Advertorial

Cloud-Anwendungen sicher genutzt

Immer mehr Unternehmen nutzen immer mehr Cloud-Anwendungen. Damit dabei die Datensicherheit gewährleistet bleibt, kommen Cloud Access Security Broker zum Einsatz. Eine technisch führende CASB-Lösung kommt von Bitglass.

Cloud-Anwendungen wie Office 365, Salesforce oder ServiceNow efreuen sich zunehmender Beliebtheit. In grösseren Unternehmen stehen zudem teils Hunderte Cloud-Applikationen im Einsatz – manche davon in Form einer «Schatten-IT» von den Mitarbeitenden eingeführt, andere selbst entwickelt und auf IaaS-Plattformen wie AWS, Azure oder Google Cloud ausgelagert.

Zwar sind die Cloud-Plattformen an sich höchstmöglich abgesichert, aber der Umgang mit den Anwendungen und Daten liegt nach wie vor in der Verantwortung der Kunden. So muss beispielsweise jederzeit nachweisbar sein, welche Daten wann und von wem an welchem Standort bearbeitet werden und wo sie abgelegt sind.

Die «Cloud Access Security Broker»-Plattform (CASB) von Bitglass ermöglicht Unternehmen jeder Grösse, bei der Nutzung von Cloud-Diensten Sicherheitsrichtlinien über die Grenzen ihrer eigenen IT-Infrastruktur hinaus durchzusetzen.

CASB: mehr Sicherheit, als die Firewall bietet

Klassische Sicherheitssysteme wie Firewalls lösen dieses Problem nicht. Dafür sind sogenannte Cloud Access Security Broker (CASB) erforderlich. Sie dienen als Schnittstelle zwischen Cloud-Apps und Endgeräten und sorgen für Sichtbarkeit und umfassenden Datenschutz über alle Cloud-Anwendungen hinweg. Eine Grundfunktion eines CASB ist die Erkennung der genutzten Cloud-Apps – der CASB sperrt den Zugang zu sanktionierten Apps. Darüber hinaus sollte er problematische Anwendungen auf Basis von Bedrohungsinformationen und Machine Learning identifizieren und automatisch blockieren.

Mit der App-spezifischen Zugangskontrolle ist die Arbeit eines vollwertigen CASB indes nicht getan. Ebenso wichtig ist der Schutz vor Datenverlust (Data Leakage Protection) – und dieser muss alle Standorte und Endgeräte abdecken. Integriert in den CASB kann der DLP-Mechanismus den gesamten Datenverkehr mit der Cloud überwachen und steuern, automatisiert auf Basis von Grundregeln für bestimmte Datentypen oder individuell festgelegt. So wird zum Beispiel eine Kreditkartennummer in einem Dokument 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. Vorzugsweise ist die Verschlüsselungsfunktion in den CASB integriert und erfasst sowohl feldbasierte Daten wie etwa bei Salesforce als auch Dateien beliebigen Typs.

Noch bequemer und sicherer wird die Cloud-Nutzung, wenn der CASB gleichzeitig als Identitätsprovider fungiert (Identity-as-a-Service). Dann ist die gesamte Cloud-Sicherheit auf einer einzigen Plattform zusammengefasst. Solch umfassende Funktionalitäten, wie sie bei Bitglass Standard sind, bieten die wenigsten CASB-Lösungen.

Grundlage für BYOD und Home Office

Der Bitglass-CASB eignet sich optimal für Home-Office-Szenarien, die heute besonders aktuell sind. Dabei behält das Unternehmen die Kontrolle über den Datenfluss und die Cloud-Apps – selbst wenn nach dem BYOD-Prinzip private Geräte zum Einsatz kommen. Dann ist ein CASB geradezu unabdingbar, denn manche BYOD-Projekte scheitern, weil die Mitarbeitenden auf ihren Geräten keine Mobile-Device-Management-Lösungen akzeptieren.

Ziel einer BYOD- oder Home-Office-Strategie ist demzufolge nicht die totale Kontrolle über die Geräte, sondern die Sicherung der Geschäftsdaten und Anwendungen. Das Wichtigste: Der CASB sollte dies ohne eine Installation auf den Endgeräten leisten können. Nur ein agentenloser Ansatz tangiert die Privatsphäre der Nutzer nicht und kommt ohne Belastung punkto CPU-Auslastung und Akkulaufzeit aus. Aktuell erfüllt nur die Lösung von Bitglass diese Voraussetzung.

Idealerweise bietet der CASB zudem die Möglichkeit, etwa beim Verlust eines Geräts oder beim Austritt von Mitarbeitenden den Zugang zu den Geschäftsdaten selektiv zu sperren. Das Fazit: Organisationen, die mehr als eine Cloud-Anwendung nutzen, kommen um eine CASB-Lösung mit möglichst umfassendem Funktionsumfang nicht herum.

Bitglass CASB: die Highlights

- Führende CASB-Lösung (Magic Quadrant for Cloud Access Security Brokers / Gartner)
- Kontextbezogene Zugangskontrolle zu Cloud-Apps
- Analyse des Nutzerverhaltens mit Erkennung auffälliger Aktivitäten
- Schutz vor Datenverlust (Cloud-weite DLP-Engine)
- Integriertes Identitätsmanagement
- FIPS-konforme zweifache Cloud-Verschlüsselung mit AES256

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch, www.boll.ch