WER, WAS, WO, WANN:

Die 4 Ws der sicheren Cloud Migration

Wenn heute in Unternehmen die anstehende digitale Transformation thematisiert wird, geht es meist um die Migration von Daten und Applikationen in die Cloud. Investitionen in Plattformen wie Amazon Web Services (AWS), Microsoft Azure etc. versprechen enorme Vorteile, denn sie ermöglichen es Organisationen, die Skalierbarkeit, Effizienz und Agilität von Geschäftsprozessen zu steigern. Cloud-Plattformen bieten Entwicklern die nötige Flexibilität, um DevOps- und Infrastructure-as-a-Code-Initiativen voranzutreiben, mit denen innovative Kundenerlebnisse gestaltet und Plattformen mit wenigen Klicks an neue Marktanforderungen angepasst werden können. Covid-19 und der damit verbundene Lockdown haben darüber hinaus verdeutlicht, wie wichtig eine hohe Agilität in Business und IT ist, um auf unerwartete Ereignisse angemessen reagieren zu können. Die Cloud ist damit zum zentralen Baustein der Widerstandsfähigkeit von Unternehmen geworden.

PRIVATE, PUBLIC, HYBRID ODER MULTI-CLOUD?

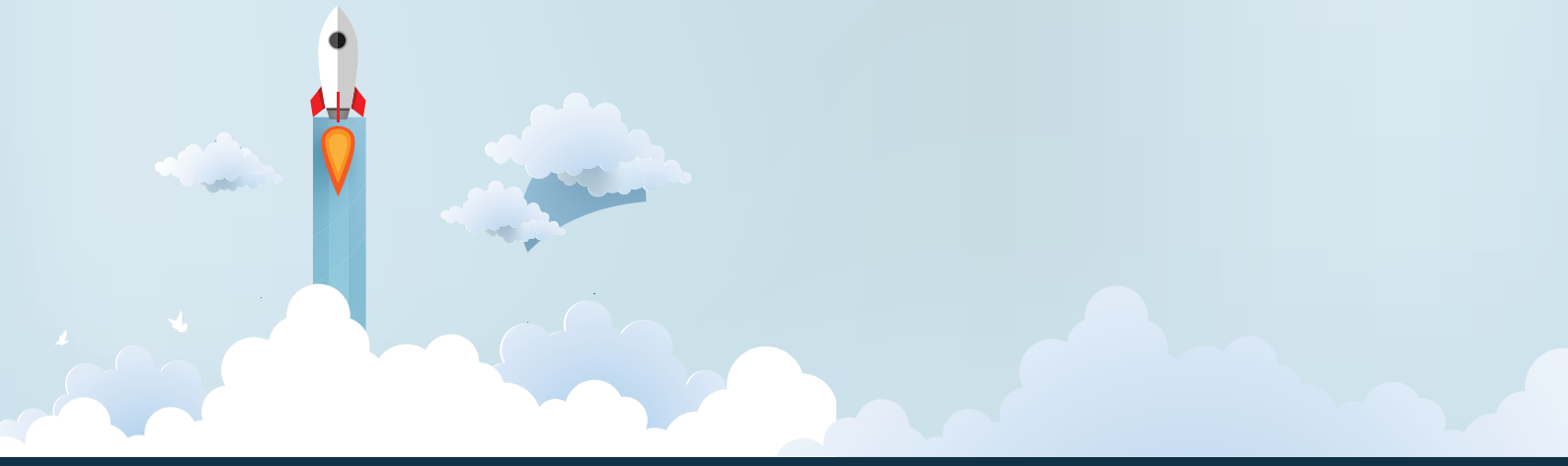
Keine zwei Clouds sind exakt identisch, auch wenn sie im Wesentlichen den gleichen Funktionsumfang bieten. Jedes Unternehmen hat unterschiedliche Anforderungen und wird daher seine eingesetzten Cloud-Technologien entsprechend anpassen. Die Basis bilden vier Arten von Cloud-Umgebungen:

Private Clouds werden für ausgewählte Benutzer über das Internet oder interne Netzwerke bereitgestellt. Die Vorteile liegen in verbesserter Skalierbarkeit und Elastizität bei vollständiger Kontrolle aller Aspekte durch das Unternehmen. Nachteil ist der Personal-, Verwaltungs- und Wartungsaufwand, der mit dem Betrieb eines herkömmlichen Rechenzentrums vergleichbar ist.

