CLOUD SECURITY POSTURE MANAGEMENT:

Sichere und Compliance-konforme Konfiguration von komplexen Cloud-Infrastrukturen

Cloud Infrastructure und Platform Services (IaaS und PaaS) ermöglichen heute ein Höchstmaß an Automation und Anwender-Self-Service. Dadurch wird die Bedeutung der korrekten Cloud-Konfiguration und der Compliance mit rechtlichen Vorgaben und Best Practices maximiert, denn die Cloud wirkt wie ein Verstärker: Ein einziger Konfigurationsfehler kann dazu führen, dass Tausende Systeme oder große Datenmengen dem Risiko eines Angriffs ausgesetzt werden. Nicht selten bleiben inkorrekte oder nicht Compliance-konforme Cloud-Konfigurationen sogar über lange Zeiträume unerkannt, denn die Vielzahl der eingesetzten Services und der Mangel an Cloud-spezifischem Sicherheits-Know-how erschweren die Identifikation von Risiken.

Im Jahr 2023 werden 99 Prozent aller Cloud-Sicherheitsvorfälle auf Fehlkonfigurationen durch Kunden zurückgehen.[1]

[1] Gartner, Innovation Insight for Cloud Security Posture Management, Februar 2019

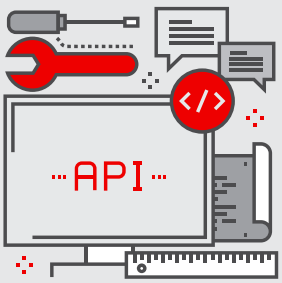
Wie verbreitet dieses Problem ist, zeigt eine interne Studie von Trend Micro: Pro Tag identifiziert die Lösung Trend Micro Cloud One – Conformity durchschnittlich 230 Millionen Fehlkonfigurationen[2], die Zugangsdaten und Betriebsgeheimnisse von Unternehmen gefährden. Erfahrungen aus der jüngsten Vergangenheit haben gezeigt, dass Kriminelle diese Fehlkonfigurationen für Ransomware-Angriffe, Krypto-Mining und den Diebstahl von Zahlungs- und Unternehmensdaten nutzen. Viele Unternehmen sind sich mittlerweile dieser Gefahr bewusst: Laut einer Studie des Marktforschungsinstituts ESG Research gaben 47 Prozent der befragten Unternehmen an, dass die Identifikation von nicht Compliance-konformen Workload Konfigurationen die wichtigste Sicherheitsherausforderung darstellt.[3]

[2] Trend Micro, Untangling the Web of Cloud Security Threats, April 2020
[3] ESG Research, Leveraging DevSecOps to Secure Cloud Native Applications, Juli 2019

KONFIGURATION IST KUNDENVERANTWORTUNG

Die Verantwortung für Cloud-Sicherheit und Compliance liegt nicht bei einer Einzelpartei, sondern wird von Cloud Service Providern (CSPs) und deren Kunden geteilt. Dieses Modell führt immer wieder zu Unklarheiten: Interne Sicherheitsteams erwarten vom Provider die Bereitstellung von Kontrollmechanismen und das Monitoring bestimmter Aspekte, obwohl diese Bereiche in die Verantwortung des Unternehmens fallen.

Ein häufig anzutreffendes Beispiel hierfür ist die Verwendung virtueller Maschinen oder Instanzen in der Cloud mit einem vorkonfigurierten Bereitstellungsdienst. In diesem Fall hat der Cloud Provider die Schritte vereinfacht, die für den Start gängiger Konfigurationen in der Cloud erforderlich sind. Doch sobald eine Konfiguration läuft, liegt die Sicherheitsverantwortung beim Unternehmensteam.



Als inoffizielle Trennlinie zwischen den Verantwortungsbereichen von Providern und Kunden wird oftmals die API-Oberfläche herangezogen. Cloud-Konfigurationen werden über die bereitgestellte API implementiert und fallen dementsprechend in die Verantwortung des Kunden.

WARUM IST DIE KORREKTE CLOUD-KONFIGURATION SO SCHWIERIG?

