Einmaleins der Container-Sicherheit

DIE GRUNDLAGEN FÜR DEN SCHUTZ VON CONTAINERN

PRISMA
BY PALO ALTO NETWORKS

MediaOps

Mittlerweile wissen Cybersicherheitsteams in aller Welt: Der Container-Geist hat seine Flasche verlassen. Container kommen immer häufiger zum Einsatz, weil sie die Entwicklung und Bereitstellung sogenannter cloudnativer Anwendungen erheblich erleichtern. Dabei beseitigt als Container verpackter Code nicht nur einen Großteil der Reibungsverluste, die normalerweise bei der Übernahme von Anwendungscode aus der Test- in die Produktionsumgebung entstehen – er lässt sich zudem überall ausführen. Auch alle Abhängigkeiten einer Anwendung sind Teil des Containers. Dadurch wird eine containerisierte Anwendung hochgradig portabel und lässt sich auf virtuellen Maschinen genauso wie auf Bare-Metal-Servern in einem lokalen Rechenzentrum oder einer Public Cloud ausführen.

Diese hohe Flexibilität ermöglicht Entwicklern enorme Produktionssteigerungen, die nicht länger ignoriert werden können. Doch wie jede neue IT-Infrastruktur müssen auch cloudnative Anwendungen geschützt werden. Container-Umgebungen können eine Reihe von Schwachstellen aufweisen, beispielsweise Bilder, Container, Hosts, Runtimes, Registrys und Orchestrierungsplattformen, die allesamt geschützt werden müssen.

Für Unternehmen besteht die Herausforderung zunächst darin, herauszufinden, wie die vielen Ebenen einer cloudnativen Computing-Umgebung miteinander interagieren. Anschließend gilt es, die richtigen Tools zu entwickeln, um eine Reihe wiederholbarer Prozesse zur Sicherung jeder Ebene zu definieren. Mögliche Cybersicherheitsprobleme im Zusammenhang mit Containern:

IMAGES: Wie jeder andere Code-Bestandteil sind auch Container-Images mögliche Schwachstellen. Der Aufbau einer Bestandsliste, die Identifikation eingebetteter Geheimnisse oder die Klassifizierung aller Ebenen eines Images – mit all diesen grundlegenden Aufgaben müssen sich Cybersicherheitsteams noch auseinandersetzen. Richtig komplex wird es dann bei der fast unüberschaubaren Anzahl von Containern, die in einer Anwendungsumgebung ausgeführt und in sehr kurzen Abständen durch neue ersetzt werden. Dank der Verbreitung von DevOps-Praktiken können Unternehmen containerisierte Anwendungen heute mehrmals pro Woche aktualisieren. Bei jedem Update, das schnell mehrere tausend Container in einer IT-Umgebung umfassen kann, besteht die Gefahr, dass in dieser Umgebung Sicherheitslücken entstehen.

CONTAINER-REGISTRYS: Eine Container-Registry ist ein praktischer, zentraler Ort zum Speichern und Verteilen von Anwendungsimages. Unternehmen speichern heute nicht selten zehntausende Images in ihren Registrys. Da die Registry ein wesentlicher Bestandteil jeder containerisierten Umgebung ist, darf ihr Schutz nicht vernachlässigt werden. Eine Registry ist wichtig, um Ordnung in mögliches Container-Chaos zu bringen, kann aber auch eine Angriffsfläche für Cyberkriminelle bieten, die sich Zugang zur gesamten Umgebung verschaffen wollen. Die kontinuierliche Überwachung von Registrys auf mögliche Schwachstellen ist eine zentrale Sicherheitsvoraussetzung, welche auch die Sicherung des Servers beinhalten muss, auf dem die Registry gehostet wird.

CONTAINER RUNTIMES: Die Container-Runtime ist einer der am schwierigsten zu schützenden Teile eines Container-Stacks, da herkömmliche Sicherheitstools nicht für die Überwachung ausgeführter Container entwickelt wurden. Bestehende Tools können in der Regel nicht den Inhalt von Containern berücksichtigen, geschweige denn definieren, wie eine sichere Container-Umgebung aussieht. Bei Sicherheitsproblemen mit Container-Runtimes müssen sich die Cybersicherheitsteams auf Aspekte der Anwendungssicherheit konzentrieren, die von bestehenden Firewalls nicht abgedeckt werden.

CONTAINER-ORCHESTRIERUNG: Ähnlich wie der Zugriff auf bestehende IT-Umgebungen gehandhabt wird, muss auch die Zugriffskontrolle für Container-Orchestrierungsplattformen wie Kubernetes zur Vermeidung von Risiken durch überprivilegierte Konten, Angriffe über das Netzwerk und unerwünschte laterale Bewegungen um Whitelisting-Verfahren ergänzt werden. Eine Container-Orchestrierungsplattform unterscheidet sich davon insofern, als dass auch die Kommunikation zwischen Pods in einem Kubernetes-Cluster, das von mehreren Anwendungen genutzt wird, geschützt werden muss.

