CLOUD SECURITY

sure[secure]

00 INHALT

01 HISTORIE

Der infrastrukturelle Wandel – von physical server zu serverless

Wie und warum vollzog sich der Wandel vom physischen Server über virtuelle Server, virtuelle Desktops, private und public Clouds, Containern zu dem Begriff serverless?

Jeder, der früher eine Web-Applikation entwickeln wollte, musste sich zunächst mit der Auswahl, dem Aufbau und der Einrichtung einer eigenen Server-Architektur befassen. Was sowohl zusätzlichen Aufwand als auch Kosten bedeutete. Eventuell sogar negativ beeinflusst durch mangelnde Expertise in diesem Bereich. Gleichzeitig bot diese Herangehensweise den Vorteil, die vollständige Kontrolle über die Systeme zu bewahren – was es im Übrigen noch immer bietet.

VIRTUELLE SERVER

Der Weg zum virtuellen Server fand seine Motivation darin, mehrere Betriebssysteme parallel auf einem Server bzw. Rechner betreiben zu können. Man spricht hier von einer Emulation von Betriebssystemen und Nutzung als Server. Dabei laufen die verschiedenen virtuellen Maschinen logisch getrennt voneinander, wobei sie alle ihre Rechenleistung aus den Ressourcen des Host-Systems beziehen. Ein Hypervisor oder ein Kernel verteilen dann die Ressourcen der Maschine an die unterschiedlichen, virtuellen Maschinen.

VORTEILE

- Nutzung mehrerer OS simultan
- Unterstützung unterschiedlicher Instruktionssätze
- Leichtere Isolation verschiedener Anwendungen
- Weniger Hardware notwendig
- Günstiger und vereinfachter Betrieb
- Einteilung der Ressourcen auf die jeweiligen VMs und virtuellen Server

NACHTEILE

- Hypervisor und Kernel, der die virtuellen Maschinen betreibt, wird benötigt
- Effizienzverlust durch Overhead pro virtuelle Maschine
- Höherer Ressourcenverbrauch durch Overhead

01 HISTORIE

VIRTUELLE DESKTOPS

Der nächste Schritt in Richtung des Cloud-Computings war die Einführung virtueller Desktops. Hierbei werden mehrere Desktops auf einem Server gehostet und Anwender können sich orts- und geräteunabhängig auf ihrem Desktop anmelden.

PUBLIC CLOUD

Danach folgte die Einführung der Public Cloud. Hier werden dem Anwender eine fixe Anzahl an Servern bzw. Rechenleistung und Speicherplatz auf Servern von einem externen Anbieter bereitgestellt. Anwender kennen nicht unbedingt den Ort, an dem sich die Ressourcen - also Server - befinden, können aber vertraglich eine Region/Land/Rechenzentrum festlegen. Die Ressourcenzuweisung erfolgt automatisch und ohne Interaktion mit dem Anbieter. Die Zuweisung der Server sowie Leistung erfolgt schnell, flexibel und dynamisch. Von einer Public Cloud spricht man dann, wenn mehrere Anwender die Services/Server eines Anbieters nutzen.

VORTEILE

- Unabhängigkeit von Systemen und Ort des Zugriffs
- Einfaches und schnelles Skalieren der Leistung
- Shared Responsibility: Je nach Modell wird ein Teil der Netzwerk- und/oder Plattformarchitektur sowie die Verantwortung dafür an den Provider übergeben
- Reduzierter Aufwand/geringe Kosten im Vergleich zu Physischen Servern

NACHTEILE

- Erhöhte Kosten im Vergleich zu Serverless (Zur Vermeidung von Bottlenecks werden eher zu viele Ressourcen gekauft)
- Weniger bis keine Kontrolle über die Plattform und das Netzwerk
- Starke Abhängigkeit zum Provider in Bezug auf:
    - Leistung
    - Bereitstellung

01 HISTORIE

CONTAINER

Container werden häufig in Cloud-Umgebungen eingesetzt, da hier eine gewisse Affinität zueinander besteht. Der Container beinhaltet einen Dienst/eine Software und alle für die Ausführung notwendigen Elemente. Das Containering ermöglicht Dienste, z.B. Anwendungen, die vom restlichen System und anderen Containern separiert betrieben werden. Mit zusätzlichen Frameworks (bspw. Containerorchestrierung mit Kubernetes) werden Skalierbarkeit und bessere Verwaltungsmöglichkeiten erreicht.