Unternehmen verlagern eine stetig wachsende Zahl von Services in die Public Cloud, während Cloud Service Provider gleichzeitig immer mehr Infrastruktur- und Plattform-Services einführen, auf die Entwickler direkt zugreifen können. Ob dabei durch die Konfiguration dieser Services neue Risiken entstehen und wo diese liegen, kann mit herkömmlichen Methoden kaum noch beantwortet werden. So erstrecken sich zum Beispiel das Setup und die Konfiguration von Amazon Web Services über mehr als 160 verschiedene Services, die jeweils über eigene granulare Autorisierungsrichtlinien verfügen. Eine manuelle Überprüfung der Sicherheit ist hier nahezu unmöglich. Häufig beobachtbare Fehler sind unter anderem:

Fehlkonfigurationen, zum Beispiel von AWS Security Groups für EC2 Server-Instanzen. Security Groups unterstützen die Sicherheit auf der Port- und Protokoll-Access-Ebene. Durch Fehlkonfigurationen einer Security Group können Angreifer unter Umständen auf cloudbasierte Server zugreifen und Daten ausschleusen. Oftmals wird zum Beispiel im Rahmen von Debugging- oder Troubleshooting-Aktivtäten der Internet-Zugriff auf einen Server über den SSH Port (22) eingerichtet, sodass Angreifer deutlich leichteres Spiel haben.

Unzureichende Zugriffsbeschränkungen, wie zum Beispiel bei den sehr verbreiteten AWS S3 Buckets mit Public Access. Diese werden von Angreifern routinemäßig für den Diebstahl kritischer Daten ausgenutzt. In einigen Fällen ist sogar der Schreibzugriff auf den Cloud Account möglich.

Fehlende Berechtigungssteuerung kann oftmals zu Sicherheitsrisiken führen, wenn Unternehmen die Rechte von Individuen und Service-Accounts nicht auf das erforderliche Minimum begrenzen (Least Privilege Principle).

Im Jahr 2021 werden 50 Prozent der Unternehmen unwissentlich und versehentlich IaaS Storage Services, Netzwerksegmente, Applikationen oder APIs verwenden, die zum Internet hin offen sind. Dies entspricht einer Steigerung von 25 Prozent im Vergleich zum YE2018.[4]

[4] Gartner, Innovation Insight for Cloud Security Posture Management, Februar 2019

Die schiere Anzahl zu schützender Cloud Services ist aber nicht das einzige Problem. Hinzu kommen anderen Faktoren, darunter die oftmals unzureichende Sichtbarkeit über Enterprise-Cloud-Bereitstellungen hinweg und das schnelle Hinzufügen neuer Systeme und Services in hoch dynamischen Umgebungen. Die Verbreitung von Multi-Cloud-Strategien, bei denen unterschiedliche IaaS- und PaaS-Provider zum Einsatz kommen, führt absehbar zu noch größerer Komplexität.

WEITERE FAKTOREN: SERVERLESS PAAS UND DEVOPS

Bei Serverless PaaS (z.B. AWS Lambda und Azure Functions) laden Entwickler ausschließlich ihren Programmcode in die Cloud, eine separate Konfiguration der genutzten Cloud-Ressourcen ist nicht erforderlich. Gleichzeitig entfallen traditionelle Kontrollpunkte der IT-Sicherheit wie das Betriebssystem oder die VM, sodass absolut korrekte Konfigurationen umso wichtiger werden.

IaaS und PaaS ermöglichen Entwicklern quasi die Selbstbedienung. Damit verliert die IT-Sicherheit die Aufsicht über Planung und Bereitstellung. Entwickler sind aber keine Sicherheitsexperten und sollten nicht dazu gezwungen sein, risikobehaftete Entscheidungen über Verschlüsselung, Service-Autorisierung usw. zu treffen, ansonsten sind Fehler und nicht korrekte Konfigurationen unvermeidbar.

