Bild: D3Damon / iStock

Dossier

Cloud Access Security Broker

In Kooperation mit **Boll Europe**

Cybersicherheit in der Cloud

osc. Es ist eines der am häufigsten gehörten Werbeversprechen der Hyperscaler. Die grossen Public-Cloud-Anbieter wie Amazon Web Services, Microsoft oder Google werden nicht müde, zu betonen, wie sicher ihre Plattformen sind. Und auf den ersten Blick stimmt das auch. Die US-Unternehmen beschäftigen Heerscharen von Informatikerinnen und Informatikern, die zur Cybersecurity von Azure, GCP & Co. Sorge tragen. Ein kleines Unternehmen kann mit diesem Dispositiv nicht mithalten.

Doch auf den zweiten Blick zeigt sich, dass Sicherheit in Cloud-Umgebungen keineswegs ein Selbstläufer ist. Die Plattformen und die Infrastruktur mögen vom Hersteller abgesichert sein, doch im Detail lauern einige Gefahren. Zahlreiche Cloud-Anwendungen laufen heute im Unternehmen parallel, unter Umständen ohne Wissen der IT. Selbstentwickelte Apps werden as-a-Service betrieben. Mitarbeitende greifen unterwegs oder aus dem Homeoffice auf Firmendaten zu. All das muss sicher und unter Einhaltung der Datenschutzregeln ablaufen. Die Cloud-Provider stellen nur die Basis zur Verfügung. Was darauf abläuft, liegt in der Verantwortung des Kunden.

Wie lässt sich die Sicherheit auf Anwenderebene gewährleisten? Eine Methode dafür stellt Joachim Walter, Geschäftsführer von Boll Europe, auf den folgenden Seiten vor: den «Cloud Access Security Broker» (CASB). Dabei handelt es sich um eine Lösung, die sich zwischen die Endgeräte einer Organisation und die Cloud schaltet und so quasi als Wächter über Apps und Daten fungiert. Walter zeigt, welche Funktionen der CASB bietet und wie die Implementierung beim Anwender abläuft. Im Interview stellt er anschliessend ein Beispiel vor.

So wird die Cloud-Nutzung sicher

Wer Cloud-Anwendungen nutzt, muss auf Geschäftsdaten besonders gut aufpassen. Denn die Datensicherheit bleibt in der Verantwortung der Unternehmen. Cloud Access Security Broker helfen dabei, Daten zu schützen und Cloud-Apps ohne Bedenken einzusetzen.

Immer mehr Unternehmen nutzen immer mehr Anwendungen aus der Cloud. Spitzenreiter in Europa ist Office 365 – Microsoft propagiert seine cloudbasierten Office-Dienste seit Jahren und hat damit erheblichen Erfolg. Auch andere Software-as-a-Service-Anwendungen (SaaS) erfreuen sich höchster Beliebtheit, zum Beispiel Salesforce und Servicenow. In grösseren Unternehmen stehen zudem teils hunderte Cloud-Applikationen im Einsatz. Manche davon wurden nicht von der IT-Abteilung eingeführt, sondern werden in Form einer «Schatten-IT» von den Mitarbeitenden genutzt. Und für den Betrieb bisher on-premises gehaltener oder selbst entwickelter Apps setzen fortschrittliche Firmen ebenfalls zunehmend auf Infrastructure-as-a-Service-Plattformen (IaaS) wie AWS, Azure oder Google Cloud.

Jede Multi-Cloud-Strategie steht vor einer grundlegenden Herausforderung: Zwar sind die Cloud-Plattformen höchstmöglich abgesichert, aber der Umgang mit den Anwendungen und besonders mit den damit verwalteten Daten liegt nach wie vor in der Verantwortung jeder einzelnen Organisation, die Cloud-Anwendungen nutzt. Und dies höchst offiziell: Datenschutzgesetze wie die DSGVO der EU sowie unternehmenseigene Compliance-Vorgaben schreiben vor, dass jederzeit nachweisbar ist, welche Daten wann und von wem an welchem Standort bearbeitet werden, wo die Daten abgelegt sind und wohin sie fliessen.

