LÖSUNGSÜBERSICHT

FireEye

Sicherheit für die Cloud

Überwachung und Schutz von Hybrid-Infrastrukturen

HIGHLIGHTS

- Zeigt Bedrohungen und Schwachstellen in Ihrer Cloud in Echtzeit an
- Erkennt und blockiert den Missbrauch von Anmeldedaten und versehentliche Fehlkonfigurationen, die Angreifern Einfallstore öffnen könnten
- Zentralisiert die Erfassung und Überprüfung von Cloud Trail-, S3- und ELB-Logdateien und vereinfacht so den Sicherheitsbetrieb

Wenn Unternehmen ihre Geschäftsprozesse in die Cloud verlagern, müssen sie sich einer ganzen Reihe von Herausforderungen rund um die Sicherheit stellen. Falsch konfigurierte Authentifizierungsmaßnahmen, nachlässige Schlüsselverwaltung und ungesicherte APIs sind nur einige Schwachpunkte, die Angreifer ausnutzen könnten, um sich Zugang zu fremden Cloud-Infrastrukturen zu verschaffen. Einmal eingedrungen, können sie dann Anwendungen infiltrieren, Anmeldedaten stehlen, die gesamte Infrastruktur ausspionieren und sensible Daten stehlen und ausschleusen. Doch obwohl die Cloud demnach ebenso anfällig und sicherheitsrelevant ist wie On-Premises-Systeme, verfügen nur wenige Unternehmen über die notwendigen Tools für ihren umfassenden Schutz.

Dies wiegt umso schwerer, da IaaS- und PaaS-Anbieter ein Modell der gemeinsamen Verantwortung nutzen, bei dem die Kunden für den Schutz ihrer eigenen Daten in der Cloud verantwortlich sind. Daher müssen Unternehmen Anmeldedaten schützen, Schwachstellen in ihrer Cloud-Infrastruktur proaktiv identifizieren und beheben und das Sicherheits-Monitoring zentralisieren.

Starke Sicherheit ist technisch machbar. Die Sicherheitsplattform FireEye Helix bietet einen umfassenden Überblick und nutzt Konfigurations-Monitoring und Analysen des Nutzerverhaltens, um komplexe Cloud-basierte Angriffe aufzudecken.

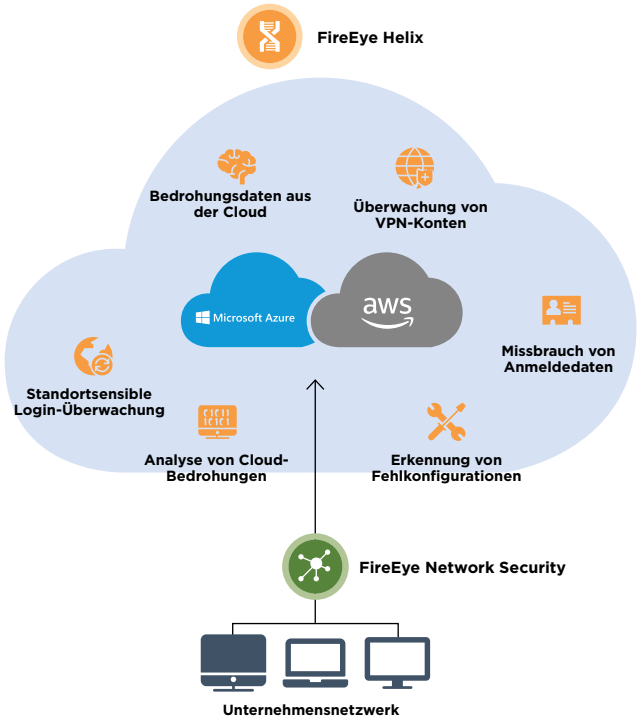

Abbildung 1: Sicherung der Cloud-Infrastruktur mit FireEye

Die Lösung von FireEye:

Enttarnt Bedrohungen durch Monitoring und Bedrohungsdaten

Verhindert Fehlkonfigurationen und den Missbrauch von Anmeldedaten

Verfolgt verteilte Ressourcen

Erkennung des Missbrauchs von Anmeldedaten

Identifiziert und meldet geknackte Konten

Standortsensible Login-Überwachung

Erkennt Anmeldeversuche, die für einen Standort ungewöhnlich sind

Cloud-Konfigurationsregeln, Analysen und Orchestrierung

Erkennt Cloud-Fehlkonfigurationen, behebt sie automatisch und erstellt Berichte

Erkennung geknackter VPN-Konten

Identifiziert potenzielle VPN-basierte Bedrohungen durch die heuristische Analyse von Anmeldeversuchen im Rechenzentrum, bei der unter anderem der Standort und die IP-Adresse des für den Zugriff genutzten Geräts überprüft werden.

Bedrohungsdaten aus der Cloud

Reichert Warnmeldungen von Amazon GuardDuty mit Kontextinformationen an, um die Bedrohungserkennung und -abwehr zu unterstützen

Netzwerküberwachung

Erkennt ungewöhnliche Aktivitäten in WAN-Verbindungen, um Angreifer daran zu hindern, vom Unternehmensnetzwerk in IaaS- und PaaS-Clouds einzudringen oder umgekehrt

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de.**

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 fungiert als nahtlose und skalierbare Erweiterung der Sicherheitsumgebung seiner Kunden 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 unterstützt FireEye Kundenunternehmen bei der Vorbereitung auf die Erkennung und Abwehr von Cyberangriffen.

FireEye