Public Clouds werden von Providern über das öffentliche Internet bereitgestellt und sind nahezu unbegrenzt skalierbar. Kunden bezahlen nur den jeweiligen Verbrauch von CPU-Zyklen, Speicher und Bandbreite. Der Provider ist für die gesamte Wartung und Verwaltung verantwortlich.

Hybrid Clouds kombinieren Private und Public Clouds, indem sie die Freigabe von Daten und Anwendungen zwischen den beiden Umgebungen ermöglichen. Unternehmen erhalten die Skalierbarkeit der Public Cloud, während unternehmenskritische Anwendungen und Daten lokal kontrolliert werden.

Multi-Clouds kombinieren mehrere Public Clouds verschiedener Provider und Private Clouds. Unternehmen können damit unterschiedlichste Anforderungen kostengünstig und flexibel abdecken, die Abhängigkeit von einem einzigen Provider vermeiden und die Betriebssicherheit durch Redundanzen steigern.



TREND ZU HYBRID UND MULTI-CLOUDS

Aufgrund der oben genannten Vorteile gehen führende Marktanalysten übereinstimmend von einer weiter steigenden Verbreitung von Hybrid- und Multi-Cloud-Umgebungen aus. So prognostiziert Gartner, dass bis zum Jahr 2021 global 75 Prozent aller mittleren und großen Unternehmen auf eine Hybrid- oder Multi-Cloud-Strategie setzen werden[1] Für Deutschland kommt eine aktuelle IDC Studie[2] aus dem Juli 2020 zu folgendem Bild:

46 Prozent
deutscher Unternehmen befinden sich bereits in einer fortgeschrittenen Phase der Cloud-Umsetzung.

27 Prozent
deutscher Unternehmen nutzen Hybrid-Clouds in produktiven Szenarien

87 Prozent
deutscher Unternehmen nutzen multiple Cloud-Ressourcen, wobei ein übergreifendes Cloud-Management nur teilweise sichtbar ist.

CLOUD COMPUTING UND COMPLIANCE

Die Entscheidung für eine Cloud-Strategie bzw. für einen Provider können Unternehmen nicht allein auf Grundlage technischer Erwägungen treffen, denn durch die DSGVO und andere Regelwerke werden Speicherung und Verarbeitung bestimmter Daten (z.B. Kundendaten und andere personenbezogene Informationen) streng reglementiert. Dabei ist zwischen der Private und der Public Cloud zu unterscheiden: Die Private Cloud steht ganz unter der Aufsicht des Unternehmens, das damit auch alleine die volle Verantwortung für die gesamte Sicherheit und Compliance tragen muss. Bei der Public Cloud wird die Verantwortung hingegen zwischen Kunde und Provider geteilt (Modell der geteilten Verantwortung). Das Unternehmen muss sich dementsprechend nur um die Sicherheit und Compliance im eigenen Aufgabenbereich kümmern, was den Aufwand stark reduziert. Dabei ist aber eine genaue Prüfung der folgenden Kriterien anzuraten:

Vertragliche Konditionen: Dem Unternehmen muss klar sein, von welchem Cloud Provider zu welchen vertraglichen Konditionen die Cloud-Services erbracht werden. Dazu gehören Person und Sitz des Cloud Providers sowie anwendbares Recht, Gewährleistung und Haftung, Service Levels, Einschaltung von Unterauftragnehmern und Rückmigration bei Vertragsende.

Sicherheit und Datenschutz: Wenn es speziell um die Speicherung und Verarbeitung datenschutzrelevanter Daten geht, sollte ein Cloud-Rechenzentrum innerhalb der EU gewählt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zudem einen Anforderungskatalog (Cloud Computing Compliance Controls Catalogue – kurz: C5) aufgestellt, mit dem die Sicherheit von Cloud-Diensten beurteilt werden kann.

DIE 4 WS DER SICHEREN CLOUD-MIGRATION

Wer ist verantwortlich?
Genauso individuell wie die Cloud-Umgebungen von Unternehmen sind auch Art und Ausmaß der Migration in die Cloud: Vom einfachen Lift-and-Shift bestehender Applikationen in die Cloud bis zum Refactoring (Neuentwicklung und Bereitstellung von Applikationen mit Cloud-nativen Funktionen) ist alles möglich. Sicherheit muss jedoch von Beginn an integraler Bestandteil aller Migrationsprojekte sein, denn in der neuen Cloud-Welt gilt das Prinzip der geteilten Verantwortung:

Provider-Verantwortung: Der Provider trägt die Verantwortung für die Sicherheit der Cloud, also den Schutz von Hardware, Software, Netzwerk und Einrichtungen, auf denen der Cloud-Service ausgeführt wird. Ob diese Verantwortung wahrgenommen wird, ist an Compliance-Attestierungen zu erkennen, wie zum Beispiel PCI-DSS, SOC1 oder ISO27001.