Der Unterschied zu virtuellen Servern stellt sich wie folgt dar: Auch Container, die auf einem Hostsystem mit Betriebssystem laufen, unterliegen einem Containerverwaltungs-Deamon. Falls Container einen Kernel oder Teile eines Kernels benötigen, sind diese bereits im Container enthalten. So greifen die einzelnen Container-Prozesse nicht direkt auf den Host-Kernel zu.

VORTEILE

- Container läuft unabhängig vom Host-System (lediglich abhängig von der Container Plattform, bspw. Docker)
- Softwareinstallationen können leicht reproduziert und verteilt werden
- Geringer Overhead, da nur nötige Komponenten in Container enthalten
- Portabilität, Skalierbarkeit, Separation

NACHTEILE

- Aktualität der Container muss selbst verwaltet werden
- Know-how zu Containern, Container-Plattformen und Orchestrierung zur Entwicklung, Verwaltung und Verteilung ist notwendig

01 HISTORIE

SERVERLESS COMPUTING

Der aktuellste Begriff des Cloud-Computings ist das Serverless Computing. An dieser Stelle darf kein Trugschluss gezogen werden: Serverless bedeutet nicht, dass keine Server mehr im Einsatz wären, sondern lediglich, dass man als Konsument weder Zugriff auf diese noch Einblick in diese hat.

Damit entfallen quasi jegliche Berührungspunkte mit Servern bzw. den Backend-Schichten. Bei dieser Form der Cloud-Technologie wird ein Backend-Service von einem externen Anbieter bereitgestellt und der Nutzer zahlt lediglich für die effektive Nutzung von Rechenzeit. Die physischen Server befinden sich dabei in den Händen des Providers.

VORTEILE

- Geringe Kosten - abhängig von benötigter Leistung
- Höhere und dynamischere Skalierbarkeit als Container - eventbasiert
- Entwickler kümmert sich nur um Single-Purpose-Funktionen
- Verringerte Latenz
- Kein eigenes Server-Management

NACHTEILE

- Sicherheitsrisiko, da gesamtes Backend beim Provider liegt
- Bedenken bei Seperation der Daten > Multitenancy: Programme mehrerer Cloud-Nutzer können auf einer Maschine laufen
- Keine Einsicht in Backend: testen und debuggen schwierig
- Ungeeignet für langlaufende Prozesse (Kostenfrage)
- Abhängigkeit vom Provider (Wechsel wird problematisch, wenn unterschiedliche Features angeboten werden)

02 CLOUD COMPUTING

Warum suchen immer mehr Unternehmen den Weg in die Cloud?

Unternehmen suchen aus vielfältigen Gründen den Weg in die Cloud. Für viele Unternehmen, die Unmengen an komplexen Daten verarbeiten und auswerten, bietet sich die Auslagerung unmittelbar an. Solche Unternehmen sind spezialisiert auf die Erhebung und Auswertung der Daten und kaufen in der Regel Anwendungen für diesen Zweck dazu oder entwickeln sie selbst. Um Entlastung zu schaffen, wird nicht noch eigene Hardware beschafft, sondern die Rechenleistung von einem Cloud-Provider zugekauft. Dieser Fall bietet sich für alle Unternehmen an, die Interesse daran haben, sowohl Initialkosten als auch Betriebskosten gering zu halten. Zusätzlich lassen sich abseits der Kosten weitere Aufwände einsparen.

Darunter zählen:

- Aufbau der Infrastruktur und Netzwerk
- Zeit zur Inbetriebnahme und Konfiguration der Hardware
- Aufbau bzw. Zukauf von Expertise zum Aufbau und Betrieb einer IT-Landschaft

Der allgemeine Nutzen des Cloud-Computings auf einen Blick:

- Dynamische Skalierbarkeit
  - Abhängig von der Auslastung kann dynamisch mehr oder weniger Rechenleistung gebucht werden
- Finanzielle Dynamik
  - Keine Investitionskosten in physische Hardware
  - Kein Hardwarebetrieb
  - Rechenleistung zugeschnitten auf den Bedarf
- Hohe Flexibilität
  - Verfügbarkeit sowie Nutzung von Software, Anwendungen und Services unabhängig vom Netzwerk, Standort und Gerät
- Reduzierter Aufwand
  - Backup-Planung liegt in der Verantwortung des Providers
  - Hardware-Konfiguration, -Wartung und Inbetriebnahme liegt in der Verantwortung des Providers
  - Redundanz verursacht einfache Desaster Recovery
- Erhöhte Datensicherheit

03 CLOUD MIGRATION

Was kann in die Cloud und was besser nicht?