Durch agile Entwicklungsmethoden wie DevOps, die den Fokus auf Geschwindigkeit legen, entstehen weitere Probleme. Herkömmliche Sicherheitsverfahren können mit den häufigen Code-Iterationen nicht Schritt halten. Hier ist ein neuer Ansatz erforderlich, der Sicherheit direkt in die DevOps-Pipeline integriert.

CLOUD SECURITY POSTURE MANAGEMENT

Cloud Security Posture Management (CSPM) ermöglicht die kontinuierliche Erkennung und Vermeidung von Risiken sowie die angepasste Reaktion in Echtzeit und über die Gesamtheit der eingesetzten Cloud-Infrastruktur hinweg. CSPM nutzt dafür in der Regel die APIs der Cloud-Plattformen und verzichtet auf Agenten.

Aufgrund der kritischen Bedeutung von CSPM Funktionalitäten und der fortlaufenden Veröffentlichung von Cloud-Sicherheitsvorfällen, die auf inkorrekte Konfigurationen und andere Fehler zurückgehen, wird [...] die Adoption Rate bis 2021 auf 20 Prozent steigen (im Vergleich zu 5 Prozent / YE2018).[6]

[6] Gartner, Innovation Insight for Cloud Security Posture Management, Februar 2019

Basis für die Risikobewertung ist der permanente Abgleich mit zentralen Frameworks (z.B. AWS Well-Architected Framework), regulatorischen Anforderungen, branchenspezifischen Best Practices und Unternehmensrichtlinien. Im Mittelpunkt steht die proaktive und reaktive Identifikation von potenziell riskanten Cloud-Service-Konfigurationen (z.B. Netzwerk- und Storage-Konfigurationen) und Sicherheitseinstellungen (z.B. Kontoberechtigungen und Verschlüsselung). Im Idealfall bietet das CSPM darüber hinaus Optionen für die automatisierte Behebung von Sicherheitsrisiken. CSPM identifiziert unter anderem:

- Neue Cloud-Workloads und Services
- Cloud-Konfigurationen, die nicht den aktuellen Anforderungen an Compliance (DSGVO, NIST, HIPAA etc.), Best Practices und Frameworks oder Unternehmensrichtlinien entsprechen.
- Konten mit exzessiven Berechtigungen oder Konten mit unnötigen Rechten, die nie genutzt werden.
- Konten und Services ohne Multifaktor- oder starke Authentifizierung
- Fehlkonfigurierte Netzwerk-Konnektivität, die das erforderliche Minimum übersteigt.
- Workloads und Services mit direkter Internetkonnektivität.
- Datenspeicher mit direkter Internetanbindung / ohne Verschlüsselung-at-Rest.
- Zum Internet offene APIs

KONFORMITÄT MIT DEM AWS WELL-ARCHITECTED FRAMEWORK

Das AWS Well-Architected Framework unterstützt Cloud-Architekten bei der Entwicklung sicherer, leistungsstarker, ausfallsicherer und effizienter Infrastrukturen für ihre Anwendungen. Unternehmen können anhand des Frameworks ihre Architekturen bewerten und Designs implementieren, die sich nach Bedarf skalieren lassen. Das Framework ermöglicht einen ganzheitlichen Blick auf die Cloud-Umgebung und erleichtert die Identifikation und Priorisierung von Bereichen, in denen Aktionen erforderlich sind.

Die allgemeinen Entwurfsprinzipien und spezifischen Best Practices des AWS Well-Architected Frameworks sind in fünf Säulen zusammengefasst: Operational Excellence, Sicherheit, Zuverlässigkeit, Leistung & Effizienz sowie Kostenoptimierung. Durch ein CSPM kann die kontinuierliche Konformität der Cloud-Konfiguration mit den fünf Säulen sichergestellt werden. Dies geschieht auf Basis einer CSPM Regel-Datenbank, deren Breite und Tiefe entscheidend ist für die effektive Umsetzung und Kontrolle der Prinzipien des AWS Well-Architected Frameworks.