Kundenverantwortung: Unternehmen tragen die Verantwortung für die Sicherheit in der Cloud, also für Schutz und Aktualisierung von Gastbetriebssystemen, Applikationen und Daten, die in der Cloud liegen.

Obwohl dieses Modell recht eindeutig ist, kommt es doch immer wieder zu Missverständnissen: Interne Sicherheitsteams erwarten vom Provider die Bereitstellung von Kontrollmechanismen und das Monitoring bestimmter Aspekte, die aber in die Verantwortung des Unternehmens fallen. Das Ergebnis sind oftmals gefährliche Fehlkonfigurationen, die Angreifern den Zugriff ermöglichen. Um der eigenen Sicherheitsverantwortung gerecht zu werden, müssen Unternehmen folgende Gruppen in die Cloud-Migration einbinden:

- **InfoSec:** Verantwortlich für die gesamte Informationssicherheit und das Risiko-Monitoring.
- **Cloud-Architekten:** Diese Position ist wichtig, damit nicht alte Prinzipien des On-Premises-Betriebs auf die Cloud übertragen werden. Ziel sollten agile Plattformen sein, die für die Automatisierung aller Prozesse inklusive der Sicherheit gebaut wurden.
- **IT/Cloud Ops:** Durch die Verlagerung in die Cloud tragen IT-Teams weniger Verantwortung für die physische Infrastruktur. Diese Teams müssen selbst eine Migration durchlaufen, um neue Fähigkeiten für den sicheren Betrieb einer hybriden Umgebung aufzubauen.

WAS MUSS GETAN WERDEN?

Bei der Entwicklung sicherer und effizienter Cloud-Infrastrukturen sollten sich Unternehmen an allgemeinen Design-Empfehlungen und spezifischen Best Practices orientieren, wie sie zum Beispiel vom AWS Well-Architected Framework und dem Azure CIS Benchmark bereitgestellt werden. Diese Frameworks ermöglichen einen ganzheitlichen Blick auf die Cloud-Umgebung und erleichtern die Identifikation und Priorisierung von Bereichen, in denen Aktionen erforderlich sind. So definiert das Well-Architected Framework folgende Prinzipien für die Sicherheit von Cloud-Umgebungen:

- **Starke Identitätsgrundlage aufbauen**
- **Nachvollziehbarkeit gewährleisten**
- **Sicherheit in allen Schichten anwenden**
- **Automation von Best Practices für Sicherheit**
- **Schutz von Daten In-Transit und At-Rest**
- **Personen von Daten fernhalten**
- **Vorbereitung auf Sicherheitsvorfälle**

WO UND WANN MUSS SICHERHEIT GEWÄHRLEISTET SEIN?

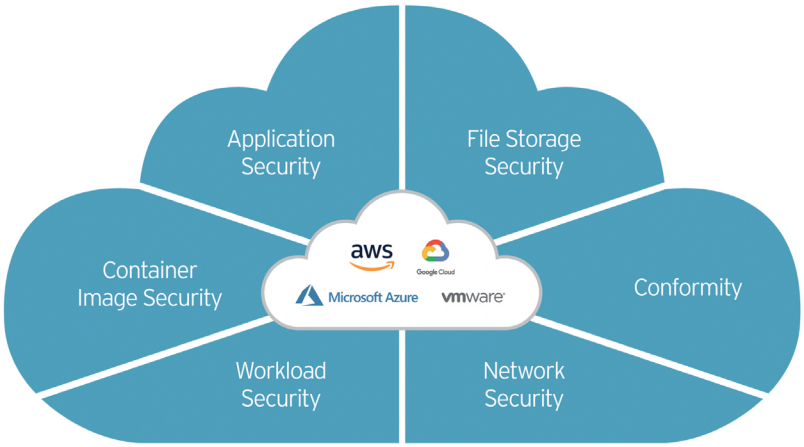
Traditionelle Sicherheitsmodelle konzentrieren sich auf Zugangskonfigurationen, die Inspektion durch Agenten und das Ziehen von Mauern, um Bedrohungen zu blockieren. Im Zuge der Umstellung auf native Cloud-Dienste funktioniert dieser Ansatz aber nicht mehr in vollem Umfang bzw. mit derselben Effizienz, denn einige Aspekte der Infrastruktur befinden sich nun außerhalb der Mauern und die Installation eines Agenten ist nicht immer möglich. Wo muss Cloud-Sicherheit angesiedelt sein und wann muss sie ansetzen?

