Die Eroberung der Cloud

Datensicherheit und Compliance mit einem CASB

Wenn Unternehmen in die Cloud migrieren, sind sie neuen Risiken in Bezug auf Datensicherheit und Compliance ausgesetzt. Mit einem Cloud App Security Broker (CASB) lassen sich diese Risiken minimieren und die digitale Transformation absichern. Ein CASB schützt die Cloud-Konten der Anwender, begrenzt den Zugriff auf vertrauliche Daten und vereinheitlicht die Richtlinien zum Schutz vor Datenverlust (DLP) für die Cloud, E-Mails und lokale Dateispeicher.

EINFÜHRUNG

Die Migration in die Cloud kann eine Zeitenwende für Ihr Unternehmen darstellen, weil dadurch die geschäftliche Agilität, Flexibilität und Effizienz steigen. Doch auch in Bezug auf die Cybersicherheit kann der Wechsel in die Cloud eine Wende bedeuten, da Anwender, Applikationen und Daten nicht mehr durch Ihre Netzwerkperipherie geschützt werden. Ihre Mitarbeiter geben vertrauliche Daten ohne ausreichende Kontrolle frei und Cyberkriminelle können die Cloud-Konten von Anwendern kompromittieren, um Gelder und wertvolle Daten zu stehlen. Neben all ihren Vorteilen erzeugen Cloud-basierte Anwendungen und Dienste neue Risiken und erschweren die Einhaltung von Compliance-Vorgaben. Für moderne Unternehmen kann es ein schwieriges Unterfangen bedeuten, diese neuen Risiken in den Griff zu bekommen, ohne die vielen Vorteile verpuffen zu lassen.

COMPLIANCE UND DIE CLOUD

Datensicherheit und Compliance sind wichtige Faktoren, um dieses Gleichgewicht herzustellen.

Da Ihre Mitarbeiter immer mehr Unternehmensdaten in der Cloud speichern und freigeben, wächst auch die Gefahr für Ihre Daten. Durch die Einführung von Cloud-Anwendungen haben Ihre Mitarbeiter die Möglichkeit, wertvolle Inhalte (z. B. sensible Inhalte wie Mitarbeiter- und Kundendaten, Quellcode, Formeln und andere vertrauliche Dokumente) über E-Mail, Link-Austausch und Nachrichten weiterzugeben.

Ihre Daten können durch schädliche Aktivitäten und selbst durch gut gemeintes, aber zu freizügiges Freigeben von Inhalten gefährdet werden. Deshalb müssen Sie überwachen und kontrollieren, wie Ihre Mitarbeiter Daten in Cloud-Anwendungen und unterschiedlichen Kanälen nutzen.

Datensicherheit

Die Hälfte aller gemeldeten Datenschutzverletzungen sind die Folge von böswilligen Angriffen, entweder durch kriminelle Akteure von außen oder aber kriminellen Insidern (Mitarbeiter, Dienstleister oder andere Dritte, die Anwenderkonten von Mitarbeitern des Unternehmens missbrauchen).[1]

Zu den Risiken für Unternehmen gehören:

- Schwache Kennwörter
- Kompromittierte Anmeldedaten (durch Phishing-Kampagnen oder Brute-Force-Angriffe)
- Fehlende Datensicherheitsmaßnahmen, wenn beispielsweise keine DLP-Lösung im Einsatz ist

1 Ponemon Institute: „Cost of a Data Breach Report 2019“ (Kosten von Datenkompromittierungen 2019), Juli 2019.

Ursache und Wirkung

Sobald Kriminelle an die Anmeldedaten von Microsoft Office 365- bzw. Google G Suite-Anwendern gelangen, können sie Ihre vertrauenswürdigen Konten missbrauchen, um Angriffe inner- und außerhalb Ihres Unternehmens zu starten.

Sie führen betrügerische Banküberweisungen durch und stehlen wertvolle Informationen wie geistiges Eigentum oder Kundendaten. Eine weitere Möglichkeit ist das Kapern Ihrer E-Mail-Infrastruktur zur Durchführung interner wie externer Cyberangriffe. All das kann die Reputation Ihrer Marke erheblich schädigen und Ihr Unternehmen finanziell schwer treffen.

Die folgenden Beispiele sollen dies exemplarisch aufzeigen:

BILDUNGSWESEN

Cyberkriminelle betrachten Schulbezirke, Hochschulen und Universitäten als leichte Beute mit einer Vielzahl an Schülern/Studenten, Lehrkräften und dezentralisierten Sicherheitsabläufen.