Sicherheit übers Unternehmensnetzwerk hinaus

Klassische Sicherheitssysteme wie Firewalls lösen diese Problematik nicht. Dafür sind sogenannte Cloud Access Security Broker (CASB) erforderlich. CASB stellen als Schnittstelle zwischen Cloud-Apps und Endgeräten einen Kontrollpunkt für komplette Sichtbarkeit und umfassenden Datenschutz über alle Cloud-Anwendungen hinweg dar – eigene Entwicklungen sowie Apps von Drittherstellern, die in einer IaaS-Cloud betrieben werden, inklusive. CASB werden oft in Form eines Cloud-Dienstes implementiert und lassen sich dann innert kürzester Zeit produktiv nutzen. Auch in grössten Umgebungen dauert der Rollout meist nur wenige Tage.

Zu den Grundfunktionen eines CASB gehören die Erkennung aller genutzten Cloud-Apps und die Kontrolle, welche davon zugelassen sind und welche nicht – der CASB sperrt den Zugang zu einer nicht sanktionierten App, lässt allenfalls eine individuelle Freigabe durch den Administrator zu oder schlägt zugelassene Alternativen vor. Darüber hinaus sollte der CASB problematische Cloud-Anwendungen auf Basis von Bedrohungsinformationen und Machine Learning identifizieren, etwa solche, die Sicherheitslücken aufweisen oder schädliches Verhalten zeigen, um diese automatisiert zu blockieren.

Datenschutz ist ausschlaggebend

Mit der anwendungsspezifischen Zugangskontrolle ist die Arbeit eines vollwertigen CASB indes nicht getan. Eine weitere wichtige Funktion ist der Schutz vor Datenverlust – und diese muss alle Standorte und Endgeräte abdecken, was bei standortbasierten Data-Loss-Prevention-Lösungen nicht der Fall ist: Diese sind machtlos, sobald die Daten das Unternehmensnetzwerk verlassen haben. Integriert in den CASB kann der DLP-Mechanismus hingegen den gesamten Datenverkehr mit der Cloud überwachen und anhand der gegebenen Richtlinien steuern – entweder automatisch auf Basis eines Katalogs von Grundregeln für bestimmte Datentypen oder individuell festgelegt, bis hin zum Zulassen oder Sperren einer Datenübermittlung anhand vorkommender Schlüsselbegriffe. So wird zum Beispiel eine Kreditkartennummer, die in einem Dokument enthalten ist, automatisch erkannt und digital «geschwärzt».

Am besten sind die Daten geschützt, wenn sie bereits vor dem Transfer in die Cloud mit unternehmensspezifischen Zertifikaten verschlüsselt werden, nach Möglichkeit sogar zweimal hintereinander mit den sichersten Encryption-Algorithmen wie AES256. Nur dann ist garantiert, dass der Betreiber der Cloud-Plattform die Daten nicht lesen kann. Idealerweise ist die Verschlüsselungsfunktion in den CASB integriert und erfasst sowohl strukturierte, feldbasierte Daten wie etwa bei Salesforce als auch Dateien beliebigen Typs.

DER AUTOR

Joachim Walter
Geschäftsführer, Boll Europe

Bild: metamorworks / iStock


Bild: metamorworks / iStock

Integriertes Identitäts- und Zugangsmanagement

Am bequemsten und sichersten wird die Cloud-Nutzung, wenn der CASB gleichzeitig als Identitätsprovider fungiert (Identity-as-a-Service, IDaaS), und zwar nicht nur für SaaS-Dienste aus der Public Cloud, sondern auch für eigene Apps und Services, die in einer IaaS-Cloud laufen. Dann ist die gesamte Cloud-Sicherheit auf einer einzigen Plattform zusammengefasst. Zu den IDaaS-Funktionen gehören zum Beispiel Single-Sign-on für alle geschützten Cloud-Anwendungen, Synchronisation mit Active Directory, Unterstützung für Cross-Domain-Identity-Management-Systeme (SCIM), Integration mit anderen Identity-Management-Systemen und Multi-Faktor-Authentifizierung.

