CROWDSTRIKE

Cloud Risk Report 2023

Das Zeitalter cloudorientierter Bedrohungsakteure

KURZFASSUNG

Die Zahl der cloudorientierten Cyberangriffe ist von 2021 bis 2022 enorm gestiegen:
Die beobachteten Cloud-Exploits haben um **95 %** zugenommen und die Angriffe auf Cloud-Umgebungen haben sich im Jahresvergleich fast verdreifacht – die Zahl stieg um **288 %**.[1]

Um Ihre Cloud-Umgebungen vor diesen Aktivitäten schützen zu können, müssen Sie wissen, wie die Bedrohungsakteure vorgehen: Wie sie in die Umgebung gelangen, mit welchen Methoden sie sich lateral bewegen, welche Ressourcen sie ins Visier nehmen und wie sie die Erkennungsmechanismen unterlaufen.

Der CrowdStrike Cloud Risk Report 2023 konzentriert sich auf Akteure, die Cloud-Umgebungen von Unternehmen angreifen, und deren Taktiken, Techniken und Prozeduren (TTPs) . Der Bericht beleuchtet wichtige Trends bei Angreiferaktivitäten, geht auf reale Angriffe auf die Cloud ein, nennt wichtige Versäumnisse, die Unternehmen angreifbar machen, und gibt Hinweise dazu, wie Sie Ihr Unternehmen vor cloudorientierten Angreifern schützen können.

1 CrowdStrike Global Threat Report 2023

Wichtigste Erkenntnisse:

Angreifer optimieren ihre cloudbezogenen TTPs.

- Zahlreiche Angreifergruppen, darunter SCATTERED SPIDER (Cyberkriminalität), COZY BEAR (mit Verbindung nach Russland), COSMIC WOLF (mit Verbindung zur Türkei) und LABYRINTH CHOLLIMA (mit Verbindung nach Nordkorea), starten immer raffiniertere sowie aggressivere Angriffe gegen Ziele in der Cloud.
- Staatliche gestützte Akteure und Cyberkriminelle verwenden Cloud-Infrastrukturen, um Dokumente mit Phishing-Ködern sowie Malware zu hosten, und erfahrene Bedrohungsakteure implementieren Command-and-Control-Kanäle (C&C), die auf bestehenden Cloud-Services aufsetzen.
- Bei 28 % der Vorfälle, die CrowdStrike während des Beobachtungszeitraums festgestellt hatte, löschten die Angreifer manuell eine Cloud-Instanz, um Beweise zu entfernen und der Entdeckung zu entgehen.*

Identität ist der kritischste Zugangspunkt zur Cloud.

- Die Angreifer nutzen zunehmend gültige Konten. Bei 43 % der Cloud-Angriffe, die CrowdStrike im vergangenen Jahr beobachtete, erfolgte der Erstzugriff auf diese Weise.
- Fast die Hälfte (47 %) der kritischen Cloud-Konfigurationsfehler entsteht durch unsichere Identitäts- und Berechtigungsverwaltung.*
- Bei 67 % der Cloud-Sicherheitsverletzungen fand CrowdStrike IAM-Rollen (Identitäts- und Zugriffsverwaltung) mit Berechtigungen, die über die erforderlichen Rechte hinausgingen. Möglicherweise hat in diesen Fällen ein Angreifer versucht, die Rollen zu umgehen, um die Umgebung zu kompromittieren und sich lateral zu bewegen.*

Menschliche Fehler erhöhen Cloud-Risiken.

- Bei 60 % der von CrowdStrike überprüften Container fehlen korrekt konfigurierte Sicherheitsfunktionen.*
- Bei 36 % der Cloud-Umgebungen gab es unsichere Standardeinstellungen des Cloud-Service-Anbieters.*

Die Erkenntnisse in diesem Bericht basieren auf Daten und Beobachtungen zu realen Cyberangriffen. Diese Vorfälle wurden durch CrowdStrike Falcon® Cloud Security, das CrowdStrike Falcon® Intelligence-Team, die verwaltete Bedrohungssuche des CrowdStrike® Falcon OverWatch™-Teams und im Rahmen von Incident-Response-Einsätzen aufgedeckt, analysiert und neutralisiert.

CrowdStrike geht davon aus, dass sich die gezielten Angriffe auf Cloud-Umgebungen verstärken werden. Um mit dieser Entwicklung Schritt zu halten, müssen Unternehmen verstehen, mit welchen Bedrohungen sie konfrontiert werden, sodass sie ihre Cloud-Umgebungen effektiv schützen können.

Vollständigen Bericht herunterladen

Fast die Hälfte (47 %) der kritischen Cloud-Konfigurationsfehler entsteht durch unsichere Identitäts- und Berechtigungsverwaltung.*

* Quelle: Beobachtete Cloud-Sicherheitsvorfälle innerhalb eines 24-stündigen Analysezeitraums