Der Angriff: 70 % aller Bildungseinrichtungen, die Cloud-Dienste nutzen, berichten von gekaperten Accounts, die durch IMAP-basierte Brute-Force-Angriffe ausgelöst wurden. Zu den besonders häufig angegriffenen Kategorien gehören „Professor“ und „Alumni“.

Die Folgen: Angreifer missbrauchen diese übernommenen Konten, um Spam-Kampagnen oder Phishing-Angriffe zu starten, wodurch die Marke dieser Bildungseinrichtungen geschädigt wird. Die Folgen dieser Angriffe gehen weit über die angegriffenen Institutionen hinaus.

REISEUNTERNEHMEN

Der Angriff: Das Cloud-Konto des CEO einer großen Fluggesellschaft wurde kompromittiert.

Die Folgen: Innerhalb von 6 Tagen wurden 40.000 Dateien heruntergeladen.

IMMOBILIEN

Laut dem FBI ist der Immobiliensektor die Branche, die am häufigsten mit Überweisungsbetrug angegriffen wird.

Der Angriff: Cyberkriminelle kompromittierten Office 365-Konten bei einem Immobilieninvestor mit 75.000 Mitarbeitern. Die Konten von fünf Führungskräften wurden übernommen.

Die Folgen: Durch den Zugriff auf die E-Mail der Führungskraft konnten die Angreifer die Bankleitzahl ändern und mehr als 500.000 US-Dollar abzweigen.

Zur Erkennung und Verhinderung von Datenschutzverletzungen in der Cloud benötigen Sie Datensicherheit, die die unterschiedlichen Risiken kennt und die in der Lage ist, eine Korrelation zwischen kompromittierten Konten und einer Datenschutzverletzung zu ziehen.

Compliance

Wenn Sie Daten in der Cloud speichern, wird die Einhaltung gesetzlicher Bestimmungen und Branchenvorschriften noch schwieriger. Die Compliance-Anforderungen ändern sich regelmäßig und legen immer größeren Wert auf die Sicherheit, den Schutz und die Souveränität der Daten.

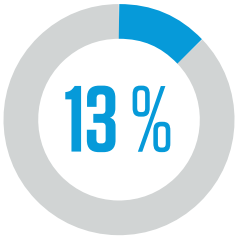
Diese Datentypen sind besonders betroffen:

- Personenbezogene Kunden- oder Mitarbeiterdaten wie Identifikationsnummern oder Geburtsdaten
- Bezahldaten (PCI-Standard)
- Geschützte Gesundheitsdaten (z. B. Krankenakten)

Die Nichteinhaltung der Vorschriften kann zu schmerzhaften Geldstrafen und Marken- und Rufschäden führen. Unverzichtbar für die Minimierung Ihrer Compliance-Risiken ist eine Übersicht über Ihre Cloud-Anwendungen, die Identifizierung und Klassifizierung von Daten in der Cloud sowie die Verhinderung der Datenweitergabe an unbefugte Personen.

Gefährliche Freigaben

Unter den untersuchten Cloud-Konten:



haben umfassende Freigabe-berechtigungen (extern und intern)

teilen Dateien auch mit persönlichen E-Mail-Konten bei beliebten Webmail-Diensten

der Dateien in der Cloud enthalten sensible Daten

Wiedererlangen der Kontrolle

Eine zuverlässige und fortschrittliche CASB-Lösung unterstützt Sie bei der Definition und Implementierung von Richtlinien, um den Zugriff Ihrer Mitarbeiter auf wichtige Unternehmensdaten zu regeln. So können Sie definieren und durchsetzen, wie, wann, wo und durch wen die Datenzugriffe erfolgen dürfen.

Wichtige Parameter von CASB-Richtlinien:

- Anwenderrollen und Risiken im Zusammenhang mit der Anmeldung
- Kontextinformationen wie Anwenderstandort, Gerätestatus usw.

Beispielsweise gelten in stark regulierten Branchen wie dem Gesundheitswesen strenge Richtlinien für den Zugriff auf vertrauliche Daten durch unverwaltete oder riskante Geräte.

Als ersten Schritt sollten Sie untersuchen, wie Daten von Ihren Cloud-Anwendungen verarbeitet werden. Ebenso wichtig ist zu wissen, wie Ihr Unternehmen die eigenen Datensicherheitsziele sowie die Vorgehensweisen für Datenidentifizierung, Dateibehebung, Forensik und Berichterstellung definiert hat.

Mit der richtigen CASB-Lösung sind Sie in der Lage, Cloud-DLP-Richtlinien zu implementieren, die mit den Richtlinien für E-Mails und lokale Dateispeicher abgestimmt sind. Weitere wichtige Aspekte sind die Integration in andere DLP-Lösungen sowie die einheitliche Verwaltung von Zwischenfällen.

CASB-WUNSCHLISTE FÜR DATENERKENNUNG, -SCHUTZ UND -COMPLIANCE

Diese Wunschliste von Datenschutz- und Compliance-Funktionen sollte Ihre neue CASB-Lösung erfüllen.

Datenerkennung

- Identifiziert vertrauliche Daten in SaaS- und IaaS-Angeboten (Infrastructure-as-a-Service):
  - Microsoft OneDrive
  - Google Drive
  - Box
  - Dropbox
  - AWS S3-Buckets
  - Salesforce
  - Microsoft Exchange-Postfächer
  - Online-Dienste für Nachrichtenaustausch (Slack und Microsoft Teams)
- Erkennt Freigabeberechtigungen für öffentliche, externe, interne sowie private Dateien und Ordner
- Identifiziert mithilfe standardmäßig enthaltener und fortschrittlicher DLP-Technologien regulierte Daten (Zahlungsdaten, personenbezogene Informationen, FINRA, HIPAA und DSGVO) und bewertet die Compliance-Risiken:
  - Identifikatoren
  - Wörterbücher
  - Näherungsabgleich
  - Kontextabgleich
  - Dokument-Fingerabdrücke
  - Exakter Datenabgleich (EDM)
  - Texterkennung mit OCR (Optical Character Recognition)
- Erkennt, wer in Ihrem Unternehmen Zugriff auf vertrauliche Cloud-Daten hat

Datensicherheit

- Nahtlose Ausdehnung aktueller DLP-Richtlinien für E-Mails und lokale Systeme auf die Cloud
- Isoliert, löscht oder entfernt umfassende Freigabeberechtigungen bei Dateien, die vertrauliche Daten enthalten
- Sendet Warnungen, sobald vertrauliche Daten nach einer Kontenkompromittierung exfiltriert werden
- Automatisiert die Richtliniendurchsetzung für Datei-Uploads, Downloads, Zusammenarbeit und Nachrichtenaustausch in der Cloud mithilfe von Regeln, die folgende Kontextdaten einbeziehen:
  - Anwender
  - Benutzergruppe
  - Standort
  - Gerät
  - IP-Adresse
  - Dateieigenschaften
  - DLP-Richtlinien
- Warnt Sicherheitsadministratoren bei Richtlinienverstößen und benachrichtigt Anwender, damit diese entsprechend geschult werden

Compliance

- Bietet umfassende Audit-Protokolle aller Dateiaktivitäten und unterstützt die Untersuchung von Vorfällen mithilfe erweiterter Forensikdaten zu:
  - Dateigröße
  - Anwender
  - DLP-Kategorien
  - Freigabeberechtigungen
- Integriert Triage-Untersuchungen von Cloud-DLP-Zwischenfällen und Berichte mit solchen Funktionen für andere DLP-Kanäle, z. B. E-Mail und lokale Datenspeicher
- Integriert SIEM-Verwaltungsplattformen für IT-Dienste (Sicherheitsinformations- und Ereignis-Management) wie ServiceNow, um Warnungen im Zusammenhang mit Dateiverarbeitungsrichtlinien, DLP-Verstößen sowie Reaktionsmaßnahmen zu erfassen
- Automatisiert Kontrollen für Drittanbieter-Anwendungen (OAuth), um die Compliance-Risiken zu verringern

FAZIT UND NÄCHSTE SCHRITTE

Datensicherheit und Compliance sind unverzichtbare Bestandteile Ihrer geschäftlichen Cloud-First-Transformation. Für einen umfassenden Schutz Ihres Unternehmens in der Cloud müssen Sie auch die Bedrohungsabwehr und Anwendungs-Governance offensiv angehen.

Eine personenorientierte CASB-Lösung bietet diese wichtigen Einblicke:

- Wer in Ihrem Unternehmen am häufigsten angegriffen wird
- Wer für Angriffe anfällig ist
- Wer privilegierten Zugriff auf vertrauliche Unternehmensdaten hat

Nur mit dieser Transparenz und Kontrolle können Sie Bedrohungen stoppen, Ihre vertraulichen Informationen schützen und Compliance-Vorschriften einhalten.

Kostenloses Whitepaper herunterladen

Im unserem kostenlosen Whitepaper Erste Schritte mit CASB erfahren Sie mehr darüber, wie sich die Migration in die Cloud mittels eines CASB absichern lässt.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.