heise Business Services

Ein eBook von

Powered by McAfee Atos

Sichere Cloud-Nutzung

Risiken erkennen, Verantwortung übernehmen, Strategien entwickeln

- **Cloud – die unterschätzte Gefahr**
  Die größten Risiken der Cloud-Nutzung
- **Geteilte Verantwortung**
  Warum Cloud-Provider und Cloud-Nutzer zusammenarbeiten müssen
- **Auf dem Weg zur sicheren Cloud-Nutzung**
  Wie Security-Werkzeuge helfen können

McAfee & Atos
Hintergrund + Interview
Gemeinsam für mehr Sicherheit

Foto: Your_photo, BigStock

Editorial

Der Nutzen von Public Cloud-Diensten ist offensichtlich. Sie lassen sich schnell und flexibel buchen, sind nahezu unbegrenzt skalierbar und machen Investitionen in neue Hard- oder Software oft überflüssig.

Diese Attraktivität darf allerdings nicht darüber hinwegtäuschen, dass mit der zunehmenden Nutzung von Cloud-Ressourcen auch das Risiko für Sicherheitsvorfälle und Datenpannen steigt. Während sich ein Rechenzentrum mit Firewalls und Intrusion-Prevention-Systemen nach außen absichern lässt, gibt es bei der Public Cloud kein „drinnen" oder „draußen" mehr. Wenn Cloud-Server falsch konfiguriert, Accounts mit leicht zu erratenden oder kompromittierten Passwörtern geschützt und sensible Daten nicht verschlüsselt werden, haben Diebe, Spione und Saboteure leichtes Spiel.

Diese Sicherheitslücken, aber auch erfolgreiche Angriffe bleiben oft unbemerkt, weil Unternehmen längst den Überblick über ihre Cloud-Ressourcen verloren haben. Wie eine Studie des Sicherheitsspezialisten McAfee ergab, sind nur 26 Prozent in der Lage, die Konfiguration von IaaS-Umgebungen zu überprüfen, 33 Prozent konnten die Zugriffe auf Cloud-Applikationen kontrollieren, und 36 Prozent schützten sich ausreichend vor Datenverlusten.

Dieses eBook geht auf die Risiken der Cloud-Nutzung ein, stellt das 360-Grad-Modell der gemeinsamen Verantwortung von Nutzern und Cloud-Providern vor und gibt Tipps, wie sich die sichere Nutzung von Cloud-Diensten realisieren lässt.

Dr. Thomas Hafen
Freier Journalist

© 2020 Heise Medien

Alle Rechte vorbehalten. Nachdruck, digitale Verwendung jeder Art, Vervielfältigung nur mit schriftlicher Genehmigung der Redaktion.

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Haftung: Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook"** an hbs@heise.de

Inhalt

ÜBER DEN AUTOR

Dr. Thomas Hafen war über 15 Jahre als Redakteur, Moderator und Manager für verschiedene IT-Fachverlage tätig. Seine fachlichen Schwerpunkte liegen in den Bereichen Digitale Transformation, Cloud Computing und Advanced Analytics. Er lebt und arbeitet heute als freier Journalist und Moderator in München.

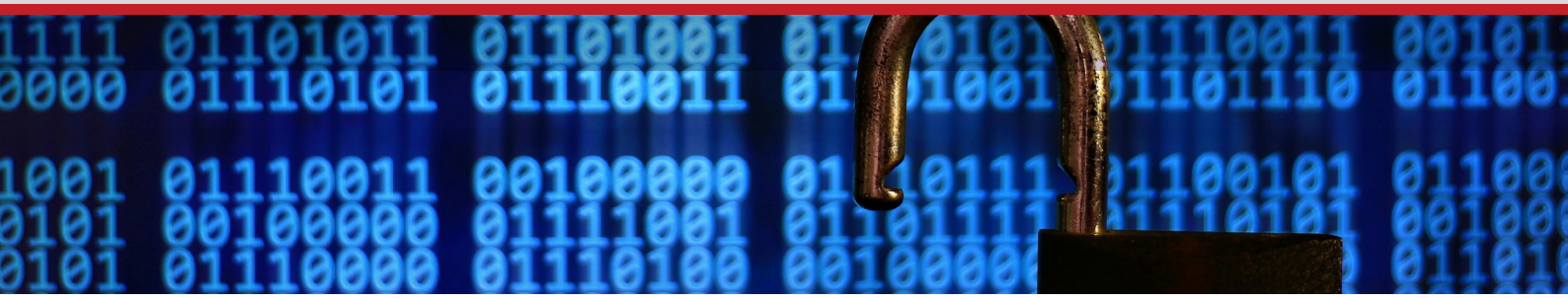


Foto: ChimS, BigStock

Kernthema Sicherheit

Cloud – die unterschätzte Gefahr

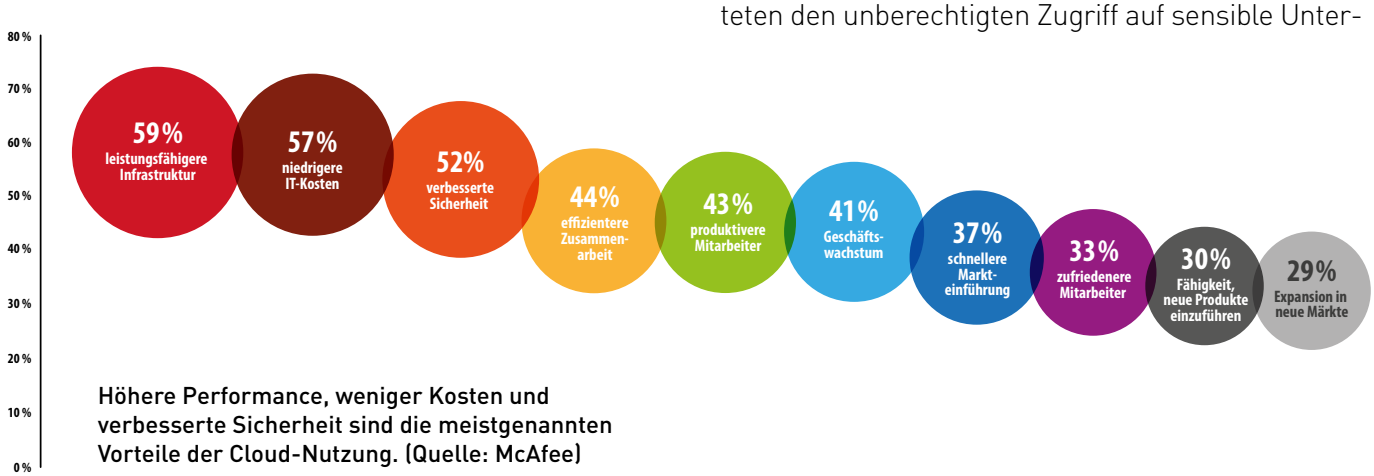
Cloud-Provider bieten in ihren Rechenzentren hervorragende technische Security-Systeme und ausgeklügelte organisatorische Sicherheitsmaßnahmen, die dazu dienen, die Ressourcen ihrer Kunden zu schützen. Unternehmen sollten sich jedoch nicht zu sehr in Sicherheit wiegen, denn Cloud-Risiken liegen oft ganz woanders.

