AllCloud

Best Practices für Cloud Sicherheitsprozesse auf AWS

INHALT

Cloud-Security-Baseline

- Identität und Zugriffsmanagement
- Protokollierung und Überwachung
- Infrastruktursicherheit für AWS
- Datenschutz in der Cloud
- Incident Management
- Kostenmanagement und -kontrolle für die Unternehmens-IT

Alles in einer Hand für einen sicheren Weg in der AWS Cloud

www.allcloud.io | de-info@allcloud.io | +49 (0)172 295 295 1

powered by aws

Cloud-Security-Baseline

Die Verantwortung für die Sicherheit der Daten und Anwendungen Ihres Unternehmens in der Cloud liegt bei Ihnen selbst. Das mag nach großem Verwaltungsaufwand klingen, aber mit den richtigen Tools und dem richtigen Support sollte Sie das nicht davon abhalten, die vielen Vorteile der Cloud-Infrastruktur auf AWS zu nutzen. Hier ist unsere Baseline, die aufzeigt, auf welche Pfeiler Sie sich konzentrieren müssen, um frühzeitig eine kontinuierliche Cloud-Sicherheit zu implementieren. Wir haben einige der notwendigen Best Practices zur Bewältigung der Herausforderungen und zur Aufrechterhaltung der Kontrolle hervorgehoben. Es kommt alles auf die Einhaltung einer Security-Baseline an.

Identität und Zugriffsmanagement

Wer kann auf Ihre Informationen in der Cloud zugreifen und wer ist berechtigt, Maßnahmen zu ergreifen? Wenn Sie es mit komplexen Unternehmen mit Hunderten oder Tausenden von Mitarbeitern, Projekten und Arbeitsaufgaben zu tun haben, benötigen Sie Transparenz und Kontrolle über Rollen und Richtlinien. Dies ist nicht nur ein "nice to have" für die Optimierung und Visualisierung, sondern oft auch ein "must-have" für die Einhaltung der Sicherheitsstandards.

Die Einrichtung und Definition Ihres IAM-Playbooks ist die Grundlage für ein sehr hohes Sicherheitsniveau in der Cloud und kann als Vorstufe für weitere Automatisierungen in Bezug auf Sicherheit insgesamt sein. Dies kann von der Erkennung von Unregelmäßigkeiten oder der Aktualisierung von Sicherheitskontrollen über das Patch-Management bis hin zur Bereitstellung von Änderungen an Sicherheitscodes reichen.

Protokollierung und Überwachung

Viele Unternehmen wechseln zur Cloud um mehr Agilität, Leistung und Skalierbarkeit zu erreichen. Ohne den richtigen Ansatz für die Protokollierung und Überwachung können Sie diese Vorteile nicht vollständig realisieren, und Sie werden wahrscheinlich einen negativen Einfluss auf Ihr Incidentmanagement erfahren, geschweige denn davon , dass Sie die Sicherheit insgesamt nicht mehr vollständig im Blick behalten.

Die Einrichtung der Überwachung sollte eines der ersten Elemente auf Ihrer To-Do-Liste sein, gepaart mit Informationen zu System- und Performanceveränderungen, des Betriebszustands und einer Übersicht über die von Ihnen verwendeten Ressourcen, insbesondere da Sie ja nur für das bezahlen wollen, was Sie wirklich für sich nutzen.

Sie sollten die richtigen Tools finden, beginnend mit Cloud-basierten Diensten wie AWS CloudTrail und AWS GuardDuty und bei Bedarf mit Lösungen von Drittanbietern ergänzen. Sie erhalten **Warnmeldungen für die verschiedensten, detaillert festgelegten Metriken, die Sie sich ansehen möchten, können diese in Ihr SIEM integrieren und Ereignisse und Protokolle an die richtige Stelle weiterleiten, neben Lösungen aus diesen verwertbaren Erkenntnissen** für Eskalation und Maßnahmen.

Infrastruktursicherheit für AWS

Es ist wichtig, über den Netzwerkzugang nachzudenken, den Sie in Ihre AWS-Infrastruktur integrieren möchten. Die Erstellung eines Security-Playbooks hilft Ihnen, genau zu definieren, was Sie benötigen, und steuert die privaten Netzwerke und Verbindungen, die Sie für Ihr Unternehmen zulassen möchten.

