E-BOOK

proofpoint.

Erste Schritte mit CASB

Transparenz und Schutz für Ihre Mitarbeiter, Anwendungen und Daten in der Cloud

proofpoint.com/de

Fluch und Segen der Cloud

Der Wechsel Ihres Unternehmens in die Cloud kann eine Wende sein, weil dadurch die geschäftliche Agilität, Flexibilität und Effizienz steigen.

Doch auch in Bezug auf die Cybersicherheit kann er eine Wende darstellen, 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 schaffen Cloud-basierte Anwendungen und Dienste neue Risiken und erschweren die Einhaltung von Compliance-Vorgaben. Für moderne Unternehmen kann es ein schwieriges Unterfangen sein, diese neuen Risiken in den Griff zu bekommen, ohne die vielen Vorteile einer Cloud-Migration verpuffen zu lassen.

Cloud-Sicherheit sollte mit der Absicherung von der IT-Abteilung genehmigter Anwendungen wie Microsoft Office 365 und Google G Suite beginnen, die Ihre wertvollsten Ressourcen enthalten. Die meisten Unternehmen benötigen jedoch mehr Transparenz und Kontrolle darüber, wie ihre Mitarbeiter auf vertrauliche Daten in der Cloud zugreifen sowie sie nutzen und teilen.

Hier kann eine CASB-Lösung (Cloud Access Security Broker) weiterhelfen.

Was ist eine CASB-Lösung?

Gartner definiert CASB als „Produkte und Dienste, die Sicherheitslücken in der unternehmensweiten Nutzung von Cloud-Diensten schließen.“[1] Auch wenn Cloud-Anbieter gewisse Sicherheitsfunktionen bieten, können nur CASBs einen umfassenden Überblick über Ihre Anwender, Cloud-Anwendungen und Daten liefern.

Mit einem CASB können Sie Ihre unternehmensweiten Sicherheitsrichtlinien auf die Cloud ausdehnen und die Cloud-Dienste besser absichern.

Wichtige Funktionen

Heutige Angriffe richten sich nicht gegen Technologien, sondern gegen Menschen. Deshalb setzt eine effektive CASB-Lösung bei der Absicherung von Cloud-Anwendungen auf einen personenorientierten Ansatz. Der richtige CASB kann Ihnen die nötige Sicherheit in einer „Cloud-First“-Umgebung geben.

Folgende wichtige Funktionen sollten enthalten sein:

- Personenorientierter Überblick über Bedrohungen und automatisierte Reaktionen
- Datensicherheit einschließlich Schutz vor Datenverlust (DLP)
- Governance für Cloud- und Drittanbieter-Anwendungen (OAuth)
- Adaptive Zugriffskontrollen für zusätzliche Sicherheitsebenen bei Personen, die ein erhöhtes Risiko darstellen

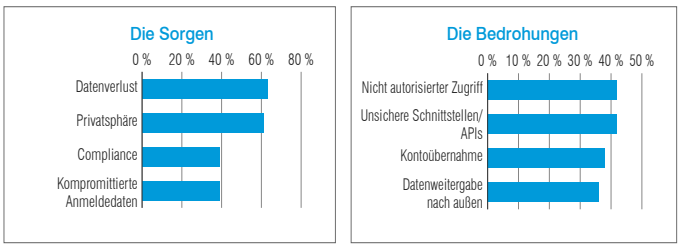
INHALT

1. Gartner: „Magic Quadrant für Cloud Access Security Broker“, Oktober 2018.

Vier Gründe für einen CASB

Immer mehr Unternehmen erkennen, dass ein CASB für die Absicherung ihrer Cloud-Anwendungen und -Dienste unverzichtbar ist. Betrachten wir ihre größten Sorgen genauer.

Häufigste Cloud-Sicherheitsprobleme



(Quelle: Cybersecurity Insiders)

1. Eindämmung von „Schatten-IT“

Schatten-IT bezeichnet Cloud-Anwendungen und -Dienste, die ohne explizites Einverständnis der IT-Abteilung genutzt werden. Sie war von Anfang an einer der wichtigsten Antriebsfaktoren hinter der CASB-Einführung. Anwender nutzen häufig nicht genehmigte SaaS-Anwendungen (Software-as-a-Service) zum Dateiaustausch, für soziale Netzwerke, Zusammenarbeit und Webkonferenzen.

Dieses Verhalten hat sich nicht geändert. Es gibt jedoch ein weiteres zunehmendes Problem: Drittanbieter-Anwendungen und Skripte mit OAuth-Berechtigungen. Per OAuth vernetzte Drittanbieter-Anwendungen greifen auf von der IT zugelassene Cloud-Dienste wie Microsoft Office 365 und Google G Suite zu. Einige davon sind fehlerhaft konzipiert und stellen Risiken dar, da sie größere Datenberechtigungen als nötig gewähren.

Welche Gefahr stellt OAuth dar? Sobald ein OAuth-Token autorisiert wurde, bleibt der Zugang zu Unternehmensdaten und -anwendungen so lange bestehen, bis er gesperrt wird.