Nach einigem Zögern ist auch die deutsche Wirtschaft in der Cloud-Welt angekommen. Laut dem Cloud Monitor 2019 von KPMG und Bitkom Research nutzen drei Viertel der deutschen Unternehmen Cloud Computing, nur noch acht Prozent lehnen Cloud-Dienste komplett ab. Diese Entwicklung kommt nicht von ungefähr. Dem „Cloud Risk & Adoption Report" von McAfee zufolge verzeichnen 87 Prozent der Firmen durch die Cloud-Nutzung Geschäftsvorteile. Zu den meistgenannten Vorzügen einer Cloud-Umgebung gehören eine höhere Performance und niedrigere Kosten der IT-Infrastruktur. Mit der allgemeinen Akzeptanz nimmt auch die Zahl derer zu, die die Cloud für sensible, geschäftskritische Daten und Anwendungen nutzen. Wie die Umfrage für den Cloud Monitor ergab, tut dies bereits ein Drittel der deutschen Unternehmen – mit deutlich steigender Tendenz.

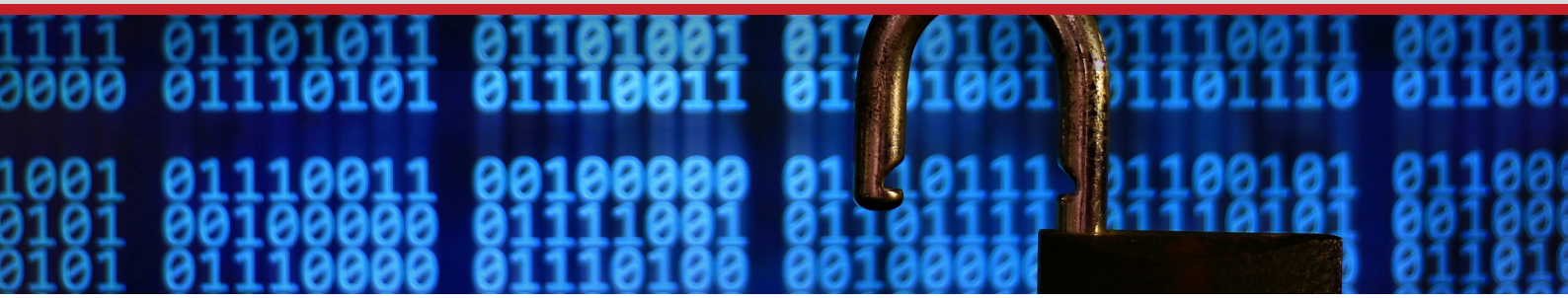
Sicherheit – ein Kernthema

Das Thema Sicherheit spielt dabei sowohl bei den Befürwortern als auch bei den Gegnern der Cloud eine große Rolle. Mehr als die Hälfte der von McAfee Befragten verzeichnete durch die Cloud-Nutzung eine Verbesserung des Sicherheitsniveaus. Bei der Umfrage zum Cloud Monitor erklärten ebenfalls über 50 Prozent, die Datensicherheit habe durch die Cloud-Nutzung zugenommen. Gleichzeitig werden aber auch die Sorgen größer: 73 Prozent der von KPMG und Bitkom Research Befragten befürchteten den unberechtigten Zugriff auf sensible Unter-

Wie Unternehmen von der Cloud profitieren



Höhere Performance, weniger Kosten und verbesserte Sicherheit sind die meistgenannten Vorteile der Cloud-Nutzung. (Quelle: McAfee)



nehmensdaten, wenn diese in einer Public Cloud gespeichert sind – ein Anstieg im Jahresvergleich um zehn Prozent.

Tatsächlich steigt mit wachsender Business-Relevanz auch das Risiko, in der Cloud Opfer von Datendiebstahl, Spionage oder Sabotage zu werden. Nur rund ein Drittel der Unternehmen ist darauf gut vorbereitet. Wie der McAfee-Report ergab, sind nur 26 Prozent in der Lage, die Konfiguration von IaaS-Umgebungen (Infrastructure-as-a-Service) zu überprüfen, nur 33 Prozent konnten die Zugriffe auf Cloud-Applikationen kontrollieren, und lediglich 36 Prozent schützten sich ausreichend vor Datenverlusten.

Millionenfacher Datenverlust in der Public Cloud

Diese Nachlässigkeit hat in den vergangenen Jahren immer wieder zu gravierenden Sicherheitsvorfällen geführt. Zu den spektakulärsten gehören die Einbrüche bei dem Kredit-Scoring-Unternehmen Equifax und der Bank Capital One, bei denen jeweils persönliche Daten wie Namen, Adressen, Konto- und Kreditkartennummern, Kredithistorien und Sozialversicherungsnummern von mehr als 100 Millionen Bürgern aus den Cloud-Repositorien der Unternehmen gestohlen wurden.

> In jeder vierten Firma laden sich Mitarbeiter sensible Cloud-Daten auf private, nicht gemanagte Endgeräte herunter.

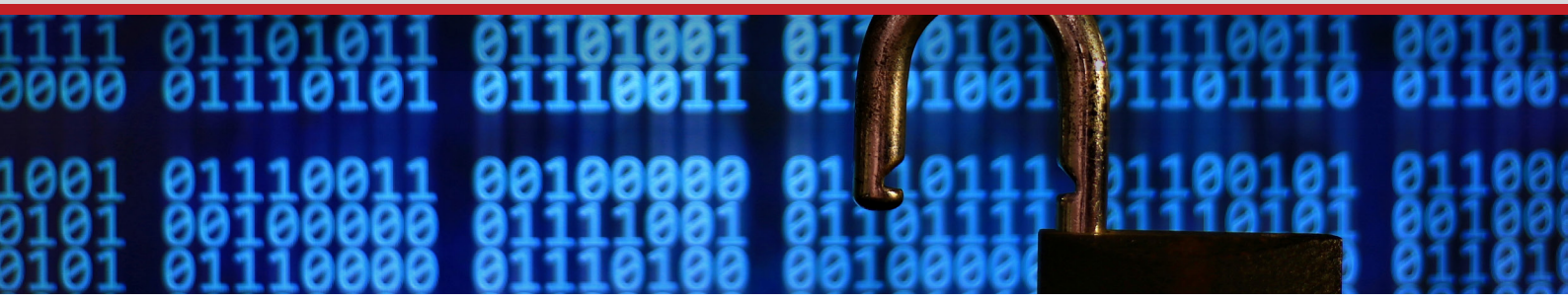
Auch wenn derart spektakuläre Einbrüche zum Glück eher selten vorkommen, sind Datenverluste aus Public Cloud-Umgebungen mittlerweile leider Alltag. Das Beratungsunternehmen Gartner schätzt, dass bis 2025 insgesamt 90 Prozent der Organisationen, die ihre Nutzung der Public Cloud nicht ausreichend kontrollieren, sensible Daten verlieren werden. In 99 Prozent der Fälle seien die Kunden selbst schuld an der Misere, so die Analysten.

Die drei größten Risiken der Cloud-Nutzung

Nur in Ausnahmefällen sind Einbrüche in Cloud-Infrastrukturen auf Sicherheitsmängel des Providers zurückzuführen. In den meisten Fällen liegen die Ursachen dagegen in den folgenden drei Bereichen:

☐ Mangelnde Sichtbarkeit

Die vielfältigen Nutzungsmöglichkeiten und die leichte Verfügbarkeit von Cloud-Ressourcen bringt es mit sich, dass Fachabteilungen häufig Services und Instanzen an der IT vorbei buchen. Es entsteht eine Schatten-IT, was die Risiken für Sicherheit und Compliance deutlich erhöht. Dem „Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk Report“ von McAfee zufolge sind in mehr als der Hälfte der Unternehmen Cloud-Services von Anbietern im Einsatz, die selbst schon einmal Opfer einer Datenpanne wurden. In jeder vierten Firma laden sich Mitarbeiter sensible Cloud-Daten auf private, nicht gemanagte Endgeräte herunter, und fast jede zehnte Datei mit sensiblen Informationen ist über einen öffentlichen Link erreichbar – mehr als doppelt so viele als noch im Jahr zuvor.



