sysdig

WHITEPAPER

Eigene Anwendungen in der Cloud betreiben – aber sicher!

Eigene Anwendungen in der Cloud betreiben – aber sicher!

Meldungen über erfolgreiche Datendiebstähle, lahmgelegte IT-Infrastrukturen und andere Angriffe gibt es täglich in den Nachrichten. Immer öfter sind dabei Instanzen in der Cloud betroffen. Für alle Unternehmen, die selbst entwickelte Anwendungen in der Cloud betreiben, existiert ein neuer Ansatz, der auf die besonderen Sicherheitsherausforderungen in der Cloud ausgerichtet ist. Er ermöglicht eine blitzschnelle Reaktion auf Angriffe.

Moderne Anwendungen laufen in der Regel als native Cloud-Apps, also aufgeteilt in viele Microservices, die als Container innerhalb einer Virtualisierungslösung ausgeführt und von einem System wie Kubernetes orchestriert werden. Dieses Prinzip hat viele Vorteile, etwa gute Skalierbarkeit, Robustheit und Wartbarkeit. Allerdings stellen die Besonderheiten von Architektur und Laufzeitumgebung auch neue Anforderungen an die Sicherheit.

Bei nativen Cloud-Anwendungen muss Sicherheit neu gedacht werden

Allein schon durch ihre vielschichtige Architektur haben Cloud-Apps eine größere Angriffsfläche als monolithisch aufgebaute Anwendungen. Der Host, die Container, die Orchestrierungslösung, die Schnittstellen und die vielen Identitäten von Personen und Diensten – sie alle könnten eine verwundbare Flanke bieten, die es abzusichern gilt.

Die hohe Dynamik, die zur Innovationsfähigkeit der cloudnativen Anwendungen beiträgt, erweist sich bei der Sicherheit als weitere Erschwernis. Denn der hohe Automatisierungsgrad über CI/CD-Pipelines und die Verwendung vieler Open-Source-Komponenten bieten günstige Bedingungen für Angriffe über die Software-Lieferkette, etwa durch Ausnutzung bekannt gewordener Schwachstellen oder durch das Einschleusen von Schadcode über Software-Bibliotheken. Schätzungen zufolge weisen über 80 % der Container-Images große oder gar kritische Lücken auf.

Die Dynamik hat außerdem auch auf der Seite der Angreifer Einzug gehalten, was zur Beschleunigung der Attacken geführt hat. Noch vor wenigen Jahren galt im Bereich der Applikationssicherheit die Faustregel, dass man 60 Minuten Zeit hat, um einen Angriff zu erkennen und abzuwehren. An diesem Zeithorizont hatten die Administratoren ihre Konzepte ausgerichtet.

5-5-5 oder warum Agilität auch in die Cloud-Sicherheit einziehen muss

Doch die 60-Minuten-Regel ist inzwischen überholt. Automatisierung, Cloud-Skalierbarkeit und neue KI-Technologien ermöglichen es Angreifern, alle Phasen ihrer Angriffe erheblich zu beschleunigen und in wenigen Minuten Schaden anzurichten. Sicherheitsverantwortliche sollten sich daher stattdessen die von Sysdig eingeführte eingängige Formel „5-5-5" einprägen. Gemeint ist damit, dass ein Angriff innerhalb von fünf Sekunden erkannt, binnen fünf Minuten nach Schweregrad klassifiziert und innerhalb weiterer fünf Minuten darauf reagiert werden muss.

Diese Zeitspanne ist knapp bemessen, sollte aber von Unternehmen als unbedingt zu erreichendes Ziel gesetzt werden, nach dem alle Prozesse und Tools auszurichten sind. Dauert die Zeitspanne zwischen Erkennung und Bekämpfung eines Angriffs insgesamt länger als zehn Minuten, hat man den Kampf gegen Angreifer früher oder später verloren.

Gerade die ersten fünf Sekunden, in denen ein Angriff erkannt werden soll, erfordern einen direkten Einblick der eingesetzten Sicherheitstools in die Vitalparameter der laufenden Container. Methoden, Angriffe zum Beispiel nur durch Log-Auswertungen zu erkennen, reichen heutzutage angesichts der aktuellen Bedrohungslage nicht mehr aus.