HOST-BETRIEBSSYSTEME: Das Betriebssystem Ihrer Container-Umgebung ist womöglich der wichtigste und am häufigsten übersehene Aspekt der Sicherung einer Container-Umgebung. Wenn es einem Angreifer gelingt, die Host-Umgebung zu kompromittieren, kann er sich Zugang zur gesamten Anwendungsumgebung verschaffen. Jeder Host muss daher über eigene Sicherheitszugriffskontrollen verfügen und kontinuierlich auf neue Schwachstellen überprüft werden, die seit der erstmaligen Bereitstellung des Hosts erkannt wurden.

DIE VORTEILE DER CYBERSICHERHEIT VON CONTAINERN

Angesichts all der Herausforderungen im Zusammenhang mit dem Schutz containerisierter Anwendungen ist es nachvollziehbar, dass so viele Experten für Cybersicherheit etwas zurückhaltend sind, was den Einsatz von Containern in einer Produktionsumgebung betrifft. Obwohl einige der Vorteile im Hinblick auf Produktivitätssteigerungen offensichtlich sind, erkennen viele Organisationen erst jetzt allmählich die Bedeutung der Tools und Prozesse, mit denen sich containerisierte Anwendungen schützen lassen. Auch wenn die Herausforderung gewaltig erscheint, so bieten Container einen strategischen Sicherheitsvorteil, den Cybersicherheitsteams tendenziell noch vernachlässigen. Da Container in der Regel schnell durch neue ersetzt werden, gestalten sich die Prozesse zur Beseitigung von Sicherheitslücken deutlich einfacher. Anstatt manchmal monatelang auf einen Patch für eine vollständige monolithische Anwendung warten zu müssen, werden neue Funktionen künftig durch den Austausch einzelner Container in einer Anwendungsumgebung umgesetzt.

Dieser Prozess beschränkt sich auf einen Teil der Anwendung, den sogenannten Microservice, und lässt sich in der Regel innerhalb von Minuten im Rahmen des Application-Lifecycle-Managements über eine Plattform für Continuous Integration (CI) bzw. Continuous Deployment (CD) wie Jenkins bewerkstelligen. Dadurch kann der Zeitraum, in dem eine Anwendung mit bekannten Schwachstellen in einer Produktionsumgebung ausgeführt wird, drastisch verkürzt werden

Diese Funktion ist wohl die treibende Kraft hinter den neuen DevSecOps-Prozessen, mit deren Hilfe Entwickler mehr Verantwortung für die Implementierung von Sicherheitskontrollen übernehmen können. Das Cybersicherheitsteam muss diese Kontrollen definieren und dafür sorgen, dass sie richtig umgesetzt werden. Da die Entwickler jedoch die Verantwortung für die Implementierung dieser Kontrollen tragen, nimmt die Zahl der Anwendungen, die eine Cybersicherheitsprüfung erfolgreich durchlaufen können, mit der fortschreitenden Reife der eingeführten DevSecOps-Prozesse stetig zu

PRISMA BY PALO ALTO NETWORKS | MediaOps

PRISMA BY PALO ALTO NETWORKS | MediaOps

TOOLS FÜR MEHR CONTAINER-SICHERHEIT

Allein im letzten Jahr sind die Tools, die Unternehmen den Schutz ihrer Container ermöglichen, sowohl funktionsreicher als auch differenzierter geworden. Unabhängig vom Reifegrad der DevSecOps-Prozesse sind Tools für Container-Sicherheit heute zugänglicher als je zuvor. Folgende Tools sollten von jedem Unternehmen eingesetzt und beherrscht werden:

CONTAINER-ÜBERWACHUNG: Tools zur Container-Überwachung sind ein zentraler Bestandteil der Maßnahmen zur Gewährleistung der Container-Sicherheit und haben die Aufgabe, die enorm flüchtigen, winzigen Computing-Einheiten zu verfolgen. Da Entwickler kontinuierlich Container durch neue ersetzen, sind Überwachungstools, mit denen Cybersicherheits- und IT-Teams Container mit Zeitmarkierungen versehen können, äußerst hilfreich, um herauszufinden, was genau sich wann in einer containerisierten Umgebung ereignet hat.

CONTAINER-SCANNING-TOOLS: Container müssen kontinuierlich auf Schwachstellen gescannt werden, und zwar sowohl vor der Bereitstellung in einer Produktionsumgebung als auch nachdem sie ersetzt wurden. Zu schnell passiert es, dass Entwickler aus Versehen eine Bibliothek mit bekannten Schwachstellen in einen Container einbinden. Auch darf nicht vergessen werden, dass beinahe täglich neue Sicherheitslücken bekannt werden. Demnach könnte sich ein heute noch komplett sicheres Container-Image schon morgen als Einfallstor für alle möglichen Arten von Malware erweisen.

CONTAINER-FIREWALLS: Eine Container-Firewall prüft und schützt den gesamten Datenverkehr zwischen den Containern und externen Netzwerken sowie bestehenden Anwendungen. Die meisten Container-Firewalls werden als sogenannte „Sidecars“ ausgeführt, mit denen ein breites Spektrum von Datenverkehr zwischen den aus mehreren Containern bestehenden Microservices abgedeckt werden kann.