☐ Fehlkonfiguration von IaaS-Umgebungen

Angriffe auf falsch konfigurierte Cloud-Infrastrukturen, sogenannte „Cloud Native Breaches" (CNB), kommen ganz ohne Malware und Phishing aus. Stattdessen können Hacker direkt die Sicherheitslücken ausnutzen, um sich beispielsweise Administratorenrechte zu verschaffen oder auf Daten zuzugreifen. Laut dem „Cloud-Native: Infrastructure-as-a-Service Adoption and Risk Report" von McAfee bleiben 99 Prozent der Fehlkonfigurationen von Infrastrukturservices in der Public Cloud unentdeckt. Während die Sicherheitsverantwortlichen selbst im Durchschnitt 37 Fehlkonfigurationen im Monat registrieren, stellt der Sicherheitsspezialist durch die Analyse anonymisierter Nutzerdaten von mehreren Millionen Cloud-Anwendern rund 3.500 solche Vorfälle pro Monat fest.

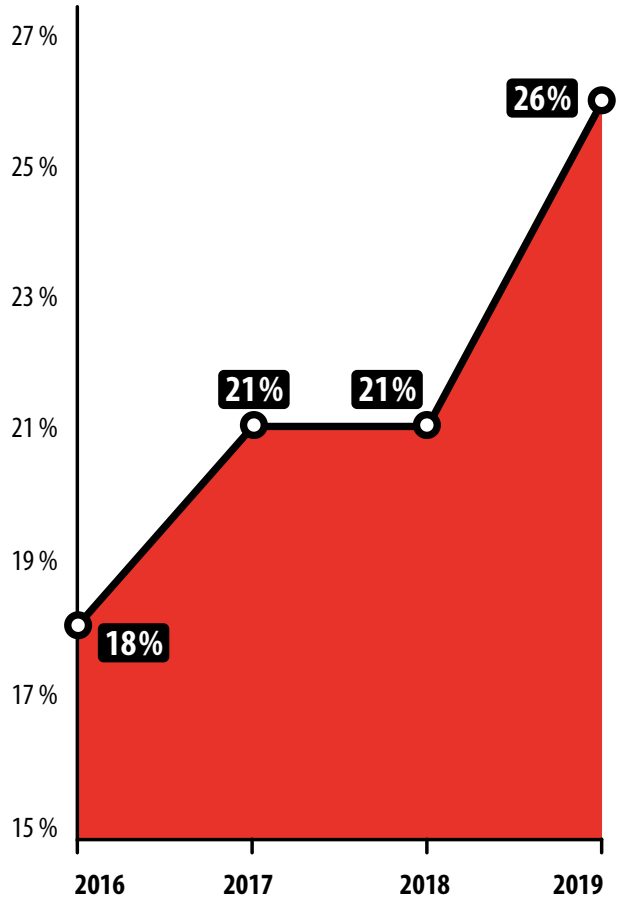
☐ Unzureichender Schutz sensibler Daten

Wie der Report „Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk" von McAfee zeigt, gehen Unternehmen nach wie vor zu sorglos mit sensiblen Daten um. In 91 Prozent der Fälle sind gespeicherte Daten (Data at Rest) nicht verschlüsselt und daher bei einem Einbruch ungeschützt. Ein Fünftel der Unternehmen hat keinen Überblick darüber, welche Daten in der Cloud gespeichert werden, und 79 Prozent erlauben den Zugang über private Smartphones oder Laptops.

Fazit

Die Einfachheit der Cloud-Nutzung hat viele Vorteile, birgt aber auch Risiken. Viele Mitarbeiter gehen nach wie vor zu sorglos mit Cloud-Diensten um, buchen Services und Infrastruktur, ohne groß über deren Absicherung nachzudenken, teilen sensible Daten über öffentliche Links oder laden sie auf ungesicherte private Endgeräte herunter. Dieses Verhalten durch technische Maßnahmen, aber auch durch Aufklärung und Schulung zu verändern ist für Unternehmen sicher eine der größten Herausforderungen des Cloud-Zeitalters. ■

Dateien mit sensiblen Daten in der Cloud



Der Anteil sensibler Daten in der Cloud hat in den vergangenen Jahren drastisch zugenommen. (Quelle: McAfee)

Foto: ogergo, BigStock

Geteilte Verantwortung

Warum Cloud-Provider und Cloud-Nutzer zusammenarbeiten müssen

Die einfache Einrichtung und der Komfort von Cloud-Services täuschen oft darüber hinweg, dass Cloud-Nutzer für die Verfügbarkeit sowie Sicherheit der Dienste und Daten mitverantwortlich sind. Je nach Art der Nutzung ergeben sich daraus unterschiedliche Grade der Verantwortung.

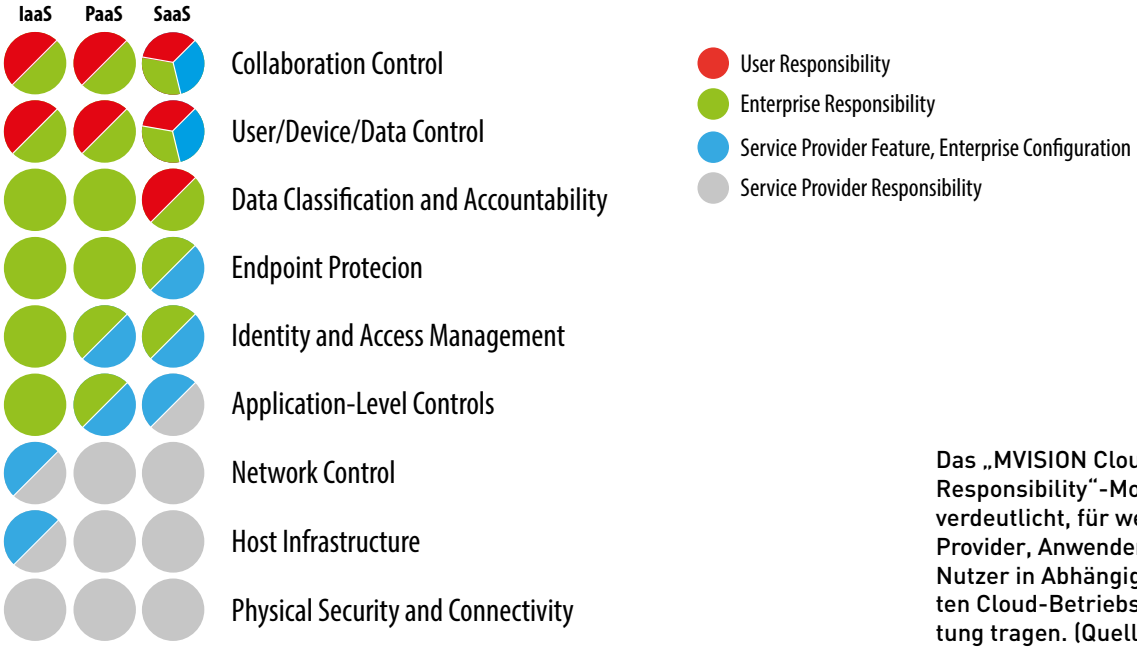
Wenn es um Sicherheit in der Cloud geht, konzentrieren sich die meisten Unternehmen auf Aspekte der Netzwerk- und Infrastruktursicherheit, der Verschlüsselung und des Datenschutzes. Sie messen Cloud-Provider daran, wie gut deren Security-Maßnahmen sind und ob sie internationale und nationale Standards wie ISO/IEC 27001, die Cloud Controls Matrix der Cloud Security Alliance (CSA) oder den Cloud Computing Compliance Criteria Catalogue (C5) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) einhalten.

