Warum und wie Sie den Laufzeitschutz in Ihre Cloud-Sicherheitsstrategie einbeziehen sollten

Cloudnative Technologien wie Container und serverlose Funktionen sind heutzutage keine wirklich neuen Ideen mehr. Schließlich sind sie seit fast 10 Jahren in ihrer aktuellen Form verfügbar. Docker gibt es beispielsweise seit 2013 und die serverlosen Funktionen von AWS Lambda seit 2014.

Was sich derzeit rasant ändert, ist die Geschwindigkeit, mit der cloudnative Technologien in die Produktion überführt werden. Einem Bericht vom März 2020 zufolge liefen beispielsweise in 29 Prozent der untersuchten Unternehmen mehr als die Hälfte der Produktionsanwendungen in Containern – und damit ca. 31 Prozent mehr als nur sechs Monate zuvor. Gartner prognostiziert, dass 70 Prozent der Unternehmen bis 2023 mindestens drei containerisierte Anwendungen nutzen werden. Und in einem Bericht von Forrester ist zu lesen, dass die stärkere Nutzung von Containern und anderen cloudnativen Technologien derzeit bei mehr als vier Fünfteln der CIOs auf der Prioritätenliste steht.

Diese schnelle Einführung cloudnativer Technologien hat zur Folge, dass DevSecOps-Tools und -Prozesse zum integralen Bestandteil des Entwicklungsprozesses werden. Das bedeutet wiederum, dass Teams zusätzliche Sicherheitsebenen implementieren, um diese cloudnativen Workloads in allen Etappen der CI/CD-Bereitstellungskette zu schützen.

Der wichtigste dieser neuen Ansätze ist der Laufzeitschutz. Er automatisiert den Schutz schnelllebiger, dynamischer Anwendungen (zum Beispiel in Containern) und wird damit den spezifischen Sicherheits- und Compliance-Anforderungen cloudnativer Umgebungen gerecht. Auf diese Weise können DevSecOps-Prozesse vollständig auf cloudnative Workloads angewendet werden.

Was ist Laufzeitschutz?

Unter Laufzeitschutz versteht man das lückenlose Monitoring und die Bewertung aller Aktivitäten in Containern, Hosts und serverlosen Funktionen.

Dazu wird zunächst anhand der Anwendungssteuerung und der Zulassungsliste für jeden Host und Container sowie jede serverlose Funktion und jedes andere Objekt in einer cloudnativen Umgebung ein Profil des normalen Verhaltens erstellt. Anschließend werden die Dateisysteme, Prozesse und Netzwerkaktivitäten in Echtzeit beobachtet, um verdächtige oder ungewöhnliche Aktivitäten zu erkennen und die zuständigen Teams bei Bedarf auf sie aufmerksam zu machen.

Das ist natürlich keine neue Idee. Plattformen für das Sicherheitsinformations- und Ereignismanagement (SIEM) sind schon seit Jahren in der Lage, Anwendungsumgebungen zu überwachen und solche Anomalien zu erkennen.

Das neue am cloudnativen Laufzeitschutz ist, dass dies in schnelllebigen Umgebungen geschieht, in denen es kein Normalverhalten im konventionellen Sinne gibt. Da Container und Instanzen serverloser Funktionen ständig hoch- und heruntergefahren werden und Load Balancer den Datenverkehr zwischen den verschiedenen Instanzen unentwegt umleiten, reichen herkömmliche Datenquellen wie Protokolle und der Netzwerkverkehr allein nicht aus, um Anomalien zu erkennen, die auf einen Sicherheitsverstoß hinweisen könnten. Daher geht man beim Laufzeitschutz tiefer und analysiert Verhaltenstrends und deren Entwicklung im Verlauf der Zeit, um ein dynamisches Verhaltensprofil zu erstellen. So können Sicherheitstools für den Laufzeitschutz Veränderungen in internen Containerprozessen, Dateisystemaktivitäten usw. erkennen, die von der Norm abweichen – auch in Umgebungen, die schnell hoch- und herunterskaliert werden.

Anders ausgedrückt beruht der Laufzeitschutz auf einer Reihe von Funktionen, die sowohl vorausschauenden als auch bedrohungsbasierten, aktiven Schutz für äußerst dynamische Umgebungen bieten.

Warum benötigen Sie Laufzeitschutz?

Der Laufzeitschutz ermöglicht die Anomalie-Erkennung in schnelllebigen Umgebungen und bietet damit eine Reihe von Vorteilen, die herkömmliche Monitoringtools in cloudnativen Umgebungen nicht bieten können.

Bedrohungserkennung in dynamischen Umgebungen

Der erste und wichtigste Vorteil ist, dass Laufzeitschutz die einzige praktikable Option für den skalierbaren Schutz cloudnativer Anwendungen ist. Wie bereits erwähnt ist es in schnelllebigen, verteilten Umgebungen schwierig, ein Profil des „normalen“ Verhaltens zu erstellen und dann Abweichungen von diesem Profil zu erkennen – insbesondere, wenn diese Umgebungen Hunderte von Containern und serverlosen Funktionen sowie Dutzende von Microservices beherbergen.

Beim Laufzeitschutz werden KI und maschinelles Lernen eingesetzt, um die Modellierung des gewünschten Verhaltens und die Anomalie-Erkennung zu automatisieren. So lässt sich diese Aufgabe auch in komplexen Umgebungen bewältigen, in denen menschliche Ingenieure das Normalverhalten nur mit großen Schwierigkeiten beschreiben könnten.

Prävention von Sicherheitsverstößen bzw. Beschränkung der Auswirkungen

Der Laufzeitschutz trägt zudem zur Härtung von Umgebungen gegen Schwachstellen bei. Mit Funktionen für den Laufzeitschutz haben Sie die Kontrolle über die Dateisysteme, Prozesse und Netzwerkaktivitäten für jeden Container und jede serverlose Funktion und können daher bei einem Sicherheitsverstoß in Ihrer Umgebung den Schaden begrenzen.

Zusätzlich können Tools für den Laufzeitschutz automatisch modellieren, welches Verhalten für Anwendungen ungefährlich ist, und Regeln durchsetzen, die gefährliche Aktivitäten in Containern und Hosts unterbinden. Somit sind Sie beispielsweise vor Szenarien geschützt, in denen manipulierte Container Prozesse ausführen, die Sicherheitsbedrohungen auf andere Container oder Hosts übertragen.

Unterstützung der Incident Response

Die von den Tools für den Laufzeitschutz erfassten Daten spielen auch bei der Reaktion auf Vorfälle (Incident Response) eine Rolle. Durch das Erfassen und Speichern von Auditdaten für cloudnative Anwendungen stellen diese Tools Sicherheitsteams die Informationen zur Verfügung, die sie benötigen, um Vorfälle zu rekonstruieren – selbst wenn die betroffene cloudnative Umgebung zum Zeitpunkt der Untersuchung nicht mehr (oder nur noch in stark veränderter Form) existiert.

Herausforderungen bei der Implementierung von Laufzeitschutz

Der Laufzeitschutz ist ein komplexes Konzept, dessen effiziente und effektive Implementierung aus mehreren Gründen schwierig sein kann. Die Herausforderungen sind nicht unüberwindbar, doch zu ihrer Bewältigung müssen Tools für den Laufzeitschutz für hochkomplexe moderne Umgebungen konzipiert werden.

Schnelllebige Umgebungen

Wie bereits erwähnt ist es aufgrund der sich ständig ändernden Konfiguration und Größe schwierig, ein aussagekräftiges Profil des Normalverhaltens einer cloudnativen Umgebung zu erstellen. Dabei müssen sehr viele Variablen berücksichtigt werden. Das Verkehrsmuster kann beispielsweise zu verschiedenen Tageszeiten und an verschiedenen Wochentagen sehr unterschiedlich aussehen. Die Art und Weise, wie Tools für die Containerorchestrierung mit Schwankungen in der Anwendungsnachfrage oder mit dem Ausfall einzelner Pods umgehen, spielt ebenfalls eine Rolle.

Diverse Technologien

Cloudnative Umgebungen umfassen ein ganzes Spektrum verschiedener Technologien, darunter Container, serverlose Funktionen, virtuelle Maschinen, Cloud-Dienste und mehr. Tools für den Laufzeitschutz müssen die architektonischen Merkmale und Verhaltensmuster jeder dieser Komponenten interpretieren und modellieren können, um gefährliches Verhalten zu unterbinden.

Das Risiko von Fehlalarmen

Es ist einfach, Warnmeldungen zu verschicken. Schwieriger ist es, sicherzustellen, dass jede Warnmeldung aussagekräftig ist, dass die Regeln für das Generieren von Warnmeldungen nicht veralten, wenn die Umgebung sich verändert, und dass manuell konfigurierte Regeln, die bislang wertvolle Warnmeldungen generiert haben, nicht plötzlich Fehlalarme versenden oder nicht greifen, wenn etwas gemeldet werden müsste.

Was können Sie vom Laufzeitschutz erwarten?

Eine korrekt implementierte Lösung für den Laufzeitschutz sollte die folgenden Kernfunktionen bereitstellen:

Automatische Modellierung des Anwendungsverhaltens

Ein Tool für den Laufzeitschutz muss automatisch erkennen können, wie sicheres Anwendungsverhalten aussieht. Wenn Sie Dutzende von Diensten verwalten müssen, die in Hunderten von Containern, serverlosen Funktionen und VMs gehostet werden, haben Sie keine Zeit, um von Hand Verhaltensmodelle zu erstellen oder auch nur die dafür erforderlichen Daten zusammenzutragen. Daher benötigen Sie Tools, die all dies automatisch erledigen.

Steuerung des Anwendungsverhaltens

Neben der Modellierung des erwünschten Anwendungsverhaltens sollte eine Lösung für den Laufzeitschutz auch automatisch definieren können, welche Verhaltensweisen für jeden Container, jede serverlose Funktion und jedes andere Objekt in der Umgebung erlaubt sind und welche nicht. Sie sollte zum Beispiel für jeden Container definieren, mit welchen anderen Containern er kommunizieren und auf welche Speichervolumes er zugreifen darf. Diese Regeln müssen konsequent durchgesetzt werden, um den bei einem etwaigen Sicherheitsverstoß entstehenden Schaden zu begrenzen.

Versand aussagekräftiger Warnmeldungen

Obwohl Tools für den Laufzeitschutz einige Gegenmaßnahmen automatisch einleiten können, müssen sie auch in der Lage sein, Ihr Team zu benachrichtigen, wenn ein menschlicher Eingriff erforderlich ist. Dazu müssen sie die cloudnative Infrastruktur überwachen und verdächtige Änderungen an Ressourcen wie Prozessen oder Netzwerkverbindungen sowie verdächtige Lese- oder Schreibzugriffe auf das Dateisystem melden.

Sie müssen auch in der Lage sein, anhand dynamischer Regeln zu entscheiden, ob sie eine Warnmeldung versenden sollten oder nicht. Ein und dieselbe Aktivität kann zu unterschiedlichen Zeiten ein Hinweis auf einen Sicherheitsverstoß oder völlig harmlos sein. Statische Regeln reichen daher nicht aus, um cloudnative Bedrohungen anzugehen.

Integration in andere Sicherheitslösungen

Der Laufzeitschutz ist nur eine Ebene in der mehrschichtigen Sicherheitsinfrastruktur, die im Sicherheitsstack Ihres Unternehmens implementiert sein sollte. Automatisierte Datensicherheitsmaßnahmen, Tools für Zugangskontrollen und Auditing, das Scannen von Container-Images und andere Sicherheitsvorkehrungen sind ebenso wichtig.

Lösungen für den Laufzeitschutz erzielen den größten Nutzen, wenn sie mit anderen Sicherheitstools verknüpft sind, um den Sicherheitsteams bei Vorfällen das maximale Maß an Detail- und Kontextinformationen zur Verfügung zu stellen und aufzuzeigen, wie sich eine Bedrohung auf einer Ebene des Technologiestacks (wie der Laufzeitumgebung) auf andere Komponenten (wie z. B. gespeicherte Daten) auswirkt.

Optimale Nutzung einer Laufzeitschutzlösung

Tools für den Laufzeitschutz bieten ein breites Spektrum an Funktionen an. Wie wertvoll diese Tools für Sie sind, hängt unter anderem von Ihrem Ansatz für den Laufzeitschutz ab. Streben Sie die folgenden Ziele an, um im vollen Umfang von Ihrer Lösung zu profitieren:

Vollständige Abdeckung

Wenn Sie nur einen Teil Ihrer Umgebung oder nur die wichtigsten Dienste in Ihrer Infrastruktur überwachen, können Sie nicht sicher sein, dass Sie alle Sicherheitsbedrohungen finden. Um die besten Ergebnisse zu erzielen, sollten Sie daher alle Ebenen Ihrer Infrastruktur durch Laufzeitschutz absichern, sowohl für die Produktions- als auch für die Entwicklungs- und Testumgebungen.

Vorfallserkennung in Echtzeit

Eine Lösung für den Laufzeitschutz kann im Falle einer Sicherheitsverletzung die Auswirkungen begrenzen. Wir empfehlen jedoch, sie vorrangig zur Erkennung und Behebung von Bedrohungen in Echtzeit zu verwenden, damit es gar nicht erst zu nennenswerten Schäden kommt.

Individuelle Behandlung jeder Ressource

Jeder Host, jede Containerinstanz, jede serverlose Funktion usw. in Ihrer cloudnativen Umgebung hat eine eigene Konfiguration und ein spezifisches Verhalten. Deshalb sollten Sie jede Ressource einzeln modellieren. Gehen Sie beispielsweise nicht davon aus, dass sich alle Container, die auf demselben Container-Image basieren, gleich verhalten. Das ist vom Ansatz her mit der Entnahme von Stichproben vergleichbar und führt zu einer ähnlich unvollständigen Übersicht über Sicherheitsvorfälle.

Laufzeitschutz mit Prisma® Cloud

Mit dem Einsatz cloudnativer Technologien wird der Laufzeitschutz zu einem kritischen Bestandteil Ihrer Sicherheitsstrategie. Sobald Sie in Lösungen wie Container, serverlose Funktionen und Cloud-Dienste investieren, sollten Sie Ihre Investitionen auch mit Maßnahmen für den Laufzeitschutz absichern.

Unsere umfassende, cloudnative Sicherheitsplattform Prisma Cloud enthält Lösungen für den Laufzeitschutz und ein breites Spektrum anderer Schutzmaßnahmen, wie Datensicherung, Zugangskontrollen und Funktionen zur Verwaltung des Cloud-Sicherheitsniveaus. Prisma Cloud ist für den Schutz aller cloudnativen Umgebungen geeignet, unabhängig davon, wie komplex sie sind und wie schnell sie skaliert werden. Fordern Sie eine Demo an, um mehr zu erfahren.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

prisma_wp_add-runtime-defense-cloud-security_041921