CROWDSTRIKE

Cloud-Sicherheit einfach gemacht

Die Cloud ist der Treiber der digitalen Transformation. Sichere Cloud-Umgebungen sind deshalb gleichbedeutend mit sicherem Wachstumspotenzial. Da Unternehmen in Rekordgeschwindigkeit cloudbasierte Dienste einführen, haben sie es mit einer immer größeren Angriffsfläche zu tun, die mit neuen Herausforderungen für Sicherheit und Betrieb einhergeht und somit besonderen Schutz erfordert.

31 %

der im Juni 2022 befragten Unternehmen gaben an, dass es bei ihnen in den letzten 12 Monaten zu einem Sicherheitszwischenfall gekommen ist.

Quelle: Fidelis 2022 AWS Cloud Security Report

95 %

der Sicherheitsexperten sind mäßig oder sehr besorgt über die Sicherheit von Public Clouds.

Quelle: Fidelis 2022 AWS Cloud Security Report

Gemeinsam bieten CrowdStrike und AWS umfassenden Schutz für Ihre Workloads und Ihre Infrastruktur. So sind Sie auf Ihrem Weg zur Cloud rundum sicher.

CROWDSTRIKE | aws

Die häufigste Ursache für Cloud-Angriffe sind nach wie vor menschliche Fehler und Versäumnisse bei der täglichen Administration. Unternehmen gewähren Mitarbeitern oft mehr Zugriff und Berechtigungen als für ihre Aufgaben eigentlich erforderlich, wodurch identitätsbasierte Bedrohungen zunehmen.

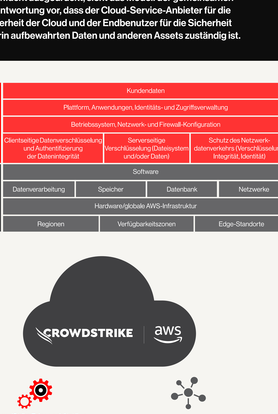
83 %

der Befragten gaben an, dass mindestens eine der Cloud-Datenschutzverletzungen in den letzten 18 Monaten im Zusammenhang mit Zugriffsrechten stand.

Quelle: IDC State of Cloud Security 2021

Durch zu schnelle Migration werden Anwendungen anfällig für Konfigurationsfehler – die häufigste Schwachstelle in Cloud-Umgebungen. Falsch konfigurierte Zugriffsrichtlinien entgehen oft der Sicherheitsprüfung und erhöhen die Wahrscheinlichkeit für eine Kompromittierung.

Ursachen für Cloud-Zwischenfälle



Quelle: Cybersecurity Insiders 2021 Cloud Security Report

67 %

der befragten Cybersicherheitsexperten sahen in den Fehlern bei der Cloud-Sicherheitskonfiguration das größte Risiko für die Sicherheit der Cloud.

Quelle: Cybersecurity Insiders 2021 Cloud Security Report

Der Schutz vor Cloud-Angriffen erfolgt nach dem Modell der gemeinsamen Verantwortung

Der Umstieg in die Cloud, ohne die Sicherheits- und Compliance-Zusammenhänge zu verstehen, erhöht das Risiko und kann Angreifern mitunter die Tür öffnen. Durch das Modell der gemeinsamen Verantwortung werden riskante Grauzonen eliminiert, da die Sicherheitspflichten der Cloud-Service-Anbieter und ihrer Kunden klar definiert sind.

8 %

der befragten IT-Führungskräfte und Cybersicherheitsexperten gaben an, das Sicherheitsmodell der gemeinsamen Verantwortung für alle Arten von Cloud-Services vollständig verstanden zu haben.

Quelle: Oracle and KPMG Cloud Threat Report 2020

Vereinfacht ausgedrückt, sieht das Modell der gemeinsamen Verantwortung vor, dass der Cloud-Service-Anbieter für die Sicherheit der Cloud und der Endbenutzer für die Sicherheit der darin aufbewahrten Daten und anderen Assets zuständig ist.

CrowdStrike Falcon schützt Ihre Workloads, die in AWS ausgeführt werden.

AWS schützt Ihre Cloud-Infrastruktur.

Wenn Sie für den Schutz Ihrer Daten auf die CrowdStrike-Lösungen für Cloud-Sicherheit zurückgreifen, dürfen Sie eine einheitliche Sicherheitsverwaltung für Cloud-Umgebungen mit Schutz für Workloads und AWS- und Hybridumgebungen erwarten. Kurzum: Sie profitieren bei Ihren Entwicklungen in der Cloud von schnellem, zuverlässigem und umfassendem Schutz.

Weitere Informationen über CrowdStrike-Cloud-Sicherheit

Folgen Sie uns

CROWDSTRIKE

Schutz, der Sie weiter bringt