> Cloud-Provider werden zu Recht nicht müde zu betonen, dass Anwender in der Cloud einen Teil der Verantwortung selbst tragen.

Diese Betrachtung ist sicher richtig, und eine sorgfältige Evaluierung des Cloud-Providers im Hinblick auf Sicherheit und Datenschutz sollte auf jeden Fall vor der Nutzung eines Cloud-Angebots erfolgen. Viele Anwender vergessen jedoch, dass es mit der Auswahl eines möglichst sicheren Dienstes nicht getan ist. Cloud-Provider werden zu Recht nicht müde zu betonen, dass Anwender in der Cloud einen Teil der Verantwortung selbst tragen. Bei Amazon Web Services (AWS) heißt das Konzept „Modell der geteilten Verantwortung", Microsoft spricht bei Azure von der „Gemeinsamen Verantwortung in der Cloud", und IBM informiert die Nutzer seiner Cloud-Services über „gemeinsam genutzte Zuständigkeiten".

Diese gemeinsame Verantwortung für die Sicherheit von Cloud-Services lässt sich gut mit der Nutzung eines Mietwagens vergleichen. Auch hier gibt es eine geteilte Verantwortung: Der Vermieter muss dafür sorgen, dass sich das Fahrzeug in einem verkehrssicheren und fahrbereiten Zustand befindet. Bremsen, Reifenprofile und andere Verschleißteile müssen daher regelmäßig überprüft und bei Bedarf ersetzt oder repariert werden. Der Mieter wiederum muss sich an die Verkehrsregeln halten und sollte durch umsichtiges, der Situation angepasstes Fahren unnötige Gefahren vermeiden. Das Unfallrisiko teilen sich Mieter und Vermieter in der Regel, indem der Kunde bei einem Schaden einen Teil der Summe bis zur vereinbarten Höhe übernehmen muss.

Geteilte Verantwortung



Das „MVISION Cloud 360° Shared Responsibility"-Modell von McAfee verdeutlicht, für welche Bereiche Provider, Anwenderunternehmen und Nutzer in Abhängigkeit vom gewählten Cloud-Betriebsmodell Verantwortung tragen. (Quelle: McAfee)

Verantwortung auf mehreren Ebenen

Ganz ähnlich verhält es sich mit der Verantwortung für Cloud-Dienste. Je nach Service sind die Anteile von Provider und Kunde jedoch sehr unterschiedlich verteilt. Bei Infrastructure-as a-Service (IaaS) stellt der Provider nur Rechenleistung, Netzwerk und Speicher zur Verfügung. Er sorgt für die physikalische sowie logische Sicherheit und Verfügbarkeit der Infrastruktur. Die Absicherung von Betriebssystemen, Applikationen, Zugängen, Endgeräten und Daten liegt im Verantwortungsbereich des Kunden. Das andere Ende des Spektrums bildet Software-as-a-Service (SaaS). Hier stellt der Provider die Applikation quasi „schlüsselfertig" zur Verfügung. Der Anwender muss sich aber dennoch selbst um die Sicherheit der Accounts, der Daten und der Endgeräte kümmern.

Um die Anteile und Verantwortlichkeiten der beteiligten Parteien besser definieren und klarer abgrenzen zu können, hat der Sicherheitsspezialist McAfee das „MVISION Cloud 360° Shared Responsibility"-Modell entwickelt. Es stellt einen Handlungsleitfaden zur Verfügung, der es Unternehmen ermöglicht, seine Anteile an der Verantwortung zu verstehen, die richtigen Schlüsse zu ziehen und die richtigen Maßnahmen zu ergreifen.

> Bei IaaS liegt die Absicherung von Betriebssystemen, Applikationen, Zugängen, Endgeräten und Daten im Verantwortungsbereich des Kunden.

Die unteren Schichten: Physik, Infrastruktur und Netzwerk

Das Modell unterteilt die zu betrachtenden Verantwortlichkeiten in insgesamt neun Segmente. Die unteren drei umfassen folgende Aspekte der Cloud-Sicherheit:

1. **Physische Sicherheit:** In diesen Bereich fallen Aspekte der Gebäudesicherheit wie Zugangsschutz und Arbeitssicherheit, aber auch der Schutz vor Ausfällen durch Brände, Naturkatastrophen, Vandalismus und andere Ereignisse. Die Verantwortung für die physische Sicherheit fällt immer in den Bereich des Providers, sofern dieser auch die Infrastruktur betreibt. Reine Anbieter von Software-as-a-Service (SaaS) müssen gegenüber ihren Kunden sicherstellen, dass die von ihnen gewählte physische Infrastrukturplattform den Anforderungen entspricht.

2. **Infrastruktur:** Dieser Bereich umfasst Computerhardware und Speicher, aber auch Plattformdienste und Betriebssysteme. Maßnahmen wie Skalierung, Load Balancing und Patching müssen dafür sorgen, dass die Infrastruktur gegen Ausfälle und Performance-Einbrüche durch Denial-of-Service-Attacken (DoS) oder Exploits geschützt ist. Der Schutz der Infrastruktur liegt primär im Verantwortungsbereich des Providers, bei IaaS-Angeboten verantwortet der Kunde allerdings sämtliche Schichten oberhalb des Hypervisors.

> Für die Sicherheit des Gebäudes, der Infrastruktur und der Netzwerke ist primär der Provider zuständig.

3. **Netzwerksicherheit:** Auch beim Thema Netzwerke ist vornehmlich der Provider gefragt. Er stellt Switches und das Gateway zur Verfügung und hat für deren sichere Konfiguration zu sorgen. Im IaaS-Modell hat der Kunde jedoch einige Freiheiten bei der Einrichtung und Segmentierung virtueller Netzwerke. Hier ist dieselbe Sorgfalt an den Tag zu legen wie bei der Konfiguration physischer Komponenten.

Segmente mit überwiegend geteilter Verantwortung

In den nächsthöheren Schichten teilen sich je nach Bereitstellungsmodell Provider und Kunde die Verantwortung zu mehr oder weniger gleichen Teilen. Dazu gehören:

4. **Applikationssicherheit:** Auf dieser Ebene ist der Schutz von Anwendungen vor Sicherheitslücken und Malware sicherzustellen. Bei SaaS-Lösungen liegt er im Verantwortungsbereich des Providers. Kunden können allerdings häufig über Sicherheitseinstellungen Einfluss nehmen und damit den Schutz stärken oder schwächen. Im IaaS-Modell teilen sich beide Seiten die Verantwortung, während beim Platform-as-a-Service (PaaS)-Betrieb das Entwickler- oder DevOps-Teams für den Applikationsschutz zuständig ist. Ein typischer Fehler auf Applikationsebene ist es, Speicherfunktionen wie Azure Blob Storage oder AWS Simple Storage Service (S3) öffentlich zugänglich zu machen. Immer wieder werden Zugangsdaten und API-Schlüssel im Software-Code gespeichert, der dann auf der Entwicklerplattform GitHub veröffentlicht wird. Forscher der North Carolina State University konnten in mehr als 100.000 GitHub-Repositories solche Daten finden.

