FIREEYE™

LÖSUNGSÜBERSICHT

So schließen Sie die Transparenzlücke in der Cloud-Sicherheit

43% von etwa 400.000 Umfrageteilnehmern gaben als Problembereich den fehlenden Überblick über die Infrastruktursicherheit an.

Cloud Security Report
Cybersecurity Insiders

Das Problem
Die meisten Unternehmen werden früher oder später Opfer eines Cyberangriffs, aber nur die wenigsten Datenlecks werden erfasst.

Und selbst dann vergehen in der Regel sechs bis zwölf Monate, bis ein solcher Vorfall entweder zufällig oder von einer externen Stelle, zum Beispiel von einem Kunden oder einem Sicherheitsexperten, aufgedeckt wird.

Die Wahrscheinlichkeit, dass ein wohlmeinender externe Akteur auf eine Sicherheitsverletzung hinweist, ist deutlich größer, als dass ein Unternehmen das Problem intern erkennt.

Überraschenderweise stammen diese Angaben aus Unternehmen, die sämtliche Compliance-Vorgaben eingehalten haben. Organisationen, bei denen Compliance und die Aufklärung von Datenlecks keinen sonderlich hohen Stellenwert haben, werden hierbei nicht berücksichtigt.

Für Unternehmen ist es natürlich besser, wenn interne Mitarbeiter ein Datenleck finden, als von Kunden darüber informiert zu werden.

Die Transparenzlücke
Transparenz ist der Schlüssel zum Erfolg, eine Grundvoraussetzung für jede Cloud-Sicherheitsstrategie. Dabei ist es egal, ob bei Ihrer Strategie Compliance, Spurensuche, Governance oder Risikominimierung im Mittelpunkt stehen.

Doch Transparenz ist ein Ziel, das viele Unternehmen nie erreichen. Jedes Jahr zeigen Umfragen unter Cybersicherheitsexperten erneut, dass der Überblick über die Sicherheitsinfrastruktur die größte Herausforderung in der Cybersicherheit darstellt.

Bevor sich Unternehmen komplexeren Sicherheitsstrategien oder -themen widmen können, müssen sie die Transparenzlücke schließen.

Die gängigsten Hürden
SecOps-Teams müssen zahlreiche Herausforderungen bewältigen, die einen zentralen Überblick über die Ausbreitung von Angreifern im Unternehmen und den Abruf entscheidender Kontextinformationen erschweren.

Wenn Unternehmen wachsen und immer mehr Mitarbeiter unterschiedliche Prozesse und Technologien einführen, die diverse Cloud-Anbieter, Konten, Regionen und Services umfassen, wird auch die Transparenzlücke immer größer.

Um ihre Prozesse effizienter zu machen, haben viele Unternehmen Self-Service-Lösungen implementiert, doch dadurch ist es noch schwieriger geworden, eine gut geschützte Infrastruktur zentral bereitzustellen und zu kontrollieren. Durch die Einführung von Cloud-Technologien entstanden größere, verteilte, dynamischere und (manchmal) temporäre Infrastrukturen. Leider können herkömmliche Sicherheitstools mit dem Umfang und der Geschwindigkeit der Clouds nicht mithalten. In den letzten

zehn Jahren haben die Technologien zur Bereitstellungsautomatisierung zudem die Technologien zur Automatisierung der Sicherheitsprozesse in Bezug auf die einfache Einführung, den Funktionsumfang und den Reifegrad überholt.

In der Vergangenheit konzentrierten sich SecOps-Teams stärker auf die Bedrohungsabwehr als auf die Bedrohungserkennung, doch alle Abwehrmaßnahmen werden irgendwann überwunden. Herkömmliche Abwehrfunktionen nutzen statisch definierte Kontrollen am Unternehmensperimeter. In der Cloud ist der Perimeter jedoch dynamisch, nicht statisch, und wird zudem eher logisch als physisch definiert.