Säule des Well-Architected Framework	Umsetzung und Kontrolle durch CSPM Regeln (Beispiele)
Operational Excellence: Beständige Optimierung von Prozessen und Verfahren, Automation von Änderungen und Reaktionen auf Vorfälle	• Automatisches Management mit CloudFormation-Skripten • Löschung abgelaufener ACM-Zertifikate
Sicherheit: Vertraulichkeit und Datenintegrität, Rechteverwaltung, Schutz von Systemen und Erkennung von Sicherheitsvorfällen	• Kein Root-Account für tägliche Aufgaben • Multi-Faktor-Authentifizierung für Root-Accounts • Kein Public Access für S3 Buckets • Automatische Schlüsselrotation
Zuverlässigkeit: Verhinderung von System- und Anwendungsausfällen, schnelle Systemwiederherstellung	• Automatisierte Backups für RDS Instanzen • Verteilung von EC2 Instanzen über mehrere Verfügbarkeitszonen • Minimum von zwei EC2 Instanzen pro ELB
Leistung & Effizienz: Richtige Nutzung von Ressourcentypen, -größen und -volumen, Überwachung der Performance	• Begrenzung der CPU-Auslastung • Upgrades für überbeanspruchte EC2 Instanzen • Neueste Versionen der EC2 Instanzen
Kostenoptimierung: Ausgabenanalyse und Anpassung an Geschäftsanforderungen	• Nur wirklich benötigte Instanzen laufen, kein Idle-Status • Anpassung nicht ausgelasteter Instanzen

EVALUIERUNG VON CSPM WERKZEUGEN

Einige Anbieter stellen CSPM Werkzeuge in Form von VM Images bereit, die in der Cloud-Infrastruktur des Kunden installiert werden. Andere Anbieter ermöglichen CSPM als Cloud-Service, bei dem über Read-Only-Accounts auf die APIs des Cloud Service Providers zugegriffen wird. Die Häufigkeit der Überprüfungen sowie Trigger (z.B. Einrichtung eines neuen Storage Objects) sollten durch das Unternehmen festgelegt werden können. Darüber hinaus sind CSPM Assessment Daten extrem sensibel, denn sie können von Angreifern missbraucht werden. Kunden benötigen daher direkte Kontrolle über ihre Daten, was insbesondere auch bei CSPM SaaS-Lösungen gewährleistet sein muss.

BREITE UNTERSTÜTZUNG FÜR CLOUD SERVICE PROVIDER

Die meisten CSPM Lösungen haben einen Kompetenzschwerpunkt beim Assessment von AWS, denn hier liegt derzeit der Großteil der IaaS Workloads. Darüber hinaus haben einige Anbieter auch Unterstützung für Microsoft Azure eingeführt. Noch wesentlich seltener anzutreffen ist hingegen die Unterstützung für das Assessment von Google Cloud Platform und VMware on-premises. Multi-Cloud-Strategien mit mehreren Cloud Service Providern werden in der Zukunft von den meisten Unternehmen genutzt werden, sodass eine breite Unterstützung der wichtigsten Cloud Services (oder eine konkrete Roadmap) in die Evaluierung einbezogen werden sollte.

BREITE UNTERSTÜTZUNG FÜR SERVICES UND COMPLIANCE-FRAMEWORKS

Nicht alle CSPM Angebote mit nominaler Unterstützung für einen Cloud Service Provider decken auch wirklich das gesamte Dienstspektrum ab, das sich zum Beispiel bei AWS auf über 160 Services erstreckt. Unzureichende Abdeckung kann hier zu blinden Flecken führen. Entscheidend ist daher der Umfang der Regel-Datenbank des CSPM und die Häufigkeit der Aktualisierung.

Je nach Unternehmensanforderungen ist darüber hinaus die detaillierte Unterstützung von Compliance-Frameworks wie PCI DSS, HIPAA, NIST, DSGVO und anderen Regularien ein weiterer wichtiger Evaluierungsfaktor.