5. **Identitäts- und Zugangsmanagement:** Das Identitäts- und Zugangsmanagement (Identity and Access Management, IAM) identifiziert Benutzer als Mitarbeiter des Unternehmens und stellt sicher, dass sie nur auf die für sie freigegebenen Ressourcen zugreifen können. Üblicherweise erfolgt die Authentifizierung über Nutzername und Passwort – ein schwacher Schutz, der leicht überwunden werden kann. Daher setzen sich immer mehr Authentifizierungsverfahren durch, die auf zwei oder mehreren Faktoren beruhen, etwa einem zusätzlichen Einmal-Passwort (One-Time-Password, OTP), das auf einem separaten Gerät oder einem Security-Token angezeigt wird. Die sichere Implementierung und Durchsetzung der IAM-Richtlinien liegen immer in der Verantwortung des Anwenderunternehmens. Ob und welche Mechanismen zur Mehrfaktoren-Authentifizierung der Provider zur Verfügung stellt, sollte bei der Wahl eines Anbieters aber durchaus eine Rolle spielen.

Wo Unternehmen und Anwender in die Pflicht genommen werden

In den folgenden Bereichen liegt die Verantwortung ganz oder zumindest überwiegend beim Anwenderunternehmen, aber auch beim einzelnen Benutzer:

6. **Endgerätesicherheit:** Mit Malware verseuchte Endgeräte können Cyber-Kriminellen als Einfallstor in die Cloud-Infrastruktur dienen. Wenn sich der Anwender mit einem solchen Client an der Cloud anmeldet und zum Beispiel ein Erpressungstrojaner hochgeladen wird, kann der Schaden erheblich sein. Aber selbst wenn gar kein Zugang zur Cloud besteht, kann ein kompromittiertes Endgerät die Cloud-Sicherheit gefährden, etwa wenn die darauf befindlichen Cloud-Zugangsdaten gestohlen werden. Um diese Gefahren zu verringern, müssen Unternehmen deshalb für einen umfassenden Schutz der Endgeräte durch Sicherheitssoftware sorgen.

7. **Klassifizierung und Schutz von Daten:** Sensible Daten wie Geschäftsgeheimnisse oder persönliche Informationen sind besonders zu schützen. Welche Daten dies sind, kann nur auf Unternehmens- beziehungsweise Fachbereichsebene entschieden werden.

8. **Benutzer-, Geräte- und Datenverwaltung:** Hierbei geht es nicht so sehr um den Schutz vor Angriffen, sondern um den Umgang mit sensiblen Daten. Es ist zu klären, welche Daten überhaupt in eine Cloud hochgeladen werden dürfen und wer welche Daten aus der Cloud auf welche Endgeräte herunterladen darf. Beim Upload sind Dateien automatisiert auf Malware zu prüfen.

9. **Kontrolle der Zusammenarbeit:** Cloud-Dienste können die Zusammenarbeit enorm erleichtern, weil sie komfortable Möglichkeiten für den Austausch und die gemeinsame Bearbeitung von Dateien zur Verfügung stellen. Diese Einfachheit birgt jedoch auch die Gefahr, dass sensible Daten unabsichtlich geteilt werden. Für die Einhaltung der Regeln trägt letztendlich der Benutzer die Verantwortung. Unternehmen müssen ihre Mitarbeiter daher schulen, damit diese die Risiken verstehen und unsichere Aktivitäten vermeiden.

Fazit: Cloud-Sicherheit lässt sich nicht delegieren

Eine sichere Cloud-Nutzung kann nur funktionieren, wenn Anbieter und Anwender ihren Anteil an der gemeinsamen Verantwortung erfüllen. Je nach Bereitstellungsmodell, Providern und Anwendungsszenario sind die Aufgaben jedoch unterschiedlich verteilt. Unternehmen müssen daher das Modell der „Shared Responsibility" verstehen, alle genutzten Cloud-Ressourcen evaluieren, geeignete Richtlinien für unterschiedliche Bereichen definieren und natürlich dafür sorgen, dass diese auch durchgesetzt werden. Für diese umfangreiche Aufgabe ist es ratsam, sich Unterstützung von einem Trusted Security Advisor wie Atos und McAfee zu holen. ■

Foto: Putilov Denis, BigStock

Cloud Access Security Broker

Auf dem Weg zur sicheren Cloud-Nutzung

Diese Maßnahmen helfen Unternehmen, Cloud-Dienste sicher zu nutzen und Risiken zu minimieren.

Die Art und Weise, wie Unternehmen Cloud-Dienste nutzen, hat sich in den vergangenen Jahren – zum Glück – drastisch verändert. Während in der frühen Phase rund 80 Prozent der Cloud-Anwendungen von Nutzern an der IT-Abteilung vorbei gebucht wurden, sind es heute nur noch rund zehn Prozent. Dies ergab eine Auswertung aggregierter und anonymisierter Cloud-Nutzungsdaten durch den Sicherheitsspezialisten McAfee. 65 Prozent der sensiblen Daten in der Cloud befinden sich demnach in Kollaborations- und Geschäftsanwendungen wie Office 365, Box und Salesforce, 25 Prozent werden in IaaS-Ressourcen (Infrastructure-as-a-Service) auf AWS, Microsoft Azure und Google gespeichert.

In derselben Zeit hat sich allerdings auch die Zahl der genutzten Ressourcen, Applikationen und Services drastisch erhöht. Allein die Zahl offiziell genehmigter Cloud-Services stieg 2019 laut McAfee im Jahresvergleich um ein Drittel.

> Unsichere Cloud-Services sollten in einem Unternehmen automatisch blockiert werden.

In drei Schritten zur sicheren Cloud

Um Cloud-Dienste sicher nutzen zu können und die Risiken zu minimieren, sind daher folgende Schritte notwendig:

1. Transparenz schaffen

Zunächst einmal gilt es, alle im Unternehmen genutzten Cloud-Dienste zu identifizieren und den Fluss von Informationen in die Cloud und aus der „Wolke“ heraus zu verstehen.

2. Policies für die Cloud-Nutzung formulieren und durchsetzen

Als Nächstes sollten Unternehmen festlegen, welche Cloud-Dienste genutzt werden dürfen und welche nicht. Unsichere Services sollten automatisch blockiert werden. Genehmigte und offiziell unterstützte Cloud-Dienste werden als „Sanctioned Cloud“ zur Verfügung gestellt. Auch für diese Dienste müssen Policies definiert werden, die etwa für bestimmte Anwendungen eine Zwei-Faktor-Authentifizierung zwingend vorschreiben.

3. Risikominimierung betreiben

Unternehmen sollten sich vorab überlegen, wie sie auf versuchte oder erfolgreiche Angriffe reagieren, und Maßnahmen festlegen, die einen Datenabfluss verhindern oder zumindest eingrenzen.

Warum Unternehmen Cloud Access Security Broker einsetzen sollten

Für die Umsetzung der drei Maßnahmen von Seite 12 empfiehlt sich der Einsatz eines Cloud Access Security Brokers (CASB). Wie der Name schon andeutet, vermittelt eine solche Lösung zwischen dem Unternehmensnetz und den genutzten Cloud-Services. Sie schafft die notwendige Übersicht über alle Cloud-Instanzen und -Dienste, ermöglicht es, Bedrohungen zu erkennen und zu bekämpfen, unterstützt bei der Einhaltung von Compliance-Richtlinien und schützt Daten vor unautorisiertem Zugriff von außen.

Bereits vor fünf Jahren prognostizierte das Marktforschungsunternehmen Gartner dem CASB-Markt eine enorme Wachstumsrate. Während 2015 weniger als fünf Prozent der Großunternehmen eine CASB-Lösung einsetzten, werden es laut Gartner bis Ende dieses Jahres 85 Prozent sein.