CASBs bieten Überblick und Kontrolle für Schatten-IT und ermöglichen die Minimierung anwenderbezogener Risiken.

2. Schutz vor Cloud-Bedrohungen

Cyberkriminelle missbrauchen häufig kompromittierte Cloud-Konten, um an wertvolle Daten und sogar Geld zu gelangen. Sobald die Angreifer die Anmeldedaten eines Cloud-Kontos in die Hände bekommen, können sie legitime Anwender imitieren und auf dieser Weise Ihre Mitarbeiter dazu verleiten, ihnen Geld zu überweisen oder Unternehmensdaten weiterzugeben, oder aber E-Mail-Konten übernehmen, um Spam und Phishing-E-Mails zu verbreiten.

Bei einer Untersuchung von mehr als 1.000 Cloud-Dienst-Mandanten und mehr als 20 Millionen Anwenderkonten stellte sich heraus, dass es allein in der ersten Hälfte 2019 zu mehr als 15 Millionen nicht autorisierten Anmeldeversuchen kam. Mehr als 400.000 dieser Versuche führten zu erfolgreichen Anmeldungen. Insgesamt wurden etwa **85 %** der Mandanten mit Cyberangriffen attackiert und bei **45 %** wurde mindestens ein Konto in ihrer Umgebung kompromittiert.[2]

Angreifer nutzen meist eine von zwei Methoden zur Kompromittierung von Konten:

- Brute-Force-Angriffe, bei denen durch Ausprobieren zahlreicher Namen oder Kennwörter die richtigen Anmeldedaten erraten werden
- Anmeldedaten-Phishing, wo mittels Social-Engineering-E-Mails versucht wird, Anwender zur Preisgabe ihrer Kennwörter zu überreden

CASBs unterstützen Sie bei der Erkennung von und Reaktion auf ungewöhnliche Kontoaktivitäten, die auf kompromittierte Anmeldedaten hinweisen können. Zudem helfen CASBs bei der Implementierung und Durchsetzung von Richtlinien zum Schutz von Cloud-Konten und -Daten.

3. Verringerung des Risikos von Datenverlusten und des Diebstahls von geistigem Eigentum

Jeden Tag nutzen Ihre Mitarbeiter Cloud-basierte Tools für Zusammenarbeit oder Nachrichtenaustausch, um Dateien und Informationen an Kollegen und Partner weiterzugeben. Dabei können sie geistiges Eigentum wie Geschäftsgeheimnisse, Entwicklungsdesigns und weitere vertrauliche Unternehmensdaten gefährden:

- Fahrlässiges Verhalten von Mitarbeitern oder fehlende Schulungen können zur übermäßigen Weitergabe von Dateien über öffentliche Links führen, auf die beliebige Personen zugreifen können.
- Datendiebstahl durch Insider ist ebenfalls eine häufige Erscheinung. Beispielsweise können Vertriebsmitarbeiter, die Ihr Unternehmen verlassen, Daten aus Cloud-basierten CRM-Diensten stehlen.

CASBs erweitern den Überblick darüber, wie Ihre Mitarbeiter mit Daten umgehen, und verbessern die Datensicherheit mithilfe von Richtlinien für die Zugangskontrolle zu Cloud-Diensten.

4. Einhaltung strenger Compliance-Vorschriften

Unternehmen in fast jeder branche kämpfen darum, Compliance-Vorschriften einzuhalten. Viele staatliche und branchengegebene Vorschriften wie die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) fordern, dass Sie den Speicherort Ihrer Daten kennen und wissen, wie sie in der Cloud genutzt werden. Verstöße gegen Datenschutz- und Speicherungsvorschriften können zu Strafen von bis zu 4 % des weltweiten Jahresumsatzes des betreffenden Unternehmens führen.

CASBs können den Compliance-Aufwand verringern und dafür sorgen, dass Audits weniger Kopfzerbrechen bereiten.

> „... bis 2022 werden 60 % aller großen Unternehmen CASBs einsetzen, um einige Cloud-Dienste zu kontrollieren, während es heute weniger als 20 % sind.“
>
> – Gartner Magic Quadrant für Cloud Access Security Broker, 2018

2. Gartner: „Magic Quadrant für Cloud Access Security Broker“, Oktober 2018.

Jeder ist beteiligt: Die Rolle von CASBs bei Geschäftsfunktionen

Eine personenorientierte CASB-Lösung kann Sicherheitsprobleme wichtiger Verantwortlicher in jedem Unternehmen lösen. Diese und weitere Verantwortliche profitieren davon.