GEFÜHRTE PROBLEMBEHEBUNG UND SELBSTREPARATUR

Für eine effiziente Problembehebung muss das CSPM klare und detaillierte Schritt-für-Schritt-Anleitungen bereitstellen, die sicher durch die Konfiguration führen. Zusätzliche Funktionen für eine automatisierte Selbstreparatur sind unbedingt erforderlich, um schnell auf akute Risiken reagieren zu können. Automatisch korrigierte Fehler müssen in Reporte aufgenommen werden, um die Implementierung von Best Practices zu unterstützen.

UNTERSTÜTZUNG DER CI/CD PIPELINE

Einige CSPM Werkzeuge ermöglichen die Überprüfung von Cloud-Risiken schon in der Entwicklungspipeline. Dazu gehört zum Beispiel das Assessment von Chef, Puppet, Ansible, AWS CloudFormation, VMware vRealize Automation und ähnlichen Scriptingsprachen / Frameworks für die Erstellung von Cloud-Umgebungen. Risikobehafte oder nicht Compliance-konforme Konfigurationen können damit zu einem frühen Zeitpunkt vor der Produktivphase identifiziert werden. Scan-Ergebnisse werden Entwicklern über Slack, JIRA oder das Developer Dashboard bereitgestellt.

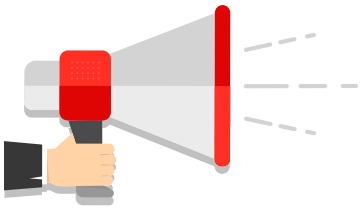
Organisationen, die ein CSPM implementieren, das sich auch auf die Entwicklung erstreckt, werden bis 2024 Cloud-Sicherheitsvorfälle aufgrund von Fehlkonfigurationen um 80 Prozent reduzieren.[7]

[7] Gartner, Innovation Insight for Cloud Security Posture Management, Februar 2019

ZENTRALES DASHBOARD MIT RISIKOPRIORISIERUNG

Cloud Security Architekten und CISOs benötigen die Möglichkeit, Snapshot-Ansichten zum Cloud-Risiko zu erstellen. Der CSPM Anbieter muss daher ein zentrales, rollen-basiertes Dashboard bieten, das in Echtzeit Auskunft über die gesamte Multi-Cloud-Infrastruktur gibt und Risiken priorisiert anzeigt. Reports müssen anpassbar sein und automatisch generiert und verteilt werden. Standard-Reports für häufige Compliance-Anforderungen erleichtern den Nachweis bei Audits.

6 EMPFEHLUNGEN FÜR DAS CLOUD SECURITY POSTURE MANAGEMENT



Sichtbarkeit für das CSPM steigern

CSPM Werkzeuge können nur überprüfen, was sie auch sehen. Unternehmen sollten daher die Verbreitung von Shadow IaaS / PaaS in ihrer Umgebung überwachen und minimieren. Dazu gehören zum Beispiel persönliche Entwickler-Accounts in AWS oder Azure.

Regelmäßige Account-Scans

Wenn mehrmals am Tag Services und Ressourcen bereitgestellt werden, muss das kontinuierliche Scanning aller Umgebungen und Instanzen in regelmäßigen Intervallen gewährleistet sein.

Investition in Präventivmaßnahmen

Sicherheitsrisiken in produktiven Umgebungen lassen sich vermeiden, indem etwas Zeit in das Scanning von Staging- bzw. Test-Accounts investiert wird, bevor Services und Ressourcen live bereitgestellt werden.

Überwachung in Echtzeit

Aktivitäten müssen in Echtzeit überwacht werden, damit ohne Verzögerung auf Bedrohungen reagiert werden kann. Nur durch permanentes Monitoring von Account-Aktivitäten ist bei verdächtigen Vorkommnissen eine sofortige Alarmierung möglich (auf Basis voreingestellter Konfigurationen).

Zeitnahe Kommunikation

Die Informationen aus dem Monitoring sind nutzlos, wenn sie nicht schnell die richtigen Personen erreichen. Zur reibungslosen Security Operation gehört daher die Übergabe von sicherheitsrelevanten Aktivitäten und Events an etablierte Informationskanäle wie JIRA, Email, SMS, Slack, PagerDuty, Zendesk, ServiceNow ITSM und Amazon SNS.