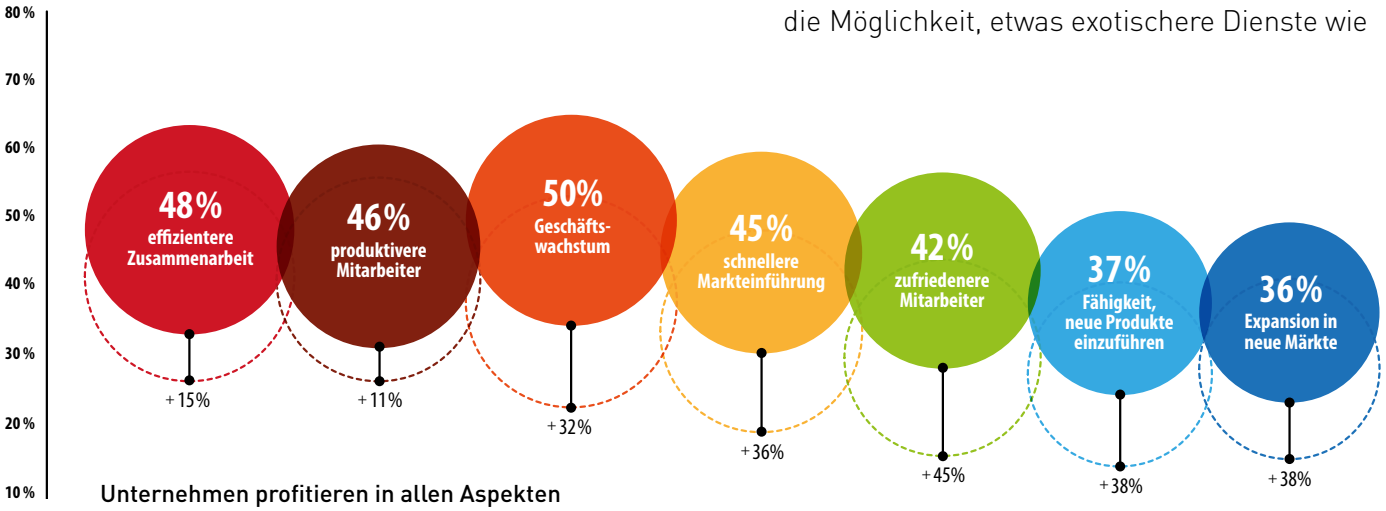
Wie der McAfee-Report zeigt, profitieren Unternehmen in allen Bereichen der Cloud-Nutzung vom CASB-Einsatz. Besonders signifikant stieg die Mitarbeiterzufriedenheit mit den Cloud-Services (+45 Prozent), aber auch die Fähigkeit, neue Produkte zu launchen (+38 Prozent), in neue Märkte zu expandieren (+38 Prozent) und Produkte schneller an den Markt zu bringen (36 Prozent), legte nach Einführung einer CASB-Lösung deutlich zu.

Auswahlkriterien für eine CASB-Lösung

Bei der Entscheidung für einen Cloud Access Security Broker sollten sich Unternehmen an folgenden Aspekten orientieren:

1. **Sichtbarkeit:** Der Nutzen eines Cloud Access Security Brokers steht und fällt mit dessen Fähigkeit, sämtliche verwendeten Cloud-Dienste sichtbar zu machen. Dies sollte neben den sanktionierten und per Schnittstelle (API) kontrollierbaren Services auch unautorisierte Cloud-Dienste umfassen. Die Plattform CASB Connect von McAfee bietet darüber hinaus auch die Möglichkeit, etwas exotischere Dienste wie

CASB – das sind die Vorteile



Unternehmen profitieren in allen Aspekten der Cloud-Nutzung vom Einsatz einer CASB-Lösung. (Quelle: McAfee)

GitHub oder Workplace von Facebook einzubinden, die nur über eine limitierte API verfügen. Über einen Reverse Proxy können auch solche Dienste kontrolliert werden. Natürlich sollte auch die native Cloud-zu-Cloud-Kommunikation vom CASB erfasst werden. Verbindet sich beispielsweise ein Anwender mit seinem privaten Smartphone mit einem der Cloud-Dienste, sollte dieser Verkehr entweder über einen Reverse Proxy umgeleitet oder nativ über die entsprechende API geschützt werden.

2. **Offenlegung und Diebstahl sensibler Daten verhindern:** CASB-Plattformen sollten Unternehmen zuverlässig davor schützen, dass Geschäftsgeheimnisse oder personenbezogene Daten in Cloud-Collaboration-, File-Sharing- oder Storage-Diensten gespeichert werden.

3. **Protokollierung:** Eine CASB-Lösung sollte sämtliche Nutzeraktivitäten protokollieren, um bei Sicherheitsvorfällen eine forensische Analyse zu ermöglichen.

4. **Umfassender Schutz:** Kompromittierte Accounts, Insider-Bedrohungen, Missbrauch privilegierter Zugänge und Malware-Infektionen stellen die größten Bedrohungen für eine cloud-basierte Unternehmensinfrastruktur dar. Ein Cloud Access Security Broker wie McAfee MVISION Cloud erkennt diese Sicherheitsprobleme zuverlässig über alle Cloud-Dienste hinweg und kann so das Risiko von Sicherheitsvorfällen drastisch reduzieren.

5. **Einfache Integration:** Ein CASB sollte schnell und ohne aufwendige Programmierarbeiten in eine IT-Umgebung integriert werden können und sich problemlos mit APIs oder Proxies von Drittanbietern verbinden lassen.

6. **Datenschutz:** Da sensible Daten durch den CASB verarbeitet werden, ist auf deren Schutz und die Einhaltung rechtlicher Regularien wie der Datenschutz-Grundverordnung (DSGVO) zu achten. Auf der sicheren Seite sind Unternehmen, wenn die CASB-Infrastruktur im europäischen Rechtsraum betrieben wird und die Daten den Hoheitsbereich der europäischen Rechtsprechung gar nicht verlassen. Im Cloud Access Security Broker sollten außerdem keine Daten gespeichert werden, um Datenschutzrisiken zu vermeiden. Log-Informationen sollten sich auf Wunsch anonymisieren lassen.

7. **Schnelligkeit:** Viele CASB-Lösungen benötigen für die Erkennung von Problemen mehrere Minuten, bevor sie aktiv werden. In dieser zeitlichen Lücke können sensible Daten aber bereits vervielfältigt oder weitergeleitet worden sein. Ein Cloud Access Security Broker sollte deshalb idealerweise Mechanismen zur Verfügung stellen, die Datentransfers in Echtzeit verhindern, wenn diese von den Unternehmensrichtlinien nicht gedeckt sind.

8. **Unterstützung von SD WAN:** Unternehmen verwenden zunehmend Software-definierte Weitverkehrsnetze (SD WAN), um ihre teure MPLS-Infrastruktur (Multi-Protocol Label Switching) zu ersetzen oder zu ergänzen. Ein CASB sollte sich daher nahtlos und transparent in SD-WAN-Umgebungen integrieren lassen.

Fazit: Cloud-Sicherheit allein genügt nicht

Mit Cloud Access Security Broker erhalten Unternehmen eine umfassende Sicht auf ihre Cloud-Umgebungen und können diese zuverlässig schützen. Endgeräte und lokale Netzwerke werden jedoch meist weiterhin durch traditionelle Security-Maßnahmen abgesichert. Dadurch entstehen zusätzliche Komplexität und ein administrativer Mehraufwand. Die Gefahr von Sicherheitslücken, Einbrüchen und Datenexfiltration steigt, wenn Erkenntnisse und Richtlinien aus beiden Welten nicht geteilt werden. Unternehmen sollten daher auf die Dienste eines Managed-Services-Providers wie Atos setzen. Diese Dienstleister verfügen über das Know-how, das erforderlich ist, um komplexe Umgebungen evaluieren, Schutzkonzepte entwerfen und diese umsetzen zu können. Mit ihrer Hilfe und Lösungen wie MVISION Cloud von McAfee ist ein umfassender Schutz realisierbar, der es erlaubt, einheitliche Richtlinien umzusetzen und diese automatisiert an den Proxy zu übergeben. So lassen sich Risiken über die gesamte Unternehmensinfrastruktur hinweg minimieren, ohne die Geschwindigkeit und Agilität auszubremsen, die die Cloud bietet. ■

Foto: VectorHot, BigStock

McAfee und Atos: Gemeinsam für mehr Sicherheit im Cloud-First-Zeitalter

Neben Innovationsbestrebungen brachte auch die globale Corona-Pandemie weitreichende Veränderungen in unseren Arbeitsalltag und beschleunigte den Transformationsprozess vieler Unternehmen. Laut des neuen Cloud Adoption & Risk Report – Work From Home-Edition von McAfee stieg die Cloud-Nutzung weltweit um 50 Prozent. Zusammen mit dem langjährigen Partner Atos arbeitet McAfee in verschiedenen Initiativen an einem höheren Sicherheitsniveau in der Cloud und der Minimierung des Risikos, Opfer von Cyber-Kriminalität zu werden.

Zahlreiche Unternehmen mussten ihre Arbeit durch die Corona-Pandemie ins Homeoffice verlagern. Für Arbeitnehmer bedeutete dies, sich einer neuen, digitalen Arbeitsumgebung anzupassen. Dazu gehört auch, dass sie mit bisher unbekannten Anwendungen konfrontiert wurden – darunter vor allem mit Cloud-Kollaborations-Tools, um die digitale Zusammenarbeit über das eigene Heimbüro hinaus zu ermöglichen. Doch gehen damit auch andere Herausforderungen im Rahmen der Nutzung von Cloud-Diensten einher. So greifen beispielweise viele Mitarbeiter auf Anwendungen zurück, mit denen sie bereits auch privat gearbeitet haben und vertraut sind. Es entsteht eine sogenannte Schatten-IT, durch die die Daten-Sicherheit erheblich gefährdet werden kann.

McAfee und Atos: Initiative für sichere und transparente Cloud-Nutzung

Mit der vermehrten Nutzung von Cloud-Services hielt nicht nur ein „neues Normal" Einzug in den Arbeitsalltag, sondern zog ebenso die Aufmerksamkeit von Cyber-Kriminellen an: So vervielfachte sich beispielsweise die Zahl cyberkrimineller Aktivitäten und auch externe Angriffe zur Datenexfiltrierung stiegen um 630 Prozent. Da viele Arbeitnehmer im Homeoffice auf ihre privaten Geräte zurückgreifen müssen, vergrößert sich das Risikopotenzial für das Unternehmensnetzwerk: Zugriffe auf Cloud-Accounts von privaten Geräten, die ausserhalb des Radars der Unternehmens-IT liegen, verdoppelte sich.

McAfee und die Atos haben es sich zur Aufgabe gemacht, das Thema Cloud-Sicherheit im achten Jahr ihrer Partnerschaft noch stärker voranzutreiben. Obwohl die Corona-Pandemie eine stärkere Nutzung der Cloud begünstigte, haben IT-Security-Spezialisten schon zuvor erkannt, dass Unternehmen auch jenseits des Krisenzustandes planen, ihr Unternehmen auf Cloud-first und Remote Working auszurichten. Schließlich ergeben sich für sie durch die Cloud-Migration zahlreiche Vorteile und Chancen: Einerseits werden dadurch Produktivität und Zufriedenheit der Mitarbeiter gefördert sowie die Effizienz und Flexibilität

von Betriebsprozessen gesteigert. Andererseits können Unternehmen agiler auf Marktentwicklungen reagieren und zeigen sich selbst offener gegenüber Innovationsansätzen. Deshalb ist es wichtig, dass der Sicherheit in der Cloud schon heute die nötige Aufmerksamkeit geschenkt wird, um auch in Zukunft nachhaltig für eine sichere Cloud-Umgebung zu sorgen.

Integrierte Lösung für mehr Sicherheit

Seit 2019 ist Atos Teil der von McAfee initiierten Security Innovation Alliance (SIA). Dieses Partnerschaftsprogramm sieht einen transparenten und kollaborativen Ansatz vor, über den sich die Partner gemeinsam dafür einsetzen, Bedrohungen schneller zu erkennen, das allgemeine Risiko zu reduzieren und somit die Einhaltung der Compliance zu gewährleisten.

Darüber hinaus ist Atos der erste Partner, der von McAfee für MVISION Cloud zertifiziert wurde und steht sowohl beratend – zum Beispiel im Rahmen eines Cloud Risk Assessments – als auch unterstützend als Managed Security Service Provider (einschließlich eines 24x7 Securtiy Operating Centers) sämtlichen Kunden zur Seite. Als Berater widmet sie sich vor allem sämtlichen Themen rund um die sichere Cloud-Nutzung. Das Cloud Risk Assessment-Programm sieht vor, Unternehmen die Nutzung der Schatten-IT (auch Shadow-IT genannt) aufzuzeigen und die Datenflüsse in der Cloud transparent zu machen.

Der Cloud Access Security Broker (CASB) McAfee MVISION Cloud bietet das Beste aus beiden Welten: Zum einen verhindert er, dass sensible Daten oder geistiges Eigentum das Unternehmen verlassen und Unternehmen einen transparenten Einblick in die genutzten Cloud-Services erhalten. Zum anderen integriert die McAfee-Lösung nahtlos auch Atos' Cyber-Sicherheitsprodukte Trustway und Evidian: So ermöglicht Trustway die Datenverschlüsselung in der Cloud und schützt somit sensible Daten. Mithilfe der Evidian-Produktreihe sind Unternehmen in der Lage, den Zugriff auf kritische Cloud-Ressourcen zu verwalten und Nutzungsprivilegien zu vergeben.

McAfee und Atos: das Rundum-Paket

Cloud-Sicherheit wird auch nach der Corona-Pandemie ein wichtiges Thema bleiben. Durch die Zusammenarbeit von McAfee und der Atos erhalten Unternehmen einerseits eine integrierte Lösung, die mehr Transparenz schafft sowie Cloud-Anwendungen und Daten direkt absichert. Andererseits stehen ihnen kompetente Partner zur Seite, die in Zusammenarbeit über Cyber-Bedrohungen aufklären und ihnen in Sachen Cloud-Sicherheit mit Rat und Tat zur Seite stehen.

Vereinbaren Sie jetzt unter bds-sales@atos.net mit dem Betreff „CRA with McAfee MVISION Cloud" einen Termin zur Durchführung eines Cloud Risk Assessments und erhalten Sie die Transparenz, die Sie zur sicheren Nutzung Ihrer Cloud benötigen.

Mehr Infos zum Thema finden Sie hier:
heise-Webinar „Haben Sie die „Visibility" über ihre Cloud-Nutzung?

www.atos.net | **www.mcafee.com**

Atos

McAfee™
Together is power.

Interview: Das perfekte Paar – Atos und McAfee

Warum ist das Thema Cloud-Sicherheit heute wichtiger denn je? Und wer ist für die Cloud-Sicherheit eigentlich zuständig?

Rolf Haas von McAfee: In den letzten Monaten mussten Arbeitnehmer weltweit aufgrund der kritischen Umstände verstärkt ins Homeoffice umziehen. Damit sind weitere Herausforderungen verbunden, mit denen Unternehmen zu kämpfen haben, denn mit der weltweit verstärkten Cloud-Nutzung sind auch die Angriffe durch Cyber-Kriminelle gestiegen. So steig beispielsweise die Anzahl externer Attacken auf Cloud-Dienste – mit dem Ziel der Datenexfiltration – um 630 Prozent.