Im Endeffekt kann nahezu alles, was lokal betrieben wird, in einer Cloud betrieben werden - von Anwendungen und Funktionen bis zu Daten. Dabei sollte dennoch immer zuerst die Frage gestellt werden: Was macht davon Sinn?

Es gibt Daten, bei denen man genau abwägen sollte. Sensible Daten, die ggf. Compliance Auflagen unterliegen, können in die Cloud ausgelagert werden, insofern der Provider die entsprechenden Auflagen dafür erfüllt. Hierzu ist es sinnvoll zusätzliche Vereinbarungen mit dem Provider zu treffen. Die Vorteile bei einer Datenauslagerung in die Cloud sind üblicherweise die Datenredundanz, der Schutz vor Datenverlust und der flexible Zugriff, wie die Bearbeitung der Daten.

Daten und Systeme, deren Auslagerung Risiken mit sich bringen, sollten nicht den Weg in die Cloud finden. Risikobehaftet sind jene, die für den Betrieb des Standortes erforderlich sind. Durch eine Unterbrechung der Verbindung zum Cloud-Provider können Systeme wie Schließanlagen, Benutzerverwaltungen – AD mit Single Sign-on etc. – oder Zeiterfassungsanlagen mit Stempelkarten ausfallen, wenn diese in der Cloud betrieben werden.

Ebenso verhält es sich mit Daten deren Kritikalität so hoch ist, dass eine kurzzeitige Verfügbarkeitsstörung signifikante Auswirkungen hätte. Diese sollten lokal vorhanden bleiben und eventuell redundant mit einem Satz dieser Daten in der Cloud sein.

03 CLOUD MIGRATION

Was sind Voraussetzungen für den Weg in die Cloud?

Unabdingbar, um sicher in die Cloud zu wechseln, ist ein solides Verständnis der grundlegenden Konzepte des Cloud-Computings, der Shared Responsibility und der Entwicklung von Anwendungen bzw. Use-Cases für Cloud-Umgebungen. Zuerst sollten die eigenen Use-Cases analysiert und auf Basis dessen ein gewünschtes Cloud- bzw. Provider-Modell bestimmt werden. Hierbei sollte immer kritisch hinterfragt werden, ob die Umsetzung und Auslagerung des Use-Cases in die Cloud zu signifikanten Vorteilen führen wird.

Dabei sollte ebenso berücksichtigt werden, ob das Design und die Entwicklung der Lösung für eine Cloudumgebung geeignet sind. Zusätzlich dazu sollten die zur Auslagerung gewünschten Use-Cases – typischerweise Anwendungen – zusätzlich abgesichert werden. Bei der Wahl des Providers ist unbedingt darauf zu achten, dass dieser seinen Teil der geteilten Verantwortung ernst nimmt. Die Sicherheitsstandards sollten hoch angesetzt werden, da die Kontrolle über den gesamten Stack dem Provider überlassen wird.

Wichtig zu beachten ist ebenfalls, dass einige Anwendungen und zu verarbeitenden Daten zuvor für die Cloud-Auslagerung freigegeben werden müssen. Sollen z.B. externe Daten in der Cloud verarbeitet werden, muss dies kommuniziert und von dem jeweiligen Dateninhaber erlaubt werden, da mit dem Cloud-Provider eine dritte Partei an der Verarbeitung beteiligt ist.

04 CLOUD SECURITY

DatenCloud oder DatenKlau – Wie sicher sind Cloud-Lösungen?

Die Sicherheit von Cloud-Lösungen ist abhängig von den Standards des Providers, dem Cloud-Modell und den eigenen Security-Aspekten. Es kann jedoch nicht von einer völligen Machtlosigkeit gesprochen werden: Maßnahmen wie die Verschlüsselung der zu verarbeitenden Daten, Security Checks und Best Practices in der Entwicklung und laufenden Anwendung sowie Identity und Accessmanagement bleiben nach wie vor Schutzmechanismen aus eigener Hand. Im Allgemeinen legen gute Cloud-Provider Wert auf Sicherheit und bringen die erforderliche Expertise zum sicheren Hardwarebetrieb mit. Aus dem einfachen Grund, dass Fehler auf Seiten des Providers massive Konsequenzen bedeuten würden und in jedem Fall alle Kunden betroffen wären.