Zunächst müssen sich Unternehmen von dem Gedanken verabschieden, dass Sicherheitsvorkehrungen an bestimmte Implementierungen gebunden sind. Das Augenmerk liegt vor allem auf der Konfiguration, den Berechtigungen und anderen Best Practices. Sicherheits-Benchmarks sind gefordert, wie AWS Well-Architected, CIS und SANS, um eine anpassungsfähige Sicherheitsrichtlinie zu erstellen, die den Anforderungen des Unternehmens gerecht wird. Dabei bietet sich die Konsolidierung von Technologien in einer Cloud-zentrierten Service-Plattform an, die es ermöglicht, Assets unabhängig von deren Art und Einsatz zu schützen. So kann im Idealfall die Sicherheit bereits fest in die Entwicklungspipeline integriert und der Schutz von serverlosen Funktionen und Containern gewährleistet werden.

Es gilt: Wo Sicherheit implementiert wird, dort ist sie vorhanden. Das bedeutet, dass Verantwortliche für die Cloud-Migration sicherstellen müssen, dass dies der geeignete Ort ist, um die Ziele der Sicherheits-Policy zu erreichen. Sicherheit muss auf jeder einzelnen Ebene der Architektur und Umsetzung eingeplant und integriert werden. Das bedeutet zum Beispiel, dass bei einer Desaster-Recovery-Migration sichergestellt ist, dass Infrastruktur, neuer Cloud Space und unterstützende Operationen bereits geschützt sind. Bei einer Anwendungsmigration ist der Zeitpunkt der Sicherheitsimplementierung darüber hinaus entscheidend für die Kostenoptimierung: Laut dem National Institute of Standard and Technology (NIST) ist die Behebung von Sicherheitslücken in frühen Entwicklungsphasen finanziell 30 Mal günstiger als in der Produktionsphase und 10 Mal günstiger als in der Testphase.[3]

TREND MICRO CLOUD ONE: EINFACHE UND AUTOMATISIERTE CLOUD-SICHERHEIT

Unabhängige Marktanalysten wie IDC und Forrester bestätigen Trend Micro als weltweit führenden Anbieter von Hybrid Cloud Workload Security. Mit Cloud One bietet Trend Micro ein umfassendes Portfolio von Cloud-Sicherheitslösungen auf einer einzigen Plattform, die sich nahtlos in Amazon Web Services (AWS), Microsoft Azure und Google Cloud integriert:



- **Workload Security:** Laufzeitschutz in physischen, virtuellen, Cloud- und Container-Umgebungen
- **Container Image Security:** Automatisierte Erkennung von Bedrohungen und Schwachstellen in Images und Registry
- **File Storage Security:** Schutz von Cloud-Services für die Datei-/ Objektspeicherung
- **Application Security:** Schutz für serverlose Funktionen, APIs und Anwendungen
- **Network Security:** IPS-Schutz für Cloud-Netzwerkebenen
- **Cloud Conformity:** Effizientes Management des Compliance- und Sicherheitsstatus

Cloud One wurde konzipiert, um einfache, automatisierte und flexible Cloud-Sicherheit zu realisieren – unabhängig davon, wie weit Unternehmen auf ihrem Weg in die Cloud bereits vorangeschritten sind. Ohne Kompromisse bei Sicherheit oder Performance lassen sich so bestehende Applikationen in die Cloud migrieren, Cloud-native Applikationen bereitstellen und Betriebsabläufe in der Cloud effizienter gestalten. Kunden profitieren von Single-Sign-On für alle Dienste, gemeinsamer Verwaltung von Nutzern und Cloud-Diensten, zentraler Management-Konsole und einem einheitlichem Preis- und Abrechnungsmodell.

[1] Smarter With Gartner, 5 Approaches to Cloud Applications Integration, May 14, 2019
[2] IDC Studie „Cloud Computing 2020+: Die Evolution in deutschen Unternehmen geht weiter", Juli 2020
[3] NISTIR 8151, Dramatically Reducing Software Vulnerabilities

TREND MICRO
Securing Your Connected World