Im Langzeit-Homeoffice werden Mitarbeiter oftmals mit einer technischen Situation konfrontiert, die sich von den Möglichkeiten an ihrem bisherigen Arbeitsplatz unterscheiden können. Dann kann es vorkommen, dass sie auf Cloud-Tools aus dem privaten Umfeld zurückgreifen und somit die Etablierung der sogenannten Schatten-IT begünstigen: Die Verwendung von privaten oder unautorisierten Geräten und Diensten, die unter dem Radar der IT-Abteilung fliegen und sich folglich auch außerhalb des Wirkungsbereichs der IT-Sicherheit des Unternehmens befinden. Atos und McAfee sind sich dieser Herausforderung bewusst und möchten über die „Reach the Cloud"-Initiative Unternehmen für das Thema Cloud-Sicherheit umfassend sensibilisieren sowie über Schwachstellen und Gefahrenpotenziale aufklären.

Erwan Smits von Atos: Zum Thema, wer für die Sicherheit in der Cloud verantwortlich ist: Wenn sich Unternehmen für eine Migration in die Cloud entscheiden, gehen viele von ihnen automatisch davon aus, dass der Cloud-Provider sämtliche Sicherheitsvorkehrungen trifft und notwendige Schutzmaßnahmen vorsieht. Dem ist jedoch nicht so. Nehmen wir zur Veranschaulichung die Fahrzeug-Sicherheit: Der Fahrzeughersteller ist dafür verantwortlich, dass der PKW sicher konstruiert und gebaut wird - im Falle von Sicherheitsgurten besteht seit den 70er Jahren sogar eine Einbaupflicht. Der Hersteller muss also dafür sorgen, dass der Sicherheitsgurt wie vorgeschrieben eingebaut wird. Es liegt jedoch in der Verantwortung des Fahrers (bzw. sämtlicher Insassen), diese anzulegen und gemäß der StVO sicher und besonnen zu fahren – darauf hat der Hersteller keinen Einfluss.

Ähnlich verhält es sich auch mit der Cloud-Sicherheit: Der Cloud-Provider ist in der Regel für den Schutz der gesamten Netzwerk- und Hosting-Infrastruktur zuständig. Der Kunde – also das Unternehmen, das das Angebot des Providers bezieht – hat dafür Sorge zu tragen, das ein funktionierendes Identity und Access Management implementiert wird, um so Nutzungsprivilegien zu verteilen. Außerdem ist das Unternehmen dafür verantwortlich, dass sämtliche Endgeräte ausreichend abgesichert sind, mit denen sich Mitarbeiter im Büro oder im Homeoffice an das Netzwerk anschließen. Den Endanwendern – sprich: sämtliche Mitarbeiter im Unternehmen – obliegt es, sich verantwortungsbewusst im Netzwerk zu bewegen, Daten nicht einfach an Dritte weiterzugeben oder potenziell schädliche E-Mail-Anhänge zu öffnen. Wenn es um Cloud-Sicherheit geht, müssen alle Parteien an einem Strang ziehen und ihren Beitrag leisten.

Atos ist nun seit vielen Jahren Partner von McAfee. Welche Funktion übernimmt sie im Rahmen dieser der Partnerschaft hinsichtlich Cloud-Sicherheit?

Erwan Smits von Atos: Als Managed Security Provider stehen wir Unternehmen zum einen beratend zur Seite. Zum anderen übernehmen wir die Implementierung sowie den Betrieb der Cloud-Sicherheit.

Wir empfehlen im ersten Schritt ein Cloud Risk Assessment durchzuführen, das für mehr Transparenz sorgt – vor allem im Hinblick auf das Thema Schatten-IT im eigenen Unternehmen. Den Betrieben wird hierbei unter anderem Folgendes aufgezeigt: Welche Systeme, Anwendungen und Dienste sind im Einsatz? Werden Cloud-Services verwendet, die nicht sicher sind? Wo fließen eigentlich die Unternehmensdaten hin?

Im zweiten Schritt werden Policies eingeführt, die verhindern, dass sensible und unternehmenskritische Daten ungewollt das Unternehmen verlassen. Dies beinhaltet auch die vollständige, dauerhafte Implementierung einer integrierten Sicherheitslösung. Über ein 24/7 Security Operating Center stehen wir den Kunden im Anschluss jederzeit zur Verfügung, um direkt auf Sicherheitsereignisse reagieren zu können.

Wie sieht diese integrierte Sicherheitslösung aus?

Rolf Haas von McAfee: Oft bleibt die nötige Überprüfung von Daten, ihrer Nutzung und welche Wege sie über verschiedene Systeme nehmen aus, also: Was passiert mit den Daten, wenn sie aus der Cloud herunter- oder in die Cloud hochgeladen werden? Der Cloud Access Security Broker MVISION Cloud liefert an dieser Stelle die nötige Transparenz. Über ihn erfährt das Unternehmen, welche Anwendungen in der Cloud zum Einsatz kommen und wie sich Daten zwischen Nutzern und den entsprechenden Anwendungen bewegen und unterbindet bei Bedarf das Abfließen von Daten in Echtzeit.

Erwan Smits von Atos: Seit Oktober 2019 sind wir Teil der McAfee Security Innovation Alliance, welche die Entwicklung offener und interoperabler Sicherheitsprodukte beschleunigt. Im Rahmen dieses offenen Kooperationsansatzes lassen sich McAfee-Lösungen mit Atos-eigenen Lösungen integrieren. Das heißt, dass Anwender das Beste aus beiden Welten erhalten: Über eine einheitliche Management-Konsole haben sie Zugriff auf sämtliche Funktionen sowohl der McAfee MVISION Cloud-Lösungen als auch der Trustway- und Evidian-Sicherheitsprodukte von Atos. Trustway erlaubt die Datenverschlüsselung innerhalb der Cloud-Infrastruktur. Evidian ermöglicht ein vielfältiges Access Management, mit dem der Zugriff auf kritische Ressourcen verwaltet sowie die allgemeine Nutzung in der Cloud reglementiert werden können.

Wieso ist gerade Atos der perfekte Partner? Was macht die Zusammenarbeit mit McAfee besonders? Und worin liegt der Mehrwert für Kunden?

Rolf Haas von McAfee: Atos bietet genau das, was wir bei einem IT-Security-Partner suchen: Als einer der führenden IT-Dienstleister, dessen Kundenstamm sich aus internationalen, global agierenden Unternehmen aus den unterschiedlichsten Branchen zusammensetzt, kann Atos mit Skalierbarkeit sowie den richtigen Ressourcen und umfassendem Know-how aufwarten – und schließlich verfolgen wir das gleiche Ziel: Die Cloud zu einem sichereren Ort zu machen.

Erwan Smits von Atos: Als wir auf die Suche nach einem Technologiepartner für Cloud-Sicherheit gingen, haben wir uns selbstverständlich auch intensiv mit dem McAfee-Portfolio auseinandergesetzt und waren über die Positionierung von McAfee MVISION Cloud innerhalb des Gartner Magic Quadrant für CASB-Lösungen beeindruckt. Ein weiterer wichtiger Punkt, der uns von McAfee als Partner überzeugt hat, ist die Skalierbarkeit und einfache sowie flexible Handhabung der MVISION-Lösungen. Für Atos als Managed Service Provider ist es wichtig, dass der Betrieb der IT-Infrastruktur – vor allem in Bezug auf die Sicherheit – für den Kunden so effizient wie möglich gestaltet wird. Diese Verbindung von Fachwissen und integrierter Lösung ebnet den Weg für die reibungslose Umsetzung einer erfolgreichen Cloud-Sicherheitsstrategie.

Atos

McAfee™
Together is power.