So sichern sich Provider von Public Clouds insbesondere gegen jene Kunden ab, die versuchen Anwendungen in der Infrastruktur des Providers auszurollen, mit dem Ziel diese zu kompromittieren und Daten dritter abzugreifen. Grundsätzlich ist davon auszugehen, dass Cloud-Provider höhere Standards in Bezug auf Sicherheit, Verfügbarkeit, Datensicherung und Redundanz einhalten und mehr Expertise in diesen Gebieten mitbringen als IT-ferne Unternehmen. So kann von einer höheren Sicherheitsstufe ausgegangen werden als bei einer lokalen Datenhaltung. Es darf nicht außer Acht gelassen werden, dass man selbst nur äußerst begrenzte Möglichkeiten besitzt, eigene Sicherheitsmaßnahmen vorzunehmen.

04 CLOUD SECURITY

Ist eine Datenredundanz unproblematisch?

Auch bei diesem Thema gilt das Abwägen zwischen der Verfügbarkeit bzw. Datensicherung und den Sicherheitsaspekten. Die Auslagerung von Daten in die Cloud bringt einen entscheidenden Vorteil: Bei einem Cyberangriff auf die eigenen Server können Daten via eines Backups aus der Cloud wieder eingespielt werden (data recovery). Bei einem Cyberangriff auf den Cloud-Provider können allerdings Daten verloren gehen, solange sich dort das einzige Backup der Daten befindet. Daher ist es unerlässlich die wichtigsten Daten und deren Backups on-premise zu halten.

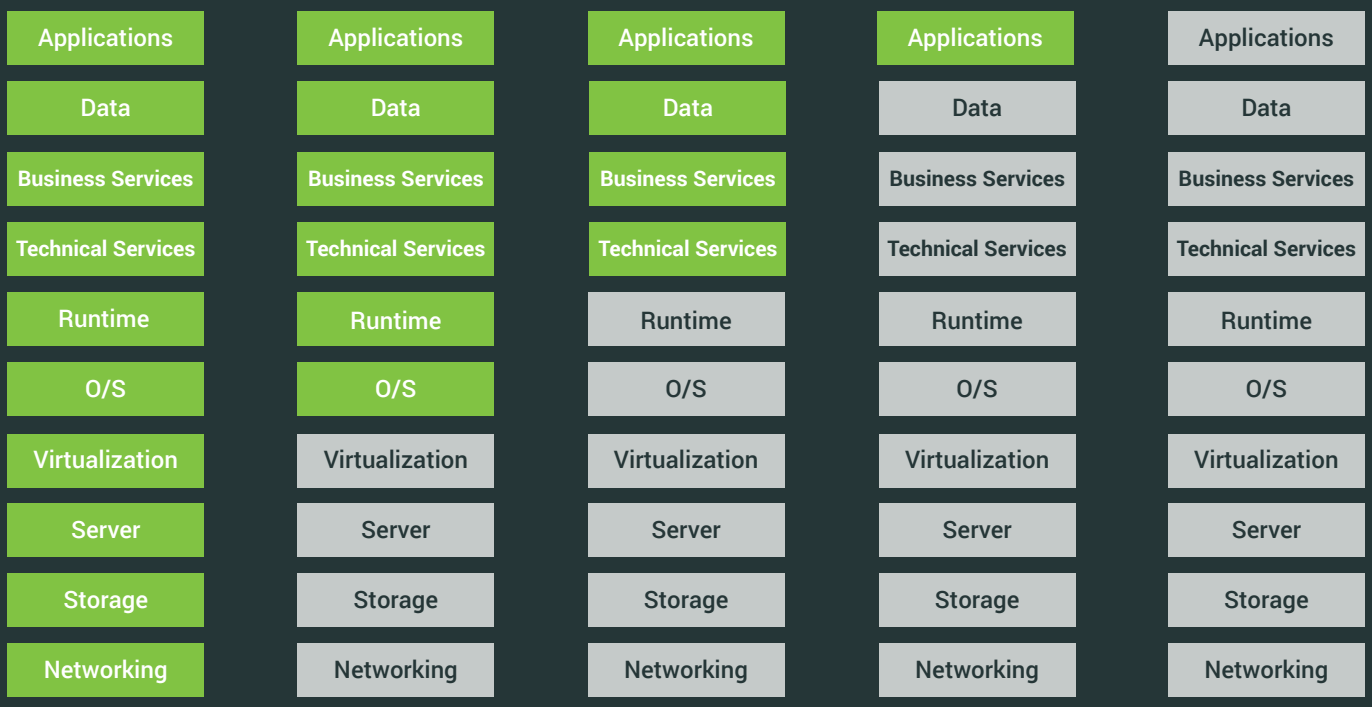
Hier sollten Ansätze der Hybrid– oder Multi-Cloud angestrebt werden. Ebenso empfiehlt es sich Backups in der Cloud eines externen Providers zu verschlüsseln, um einen Missbrauch sowie einen Verlust weniger drastisch zu gestalten. Der klassische Weg von offline Backups auf entsprechenden Datenträgern als Notfallabsicherung ist noch immer sicher. Dennoch gilt es zu beachten, dass Backups hochkritischer Daten - abhängig von Vorschriften und Gesetzen - gegebenenfalls nicht in einer Cloud gespeichert werden sollten.