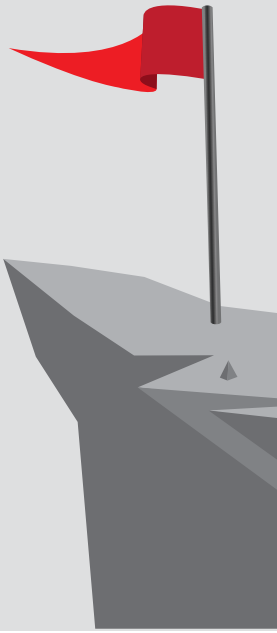
Unterstützte Problemauflösung

Auf Identifikation und Benachrichtigung folgt die eigentliche Behebung von Konfigurationsproblemen. Ein simpler Hinweis auf den Handlungsbedarf reicht hier nicht aus: Angesichts der Komplexität benötigt das IT-Personal klar strukturierte und einfach nachvollziehbare Lösungsschritte, sodass Konfigurationen auch ohne spezialisiertes Cloud-Security-Know-how durchgeführt werden können. Im Idealfall entsteht dadurch ein Lerneffekt, der die Kompetenzen des IT-Personals vertieft und zu einer aktiven Auseinandersetzung mit dem Thema motiviert.

TREND MICRO CLOUD ONE – CONFORMITY

Durch CSPM mit Trend Micro Cloud One - Conformity gewinnen Unternehmen die Gewissheit, dass innerhalb ihrer Cloud-Infrastruktur alle einschlägigen Compliance-Anforderungen, Best Practices und Branchenstandards zuverlässig umgesetzt werden – inklusive aktueller Anpassungen. Die SaaS (Software as a Service)-Plattform gewährleistet kontinuierliche Sicherheit, Compliance und Steuerung durch Identifikation und Behebung von Fehlkonfigurationen in der gesamten Multi-Cloud-Umgebung. Ein einziges, zentrales Multi-Cloud-Dashboard sorgt für vollständige Transparenz von AWS, Microsoft Azure und demnächst auch Google Cloud Platform Infrastrukturen in Echtzeit.

Herausforderung	Cloud One - Conformity
Vollständige, zentralisierte Sichtbarkeit der AWS oder Azure Infrastruktur	Eine einzige Oberfläche zeigt alle Risiken und Compliance-Verstöße in der Multi-Cloud
Überlastung durch zu viele Alarme und Schwierigkeiten bei der Priorisierung	Nahtlose Integration in bestehende Workflows mit Best-Practice-Priorisierung
Fehlendes Know-how zu AWS oder Azure	Klare Schritte zur Problemlösung auf Basis von AWS und Azure Best Practices
Permanente Veränderungen bei Compliance-Anforderungen und Branchenstandards	Kontinuierliche Überprüfung der Compliance mit aktuellen Standards wie DSGVO, PCI-DSS, NIST und anderen



Das Herzstück von Comformity ist eine branchenführende Knowledge Base mit mehr als 600 (Stand: Juli 2020) direkt verwendbaren Infrastrukturregeln und Kontrollen für AWS und Azure Accounts, die wöchentlich erweitert wird. Für eine besonders schnelle Auflösung akuter Risiken bietet Conformity eine Selbstreparaturfunktion mit mehr als 70 Steuerelementen für die automatische Problembehebung.

- Mehr als 600 Konfigurationskontrollen für AWS und Azure
- Compliance-Prüfungen für DSGVO, PCI DSS, NIST, HIPAA, CIS
- Kontrolle von Best Practices für das AWS Well-Architected Framework und CIS Microsoft Azure Foundations
- Integration in die CI/CD Pipeline
- Detaillierte Anleitungen zur Problembehebung und Selbstreparatur

Weitere Informationen zu Trend Micro Cloud One – Conformity unter:
https://www.trendmicro.com/de_de/business/products/hybrid-cloud/cloud-one-conformity.html

TREND MICRO
Securing Your Connected World

Copyright © 2020 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.