CISO, Sicherheitsdirektor, (Cloud-)Sicherheitsarchitekt, Sicherheitstechniker
Diese Personen sehen sich mit folgenden Problemen konfrontiert:

- Cloud-Bedrohungen, die finanzielle und Markenschäden nach sich ziehen können
- Datenverluste in der Cloud und Diebstahl geistigen Eigentums
- Nicht autorisierter Zugriff auf Cloud-Daten und -Dienste

So kann ein CASB helfen:

- Stoppt Cloud-Bedrohungen, bevor sie den Ruf des Unternehmens beschädigen können
- Verringert die Exfiltration wertvoller und vertraulicher Informationen
- Dämmt Schatten-IT ein

CTO, CIO, Verantwortlicher für IT/Netzwerke/Infrastruktur
Diese Personen sehen sich mit folgenden Problemen konfrontiert:

- Sichere Implementierung von seitens der IT zugelassenen Cloud-Anwendungen bei gleichzeitiger Gewährleistung der Anwenderproduktivität
- Kontrolle des Zugriffs auf von der IT zugelassene Cloud-Anwendungen, ohne die Anwenderproduktivität zu gefährden
- Absicherung von Cloud-Daten

So kann ein CASB helfen:

- Behebt die Risiken von Cloud-Anwendungen mithilfe personenorientierter adaptiver Kontrollen, ohne die Produktivität zu beeinträchtigen
- Sichert Cloud-Daten ab, ohne die Zusammenarbeit zu beeinträchtigen
- Entdeckt und kategorisiert Cloud-Anwendungen und identifiziert die Cloud-Nutzung

Chief Compliance Officer oder Risiko- und Datenschutzverantwortlicher, SOC-Manager
Diese Personen sind für die Einhaltung der heutigen strengen Datensicherheits- und Datenschutzvorschriften verantwortlich.

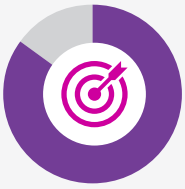
So kann ein CASB helfen:

- Bietet Funktionen für „risikobewusste“ Datensicherheit und Schutz vor Datenverlust (DLP), die nicht autorisierte Zugriffe auf regulierte Cloud-Daten verhindern
- Minimiert Compliance-Risiken dank umfassender Cloud-Erkennung und Governance sowie automatisierten Kontrollen für Drittanbieter-Anwendungen (OAuth)

Kompromittierung von Cloud-Konten

Angreifer haben eine fast 50-prozentige Chance, über Cloud-Konten in eine angegriffene Umgebung einzudringen. Ein einziges kompromittiertes Konto kann gravierende Folgen für Ihre Sicherheit nach sich ziehen.

Bei den in unserer Untersuchung erfassten angegriffenen Unternehmen zeigte sich:



85 % wurden mindestens einmal angegriffen

45 % verzeichneten mindestens eine Cloud-Kontenkompromittierung

6 % entdeckten die Kompromittierung von VIP-Konten

13 aktive Konten registrierten im Durchschnitt nicht autorisierte Anmeldungen

(Quelle: Proofpoint)

Branchen-Fokus

So löst eine personenorientierte CASB-Lösung die größten Probleme der Branche.

Branche	Größtes Problem	**CASB-Mehrwert:** Sichert Office 365 sowie andere von der IT zugelassene Cloud-Anwendungen ab und bietet folgende Vorteile:
Finanzdienstleister	Compliance mit heutigen strengeren Datensicherheits- und Datenschutzvorschriften	Schutz der Kundendaten durch Kontrolle des Zugriffs auf Cloud-basierte Finanzdaten
Gesundheitswesen	Patientensicherheit und Einhaltung von Compliance-Vorschriften	Schutz der Patienten und ihrer Daten durch Kontrolle des Zugriffs auf Cloud-basierte Gesundheitsdaten
Behörden	Beschleunigung der Cloud-Implementierung	Schutz der Daten von Mitarbeitern und Bürgern durch Kontrolle des Zugriffs auf Cloud-basierte vertrauliche Informationen
Bildungswesen	Verhinderung von Kontenkompromittierung und Schutz der Schüler-/Studentendaten	Schutz dieser Daten durch Kontrolle des Zugriffs auf Cloud-basierte personenbezogene Informationen sowie Abwehr von Kontenkompromittierung
Einzelhandel	Innovation und schnellere Cloud-Implementierung	Schutz der Kundendaten durch Kontrolle des Zugriffs auf Cloud-basierte personenbezogene und Zahlungskartendaten
Fertigungsindustrie	Innovation und schnellere Cloud-Implementierung	Schutz von Kundendaten und geistigem Eigentum durch Kontrolle des Zugriffs auf Kunden- und IoT-Projektinformationen

Drei CASB-Anwendungsszenarien

CASBs helfen Ihnen dabei, die Komplexitäten der Cloud-Sicherheit zu bewältigen, insbesondere wenn sie einen personenorientierten Ansatz verfolgen. Sie unterstützen Sie bei der Verbesserung Ihrer Sicherheitslage, indem sie Ihre Mitarbeiter und Daten vor hochentwickelten Bedrohungen schützen, Datenverluste verhindern und Compliance-Vorschriften einhalten sowie den Zugriff auf SaaS-Anwendungen kontrollieren.

Im Folgenden stellen wir diese drei wichtigen CASB-Anwendungsszenarien vor:

1. Schutz vor Cloud-Bedrohungen
2. Sicherheit und Compliance für Cloud-Daten
3. Governance von Cloud-Anwendungen

ANWENDUNGSSZENARIO 1: Schutz vor Cloud-Bedrohungen

Heutige Angriffe richten sich nicht gegen Technologien, sondern gegen Menschen. Das gilt sowohl für die Cloud als auch für die lokale Umgebung. Wenn Unternehmen ihre Plattformen für Nachrichtenaustausch und Zusammenarbeit aus dem Unternehmensnetzwerk in die Cloud verschieben, werden sie damit anfällig für Angriffe.

Cyberkriminelle nehmen gern beliebte SaaS-Anwendungen wie Microsoft Office 365 und Google G Suite ins Visier. Fast jeder Mitarbeiter in Ihrem Unternehmen nutzt diese Anwendungen, die den Schlüssel zu wichtiger geschäftlicher Kommunikation und Daten darstellen. Die Angreifer nutzen eine Vielzahl an Techniken, mit denen sie an die Anmeldedaten von Cloud-Konten gelangen und anfällige Anwender kompromittieren.

Geofencing bzw. das Blockieren von Netzwerkverkehr aus Regionen, die bekanntermaßen Probleme bereiten, löst das Problem nicht, weil viele Bedrohungen ihren Ursprung im Land oder der Region des Unternehmens haben. Zudem kann Geofencing gerade für weltweit agierende Unternehmen oder solche mit Mitarbeitern, die auf der ganzen Welt unterwegs sind, ungeeignet sein.

Ein besserer Ansatz sind adaptive Zugangskontrollen wie risikobasierte Authentifizierung, insbesondere wenn hohe Zugriffsstufen erforderlich sind. Adaptive Kontrollen können Ihnen helfen, Mehrfaktor-Authentifizierung während und nach der Anmeldung entsprechend den Sicherheitsrisiken und nicht nur basierend auf dem Standort durchzusetzen.

Ein CASB mit einer breit aufgestellten Palette von Sicherheitslösungen mit zuverlässiger Erkennung, Problembehebung und risikobasierter Authentifizierung bietet den besten Schutz vor aktuellen personenorientierten Bedrohungen wie Brute-Force- und Phishing-Angriffen sowie schädlichen Dateifreigaben.

Intelligente Brute-Force-Angriffe

Automatisierte Tools probieren unterschiedlichste Kombinationen aus Anwendernamen und Kennwörtern, die aus großen kompromittierten Anmeldedaten-Paketen stammen. Solche Listen mit E-Mail-Adressen, Kennwörtern und anderen Informationen werden nach einer Kompromittierung online veröffentlicht. Angreifer können sogar Mehrfaktor-Authentifizierung umgehen, indem sie auf veraltete E-Mail-Protokolle wie IMAP (Internet Message Access Protocol) zurückgreifen. Dieses häufig genutzte Protokoll ermöglicht E-Mail-Zugriffe von unterschiedlichen Geräten auf den E-Mail-Server und ist besonders anfällig für Cloud-Angriffe.

Hochentwickelte Phishing-Kampagnen

Diese gezielten und raffiniert gestalteten Kampagnen sind vielgestaltig und sollen Menschen zur Preisgabe ihrer Anmeldedaten verleiten. Dadurch erhalten Angreifer die Möglichkeit, Cloud-E-Mail-Konten zu übernehmen und geschäftliche Identitäten zu imitieren.

Laut Untersuchungen kam es bei mehr als 31 % aller Unternehmen oder Gruppen, die Cloud-Dienste einsetzen, zu Kontenkompromittierungen, die mit Phishing-Kampagnen begannen.[3] Zum Verwischen ihrer Spuren nutzen Angreifer manchmal VPNs (virtuelle private Netzwerke) oder Tor-Nodes, die die Privatsphäre und Identität ihrer Anwender schützen. Diese Verbindungsmethoden können bestimmte Netzwerkzugriffssteuerungen in Office 365 sowie ausschließlich auf dem Standort basierende Anwenderauthentifizierungen umgehen.

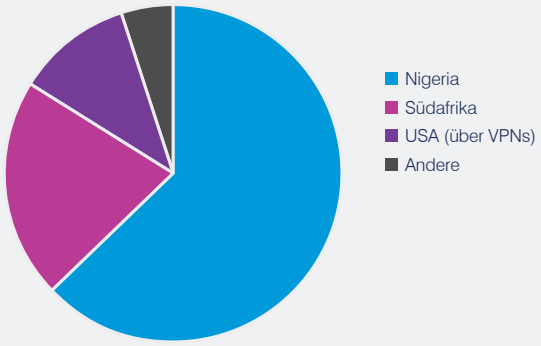
Email Account Compromise (EAC) und Business Email Compromise (BEC) sind Phishing-Formen, die Unternehmen sowie Anwender angreifen, die Geldüberweisungen durchführen können oder Zugriff auf vertrauliche Mitarbeiterdaten (z. B. Steuerdaten) haben. Cyberkriminelle geben sich dabei meist als Führungskräfte oder Geschäftspartner aus und missbrauchen das Vertrauen der Opfer.

