren.

**Nach Gartner gehört Cloud Security Posture Management (CSPM) für die kontinuierliche Evaluierung von Sicherheitsinfrastrukturen und die Überwachung aller Compliance-Vorgaben fest zum Cloud-Konzept.**




Auf Basis bestehender Policys lassen sich Cloud-Sicherheitsvorgaben für IaaS-, PaaS- und SaaS-Plattformen ableiten und entwickeln. Das Vorgehensmodell von Computacenter hat alle definierten Policys im Griff. So können wir mühelos branchenspezifische, technische Sicherheitsrichtlinien entwickeln, implementieren und fortlaufend den Compliance-Status prüfen.

Sie möchten mehr erfahren?
Sprechen Sie gern Ihr Account Management an oder kontaktieren Sie uns über
**www.computacenter.com/de**

Computacenter

**Computacenter AG & Co. oHG**
Computacenter Park 1, 50170 Kerpen