Für die vielen genannten Herausforderungen cloudnativer Anwendungen in Sachen Sicherheit gibt es einzelne, spezialisierte Tools. Doch es ist schwierig, eine ganzheitliche Sicht auf die aktuellen Bedrohungen und die Sicherheitslage insgesamt zu erhalten. Weil die Zusammenführung und Bewertung der einzelnen Erkenntnisse in der Regel den Team-Mitgliedern überlassen bleibt, ist die Personalbelastung hoch, wodurch die Reaktionszeiten bei Vorfällen entsprechend lang ausfallen. Dem Problem durch personelle Verstärkung zu begegnen, ist ebenfalls schwierig. Denn weil jedes Unternehmen einen eigenen Werkzeugkasten für die verschiedenen Sicherheitsaspekte zusammengestellt hat, gibt es kaum Bewerbungen, die präzise auf das ausgeschriebene Profil passen – abgesehen davon, dass der Arbeitsmarkt ohnehin schon schwierig genug ist.

Ein Plattformansatz bietet sich als Lösung für Cloud Native an

Einmal mehr sind es die Analysten von Gartner, die unter dem Begriff „Cloud-Native Application Protection Platform" (CNAPP) der IT-Welt ein neues Konzept beschert haben. CNAPP wird vermutlich nicht nur eine kurzlebige Erscheinung bleiben, sondern länger Bestand haben. Im Kern geht es dabei weniger um Innovationen, sondern vielmehr um die Konsolidierung bereits bekannter Sicherheitskonzepte wie CSPM, CIEM, IAM oder CWPP, die bislang immer nur Erkenntnisse in einem Teilbereich ergeben haben. Der wichtigste Punkt von CNAPP ist also der Plattformansatz, der einen breiten Wirkungsbereich ermöglicht und sämtliche Sicherheitsaspekte nativer Cloud-Anwendungen berücksichtigen kann.

Neben der Konsolidierung ist bei CNAPP die Umsetzung des Prinzips „Shift left, shield right" ein wichtiger Gewinn. Zum Verständnis dieser bildhaften Beschreibung hilft es, sich den Lebenszyklus einer Anwendung oder einer neuen Programmversion auf dem Zeitstrahl vor Augen zu führen: Ganz links steht die Entwicklungsphase, dann kommen Tests und das Deployment, ganz rechts steht die fertige Anwendung. Während zur Laufzeit (also „rechts") die Anwendung vor allen Gefahren abgeschirmt wird, sollen sicherheitsrelevante Prozesse, Werkzeuge oder Kenntnisse über Gefahren und Verwundbarkeiten nach „links" und damit in die Entwicklungsphase verschoben werden – was auch dem Grundgedanken von DevSecOps entspricht. So wird eine frühe Erkennung von Problemen erreicht und ein proaktives statt rein reaktives Vorgehen gefördert. Der schützende „Schild" zur Laufzeit der Anwendungen besteht bei CNAPP aus der Überwachung von Sicherheitsbedrohungen und der Anwendung der bekannten Mechanismen zur Verhinderung von Sicherheitsvorfällen.

Nicht erkannte Probleme sind für Sicherheitsteams eine Herausforderung. Dasselbe gilt allerdings auch für das Gegenteil: Wenn zu viele Warnmeldungen eintreffen, fällt es den Teams schwer, sich auf diejenigen zu konzentrieren, hinter denen die tatsächlichen Bedrohungen lauern. Das gilt vor allem dann, wenn Sicherheitswerkzeuge zum Zuge kommen, die jede Schwachstelle, jede Fehlkonfiguration und jede Drift melden, statt das hervorzuheben, was ein tatsächliches Risiko darstellt. Die Überlastung des Security-Teams mit solchen Meldungen und die daraus resultierende Alarmmüdigkeit verzögern dann den Transfer der Erkenntnisse in die Programmentwicklung, also das „Shift left". Dieser Zeitverzug wiederum vergrößert die Gefahren zur Laufzeit, denn Angreifer könnten bereits die Kontrolle übernommen haben. Die Gefahrenerkennung und die Reaktion sollten in Echtzeit passieren, damit die Sicherheit gewahrt bleibt.

Der einzig sinnvolle Weg, dies zu erreichen, ist ein Ansatz, bei dem die Sicherheitslösung kompletten Einblick in alle relevanten Datenquellen und umfangreiche Kontrollmöglichkeiten hat. Dazu gehören:

- **Informationen über die Nutzung von Komponenten zur Laufzeit** – erst dann kann z. B. entschieden werden, ob eine bekannt gewordene Schwachstelle in einem Software-Modul überhaupt eine echte Gefahr darstellt.
- **Automatisches Stoppen erkannter Angriffe** (statt wie bisher Probleme erst im Nachgang zu analysieren) – dadurch wird die zeitliche Sichtbarkeitslücke geschlossen, die immer dazu führt, dass der Schaden noch größer wird.
- **End-to-End-Sicht mit Verknüpfung von Erkenntnissen aller Art** – dazu gehören Workloads, Identitäten und das gesamte Verhalten der Cloud-Anwendung; nur so lässt sich fortgeschrittenen Angreifern begegnen, die sich quer durch die Umgebung fortbewegen.

CNAPP bietet die Voraussetzungen dafür. Die jeweilige Plattform muss diese Vorteile aber auch tatsächlich nutzen und aus der Flut von Meldungen diejenigen herauspicken, die tatsächlich im Moment relevant sind.

Funktionen und Kriterien einer leistungsstarken CNAPP-Lösung

Es kommt darauf an, dass die jeweilige Lösung das End-to-End-Prinzip sowohl in der Breite als auch in der Tiefe umsetzt. Die Breite definiert sich über die im Cloud-Kontext wichtigen Instanzen: die Container, Cloud-Dienste, Hosts, Identitäten und die Software-Lieferkette. Doch nötig ist ebenso, dass die Lösung in die Tiefe geht und das ganze Arsenal an sinnvollen Funktionen ausschöpft, etwa regelbasiertes Erkennen (z. B. über die bewährte Open-Source-Lösung Falco), Drift-Vermeidung, Threat-Intelligence-Feeds oder Methoden künstlicher Intelligenz. Wichtig ist auch, dass der Hersteller ein kompetentes Team von Fachleuten aufgestellt hat, das ständig Erkenntnisse über aktuelle Bedrohungen sammelt und diese Erkenntnisse per Feed allen Kundensystemen zukommen lässt.

Zur Gewinnung der Informationen, die eine CNAPP-Lösung für ihre Auswertungen benötigt, gibt es grundsätzlich zwei unterschiedliche Ansätze. Bei der Variante ohne Agenten (agentless) bekommt die Lösung diese Daten allein durch das Anzapfen verfügbarer Datenquellen, etwa der APIs der Cloud-Verwaltung, aus

Kubernetes-Audit-Logs oder aus klassischen Log-Dateien. Der Einsatz von Agenten bedeutet dagegen, dass innerhalb der zu untersuchenden Objekte – der Container oder der Cloud-Umgebung – Hilfsprogramme installiert werden, die spezielle Informationen sammeln und an die Sicherheitslösung weiterreichen.

Ohne Agenten lassen sich zwar gut Informationen (z. B. über Cloud- und Netzwerkkonfigurationen) einholen oder durch Analyse der enthaltenen Software-Komponenten bekannte Schwachstellen aufspüren. Die Methode ist von der Bereitstellung her einfach und erzeugt wenig Overhead, weil sie die Workloads nicht direkt beeinflusst. Der Nutzen der agentenlosen Methoden ist allerdings eng an die Möglichkeiten geknüpft, die der Cloud-Provider anbietet. Geben dessen APIs nur sparsame Auskünfte, bekommt die CNAPP weniger Einblick. In manchen Umgebungen ist die agentenlose Variante allerdings die einzig mögliche Arbeitsweise. In Amazon ECR oder AWS funktioniert der Einsatz von agentenbasierten Datenquellen z. B. nicht.

Wo Agenten einsetzbar sind – und das ist eher der Regelfall –, ergeben sich daraus tiefergehende Echtzeiteinblicke in die laufenden Anwendungen (sog. „Runtime Insights"); sichtbar werden damit etwa auftretende Drifts oder die Abhängigkeiten zwischen den derzeit aktiven Prozessen. Die Agenten lassen sich nahe an den zu überwachenden Objekten platzieren, wodurch sie in Echtzeit leicht auf alle relevanten Daten zugreifen können. Ohne Agenten wäre es z. B. nicht möglich, Drift-Kontrolle in Echtzeit durchzuführen. Das bedeutet: Wenn Manipulationen an einem laufenden Container – etwa durch das Einloggen in die Shell des Containers – festgestellt werden, kann das System den Container automatisch herunterfahren und eine neue, unmanipulierte Instanz starten.

Die Agenten verwenden beispielsweise eBPF, um Systemaufrufe effizient und mit minimalen Leistungseinbußen zu überwachen. Trotzdem bremsen Agenten die Anwendungen ein wenig aus, weshalb ein ausschließlicher und umfangreicher Einsatz keinen Sinn ergeben würde. Darum ist es wichtig, dass die gewählte CNAPP-Lösung einen guten Mittelweg zwischen der Datengewinnung mit und ohne Agenten wählt, bei dem keine blinden Flecken entstehen und trotzdem die Leistung der Workloads nicht leidet.

Continuous Monitoring – klingt besser, als es ist

Bei Produkten, die agentenlos arbeiten und mit der Fähigkeit „Continuous Monitoring“ beworben werden, ist Vorsicht angebracht. „Kontinuierliche Überwachung“ klingt zwar gut, tatsächlich stecken dahinter meist aber lediglich periodische Scans des Systemstatus. Dieser wird dann mit dem vorhergehenden verglichen, sodass Abweichungen erkennbar werden. Je nach Abfragefrequenz ist diese Methode zu schwerfällig, um einen laufenden Angriff überhaupt erkennen zu können. Gerade wegen der kurzen Lebenszeiten von Containern ist das Risiko groß, dass die Security-Teams blind für gefährliche Situationen bleiben. Nur ein Echtzeitansatz kann hier den nötigen Einblick bieten.

Wichtig ist auch die Korrelation der Daten aus den Varianten mit und ohne Agenten. Dann kann die CNAPP z. B. die Informationen aus dem Kubernetes-Audit-Log und aus der agentenbasierten Überwachung der Systemaufrufe des Host-Systems zusammenführen und auf diese Weise erfahren, wann und wodurch ein bestimmter Container gestartet wurde und was während seiner Laufzeit passiert ist. Die Datenanreicherung geht bei Lösungen wie der Plattform von Sysdig sogar noch weiter, indem dort auch Drittanbieterdaten einfließen, etwa von der Identitätsplattform Okta. Auf diese Weise ergibt sich ein vollständiges Bild der Sicherheitslage. Nur durch diese umfassende Korrelation ist es einem CNAPP möglich, das zweite Ziel der 5-5-5-Regel zu erreichen und innerhalb von 5 Minuten nach Erkennen eines potenziellen Angriffs die richtigen Schlüsse zu ziehen und gegebenenfalls Abwehrmaßnahmen einzuleiten.

Viele Bedrohungen, gegen die sich Unternehmen und Organisationen wappnen müssen, kommen gar nicht in der Form einer aktiven Attacke, sondern schleichen sich über die Software-Lieferkette ein. Denn immer mehr Anwendungen setzen auf Open-Source-Komponenten, gerade im containerisierten Cloud-Umfeld. Wenn nun jemand die Kontrolle über ein GitHub-Repository erlangt und dort schädlichen Code einbaut, wird dieser über das nächste Update in die Anwendungen eingeschleust. Dagegen hilft es, wenn der CNAPP-Hersteller verdächtige Veränderungen an Repositorys erkennt und die Entwicklungsteams davor schützt, dass Malware auf diesem Weg in ihre Anwendungen gelangt.

Einige CNAPP-Lösungen bieten darüber hinaus erweiterte Ansichten der aktuellen Lage, die sonst unsichtbare oder unklare Details ans Tageslicht bringen. So kann ein Process Tree z. B. Sequenzen von Prozessaufrufen mit Kontext anzeigen, etwa in Bezug auf ein ausgewähltes User-Konto. Dadurch ergibt sich die Möglichkeit, eine Attack Journey zu zeigen, also die visualisierte Verkettung einzelner Schritte, die erst in ihrer Gesamtheit als Angriff erkennbar werden. Das könnte z. B. ein von einem Java-Prozess ausgelöster Netcat-Aufruf sein, dessen Resultat unter einem anonymen User-Konto als weiterer Prozess gestartet wird. Während jede der einzelnen Aktionen für sich genommen keine große Sicherheitsverletzung darstellt, zeigt die Verknüpfung verdächtige Muster klar und deutlich.

