Cloud Security mit einem Cloud Access Security Broker (CASB)

first frame networkers

IT, die Sie weiterbringt

Inhalt

Impressum

Autoren
Claude Bollag, first frame networkers ag
Reto Wagner, first frame networkers ag

Inhalt und Redaktion
first frame networkers ag
Haldenstrasse 1
CH-6340 Baar

Telefon +41 41 768 08 00
Fax +41 41 768 08 08
info@firstframe.net

1 Einleitung

Wussten Sie, dass Grossunternehmen bereits heute durchschnittlich mehr als 1000 Cloud-Dienste nutzen, von welchen über 60% von der IT weder verwaltet noch überwacht werden?[1]

Dies wirft wahrscheinlich auch bei Ihnen manche Fragen zum Thema Sicherheit auf. In diesem Dokument geben wir Ihnen einige Impulse bezüglich sicherheitstechnischer Aspekte, welche bei der parallelen Nutzung von Cloud-Diensten und -Plattformen mehrerer Cloud Provider zu berücksichtigen sind. Dabei zeigen wir Ihnen auf, wie Sie mit dem Einsatz eines Cloud Access Security Broker (CASB) Risiken minimieren und die Sicherheit Ihrer Unternehmensdaten und -identitäten erhöhen können.

1.1 Beliebtheit von Cloud-Diensten & Multi-Cloud

Die Nutzung Cloud-basierter Dienste ist heute sowohl für KMU wie auch Grossunternehmen keine Seltenheit mehr. Gesteigerte Produktivität, Kosteneffizienz, erhöhte Flexibilität und Skalierbarkeit sowie Zuverlässigkeit und Sicherheit sind nur einige der vielfältigen Gründe, weshalb moderne Unternehmen auf Cloud-Dienste setzen.

Bei der paraten Nutzung von Cloud-Diensten und -Plattformen mehrerer Cloud Provider spricht man auch von «Multi-Cloud». Diese Multi-Cloud kann, wie die Hybrid Cloud, die beiden Cloud-Modelle Private Cloud und Public Cloud integrieren. Typischerweise kommen dann verschiedene Kombinationen von Cloud-Diensten zum Einsatz. Bei den Haupttypen dieser Cloud-Dienste wird oft zwischen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) unterschieden. Hierbei sind bei der Auswahl der für Ihr Unternehmen geeigneten Cloud Provider und Cloud-Dienste sowohl funktionale wie auch nicht funktionale Anforderungen zu berücksichtigen (eingesetzte Technologien, Abhängigkeit vom Provider, Integrierbarkeit in bestehende Systemlandschaft, Bedienbarkeit, Support usw.).

1 Aus Microsoft eBook «Discover of Shadow IT with Microsoft Cloud App Security»

1.2 Datensicherheit in der Multi-Cloud

Egal für welche Cloud Provider und Cloud-Dienste Sie sich entscheiden: Trotz aller Vorteile stellt die Nutzung dieser verteilten Cloud-Dienste einen neuen Bedrohungsvektor für Unternehmen dar. Denn Anwender von Cloud-Diensten können absichtlich oder versehentlich die Daten und Identitäten Ihres Unternehmens geschäftskritisch gefährden. Sei dies durch Exfiltration von Unternehmensdaten oder Nutzung unternehmensfremder, unsicherer Cloud-Dienste.

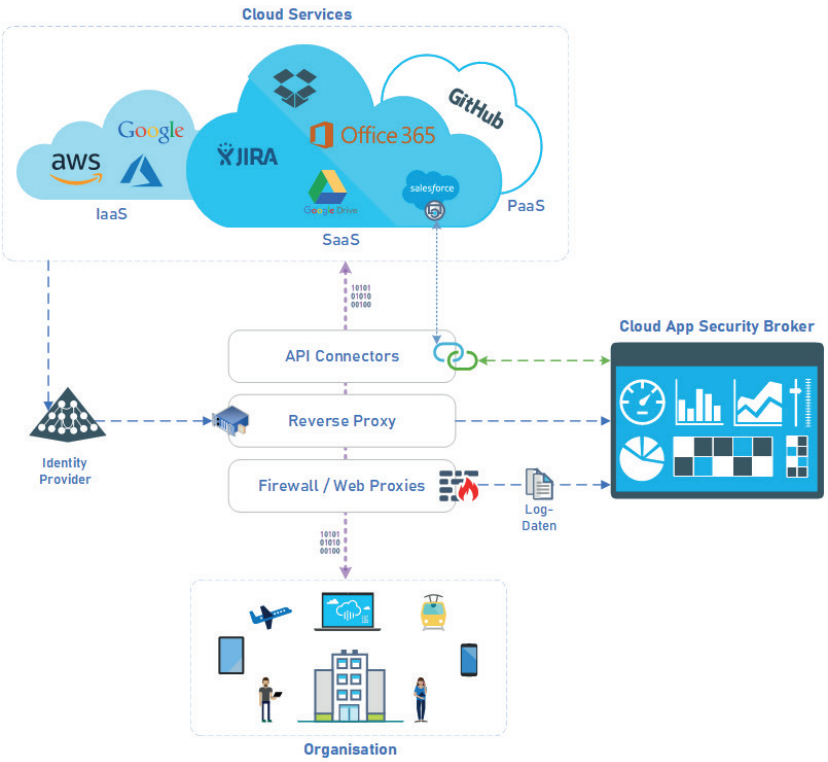
Multi-Cloud erfordert einen neuen Sicherheitsansatz. Dieser soll es Ihrem Unternehmen ermöglichen, eine die Cloud Provider übergreifende Transparenz der Datenflüsse und Zugriffe Ihrer Unternehmensdaten und -identitäten zu schaffen und, falls notwendig, geeignete risikominimierende Massnahmen zu ergreifen. Der Einsatz eines Cloud Access Security Broker (CASB) ermöglicht Ihnen genau das und unterstützt Sie somit dabei, die sicherheitstechnischen Herausforderungen der Multi-Cloud zu meistern.

2

Was ist ein Cloud Access Security Broker?

Die zentrale Aufgabe des Cloud Access Security Broker (CASB) ist der den Cloud-Anbieter und die Cloud-Anwendung übergreifende Schutz von Daten und Identitäten eines Unternehmens. CASB ist ein Dienst oder eine Software, welche den Zugriff auf Cloud-Anwendungen analysiert und steuert. Zugriffe können erlaubt oder verhindert werden. Alle Zugriffe werden protokolliert, damit eine transparente, lückenlose Dokumentation der kompletten Kommunikation und ausgeführten Aktionen entsteht. Nicht erwünschte Zugriffe lassen sich unterbinden und bei verdächtigen Aktionen werden die Administratoren alarmiert.

Bei der Implementierung kann man zwischen zwei Architekturen unterscheiden: einerseits dem Gateway-basierten und andererseits dem API-basierten Cloud Access Security Broker. Der Gateway-basierte CASB befindet sich unmittelbar zwischen der Cloud-Anwendung und den Usern. Im Fall des API-basierten CASB befindet sich die kontrollierende Instanz ausserhalb des eigentlichen Datenstroms von Anwender und Cloud-Dienst.



3

5 Tipps für mehr Sicherheit in der Multi-Cloud[2]

Da Multi-Cloud-Umgebungen eine grössere Angriffsfläche für verschiedene Bedrohungen darstellen, gestaltet sich auch die Entwicklung einer geeigneten IT-Sicherheitsstrategie deutlich komplexer. Damit potenzielle Sicherheitslücken gar nicht erst entstehen, sollte eine übergreifende Top-Down-Security-Strategie implementiert werden.

Um eine Multi-Cloud-Umgebung erfolgreich zu verwalten und sicherzustellen, sollte zunächst überprüft werden, wie Daten, Anwendungen und Workflows zwischen Cloud-Diensten und den verbundenen Geräten zusammenhängen. Daraus können die erforderlichen Massnahmen abgeleitet werden, um die Datensicherheit zu gewährleisten.

Die folgenden fünf Tipps können Unternehmen dabei unterstützen, eine Sicherheitsstrategie zu entwickeln, die potenziellen Herausforderungen von Multi-Cloud-Umgebungen gewachsen ist.

3.1 Kontrolle über alle Unternehmensdaten gewinnen

Die Fähigkeit, Einblick in jede Cloud-Instanz zu haben, ist von entscheidender Bedeutung, um ungewöhnliche Verhaltensweisen zu identifizieren und den Datenverkehr während des Betriebs im Netzwerk zu überwachen. Mit der Einführung weiterer Cloud-Dienste wird die Überwachung dieser Datenströme exponentiell schwieriger, aber auch unerlässlich.

In einer sich ständig verändernden Umgebung müssen Unternehmen darauf vertrauen können, dass sie jederzeit die Kontrolle über Geräte und Daten behalten. Richtlinien sollen angewendet und gepflegt werden können, wenn sich diese im Laufe der Zeit ändern. Wichtige Funktionen dabei sind anwendungsübergreifende Aktivitätsprotokolle, Verschlüsselung und Kontrolle über Schatten-IT.

3.2 Geeignete Identitäts- und Autorisierungskontrollen nutzen

Viele Unternehmen machen den Fehler, davon auszugehen, dass die Sicherheit bei der Ausführung ihrer Workloads in der Cloud die alleinige Sache des Cloud-Anbieters ist. Dieser ist für die Bereitstellung bestimmter Sicherheits- und Datenschutzniveaus in seinen Angeboten zuständig. Die Verantwortung für die Kontrolle, wer auf die Daten zugreifen darf, liegt aber beim Kunden.

Dies bedeutet, dass Unternehmen über geeignete Tools verfügen müssen, um sich vor Bedrohungen wie kompromittierten Anmeldeinformationen und bösartigen Insidern zu schützen. Folglich müssen sie wissen, wo sich ihre Daten befinden, wohin sie gehen und wer berechtigt ist, auf sie zuzugreifen. Mit robusten Authentifizierungsfunktionen kann ein

wichtiger Grundstein für die IT-Sicherheit gelegt werden. Erforderliche Kontrollmechanismen zur Unterstützung sind:

- Verhinderung der Datenexfiltration (nicht autorisierter Transfer von Daten) von einem genehmigten zu einem nicht genehmigten Cloud Service
- Authentifizierung von Benutzern in allen Cloud-Anwendungen
- Erkennung von Anomalien bei der Benutzeranmeldung

3.3 Datenschutz während der Übertragung der Daten

Um Datenverlust in Multi-Cloud-Umgebungen vorzubeugen, benötigen Unternehmen leistungsstarke, Cloud-basierte Tools, die die Kontrolle über den Datenzugriff ermöglichen, das Online-Verhalten der Benutzer in Echtzeit überwachen, den Zugriff von nicht verwalteten Endgeräten regeln und die Dateifreigabe steuern können.

Folgende Funktionen sollten die Sicherheitstools bieten:

- Unterscheidung zwischen persönlichen und geschäftlichen Instanzen von Cloud
- Anwendungen und entsprechende Durchsetzung verschiedener Richtlinien
- Kontextabhängige Data Loss Prevention (DLP)

3.4 Endpoint Security

Da immer mehr Mitarbeitende mit ihren privaten Geräten auf Cloud-Ressourcen im Unternehmen zugreifen, steigt das Risiko eines Verlustes sensibler Informationen exponentiell an. Um einen ausreichenden Schutz zu gewährleisten, ist es wichtig, dass ein sicherer Zugriff auf die benötigten Daten von extern ermöglicht wird. Für Unternehmen, die Bring Your Own Device (BYOD) eingeführt haben, lässt sich durch agentenlose Sicherheitslösungen mit geringem Verwaltungsaufwand ein hohes Sicherheitsniveau herstellen. Diese gewähren Schutz während des Zugriffs, nutzen Verschlüsselungstechnologien, nehmen erforderliche Geräteeinstellungen vor und ermöglichen im Fall von Verlust oder Diebstahl die Entfernung der Daten auf dem Gerät per Fernzugriff.

3.5 Interoperabilität zwischen sämtlichen Security Tools

Ein ausreichender Daten- und Bedrohungsschutz sowie Transparenz und Zugriffssicherheit über die gesamte Cloud-Umgebung gehören zu den obersten Prioritäten eines Unternehmens. Deshalb muss sichergestellt werden, dass sich die eingesetzten Cloud-Sicherheitslösungen nahtlos ineinander und mit bestehenden Tools vor Ort integrieren lassen. Eine unzusammenhängende IT-Umgebung kann zu inkonsistenter Cybersicherheit und damit zu Schwachstellen führen. Beispielsweise müssen Cloud-Sicherheitslösungen eine Erweiterung der lokalen DLP-Richtlinien auf die Cloud und die Integration mit SIEM-Tools (Security Information Management) für das Sicherheitsinformations- und Vorfallmanagement bieten.

2 Webseite BOLL Engineering AG "Tipps für Datensicherheit in der Multi-Cloud" von Bitglass

4
Fazit

Die erfolgreiche Umsetzung einer Multi-Cloud-Strategie erfordert einen ganzheitlichen Sicherheitsansatz. Die Sicherheit sensibler Informationen muss in jeder Cloud-Anwendung und auf jedem Gerät gewährleistet sein – rund um die Uhr.

Das bedeutet, dass Unternehmen ihre Daten auch jenseits ihrer klassischen Infrastruktur verwalten und schützen müssen, um langfristig ihre Wettbewerbsfähigkeit zu stärken.

Unsere Partner für Cloud Security

ENGAGE
FORTINET EXPERT PARTNER
Integrator

FortiCASB-SaaS ist ein Cloud Access Security Broker (CASB), den Sie als nativen Cloud-Dienst abonnieren können. Damit erhalten Sie die Transparenz, Compliance, Datensicherheit und Bedrohungsabwehr, die jedes Unternehmen für cloudbasierte Dienste haben sollte.

Gold
Microsoft Partner
Microsoft

Microsoft Cloud App Security ist eine Multimode-CASB-Lösung (Cloud Access Security Broker), die Ihnen umfassende Transparenz und Kontrolle bei der Datenübertragung bietet. Modernste Analysen tragen dazu bei, Cyberbedrohungen in allen Clouddiensten zu erkennen und abzuwehren.

Ihr Business fragt nach Lösungen? Damit Sie sich voll auf Ihr Kerngeschäft konzentrieren können, entlasten wir Sie wirksam in allen Belangen der IT. Dank einer auf verschiedene Kundengrössen ausgerichteten Organisation erhalten die Kunden alles, was ein modernes Unternehmen benötigt – von der Beratung über die Installation bis hin zum Betrieb. Die first frame networkers ag wurde 1997 gegründet und beschäftigt heute rund 70 Mitarbeitende. Als verlässlicher IT-Partner arbeiten wir effizient, partnerschaftlich und kalkulierbar. Hohe Qualität, faire Konditionen, eine hochstehende Ausbildung und eine gute Unternehmenskultur sind unsere zentralen Werte.

first frame networkers

IT, die Sie weiterbringt

first frame networkers ag
Haldenstrasse 1
CH-6340 Baar

www.firstframe.net
info@firstframe.net
+41 41 768 08 00