Ältere Sicherheitstools wie physische und virtuelle Firewalls sind für die Erkennung und Abwehr von Angriffen in verteilten, dynamischen Cloud-Umgebungen daher kaum geeignet. Die rasanten Veränderungen in der Cloud und die zunehmend verteilten und vielfältigen Unternehmensinfrastrukturen erschweren die Suche nach einer einzigen Sicherheitslösung, die umfassende Transparenz in allen Umgebungen bietet.

Anforderungen an eine Lösung
Die richtige Lösung zur Schließung der Transparenzlücke muss einen umfassenden Überblick bieten und dazu sowohl aktuelle Konfigurationen als auch historische Sicherheitsereignisse im Detail überwachen.

Dazu müssen folgende Voraussetzungen erfüllt werden:

- **Umfassende Überwachung des Inventars für alle Ressourcen zu jedem Zeitpunkt**
  Ohne eine transparente Überwachung des (aktuellen und historischen) Inventars aller Ressourcen sind Compliance-Audits und Sicherheitsanalysen unvollständig und/oder irreführend.
- **Durchsuchbare, detaillierte Kontextinformationen zum aktuellen Status aller Ressourcen**
  Ohne einen umfassenden Überblick über den aktuellen Status aller Ressourcen kann kein Kontext erfasst werden. Ohne Kontext funktionieren wichtige Konzepte wie die Sicherstellung der Compliance und die Erkennung von Anomalien nicht.
- **Umfassender Überblick über die historischen Sicherheitsereignisse für alle Ressourcen**
  Wenn Sicherheitsteams keinen Überblick über das tatsächliche Verhalten der Workloads und Anwender haben, können sie nicht feststellen, ob Governance-Richtlinien greifen und ob die Infrastruktur bereits von einem Angreifer infiltriert wurde.

Logdateien reichen zum Ermitteln der Inventar- und Ressourcendaten nicht aus, da eine durchgängige Aufzeichnung aufgrund von Startphasen, Serviceunterbrechungen und anderen Problemen nicht immer gewährleistet ist.

Wenn sich der aktuell konfigurierte Status einer Ressource nicht über die entsprechende API des Cloud-Anbieters ablesen lässt, ist die Inventarüberwachung nicht vollständig und Angreifer könnten problemlos unerkannt bleiben. Logdateien sind hilfreich, aber APIs bieten wesentlich mehr.

Eine effektive Lösung muss daher einen umfassenden Überblick über komplexe und verteilte Umgebungen bieten, einschließlich Hybrid- und Multi-Clouds, die sehr groß, temporär oder serverlos angelegt sein können. Außerdem muss sie eine zentrale, durchsuchbare Übersicht über alle Kontextdaten für alle Ressource bereitstellen. Anwender sollten Ad-hoc-Abfragen – über die Benutzeroberfläche oder eine API – für alle aufgezeichneten Kontextinformationen aller Ressourcen durchführen können. Dazu muss eine zentrale Oberfläche für cloudübergreifende Sicherheitsanalysen und Compliance-Audits bereitgestellt werden.

Anwender sollten die Möglichkeit haben, einmalige Audit-Abfragen ganz einfach in wiederkehrende Compliance-Prüfungen umzuwandeln. Damit wird nicht nur die Transparenzlücke geschlossen, sondern Sicherheitsteams können dank des umfassenden Überblicks auch komplexere Sicherheitsmaßnahmen für Compliance, Governance und die Spurensuche einführen.

TRANSPARENZ MIT CLOUDVISORY

Cloudvisory bietet in einer zentralen Konsole einen umfassenden Überblick über die Sicherheitsmaßnahmen in der gesamten Infrastruktur. Die Ressourcenerkennung wurde vollständig automatisiert und Cloudvisory führt eine umfassende Bestandsüberwachung der Ressourcen in Echtzeit durch. Dank der automatisierten Erkennung über die APIs des Cloud-Anbieters stehen detaillierte Kontextinformationen zur Verfügung, da Cloudvisory die Details des letzten bekannten Status zu jeder Ressource speichert, die in einer überwachten Umgebung vorhanden war. Der Status einer Ressource setzt sich aus verschiedenen detaillierten Kontextinformationen zusammen. Dazu gehören:

