WARUM CASB ALLEIN **NICHT GENÜGT**

Fakt ist: Die herkömmlichen Unternehmensgrenzen gibt es nicht mehr. Früher gab es dank Firewalls, IDS und AV ein klares Drinnen und Draussen. Doch mit der Cloud haben sich diese Grenzen in Luft aufgelöst.

EINFÜHRUNG

Bei einem cloudbasierten Arbeitsplatz spielt es keine Rolle, wo man arbeitet: im Büro, im Café oder am Strand – Applikationen oder Webseiten lassen sich unabhängig von den Compliance- oder Sicherheitsnormen des Unternehmens nutzen. Doch genau hier beginnt die Schatten-IT.

Und da liegt auch das Problem. Cloud, Schatten-IT und Unternehmensgrenzen stellen neue Herausforderungen an Netzwerk und Sicherheit. Nicht genehmigte Geräte und ungehinderter Zugang zu freigegebenen und nicht freigegebenen Applikationen haben die Sicherheitslücken kometenhaft ansteigen lassen. Mitarbeiter, die ihren Computer unbeaufsichtigt lassen, während sie im Coffee Shop arbeiten. Heruntergeladene Filme und Dateien, die mit Schadprogrammen behaftet sind. Phishing-Attacken und Drive-by-Angriffe, über die die Nutzer an unerwarteten Orten Malware einfangen. Es braucht nur einen einzigen Klick auf einen schädlichen Link und das gesamte Netzwerk ist sofort mit Ransomware oder Schadprogrammen infiziert, die die Kundendaten kompromittieren.

Als wäre das nicht schon schlimm genug, setzen die folgenden Vorschriften die Unternehmen noch stärker unter Druck: die Datenschutz-Grundverordnung (DSGVO), das Gesetz zur digitalen Betriebsresilienz (DORA) und die Richtlinie über Netz- und Informationssicherheit 2 (NIS2)[1]. Da steigt auch die Höhe der Bussgelder. Kein Wunder also, dass Unternehmen, die der Cloud-Nutzung zuvor keine grosse Beachtung schenkten, neuerdings eine härtere Linie fahren.

FIREWALLS UND KLASSISCHE SICHERHEITS-TOOLS REICHEN NICHT MEHR AUS

Doch welche Alternativen gibt es? Man kann die Cloud-Infrastruktur sichern, indem man bestimmte Kategorien von Applikationen, beispielsweise die persönliche Ablage, blockiert. Solche Methoden führen jedoch nur dazu, dass die Nutzer nach anderen Wegen suchen, die vom Proxy nicht entdeckt werden. Kaum ist der Zugang zu Dropbox gesperrt, taucht am nächsten Tag SugarSync im Netzwerk auf. Die so entstehende Schatten-IT ist für viele Verletzungen der Datensicherheit verantwortlich.

Alternativ erlauben einige Unternehmen die unbegrenzte Nutzung von Cloud-Applikationen. Sie verpflichten aber die Nutzer, eine Erklärung zu unterschreiben, wonach sie keine vertraulichen Daten mit nicht vertrauenswürdigen Anbietern teilen dürfen. Dieses auf Vertrauen basierende System schafft zwar keine Schatten-IT, stützt sich aber auf einen der unzuverlässigsten Faktoren im Bereich der Sicherheit am Arbeitsplatz: den Nutzer selbst.

Überraschend und beängstigend zugleich: Es gibt Unternehmen, die ihren Nutzern eine uneingeschränkte Nutzung des Internets erlauben (obwohl dies nur wenige zugeben).

CASB SICHERT DIE CLOUD

Ein Cloud Access Security Broker (CASB) füllt diese Sicherheitslücke, denn er sitzt zwischen der On-Premise-Infrastruktur einer Organisation und der Cloud. Dabei funktioniert er wie eine Art Wächter, der für Organisationen Sicherheitsrichtlinien durchsetzt, wenn User die Cloud-Applikationen und -Ressourcen nutzen wollen. Während Firewalls die Schichten drei und vier nach Bedrohungen absuchen und IPS Schadprogramme erkennen, prüft ein CASB die Cloud-Applikationsschicht.

> **CASB sitzt zwischen der On-Premise-Infrastuktur einer Organization und der Cloud. Dabei funktioniert er wie eine Art Wächter, der für Organisationen Sicherheitsrichtlinien durchsetzt.**

Ein CASB übernimmt vier kritische sicherheitsbezogene Aufgaben:

- **Transparenz:** Überblick über die Nutzung von Applikationen und entsprechende Risikoeinstufung bzgl. der Folgen für die Sicherheit des Unternehmens.
- **Schutz:** Proaktiver Schutz mittels Unterstützung der Sicherheitsteams bei der Durchsetzung von Richtlinien und der Verhinderung von Datenin-filtration sowie -exfiltration.
- **Erkennung:** Einfachere Erkennung von Sicherheitsvorfällen, indem Security-Teams Transparenz über die Nutzung von freigegebenen und gesperrten Cloud-Applikationen erhalten und entsprechende Anomalien identifizieren können.
- **Reaktion:** Dank grösserer Transparenz und Kontrolle ist eine schnellere und präzisere Reaktion auf Vorfälle möglich.

Um diese Ziele zu erreichen, kombiniert ein CASB verschiedene Funktionen wie Authentifizierung, Single Sign-On, Abgleich von Berechtigungen, Verschlüsselung sowie Malware-Erkennung und -Prävention.

CASBs sorgen für mehr Kontrolle, Transparenz und Einblicke in Cloud-Dienste. Sie unterstützen Security-Teams bei der Verwaltung von Zugriffen und Aktivitäten, sie sichern Daten und verhindern Datenverlust, sorgen für Compliance-Kontrollen und schützen die Organisation vor internen und externen Bedrohungen wie Ransomware und anderen Formen von schädlichen Codes.

CASBs sind der dringend benötigte Checkpoint, der Security-Experten einen detaillierten Überblick über alle genutzten Cloud-Applikationen verschafft und innerhalb des ausufernden Cloud-Perimeters wieder für Kontrolle und Transparenz sorgt.

CASB-ANWENDUNGEN ALLEINE REICHEN NICHT AUS

Trotz ihrer Stärken stehen Inhouse-CASB-Lösungen heute vor grossen Herausforderungen: Wollen sie die Sicherheitsrichtlinien durchsetzen, müssen CASBs den Datenfluss überprüfen und blockieren können. Bei einem einzigen Standort befindet sich der CASB auf dem zentralen Gateway. Hier ist die Überwachung des internetbasierten Datenflusses relativ einfach.

Hat das Unternehmen allerdings mehrere Standorte, steht es vor verschiedenen architektonischen Herausforderungen. Ein CASB an jedem Standort ist unpraktisch. Den gesamten Datenfluss zwecks Prüfung in ein zentrales CASB zurückzuführen verlangsamt die Internetsessions. Man kann ein CASB auch reaktiv für die Identifizierung vergangener Regelverletzungen einsetzen. Eine solche Methode hat aber Nachteile für die IT und erfordert eine komplexe Konfiguration, da die lokalen Firewalls und Sicherheits-Tools an den verschiedenen Standorten ihre Logs zur Analyse an den CASB schicken müssen. Dem Unternehmen entstehen dadurch Kosten für die interne Sicherheitsexpertise in Bezug auf die CASB-Alarme und Bearbeitung eventueller Regelverstösse.

CASB-SERVICES BIETEN EINE TEILLÖSUNG

CASB-Cloud-Services sollen diese Probleme lösen. Mit ihnen vermeidet man Traffic Backhaul und chaotische Konfigurationen. Die IT kann Sicherheitsverletzungen proaktiv blockieren. Der CASB-Service arbeitet reverse-proxy-basiert und prüft den Datenfluss, sobald er den Kundenstandort verlassen hat. Sämtlicher Internet- und Cloud-Traffic wird an den lokalen Point of Presence (PoP) des CASB-Cloud-Services zurückgeschickt, geprüft und dann entweder gekennzeichnet, blockiert oder an sein Ziel weitergeleitet.

Ein CASB-Cloud-Service löst viele Probleme im Zusammenhang mit einer CASB-Anwendung. Allein kann er es allerdings nicht richten. Er muss zusammen mit einem Secure Web Gateway (SWG), Firewalls und anderen IT-Kontrollen eingesetzt werden. Das Unternehmen steht vor der Herausforderung, den Cloud-Service in seine bestehende Sicherheitsinfrastruktur zu integrieren – oftmals eine unmögliche Aufgabe. Werden die Sicherheitsfunktionen nicht eng miteinander verknüpft, wird das Management extrem komplex. Dies wiederum geht zulasten der Transparenz, da sich der Kontext über mehrere Plattformen verteilt.

DIE PLATTFORM FÜR UMFASSENDEN SCHUTZ IM INTERNET

Gefragt ist nicht nur ein CASB-Service, sondern ein Service mit einem umfassenden Schutz im Internet. Dieser muss von Sicherheitsexperten gemanagt und gewartet werden, die sich gleichzeitig auch um die Integration der Sicherheitsarchitektur kümmern. Eine solche Lösung ist umfassend und bringt alle Bedrohungen aus dem Internet „auf den Radar". Sie verfügt über eine Managementebene, mit der man die Konfiguration, Integration und Event-Analyse bearbeiten kann. Eine Plattform für umfassenden Schutz im Internet übernimmt im Speziellen folgende Aufgaben:

- **Einfache Datenaufnahme vom Proxy:** Jemand muss den Import aller Sicherheitslogs in den CASB vornehmen.

- **Entschlüsselung des SSL-Verkehrs:** Der Zugriff auf alle Logs allein genügt nicht. Es braucht eine Man-in-the-Middle-Entschlüsselung, um einen genauen Einblick in den SSL-Verkehr zu erhalten.

- **Transparenz über Useraktivitäten:** Der CASB deckt auf, was die Nutzer aus dem Netz fischen, beispielsweise unerwünschte Dropbox-Konten oder andere nicht freigegebene Tools. APIs machen ihre Arbeit unabhängig vom Nutzer. Die APIs überwachen SharePoint und OneDrive und suchen nach Daten, die nicht dort sein sollten, wie etwa Kreditkartennummern und persönliche ID-Informationen oder Unternehmensdokumente, die öffentlich geteilt werden.

- **Regelfilter:** Der CASB sollte nach Ihren individuell definierten Regeln filtern. Sind vertrauliche Dokumente beispielsweise mit Metadaten versehen, können sie gegen eine unerlaubte Verteilung ausserhalb der Organisation blockiert werden. Möglich macht dies eine DLP-Lösung (Data Leakage Protection), die die Dokumente scannt und nach spezifischen Datenelementen sucht.

- **Blockierung von Applikationen über eine zentrale Konsole:** Eher unüblich, da viele „False-Positives" möglich sind und eine sorgfältige Handhabung erforderlich ist. Die meisten Unternehmen sind gescheitert, da jeder Zugriff auf die App (z. B. Google Drive) blockiert werden muss und dies die Nutzer sehr verärgert. Die Technologie hat sich bislang noch nicht bewährt und führt weiterhin zu „False-Positives".

CASB-EINFÜHRUNG: PRAKTISCHE TIPPS

Beginnen Sie mit einer Out-of-Band-Lösung. Aufdeckung und Reaktion haben Priorität, bis Sie die Grundlagen für eine Strategie zur Cloud-Nutzung definiert haben. Das kann On-Premise oder in der Cloud geschehen, da dies keinen Einfluss auf die Performance hat. Wenn es sich mit Ihrer Compliance vereinbaren lässt, ist die Cloud die

bessere Lösung, da sie flexibel ist und standardmässig eine hohe Verfügbarkeit bietet.

Wollen Sie primär die Sicherheitsrichtlinien für Ihre Cloud-Apps durchsetzen? Das ist bei den meisten Organisationen der Fall. Dann müssen Sie mit der Reverse-Proxy-Methode arbeiten. Oder möchten Sie die Nutzung von nicht freigegebenen Cloud-Apps verhindern? Dann brauchen Sie einen Forward-Proxy. Die entsprechende Implementierung dauert im Durchschnitt ein bis zwei Jahre. Viele CASB-Anbieter werden bis dahin ihre weltweite Abdeckung von Cloud-PoPs verbessert haben, was eventuelle Performance-Bedenken entkräftet.

Sobald Sie die aktiven Komponenten (nicht nur die passive Überwachung) Ihrer CASB-Lösung implementiert haben, werden Sie mit Themen wie Fehleinschätzungen oder Whitelists, die es für gewisse Applikationen braucht, konfrontiert. Das kommt bei jeder Implementierung vor und sollte Sie daher nicht beunruhigen. Sie sollten aber so rasch wie möglich Schadensbehebungen und Change Management einführen – ein Kernelement des Managed CASB-Services mit umfassendem Schutz im Internet.

[1] Leitfaden, **Wegweiser durch das Labyrinth der Vorschriften**, Open Systems, 2025

Open Systems bietet co-managed SASE-Betriebsmodelle, die sichere Konnektivität, Zero-Trust-Modelle und transparenten 24×7 Betrieb für komplexe hybride und Multi-Cloud-Unternehmensumgebungen in mehr als 180 Ländern vereinen.