Das Security-Playbook sollte eine Strategie für Amazon VPCs (Virtual Private Cloud) und Subnetze definieren sowie eine Basis für Sicherheitsgruppen festlegen. Im Playbook **sollten VPC Flow Logs aktiviert und konfiguriert sein, um Protokolle an ein dediziertes Logging-Tool zu liefern.** Dies gilt auch für die Überwachung der Überwachungsregeln selbst. Andere Strategien, die im Playbook behandelt werden sollten, sind Direct Connect/VPN für Verbindungen mit lokalen Umgebungen und eine CIDR-Strategie für eine bessere Kontrolle der IP-Verbindungen in Ihrem Unternehmen.

Es gibt zwei wichtige DevOps-Praktiken, die genutzt werden sollten. Erstens, **die grundlegenden Sicherheitsregeln sollten über "Infrastructur as Code" erstellt werden,** so dass Ihre Best Practices automatisiert und integriert sind, und auch um Sie vor Schwachstellen zu schützen. Zweitens, die **AMI-Bakery mit den installierten SSM- und Inspektor-Agenten entwickeln, um die Bootzeit Ihrer EC2-Instanzen zu verkürzen.**

Bei richtiger Einrichtung kann AWS auch sicherstellen, dass Sie der Verkehr über alle Dienste hinweg verschlüsselt ist, auch "in transit".

Datenschutz in der Cloud

Für die meisten Unternehmen würde der Kontrollverlust über ihre Daten das Vertrauen ihrer Kunden schädigen beispielsweise durch die Offenlegung sensibler Informationen gefährden. Der Datenschutz hat daher für viele Unternehmen, die in die Cloud wechseln, oberste Priorität. Die **Sicherstellung, dass Ihre Daten sowohl während der Übertragung als auch im "Rest-Zustand" immer verschlüsselt sind, ist ein integraler Bestandteil.** Unternehmen müssen verstehen, wie sie **den AWS Key Management Service (KMS) verwalten müssen, um auf Daten und Speicher sicher, konform und dennoch schnell zuzugreifen und gleichzeitig diese zu schützen.**

Wenn es um Datenspeicherung geht, haben Sie viele sichere, bedarfsgerechte Optionen in Bezug auf Kosten, Leistung und Kapazitäten. Für einige Unternehmen ist die Standard-S3-Verschlüsselung die richtige Wahl, während für Anwendungsfälle wie Data Warehousing oder Analyse-Engines der Elastic Block Store (EBS) eine alternative, intelligentere Wahl sein kann.

Incident Management

Vorbeugende Maßnahmen haben ihre Grenzen. Die heutige Bedrohungslage ist gekennzeichnet durch das Unbekannte; Zero-Day-Threats und neue attackierende Vektoren, die nicht immer rechtzeitig vorhergesagt werden können. Die Begrenzung der Angriffsdauer macht jedoch den Unterschied zwischen einem überschaubaren Vorfall und etwas, von dem sich Ihr Unternehmen nicht erholen kann. **Definieren Sie ein Cloud-spezifisches Incident Response Playbook, das ein geeignetes Ticketing-Management-System und die richtigen Analysewerkzeuge enthält und die IoC-Erkennung und die Antwort und Reaktion bereits auf Code-Ebene automatisiert.** Die Ergebnisse zeigen es: Sie können jede Bedrohung für Ihre Cloud-Infrastruktur so schneller lokalisieren, isolieren und beseitigen.