Schädliche Dateifreigaben

Bei diesen Angriffstypen kommen meist Phishing-Links, Anmeldedaten-Diebe und Downloader zum Einsatz. Die Bedrohungsakteure verteilen auch Malware mithilfe von Cloud-Diensten wie Dropbox. Sie verwenden diese Plattformen in erster Linie deshalb, weil fast jeder solche Dienste nutzt und die IT-Sicherheit sie deshalb wahrscheinlich nicht blockiert. Besonders gefährdet sind Kunden-Support-Teams, da sie häufig Dateianhänge von Kunden erhalten und die Gefahr besteht, dass diese Kunden in Wirklichkeit Bedrohungsakteure und Anhänge schädliche Dateien sind.

Phishing weltweit

Hier haben die meisten Phishing-Kampagnen ihren Ursprung:



(Quelle: Proofpoint)

CASB-Wunschliste für den Schutz vor Cloud-Bedrohungen

Diese Wunschliste von Schutzmaßnahmen für Cloud-Bedrohungen sollte Ihre neue CASB-Lösung erfüllen.

Erkennung

- Identifiziert riskante Anwender, die häufig angegriffen werden oder Zugriff auf kritische Systeme oder Daten haben
- Ermöglicht dank Machine Learning und Bedrohungsdaten die zuverlässige Erkennung von Cloud-Kontenkompromittierung
- Korreliert E-Mail- und Cloud-Bedrohungen und zeigt auf diese Weise, wie Kontenkompromittierung mit Phishing möglich ist
- Erkennt Zugriffsversuche auf Daten nach Kontenkompromittierung
- Verfolgt laterale Bewegungen von Bedrohungen nach einer Kontenkompromittierung, z. B. E-Mail-Weiterleitung und -Delegierung (ermöglicht der delegierten Person das Lesen, Senden und Löschen von Nachrichten im Namen des Anwenders)
- Erstellt Audit-Protokolle aller Anwenderaktivitäten, um Untersuchungen zu unterstützen, einschließlich erweiterter Forensikdaten zu IP-Adresse, Benutzeragent, Standort uvm.

Behebung

- Sendet eine Warnung, sobald eine Kontenkompromittierung oder daran anschließende Aktivitäten erkannt werden
- Verringert automatisch das Risiko von Kontenkompromittierungen, z. B. durch Unterstützung hybrider Microsoft Active Directory-Bereitstellungen (Beispielaktionen: Beenden von Sitzungen, Sperren von Anwenderkonten oder Zurücksetzen des Kennworts durch den Anwender oder Administrator)
- Löscht oder isoliert schädliche Dateien nach der Erkennung automatisch
- Umfasst Tools zur Integration und Anreicherung von SIEM-Warnungsdaten zu Bedrohungen
- Setzt Berechtigungen für Dateifreigaben zurück
- Entfernt Delegierungen und Regeln zur E-Mail-Weiterleitung
- Entfernt OAuth-Token
- Filtert und dokumentiert Kontextdaten wie Anwender, Gruppen, Standort, Netzwerke, Benutzeragent und IP-Kategorien wie TOR, VPN, Proxy u. a.

Risikobasierte Authentifizierung

- Kontrolliert den Zugriff über bedingte Zugriffsregeln wie das White- und Blacklisting von Ländern, Netzwerken oder die IP-Reputation (z. B. TOR Nodes)
- Kontrolliert den Zugriff basierend auf Anwendern und Gruppen, z. B. privilegierte Anwender mit Zugriff auf kritische Systeme oder vertrauliche Daten (z. B. IT-Administratoren), häufig angegriffene Personen (z. B. Leiter der Personalabteilung) und VIPs (z. B. Vorstandsmitglieder)
- Verhindert riskante Zugriffe basierend auf den Spuren bekannter Bedrohungsakteure, z. B. IP-Adressen, Benutzeragenten und anderen Kompromittierungsindikatoren
- Erzwingt verschärfte Authentifizierungsrichtlinien und beschränkt Zugriffsebenen für Geräte außerhalb des Netzwerks oder basierend auf dem Gerätestatus

3. Proofpoint: „Cloud Attacks Prove Effective Across Industries in the First Half of 2019“ (Cloud-Angriffe beweisen die Effektivität in den Branchen in der ersten Jahreshälfte 2019), September 2019.

ANWENDUNGSSZENARIO 2: Sicherheit und Compliance für Cloud-Daten

Da Ihre Mitarbeiter immer mehr Unternehmensdaten in der Cloud speichern und freigeben, wächst auch die Gefahr einer Kompromittierung. 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 verschiedene Kanäle weiterzugeben: E-Mail, Link-Austausch und Nachrichten.

Ihre Daten können durch schädliche Aktivitäten und selbst durch gut gemeintes, aber zu freizügiges Freigeben von Inhalten gefährdet werden. Datenverluste und Kompromittierungen lassen sich nur dann verhindern, wenn 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 Attacken von Angreifern oder kriminellen Insidern (Mitarbeiter, Dienstleister oder andere Dritte).[4]

Schwache Kennwörter oder kompromittierte Anmeldedaten durch Phishing-Kampagnen und Brute-Force-Angriffe sowie fehlende Datensicherheitsmaßnahmen wie Data Loss Prevention (DLP) führen dazu, dass Unternehmen eventuellen Attacken nichts entgegenzusetzen haben. Zur Erkennung und Verhinderung von Datenschutzverletzungen in der Cloud benötigen Sie risikobewusste Datensicherheit, die die Verbindung zwischen kompromittierten Konten und einer Datenschutzverletzung ziehen kann.

Compliance

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

Besonders davon betroffene Datentypen sind personenbezogene Kunden- oder Mitarbeiterdaten wie Identifikationsnummern oder Geburtsdaten, Zahlungskartendaten sowie geschützte Gesundheitsdaten (z. B. Krankenakten). Die Nichteinhaltung der Vorschriften kann zu schmerzhaften Geldstrafen und potenziellen 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:

13 % haben umfassende Freigabeberechtigungen (extern und intern)

5 % verwenden persönliche Konten, die beliebte E-Mail-Dienste nutzen

4 % der Dateien in der Cloud enthalten sensible Daten

(Quelle: Proofpoint)

Übernahme der Kontrolle

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

Die Parameter der CASB-Richtlinie sollten Anwenderrollen, Risiken im Zusammenhang mit der Anmeldung sowie Kontextinformationen wie Anwenderstandort, Gerätestatus u. a. umfassen. Beispielsweise gelten in Unternehmen in stark regulierten Branchen wie dem Gesundheitswesen strenge Richtlinien für den Zugriff auf vertrauliche Daten durch unverwaltete oder riskante Geräte.

Für den Einstieg 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 sollten Sie in der Lage sein, Cloud-DLP-Richtlinien zu implementieren, die mit den Richtlinien für E-Mails und lokale Datei-Repositorys abgestimmt sind. Weitere wichtige Aspekte sind die Integration in andere DLP-Lösungen sowie die einheitliche Verwaltung von Zwischenfällen.

Ursache und Wirkung

Sobald Kriminelle an die Anmeldedaten von Office 365- bzw. 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.

Dies sind nur einige Beispiele:

Bildungswesen ist am anfälligsten

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, haben Kontoübernahmen aufgrund IMAP-basierter Brute-Force-Angriffe erlebt. 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, was Markenmissbrauch zur Folge hat. Die Folgen dieser Angriffe gehen weit über die angegriffenen Institutionen hinaus.

Vertrauliche Daten und Diebstahl geistigen Eigentums

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

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

Überweisungsbetrug im Immobiliensektor

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

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

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-Diensten (Infrastructure-as-a-Service):
  - Microsoft OneDrive
  - Google Drive
  - Box
  - Dropbox
  - AWS S3-Buckets
  - Salesforce
  - Postfächer in Microsoft Exchange
  - 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 Richtlinienerzwingung für Datei-Uploads, Downloads, Zusammenarbeit und Nachrichtenaustausch in der Cloud mithilfe kontextbasierter Regeln: Anwender, Benutzergruppe, Standort, Gerät, IP-Adresse, Dateieigenschaften und DLP-Richtlinien
- Warnt Sicherheitsadministratoren bei Richtlinienverstößen und benachrichtigt Anwender, damit diese entsprechend geschult werden

Compliance

- Bietet umfassende Audit-Protokolle aller Dateiaktivitäten und unterstützt Vorfalluntersuchungen mithilfe erweiterter Forensikdaten zu Dateigröße, Anwender, DLP-Treffer, Freigabeberechtigungen uvm.
- 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

DLP-Begriffe

Diese DLP-Funktionen dienen zum Identifizieren regulierter Daten.

Identifikatoren: Vordefinierte reguläre Ausdrücke oder Algorithmen, die zum Identifizieren bestimmter Zahlenmuster oder Zeichenfolgenmuster (z. B. mathematische Formeln) verwendet werden können. Das kann beispielsweise der Luhn-Algorithmus sein, ein Modulus-10-Algorithmus zum Identifizieren gültiger Kreditkartennummern.

Wörterbücher, Schlüsselwörter: Sammlung von Wörtern bzw. Phrasen, die häufig auf bestimmte Vorschriften oder Branchen wie Gesundheitswesen, HIPAA, Finanzen, PCI oder andere damit verwandte Begriffe abgestimmt sind.

Näherung: Bestimmt, wie weit entfernt zwei identifizierende Elemente sein können. Beispielsweise können ein regulärer Ausdruck und ein Wörterbuch-Schlüsselwort einen Näherungsfaktor von bis zu 20 Wörtern haben. Dies teilt der Richtlinie mit, dass sie durchgesetzt werden soll, wenn der Ausdruck und das Schlüsselwort maximal 20 Wörter voneinander entfernt sind.

Kontext: Umfasst externe Faktoren wie Header, Größe, Format u. a. – alles, was nicht zum Inhalt des Dokuments gehört.