Shared Responsibility – was heißt das eigentlich?

Das Security-Standards vom Provider eingehalten werden, heißt nicht zwangsläufig, dass die Daten sicher sind. Um hier die Abgrenzungen zu erkennen, muss man sich explizit mit dem Thema Shared Responsibility auseinandersetzen. Heißt: Wo greifen die Sicherheitsmechanismen des Providers und wofür ist man selbst verantwortlich?

Hierfür gibt es keine Pauschalantwort, denn diese Struktur ist immer abhängig vom gewählten Cloud-Modell. Damit ist die Sicherheit in der Regel bis zur Verfügung gestellten Ebene Sache des Providers, da User diesbezüglich keinerlei Berechtigungen besitzen. Alles was jedoch auf der infrastrukturellen- bzw. Plattform-Ebene selbst betrieben wird, liegt in eigener Verantwortung. Dennoch gilt es das Weakest-Link-Prinzip zu beachten: Selbst wenn der Provider in einem Software as a Service (SaaS) Modell jeglichen Betrieb übernimmt, ist es notwendig die Anwendungen und Daten im eigenen Netzwerk auf allen Ebenen abzusichern. Es wird deutlich, dass eine starke Abhängigkeit im Bezug zur Zuverlässigkeit des Providers vorherrscht. Daher sollten diese gewissenhaft ausgesucht werden.

05 CLOUD MODELLE



Diese Grafik veranschaulicht die abnehmende Verantwortlichkeit (von links nach rechts) des Cloud-Nutzers je nach Modell.