CASB als Grundlage für BYOD und Homeoffice

Mit all diesen Funktionen eignet sich ein CASB optimal für Homeoffice-Szenarien, die heute besonders aktuell sind: Das Unternehmen behält – egal ob dabei Firmen- oder Privatgeräte genutzt werden – die Kontrolle über den Datenfluss und die Cloud-Anwendungen. Und sobald Privatgeräte ins Firmennetz integriert werden, ist ein Cloud Access Security Broker geradezu unabdingbar. Dies auch aus folgendem Grund: Manche Bring-your-own-Device-Projekte (BYOD) scheitern, weil die Mitarbeitenden nicht zulassen wollen, dass dabei auf ihren Endgeräten eine Mobile-Device-Management-Lösung installiert wird. Laut der Umfrage eines CASB-Anbieters lehnen dies 57 Prozent der Belegschaft der befragten Unternehmen ab.

Dementsprechend darf das Ziel einer BYOD- oder Homeoffice-Strategie nicht die totale Kontrolle über die Geräte sein, sondern die Sicherung der darauf verwendeten Geschäftsdaten und Anwendungen, die wiederum in die Kompetenz von CASB-Lösungen fällt. Das Wichtigste dabei: Auch der CASB sollte dies ohne die Installation eines Agenten auf den Endgeräten leisten können. Nur ein agentenloser Ansatz greift nicht in die Privatsphäre der Nutzer ein und kommt ohne Belastung des Geräts punkto CPU-Auslastung und Akkulaufzeit aus.

Die Nutzer können weiterhin ihre Lieblings-Apps verwenden und trotzdem bleibt die Compliance gewährt, denn nur für die Nutzung freigegebene Daten gelangen überhaupt aufs Gerät – und auch dies ausschliesslich in verschlüsselter Form und abgesichert durch die Authentifizierung jeder einzelnen App, die dabei für die Kommunikation mit dem CASB konfiguriert wird. Idealerweise bietet der CASB zudem die Möglichkeit, beim Verlust eines Geräts, beim Verlassen des Firmen-Campus oder beim Austritt eines Mitarbeiters oder einer Mitarbeiterin den Zugang zu den Geschäftsdaten selektiv zu sperren, weil die Authentifizierung nicht mehr gültig ist. Das Fazit: Ganz egal, ob Homeoffice oder mobile Mitarbeitende – Organisationen, die mehr als eine Cloud-Anwendung nutzen, kommen um eine CASB-Lösung mit möglichst umfassendem Funktionsumfang nicht herum. Nur so ist sichergestellt, dass die Geschäftsdaten nicht in unbefugte Hände abwandern. Und ein solcher Next-Generation-CASB ist eine Kernkomponente der modernen Sicherheitsstrategie Secure Access Service Edge (SASE), bei der Sicherheitslösungen für die Cloud auf einer flexiblen Cloud-first-Plattform konsolidiert und integriert werden.

Organisationen, die mehr als eine Cloud-Anwendung nutzen, kommen um eine CASB-Lösung mit möglichst umfassendem Funktionsumfang nicht herum.

« Die meisten wissen, dass sie punkto Sicherheit etwas unternehmen müssen »

Anwendungen aus der Cloud werden immer öfter genutzt. Damit dabei die Datensicherheit gewährleistet bleibt, kommen Cloud Access Security Broker zum Einsatz. Joachim Walter, Geschäftsführer von Boll Europe, berichtet über eine besonders gelungene CASB-Lösung. Interview: Oliver Schneider

Sind Anwendungen aus der Cloud prinzipiell unsicher?
Joachim Walter: Die Cloud ist per se nichts Schädliches – aber man muss sie sinnvoll und sicher nutzen. Wer Cloud-Anwendungen einsetzt, sollte sehr sorgfältig mit den Applikationen und Daten umgehen, damit keine Datensicherheitsprobleme auftreten. Und wer seine User übers ganze Land verteilt hat, muss sich Gedanken machen, wer auf welchem Device welche Daten nutzen darf. Dabei hilft ein Cloud Access Security Broker, kurz CASB.