Dokument-Fingerabdruck: Legt fest, wann Textblöcke oder Formulare für DLP identifiziert werden müssen. Algorithmen können Dokumente und Dateien kürzeren Textzeichenfolgen zuordnen.

Exakter Datenabgleich (EDM): Diese Funktion erfasst bestimmte Datenbankfelder und sucht nach dem genauen Inhalt dieser Felder beim Anwenden von DLP. Sie wird häufig im Gesundheitswesen eingesetzt, um Dokumente mit bestimmten Patientenkennzahlen zu identifizieren.

OCR (Optical Character Recognition): Diese Funktion zum Erkennen von Text in einem Bild dient häufig dazu, vertrauliche Informationen in eingescannten Formularen oder Dokumenten zu identifizieren.

ANWENDUNGSSZENARIO 3: Governance von Cloud-Anwendungen

Es war noch nie so wichtig wie in der heutigen Cloud-First-Welt, den Anwenderzugriff auf von der IT autorisierte sowie nicht autorisierte Anwendungen (Schatten-IT) zu kontrollieren. Unternehmen nutzen durchschnittlich 1.000 Cloud-Anwendungen. Einige davon weisen schwerwiegende Sicherheitslücken auf, die das Potenzial haben, Unternehmen zu gefährden und die Verletzung von Compliance-Vorschriften zu ermöglichen.

Ein Beispiel ist die Gewährung umfassender OAuth-Berechtigungen für Drittanbieter-Anwendungen durch die Anwender, was gegen Datenspeicherungsvorschriften wie die DSGVO verstößt. Hinzu kommt, dass Angreifer häufig auf Drittanbieter-Add-ons und Social Engineering setzen, um Mitarbeiter zur Gewährung von umfassendem Zugriff auf Ihre zugelassenen SaaS-Anwendungen (z. B. Office 365, G Suite und Box) zu verleiten, die meist vertrauliche Daten enthalten.

Antworten auf wichtige Fragen

Für einen genaueren Überblick darüber, wer SaaS-Anwendungen nutzt, müssen Sie folgende Fragen beantworten:

- Welche Cloud-Anwendungen werden in meinem Unternehmen genutzt?
- Welche Trends zeigt die SaaS-Einführung und -Nutzung? Welche SaaS-Anwendungen überschneiden sich?
- Wer nutzt welche Anwendung?
- Wie werden diese Anwendungen genutzt? Erfolgt die Nutzung dieser Anwendungen im Einklang mit den Unternehmensrichtlinien?
- Sind diese Anwendungen in Bezug auf Sicherheit (Schwachstellen und Bedrohungen) sowie Compliance riskant?
- Welche SaaS-Anwendungen zeigen Datei-Upload- und Download-Aktivitäten?
- Welche Datei-Uploads und -Downloads in SaaS-Anwendungen verstoßen gegen DLP-Regeln?
- Wer lädt Dateien mit DLP-Verstößen hoch oder herunter?

Regulierung der Cloud-Nutzung

Eine CASB-Lösung bietet eine zentrale Übersicht Ihrer Cloud-Umgebung und unterstützt Sie auf diese Weise bei der Kontrolle der von Ihren Mitarbeitern genutzten Cloud-Anwendungen und -Diensten. Dadurch erhalten Sie einen Überblick darüber, wer auf welche Anwendungen und Daten in der Cloud zugreift und von welchem Standort sowie mit welchem Gerät das geschieht.

Ein CASB katalogisiert Cloud-Dienste (einschließlich Drittanbieter-OAuth-Anwendungen), bewertet die Risikostufe und allgemeine Vertrauenswürdigkeit von Cloud-Diensten und weist ihnen einen Wert zu. Darüber hinaus bieten CASBs sogar automatisierte Zugangskontrollen zu und von Cloud-Diensten, wobei sie deren Risikostufen und weitere Parameter berücksichtigen, beispielsweise die Anwendungskategorie und Datenberechtigungen.

CASB-Wunschliste für die Kontrolle von Cloud-Anwendungen

Diese Wunschliste von Kontrollmaßnahmen für Cloud-Anwendungen sollte Ihre neue CASB-Lösung erfüllen.

Überblick

- Erkennt verwendete Cloud-Dienste und katalogisiert sie mit folgenden Methoden:
  - Erfassung automatischer Datenverkehrprotokolle von Firewalls sowie sicheren Webgateways wie Zscaler, Palo Alto Networks, Checkpoint u. a.
  - Erkennung und Bewertung von OAuth-Berechtigungen für Drittanbieter-Anwendungen, die auf Cloud-Anwendungen wie Office 365 und G Suite zugreifen
- Erkennt die Anzahl der Anwender sowie den Datenverkehr von Cloud-Diensten
- Erkennt, wer in Ihrem Unternehmen auf welche Cloud-Dienste zugreift
- Kategorisiert alle Cloud-Anwendungen und -Dienste (z. B. Finanzen, Spiele oder Personal)
- Bewertet die Sicherheitsrisiken und Compliance-Lücken von Cloud-Diensten und weist jedem Dienst einen Risikowert zu
- Identifiziert Datei-Uploads und -Downloads sowie die dazugehörigen Anwender

Kontrollen

- Bietet Warnungs- und Coaching-Möglichkeiten für Endnutzer
- Bietet Compliance-Berichte
- Wendet Cloud-Governance-Richtlinien an und automatisiert Kontrollen für den Cloud-Zugriff an (z. B. „zulassen“, „schreibgeschützt“ oder „blockieren“) basierend auf dem Risikowert und der Kategorie der Anwendung
- Widerruft OAuth-Berechtigungen für Drittanbieter-Anwendungen basierend auf Risikograd, Anwendungsumfang, Kategorie und weiteren Eigenschaften wie Anwendern/Gruppen
- Kontrolliert Datei-Uploads zu und Downloads von unzulässigen Cloud-Anwendungen durch Web-Isolierung sowie DLP-Technologien und schützt dadurch Anwender vor Bedrohungen und Datenverlusten

Wolkige Aussichten

Der *2019 Cloud Security Report* (Bericht zur Cloud-Sicherheit 2019) zeigt, dass SOC-Teams mit folgenden großen Problembereichen zu kämpfen haben:

Compliance (34 % der Befragten)
Vor der Implementierung von Cloud-Anwendungen oder ihrer Zulassung müssen die IT-Teams sicherstellen, dass diese Anwendungen Datenschutzvorschriften wie DSGVO, PCI DSS, HIPAA u. a. einhalten.

Fehlende Transparenz (33 % der Befragten)
Transparenz bezieht sich nicht nur auf Sicherheits- und Compliance-Lücken, sondern auch auf Möglichkeiten zur Beseitigung von Redundanzen, Implementierung beliebter werdender Cloud-Anwendungen sowie deren Bereitstellung in anderen Teilen des Unternehmens.

(Quelle: Cybersecurity Insiders)

Fazit: Nächste Schritte

Sicherheit ist ein unverzichtbarer Bestandteil Ihrer geschäftlichen Cloud-First-Transformation. Für einen umfassenden Schutz Ihres Unternehmens in der Cloud müssen Sie die Bedrohungsabwehr, Datensicherheit und Anwendungs-Governance offensiv angehen. Eine personenorientierte CASB-Lösung berücksichtigt, wer am häufigsten angegriffen wird, wer für Angriffe anfällig ist und wer privilegierten Zugriff auf vertrauliche Unternehmensdaten hat.

Dank dieser Transparenz und Kontrolle können Sie Bedrohungen eindämmen, Ihre Informationsressourcen schützen und Compliance-Vorschriften einhalten. Proofpoint bietet die einzige CASB-Lösung, die alle Anforderungen von Sicherheitsverantwortlichen in Bezug auf Cloud-Bedrohungen, Datenverluste und Amortisierungszeit erfüllt. Proofpoint CASB basiert auf einer agentenlosen Cloud-Sicherheitsarchitektur. Die Lösung schützt Ihre wertvollsten Cloud-Ressourcen und beschleunigt Ihre Migration in die Cloud.

Proofpoint Cloud App Security Broker

Für Sicherheitsverantwortliche, denen Cloud-Bedrohungen, Datenverluste und Amortisierungszeit Sorgen bereitet, bietet Proofpoint CASB alle gewünschten Funktionen.

Mit Proofpoint CASB profitieren Sie von folgenden Vorteilen:

- Ausdehnung der personenorientierten Bedrohungsübersicht sowie der adaptiven Kontrollen auf Cloud-Anwendungen
- Implementierung von Cloud-DLP-Richtlinien, die mit denen für E-Mail und lokale Datei-Repositorys abgestimmt sind, sowie Zentralisierung der DLP-Vorfallverwaltung für Cloud-Anwendungen und andere Proofpoint-DLP-Lösungen in der CASB-Konsole
- Erkennung von Cloud-Anwendungen und Eindämmung von Schatten-IT, z. B. Drittanbieter-OAuth-Anwendungen, die auf Daten in Office 365 und G Suite zugreifen

Bedrohungsschutz

- Erkennung und Behebung kompromittierter Konten
- Malware-Schutz

Datensicherheit

- Einheitlicher Schutz vor Datenverlust für alle Kanäle
- Integrierte Datenklassifizierung

Cloud-Governance

- Überblick über Schatten-IT
- Schutz für OAuth-basierte Drittanbieter-Anwendungen

Zugriffssteuerung

- Risikobasierte Authentifizierung
- Adaptive Zugriffsberechtigungen
- Koordinierung von Sicherheitsmaßnahmen

Integration von Cloud-Diensten

Dropbox, Office, slack, amazon web services, box, G Suite, Teams, okta, salesforce

WEITERE INFORMATIONEN

Erfahren Sie, wie wir Sie dabei unterstützen können, Ihre Cloud-Strategie sicher umzusetzen: **proofpoint.com/de/products/cloud-app-security-broker**

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.com**.

proofpoint.