FAZIT:

CNAPP ist eine Strategieentscheidung

CNAPP macht sicher nicht alle Sicherheitswerkzeuge obsolet, die bereits im Einsatz sind – das gilt besonders für Unternehmen, die ihre Workloads zumindest teilweise noch länger on premises betreiben werden. Die Optionen zur Konsolidierung ermöglichen eine effizientere und umfassendere Überwachung der Anwendungssicherheit, was den Übergang zu CNAPP nahezu unvermeidlich macht. Unternehmen sollten die Wahl des Produkts allerdings mit viel Sorgfalt angehen, weil diese Lösung sie ziemlich sicher noch viele Jahre begleiten wird.

Glossar

CIEM
Das **Cloud Infrastructure Entitlement Management** überwacht Berechtigungen und Aktivitäten, um Datenpannen in Public Clouds zu verhindern.

CDR
Cloud Detection and Response ist der Kern einer CNAPP. CDR ist für die Bedrohungserkennung und für Reaktionen zuständig. Es ist das Gegenstück zu EDR (Endpoint Detection and Response), dessen Wirkungsbereich ein Endpunktsystem ist, etwa ein Arbeitsplatz-PC.

CI/CD
Continuous Integration/Continuous Delivery ist eine DevOps-Praxis, die fortlaufend einzelne Komponenten zu einem Hauptstrang fügt (kontinuierliche Integration) und Neuerungen ebenso fließend in die Produktion gibt (kontinuierliche Bereitstellung).

CNAPP
Cloud-Native Application Protection Platform ist ein von Gartner geprägter, breiter Ansatz zur Absicherung von cloudnativen Anwendungen.

CSPM
Mithilfe von **Cloud Security Posture Management** werden Fehlkonfigurationen und Compliance-Risiken in der Cloud-Konfiguration erkannt und behoben.

Viele Informationen hierzu finden Sie auf
https://sysdig.com/555-benchmark/

CWPP
Eine **Cloud Workload Protection Platform** überwacht ständig die Ausführung aller Container und ihre Host-Umgebung, identifiziert Probleme und behebt sie.

DevSecOps
Das Konzept von DevOps, also der optimierten Verschränkung der Prozesse von Entwicklung (Development) und IT-Betrieb (IT Operations), wird mit DevSecOps noch um den Bereich Security erweitert.

IAM
Ein **Identity and Access Management** ermöglicht die zentrale Verwaltung von Identitäten und deren Zugriffen auf Ressourcen und Anwendungen. Damit können User, Rollen und Berechtigungen wirksam gemanagt und dokumentiert werden.

eBPF
Die Sicherheitsarchitektur **extended Berkeley Packet Filter** arbeitet mit dem Konzept einer virtuellen Maschine, die im Kernel residiert und über klar definierte Schnittstellen mit dem Host-System kommunizieren kann. Dieses flexible Konzept ermöglicht Lösungen fürs Tracing oder für Firewalls, die kaum Performance-Einbußen mit sich bringen.

Über Sysdig

In der Cloud zählt jede Sekunde. Angriffe erfolgen mit Höchstgeschwindigkeit, und Sicherheitsteams müssen das Unternehmen schützen, ohne es zu verlangsamen. Sysdig stoppt Cloud-Angriffe in Echtzeit durch die sofortige Erkennung von Risikoveränderungen mithilfe von Runtime Intelligence und der Open-Source-Software Falco. Sysdig korreliert Signale über Cloud-Workloads, Identitäten und Services hinweg, um versteckte Angriffspfade aufzudecken und echte Risiken zu priorisieren. Von der Prävention bis zur Abwehr hilft Sysdig Unternehmen, sich auf das Wesentliche zu konzentrieren: Innovation.

Sysdig - Secure Every Second

Kontaktieren Sie uns