CROWDSTRIKE

Die häufigsten Cloud-Angriffs-techniken

und deren Abwehr

Die Cloud ist eine ständig wachsende, dynamische Angriffsfläche. Um diese Umgebung vor den zunehmenden Cloud-Angriffen zu schützen, sind fundierte Kenntnisse über die Aktivitäten von Bedrohungsakteuren notwendig. Hier erfahren Sie, welche drei Cloud-Angriffstechniken das CrowdStrike Intelligence-Team am häufigsten beobachtet hat und wie Sie sich davor schützen können.

Bedrohungsakteure nehmen immer häufiger die Cloud ins Visier

Cloud-Umgebungen wachsen immer weiter:

41,4 %
der Unternehmen erklärten, dass sie verstärkt auf cloudbasierte Services und Produkte setzen werden[1]

33,4 %
planen die Migration von Legacy-Unternehmenssoftware zu cloudbasierten Tools[1]

32,8 %
führen eine Migration der lokalen Workloads in die Cloud durch[1]

Und Bedrohungsakteure wissen das auch.

Beobachtungen von CrowdStrike aus 2022:

95 %
Zunahme von Cloud-Exploits

300 %
mehr Vorfälle mit cloudorientierten Bedrohungsakteuren

71 %
der Angriffe erfolgten malwarelos

Warum werden Cloud-Umgebungen angegriffen?

Multi-Cloud-Umgebungen sind komplex und lassen sich daher schwerer schützen

Durch rasche Software-Entwicklungsprozesse sind cloudnative Anwendungen für Schwachstellen und Konfigurationsfehler anfällig

Bei nicht autorisierten und Schatten-Cloud-Umgebungen fehlen Sicherheitskontrollen und Transparenz

Isolierte Einzellösungen hinterlassen blinde Flecken, durch die Angreifer unbemerkt bleiben

Bedrohungsakteure sind cloudorientiert und verfeinern ihre Taktiken zum Missbrauch von Cloud-Diensten und zur Ausnutzung von Cloud-Schwachstellen. Dies sind die drei häufigsten Cloud-Angriffstechniken, die das CrowdStrike Intelligence-Team im Jahr 2022 bei der Verfolgung von über 200 Bedrohungsakteuren beobachtet hat:

Laterale Bewegungen in der IT-Infrastruktur

Immer mehr Bedrohungsakteure greifen gezielt herkömmliche Endgeräte an, um auf die Cloud-Infrastruktur zuzugreifen – und umgekehrt wird die Cloud-Infrastruktur als Einfallstor für herkömmliche Endgeräte genutzt. Nur wenige Unternehmen haben den Überblick, um diese Aktivitäten stoppen zu können, da viele von ihnen zahlreiche Einzellösungen erworben haben, die die lokale Umgebung und seit Kurzem auch Cloud-Umgebungen schützen sollen.

Um laterale Bewegungen zu stoppen, benötigen Unternehmen einen umfassenden Überblick über die gesamte IT-Infrastruktur, sowohl lokal als auch in der Cloud.

Cloud-Konfigurationsfehler, die zu Kompromittierungen führen

CrowdStrike untersucht regelmäßig Cloud-Kompromittierungen, die bei korrekter Konfiguration der Cloud-Sicherheitseinstellungen früher hätten erkannt oder verhindert werden können. Konfigurationsfehler erhöhen nicht nur das Risiko für Kompromittierungen, sondern werden mit der zunehmenden Erweiterung der Cloud-Infrastruktur auch immer häufiger und problematischer.

Platz 1
Die am häufigsten ausgenutzte Schwachstelle in Cloud-Umgebungen.

60 %
Bei 60 % der von CrowdStrike überprüften Container fehlen korrekt konfigurierte Sicherheitsfunktionen.

36 %
Bei 36 % der Cloud-Umgebungen gibt es unsichere Standardeinstellungen des Cloud-Service-Anbieters.

Cloud-Identitäten als neuer Perimeter

Als neuer Perimeter sind Identitäten der Schlüssel zur gesamten Unternehmensumgebung geworden. Statt sich auf die Deaktivierung von Virenschutz und Firewalls zu konzentrieren, setzen Bedrohungsakteure zunehmend auf die Modifizierung von Authentifizierungsprozessen und Angriffe auf Identitäten. Mit der fortschreitenden Verbreitung von cloudbasierten Anwendungen und Diensten steigt die Zahl der Identitäten, die von Angreifern ins Visier genommen und ausgenutzt werden können.

Legitime Benutzerkonten wurden bei 43 % der Cloud-Angriffe für den Erstzugriff missbraucht.

47 % der kritischen Cloud-Konfigurationsfehler **entstehen durch unzureichende Identitäts- und Berechtigungsverwaltung.**

Bei **67 %** der Cloud-Sicherheitsverletzungen **fand CrowdStrike IAM-Rollen (Identitäts- und Zugriffsverwaltung) mit mehr Berechtigungen, als erforderlich waren. Das ist ein deutlicher Hinweis auf einen Angreifer, der versucht hat die Rolle zu missbrauchen, um die Umgebung zu kompromittieren und sich lateral zu bewegen.**

CrowdStrike für Cloud-Sicherheit

Ebenso wie die Cloud-Umgebungen wachsen, werden auch die cloudorientierten Angriffe zunehmen. Es ist unmöglich, alle Cloud-Schwachstellen, Konfigurationsfehler und Benutzerfehler zu erkennen, geschweige denn über die neuesten TTPs der Bedrohungsakteure auf dem Laufenden zu sein. Unternehmen benötigen daher einen Partner, der sich ausgezeichnet mit dem Verhalten von Bedrohungsakteuren und der Cloud auskennt.

Als [weltweit führender Anbieter für agentenbasierte Endpoint-Sicherheit](#) verfolgt CrowdStrike einen visionären Ansatz zur Entwicklung skalierbarer und effektiver Cloud-Sicherheit, die sich problemlos auf einer einzigen Plattform bereitstellen und verwalten lässt. CrowdStrike Falcon® Cloud Security wurde speziell für agentenlosen und agentenbasierten Schutz entwickelt. Unternehmen können die Lösung einfach aktivieren und den Schutz von den Endgeräten auf die Cloud erweitern, um die gesamte IT-Infrastruktur mit nahtlosem, einheitlichem Schutz abzudecken. Falcon Cloud Security vereint Lösungen zur Sicherheitsverwaltung für Cloud-Umgebungen, Cloud-Workload-Schutz und Berechtigungsverwaltung für Cloud-Identitäten in einer vollständig integrierten cloudnativen Plattform für Anwendungsschutz (CNAPP).

Laden Sie das Whitepaper „Insider-Leitfaden für Cloud-Schutz" herunter.

Weitere Informationen →

Über CrowdStrike

CrowdStrike (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit einer der weltweit fortschrittlichsten cloudnativen Plattformen für Endgeräte- und Workloadschutz sowie Identität und Daten die Sicherheit grundsätzlich für Unternehmensbereiche neu.

Die CrowdStrike Falcon® Plattform nutzt die CrowdStrike Security Cloud und erstklassige KI, um Echtzeit-Angriffsindikatoren, Bedrohungsanalysen, veränderte Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform äußerst präzise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren.

CrowdStrike Falcon® wurde für den Cloud-Einsatz entwickelt und nutzt einen einzigen schlanken Agenten, um schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite zu ermöglichen.

CrowdStrike: We stop breaches.

Folgen Sie uns

CROWDSTRIKE