Boll hat sich für die Distribution der CASB-Lösungen von Bitglass entschieden. Was war dabei ausschlaggebend?
Bitglass enthält diverse Funktionen, die aktuell kein anderer CASB erbringt. Und es ist insgesamt der umfassendste und vollständigste CASB. Dies hat auch Gartner erkannt und Bitglass im «Magic Quadrant for Cloud Access Security Brokers 2018» in den Leader-Status erhoben. Darüber hinaus eignen sich die Bitglass-Lösungen als Grundlage für eine zukunftsorientierte, cloudfokussierte Secure-Access-Service-Edge-Strategie, kurz SASE.

Was ist denn nun das Besondere an der Bitglass-Lösung?
Es fängt beim Grundkonzept an. Während andere CASB sich auf die Erkennung und Freigabe oder Blockierung der Cloud-Apps konzentrieren, legt Bitglass zusätzlich hohen Wert auf die Identifikation, die automatische Klassifizierung und den Schutz von vertraulichen Daten.

Wie funktioniert das?
Dazu enthält die Lösung Funktionen wie Watermarking von Dokumenten für eine granulare Überwachung der übermittelten Inhalte, starke Verschlüsselung noch vor der Übertragung der Daten in die Cloud – wobei sowohl Feld- als auch File-Encryption möglich sind – und Data Loss Prevention, aber auch integrierte Identity-Services und optional die Erkennung und Abwehr von raffinierten Bedrohungen, also Advanced Threat Prevention.

Ausserdem soll Bitglass auch Geräte abdecken, die nicht vom Unternehmen verwaltet werden …
Richtig. Die Basis dafür ist die Abstraktionsschicht «AJAX Virtual Machine», die nur Bitglass bietet. Sie ermöglicht, dass die Daten auf Mobilgeräten geschützt bleiben, ohne auf den Devices einen Agenten zu installieren, wie es bei klassischen MDM-Lösungen nötig wäre – ideal für BYOD, das nur dann wirklich funktioniert, wenn man es agentenlos implementieren kann.

« Es wird auch weiterhin Firewalls brauchen, aber weniger als bisher. »

Joachim Walter, Geschäftsführer, Boll Europe

Für wen eignet sich Bitglass?
Kurz gesagt für alle Organisationen ab rund 100 Nutzern. Aber auch für sehr grosse Umgebungen: Der grösste Kunde, eine US-Universität, verzeichnet 200 000 User. Die Kosten sind überschaubar. Die Standard-Edition für drei Anwendungen, zum Beispiel Office 365, Salesforce und Servicenow, schlägt mit rund 100 Franken pro User und Jahr zu Buche.

Wer sind die Mitbewerber?
Die Hauptkonkurrenten sind Netskope, McAfee und Symantec. Sie alle kommen aus dem Dunstkreis der Schatten-IT, verstehen sich somit gut auf die Identifikation der genutzten Cloud-Apps. Weniger stark sind sie beim Lösen des Datensicherheitsproblems. Neu ist Microsoft mit der Lösung MCAS hinzugekommen.

Wie entwickelt sich der Markt für Boll und Bitglass?
Es ist eine ausgesprochen erfolgversprechende Lösung. Wenn wir in eine Evaluation einbezogen werden, haben wir grosse Chancen, das Projekt zu gewinnen. Und wir haben viele Kundenanfragen – darunter auch grosse Unternehmen mit zehntausenden Nutzern.

Lösen CASB die herkömmlichen Sicherheitssysteme ab?
Nur zum Teil. Es wird auch weiterhin Firewalls brauchen, aber weniger als bisher. Für Distributoren und Händler können CASB sogar zur Erweiterung des Business werden: Die meisten Firmen wissen, dass sie punkto Cloud-Sicherheit etwas unternehmen müssen.