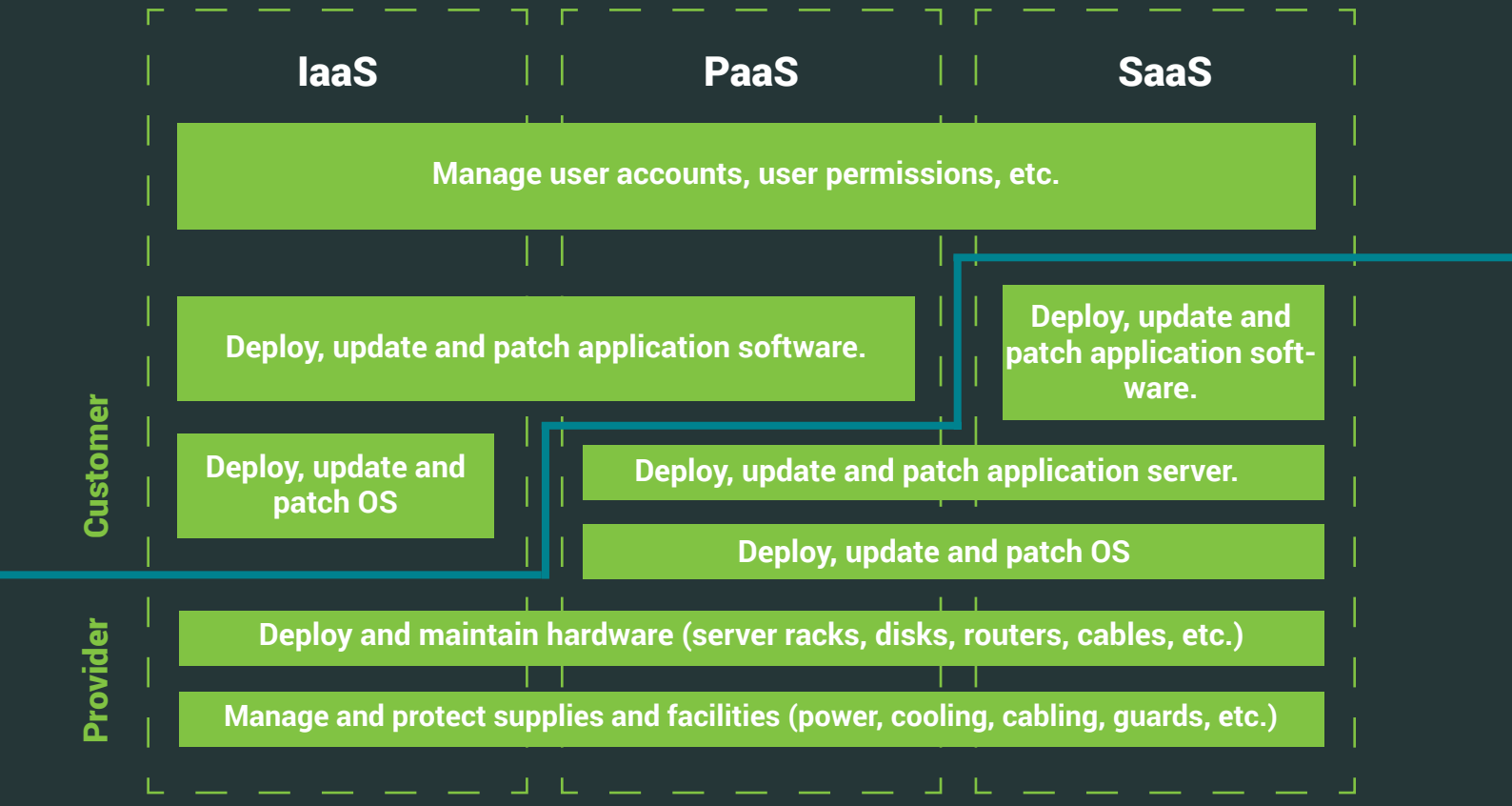
Bei einem Infrastructure as a Service (IaaS) Modell stellt der Cloud-Provider lediglich die Hardware, wie den Betrieb dieser. Unter Umständen kann hier noch das Betriebssystem inklusive sein. Bei dem Modell Platform as a Service (PaaS) stellt der Provider jeglichen Betrieb bis zur Plattformebene. In Container-Umgebungen werden typischerweise Kubernetes und Docker zur Verfügung gestellt.

Die Verantwortlichkeiten des Betriebs werden in dem Modell Software as a Service (SaaS) vollständig an den Provider übergeben.

05 CLOUD MODELLE

Zur Verdeutlichung beschreibt diese Grafik die genauen Unterschiede der Verantwortlichkeiten anhand der meistgenutzten Modelle:

- Infrastructure as a Service
- Platform as a Service
- Software as a Service



06 CLOUD PROVIDER

Wie erkennt man einen guten Cloud-Provider?

Um einen zuverlässigen und sicheren Cloud-Provider zu identifizieren, gibt es einige Ansatzpunkte, die betrachtet werden können. Zuerst lohnt es sich zu evaluieren, welcher Provider die Services zur Verfügung stellt, die in Anspruch genommen werden sollen. Dann sollte Ausschau nach Kennzahlen gehalten werden: Verfügbarkeit der Services, Anzahl an Aus- und Vorfällen und Metriken wie KPIs. Stehen diese nicht einsehbar zur Verfügung, sollte man gezielt danach fragen. Gute Provider legen Wert auf Transparenz und stellen solche Zahlen zur Verfügung. An dieser Stelle lohnt es sich ebenfalls mithilfe eines Fragenkatalogs über die Umgebung, Security-Konzepte und -Maßnahmen sowie Support und Services die direkte Kommunikation zum Provider aufzunehmen.

Neben diesen eher formlosen Indizien gibt es eine Reihe an Zertifizierungen, die Cloud-Provider erlangen können und sollten. Hier gilt es insbesondere auf verbreitete Standards wie ISO, PCI und SOC zu achten.