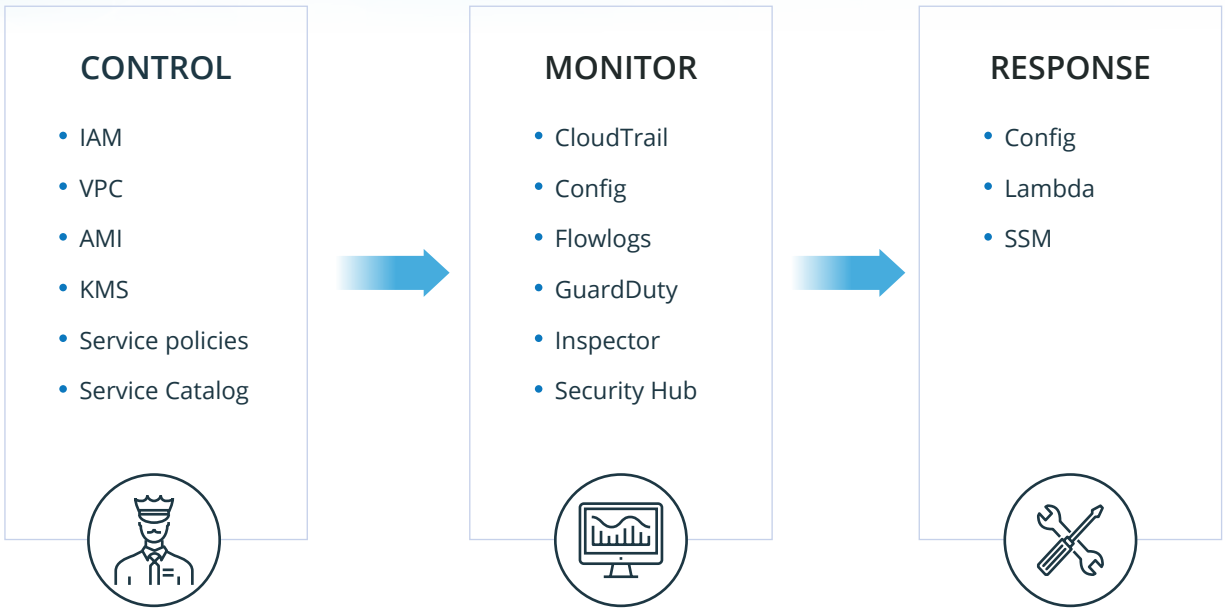
Laut dem letzten SANS-Bericht, haben 50% der Unternehmen keinen Zugang zu den Systeminformationen und Protokolldateien, die für die tiefergehende Untersuchung eines Sicherheitsverstosses benötigt werden, während 40% aufgrund der Mandantenfähigkeit Schwierigkeiten damit haben. Die Erstellung eines Playbooks für die Reaktion auf Vorfälle bedeutet, dass Ihr Unternehmen nicht unter mangelnder Transparenz, Massen an Ereignisdaten und Aussagen, Kompetenzlücken oder fehlenden Kontrollen und Prozessen leidet, wenn Sie gleichzeitig versuchen, in der Krise schnell zu handeln.

Kostenverwaltung und -kontrolle für die Unternehmens-IT

Natürlich muss Ihr Sicherheitsverfahren bezahlbar sein, oder Sie haben überhaupt kein funktionierendes Cloud-Geschäft. Der richtige Prozess beginnt mit der Einrichtung von Kostenstellen und der Zusammenführung von Accounts, der Budgetverwaltung und einem von Anfang an berücksichtigten Kostenverteilungsschlüssel. Dies liefert Transparenz über das gesamte Projekt und bietet eine Grundlage für die Budgetierung und Entscheidungsfindung, wenn sich die Dinge während des Business Transformationsprozesses ändern.

Wenn Ihre Instanzen mehr kosten als Sie erwarten, können Warn- und Alarmmeldungen, automatisierte Aktionen und Verfahren Ihren digitalen Workflow rationalisieren. Dieser Prozess verfolgt nicht nur die Ausgaben und Kosten, sondern integriert das Finanzmanagement auch in Ihre gesamte Cloud-Strategie. Auf diese Weise vermeiden Sie unverantwortliches Finanzmanagement, das negative Auswirkungen bei 80% der Finanz- und IT-Führungskräfte beim Wechsel in die Cloud haben.

AWS Security Lifecycle



Alles in einer Hand für einen sicheren Wechsel zur Cloud auf AWS

Mit der richtigen Beratung und einem umfänglich, gelebten "Best Practice"-Playbook muss der Weg in die Cloud nicht gepaart sein mit Sicherheitsproblemen und mangelnder Kontrolle. Tatsächlich sind die Werkzeuge alle da, um die Sicherheit zu ermöglichen und stetig zu verbessern und trotzdem gleichzeitig die Skalierbarkeit, Flexibilität und Innovation einer Cloud-Infrastruktur zu nutzen.

Wenn Sie nach einer sicheren Möglichkeit suchen, Ihre Workloads in die Cloud zu übertragen, verfügt AllCloud mit diesen standardisierten Best Practices und mit über 11 Jahren Erfahrung in der Handhabung von Hunderten von Cloud-Implementierungen. Unser White Paper zur unternehmensweiten Landing Zone informiert ausführlich über diesen Prozess. Dabei handelt es sich um ein automatisiertes Framework, das Ihrem Unternehmen hilft, in der Cloud den Sprung von "geht nicht" zu "erfolgreich“ zu schaffen.

aws partner network

Premier Consulting Partner

DevOps Competency
Security Competency
MSP Partner

AllCloud verfügt über AWS-Sicherheitsexperten in ganz Deutschland, die Ihnen beim Aufbau Ihrer Cloud-Sicherheits-Baseline helfen können. **Kontaktieren Sie uns noch heute!**