- **Cloud-Kontext:** Details zu den mit der Ressource verknüpften Cloud-Anbietern/Konten/Regionen/Gruppen/Rollen usw.
- **Historischer Kontext:** Analysen der historischen Sicherheitsereignisse, die während der Nutzung einer Ressource erfasst wurden
- **Sicherheitskontext:** Aktuelle Konfigurationen der Sicherheitsfunktionen einer Ressource
- **Systemkontext:** Aktuelle Statusinformationen, die direkt im Betriebssystem der Ressource erfasst wurden

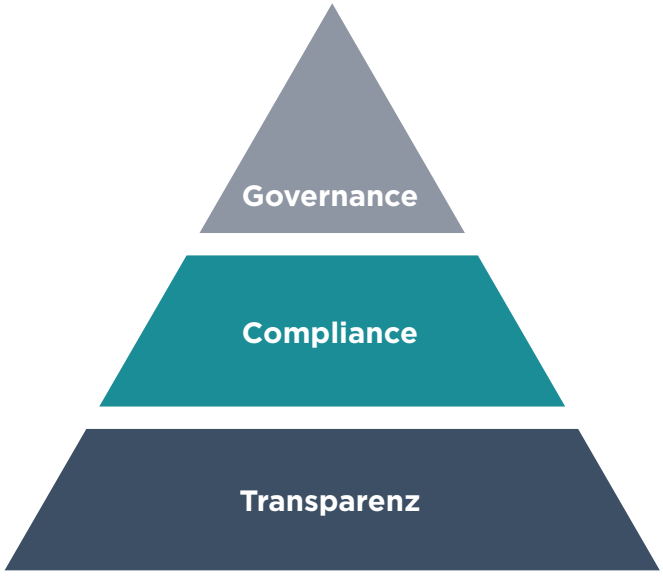
Was spricht für Cloudvisory?

Cloudvisory ist eine Komplettlösung, die den besten Überblick über alle Multi-Cloud-Umgebungen mit diversen Betriebssystemen bietet und deren einzelnen Komponenten (Transparenz, Compliance und Governance) für die Zusammenarbeit optimiert wurden.

Es gibt zahlreiche Lösungen auf dem Markt, mit denen sich der Sicherheitsstatus für mehrere Bereitstellungen und Konten eines bestimmten Cloud-Anbieters einschätzen lässt. Die meisten Unternehmen nutzen jedoch eine Hybrid-Cloud- oder Multi-Cloud-Strategie und es fehlt ihnen an Sicherheitsfunktionen für die Cloud. Vor diesem Hintergrund gibt es nur eine Sicherheitslösung mit Multi-Cloud-Kompatibilität, die (dank der umfassenden Transparenz) einen unmittelbaren ROI bietet und auch auf lange Sicht die Effizienz steigert und die Sicherheit stärkt: Cloudvisory.

Zusammen noch effektiver

Transparenz ist die Grundlage für Compliance, aber regelmäßige Compliance-Prüfungen generieren auch Daten für mehr Transparenz. Diese Synergie schafft eine zusätzliche Sicherheitsebene und bietet historische Kontextdaten, die die Governance unterstützen. Algorithmen für das maschinelle Lernen nutzen die Kontextdaten und generieren damit intelligente, rollenspezifische Governance-Richtlinien.



Unterstützte Cloud-Serviceanbieter

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Unterstützte Betriebssysteme

- CentOS
- Red Hat
- Ubuntu Linux

Gartner Cool Vendor 2018

Cloudvisory wurde im Bericht „Cloud Security 2018“ als „Gartner Cool Vendor“ ausgezeichnet.

CIO Applications Top 25 Amazon Solution Providers 2017

CIO Applications führt Cloudvisory unter den „Top 25 Amazon Solution Providers“ auf.

AICPA SOC

Cloudvisory-SaaS wurde von einer unabhängigen Stelle gemäß SOC-2 zertifiziert.

Weitere Informationen zu Cloudvisory erhalten Sie unter: **www.FireEye.de/cloudvisory**

FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

Über FireEye, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE