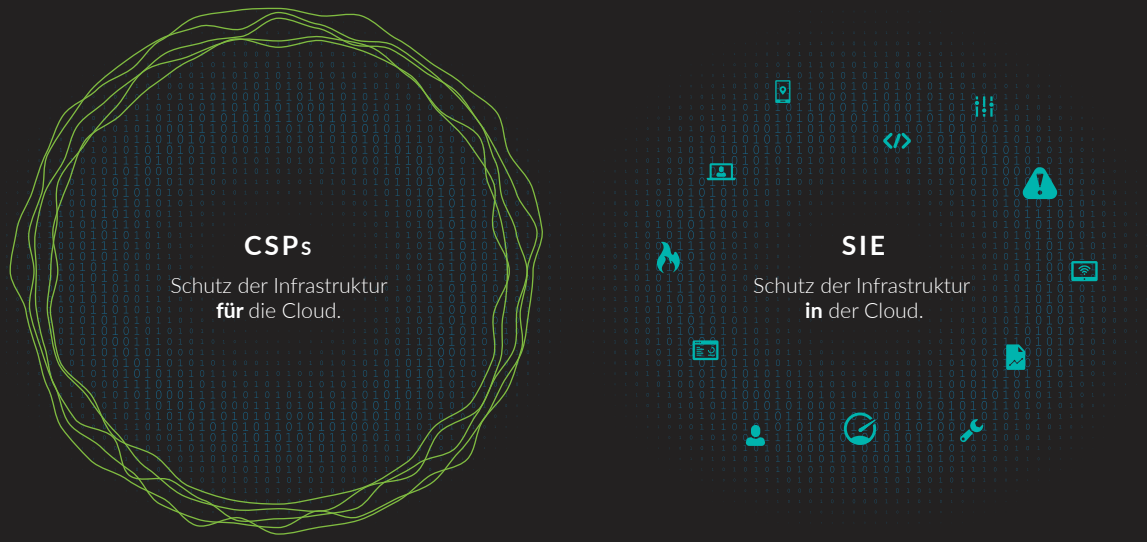
ExtraHop

Gemeinsame Verantwortung in der Cloud

VERANTWORTUNG DES UNTERNEHMENS FÜR DIE CLOUD-SICHERHEIT

Als Cloud-Kunde sollten Sie sich stets vor Augen halten, dass es sich bei Amazon Web Services (AWS) und Microsoft Azure um Cloud-Dienstleister (Cloud Service Provider, CSP) handelt, nicht um Anbieter von Sicherheitslösungen. Aus diesem Grund weisen diese Anbieter auch überaus deutlich darauf hin, dass ihre Sicherheits- und Compliance-Maßnahmen Ihnen nur begrenzten Schutz bieten. Um die Verantwortlichkeiten von CSPs und Kunden klarer zu trennen, haben AWS und Azure jeweils ein eigenes Modell der gemeinsamen Verantwortung entwickelt.



Was heißt das?

Gemeinsame Verantwortung heißt, dass Cloud-Dienstleister ihre Ressourcen (alles unterhalb des Hypervisors) und Kunden ihre eigenen Ressourcen (alles oberhalb des Hypervisors) sichern.

Das Modell der gemeinsamen Verantwortung bietet Ihnen keinen ausreichenden Schutz

CSPs wurden bisher kaum Opfer schwerwiegender Verletzungen der Datensicherheit. Da sie einige der besten Sicherheitsprofis der Welt in ihren Reihen haben, werden ihre Infrastrukturen im Laufe der Zeit immer sicherer. Bei normalen Cloud-Kunden sieht die Sache leider anders aus. Prognosen von Gartner zufolge werden bis zum Jahr 2022 mindestens 95 % aller Cloud-Sicherheitspannen in den Verantwortungsbereich des Kunden im Rahmen des Modells der gemeinsamen Verantwortung fallen.

Dieser hohe Anteil ist beunruhigend. Doch je besser Sie Ihre Verantwortlichkeiten verstehen und sich mit den wesentlichen Bedrohungen auseinandersetzen, durch die solche Datenlecks verursacht werden, desto besser kann Ihr Unternehmen seinen Teil der Verpflichtungen erfüllen und zu mehr Sicherheit in der Cloud beitragen.

APPLIKATIONEN UND INHALTE

Ereignisse des Azure Security Center ergänzen die netzwerkbasierte Bedrohungserkennung um wertvollen Kontext (deaktivierte Protokollierung, auffällige Prozesse, verdächtige Dateiausführungen).

TLS 1.3 wird vollständig in Echtzeit decodiert und die Transaktionslast geprüft, um Bedrohungen zu erkennen und Risiken zu bewerten, sogar für PFS-Bereitstellungen.

NETZWERK-SICHERHEIT

- Informationen zu Zugriffsversuchen vom Rechenzentrum auf die Cloud über private Netzwerkverbindung zur Beobachtung lateraler Aktivitäten
- Rechenschaftspflicht für Fernzugriffe

BESTAND UND KONFIGURATION

- Automatische Erfassung und Klassifikation aller Cloud-Ressourcen
- Beobachtung auffälliger Instanzen, sogar bei deaktivierter Protokollierung
- Sofortige Meldung offengelegter Ressourcen (d. h. per Internet erreichbarer Azure Blob Storage)

DATEN-SICHERHEIT

- Volle Unterstützung für Azure SQL-Datenbanken und Protokolle von Azure Blob Storage zugunsten transparenter Einblicke in Verhaltensmuster statt nur Aktivitäten
- Machine Learning auf Applikationsebene ermöglicht sofortige Erkennung von versuchter Datenausschleusung

ZUGRIFFS-KONTROLLE

- Integration mit Azure Activity Monitoring zugunsten feingranularer Protokollierung von Manipulation an Benutzerprivilegien
- Analyse von Transaktionen mit Active Directory und Hervorhebung auffälliger Verhaltensweisen (Zugangsdatenabfragen, Brute Force) mittels Machine Learning

Cloud-native Sicherheit vs. cloud-kompatible Sicherheit

Trotz aller Bemühungen für eine klare Trennung der Verantwortlichkeiten von CSP und Kunde bieten AWS und Azure ihren Kunden immer noch cloud-native Sicherheitslösungen an. Für viele Unternehmen – vor allem jene ohne Erfahrungen mit der Cloud – bieten solche Lösungen direkte Vorteile, beispielsweise eine vertraute Benutzeroberfläche, kürzere Markteinführungszeiten und einsatzbereite Konfigurationen.

ExtraHop unterstützt Machine Learning in der Cloud, wodurch sehr viel bessere Erkennungsmechanismen zum Aufspüren von Bedrohungen zur Verfügung stehen. Bei Cloud-nativen Sicherheitslösungen wie AWS Guard Duty, AWS CloudWatch oder Azure Monitor basieren die ML-Algorithmen jedoch auf Datenflussprotokollen. Die Ergebnisse der Lösungen von AWS und Azure sind aufgrund ihrer Abhängigkeit von Protokollen somit eher oberflächlich und beruhen nicht auf Verhaltensmustern. Dadurch entgehen ihnen bestimmte Angreifer, einschließlich ungemeldeter auffälliger Instanzen. Ein Elastic Load Balancer bietet Ihnen lediglich Informationen zu den Aktivitäten, deren Protokollierung Sie angewiesen haben, aber nicht zu seinem vollständigen Verhalten.

UNTERSTÜTZUNG DURCH EXTRAHOP

Durch die Integration und Kontextualisierung von Cloud-Ereignissen mit anderen Infrastrukturaktivitäten zugunsten einer ganzheitlichen Analyse- und Auswertungsumgebung für SOC-Teams bietet Reveal(x) für Azure und AWS eine unterbrechungsfreie, durchgängige Analyse der Applikationsebene in der gesamten hybriden Architektur. Dank Machine Learning anhand von über 4.700 Metriken erkennt Reveal(x) fortgeschrittene Angriffe äußerst zuverlässig. Die kontextbezogene Darstellung erleichtert den Teams für Cloud-Sicherheit die sofortige Untersuchung und Reaktion.

ÜBER EXTRAHOP NETWORKS

ExtraHop bietet Unternehmen detaillierte Daten und Analysen zur Stärkung der Sicherheit und Leistung ihrer Infrastruktur. Unser innovativer Ansatz analysiert sämtliche Netzwerkinteraktionen und sorgt mittels modernem Machine Learning für höchste Transparenz, Bedrohungserkennung in Echtzeit und automatische Prüfungen Ihrer Ressourcen in der Cloud. Wir sorgen für Einblicke statt Datenmüll in Form von unübersichtlichen Warnmeldungen, Abläufen und Technologien. Führende Unternehmen aus der ganzen Welt können dank ExtraHop Bedrohungen schneller erkennen, die Verfügbarkeit wichtiger Applikationen sicherstellen, ihre Cloud-Investitionen schützen und ihre Geschäftsabläufe erfolgreich beschleunigen.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101, USA
+1 877 3339872 (Tel.)
+1 206 2746393 (Fax)
info@extrahop.com
www.extrahop.com