Zertifizierungen auf einen Blick

- **ISO 9001:** Qualitätsmanagement – Verfügbarkeit der Leistung und Latenzen
- **ISO 27001:** Sicherheit – im Einklang mit dem IT-Grundschutz
- **ISO 27017:** Cloudspezifische Kontrollen
- **ISO 27018:** Schutz personenbezogener Daten
- **PCI DSS:** Payment Card Industry – Data Security Standard – primär für Finanzbranche
- **SOC1, SOC2, SOC3:** Standards, die unter anderem Security Kriterien bewerten

07

CLOUD SOLUTIONS

Welche Sicherheitslösungen bietet die suresecure?

Zusätzlich zur klassischen IT-Security – Schutz des lokalen Netzwerks, lokaler Endpunkte, Server, Anwendungen und Datenbanken – müssen auch Cloud-Umgebungen und Anwendungen abgesichert werden. Vor dieser Aufgabe steht man unweigerlich, wenn in die Cloud migriert oder expandiert werden soll. Um diese Herausforderungen zu meistern und die Cloud-Migration durch Sicherheitsmaßnahmen nicht komplexer zu machen bieten wir folgende Lösungen unseres best-of-breed Trend Micro an:

Trend Micro Cloud One ist eine Security as a Service Lösung und schützt mit unterschiedlichen Modulen die unterschiedlichen Ebenen des Stacks von Servern und Netzwerken bis zu Anwendungen.

- **Cloud One - Workload Security** bietet Laufzeitschutz von Workloads in virtuellen, physischen, Cloud- und Container-Umgebungen.
- **Cloud One - Container Image Security** bietet die Möglichkeit Container-Images bereits während der Entwicklung auf Schwachstellen zu prüfen und so Schwachstellen in der Produktionsumgebung zu vermeiden sowie die Kosten und Zeit zur Behebung solcher Schwachstellen zu minimieren. Großer Wert wurde hier auf die reibungslose Integration in bestehende DevOps Pipelines gelegt.
- **Cloud One - File Storage Security** bietet Schutz für in der Cloud gespeicherte Daten wie Dateien und Objekte (bspw. Datenbanken).
- **Cloud One - Application Security** schützt Applikationen, APIs und Serverless Functions in der Cloud.
- **Cloud One - Network Security** bietet IPS-Schutz (Intrusion Prevention System) für Cloud-Netzwerkebenen.
- **Cloud One - Conformity** bietet eine Vielzahl automatisierter Checks für die Einhaltung von spezifischen Compliance-Standards und Best Practices zur Cloud-Sicherheit. Mithilfe derer Sicherheits- und Compliance-Status der Cloud-Infrastruktur kontinuierlich verbessert werden.

Einzellösungen:

- **Trend Micro Deep Security** ist eine lokal installierte und betriebene Lösung, die Laufzeitschutz für Workloads in Umgebungen jeglicher Art bietet.
- **Trend Micro SmartCheck** wird lokal ausgerollt und betrieben, Container-Images auf Schwachstellen zu scannen.

08 TOP 5 CLOUD TIPPS

TOP 1

Ein Grundverständnis von Cloud-Konzepten und Cloud-Computing zu besitzen. Es ist wichtig, Anwendungen und Daten genau zu betrachten und sich zu fragen, was sinnvoll und möglich ist, in die Cloud auszulagern – nicht alles kann oder muss in die Cloud.

TOP 2

Ein verlässlicher Provider, der hohen Wert auf die Sicherheit der Cloud-Umgebung und dort liegenden Daten legt und benötigte Services hoher Qualität liefert.

TOP 3

Eine Cloud-Migration und/oder Expansion in die Cloud macht klassische Security und den Schutz der lokalen Umgebung, Systeme und Daten NICHT obsolet. Beide Umgebungen, lokal wie auch in der Cloud, müssen geschützt werden.

TOP 4

Sich bewusst zu sein, welche Daten in der Cloud gespeichert werden dürfen und sollten. Hier ist es wichtig, Gesetze und Vorschriften einzuhalten. Wird die Cloud in die Backup-Strategie integriert, sollten Vorkehrungen gegen einen Datenverlust getroffen werden. Klassische Backup-Methoden und Offline-Backups sind nach wie vor notwendig und können durch die Cloudnutzung für zusätzliche Redundanz und Verfügbarkeit ergänzt werden.

TOP 5

Zur Hilfenahme eines externen Dienstleisters wie die suresecure mit fundiertem Know-how, um den Weg in die Cloud sicher zu vollziehen.

IT-Security made with  in Willich

suresecure GmbH
Hausbroicher Str. 296D
47877 Willich

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de