RICHTLINIEN-ENGINES: Moderne Cybersicherheitstools ermöglichen Sicherheitsexperten die Definition von Richtlinien mit Whitelists für den Zugriff auf bestimmte Microservices. Unternehmen brauchen einen Rahmen, in dem sie zunächst diese Richtlinien definieren und anschließend sicherstellen können, dass die Richtlinien in der gesamten hochgradig dezentralen Container-Anwendungsumgebung konsequent durchgesetzt werden.

VERTEIDIGUNG DER HYBRIDEN ANGRIFFSFLÄCHE

Da Container den Einsatz containerisierter Anwendungen auf verschiedenen Plattformen ermöglichen, müssen Unternehmen in der Lage sein, zuerst geeignete Richtlinien für Cybersicherheit umzusetzen und dann mögliche Probleme im Hinblick auf die verschiedenen Plattformen zu beheben. Die meisten Container werden heute auf herkömmlichen virtuellen Maschinen bereitgestellt, um eine gewisse Trennung von Anwendungsworkloads auf der gleichen Plattform sicherzustellen.

Es gibt jedoch auch immer mehr Fälle, in denen Organisationen auf virtuelle Maschinen verzichten wollen, um den damit verbundenen Mehraufwand, der sich negativ auf die Anwendungsleistung auswirken kann, zu vermeiden. In diesen Szenarien stellen Entwickler ihre Container eher auf Bare-Metal-Servern oder auf Basis einer Reihe von zunehmend leichteren virtuellen Maschinen bereit. Dies gilt vor allem für Umgebungen mit Grafikprozessoren (GPUs), die andere Virtualisierungsmethoden als Container nicht unterstützen. Ein weiterer Grund für die Bereitstellung von Containern auf einem Bare-Metal-Server ist die Einsparung der Lizenzgebühren für kommerzielle Software für virtuelle Maschinen.

Unabhängig von den Beweggründen können Cybersicherheitsteams fest davon ausgehen, dass containerisierte Anwendungen sich sowohl lokal als auch in verschiedenen Public-Cloud-Umgebungen immer mehr etablieren werden. Jede Computing-Umgebung wird sich dabei aus mehreren Arten von virtuellen und physischen Maschinen zusammensetzen, auf denen Container ausgeführt werden, die alle über ein gemeinsames Framework geschützt werden müssen.

Noch komplizierter wird es durch die Tatsache, dass auf Containern basierende serverlose Computing-Frameworks eine weitere Angriffsfläche bieten, die es abzusichern gilt. Serverlose Computing-Frameworks auf Basis einer ereignisgesteuerten Architektur ermöglichen Entwicklern bei Bedarf den Aufruf untergeordneter Prozesse innerhalb ihrer Anwendungen. Dadurch entfällt die Notwendigkeit, für sporadisch auszuführende Funktionen eigenen Code in die Anwendung zu integrieren. Je weniger Code eine Anwendung enthält, desto einfacher lässt sie sich schützen. Wichtig ist jedoch, dass das serverlose Computing-Framework ausreichend gesichert wird.

CYBERSICHERHEIT: DER GROSSE WIDERSPRUCH

Bereits heute sind Millionen von Stellen im Bereich der Cybersicherheit unbesetzt. Da das Volumen des zu schützenden Anwendungscodes vor allem durch den zunehmenden Einsatz von Containern weiter exponentiell wächst, können Cybersicherheitsteams und Anwendungsentwickler mit dem Tempo der Veränderungen nur Schritt halten, wenn sie verstärkt auf Automatisierung setzen.

Selbst wenn der Mangel an Sicherheitsexperten komplett beseitigt würde, hätten die meisten Unternehmen nach wie vor Schwierigkeiten, genug Know-how aufzubauen und vor allem aufrechtzuerhalten. Die einzige Möglichkeit, die Auswirkungen von Personalfluktuationen im Bereich der Cybersicherheit zu begrenzen, ist die Automatisierung möglichst vieler manueller Prozesse. Dadurch wird nicht nur die Wahrung bestehender Richtlinien für Cybersicherheit einfacher. Die Cybersicherheitsteams haben auch mehr Zeit für Aufgaben wie die rechtzeitige Identifikation von Malware.

Künftig wird es also nicht mehr darum gehen, ob Sicherheitsaufgaben automatisiert werden, sondern wie und in welchem Ausmaß.

MIT VEREINTEN KRÄFTEN

Angesichts der zunehmenden Verbreitung des cloudnativen Computings in allen seinen auf Containern basierenden Formen besteht eindeutig die Notwendigkeit eines Konzepts für Cybersicherheit, das sich auf Container und zugehörige serverlose Computing-Frameworks anwenden lässt. Dieses Argument ist allerdings nicht auf cloudnative Computing-Anwendungen beschränkt. Cloudnative Computing-Anwendungen werden auf absehbare Zeit nicht den gesamten monolithischen Anwendungscode ersetzen. Noch bis Ende des nächsten Jahrzehnts werden Unternehmen aller Größen mit einer Mischung aus bestehenden und neuen cloudnativen Anwendungen arbeiten. Die nächste große Herausforderung für die Cybersicherheit wird darin bestehen, eine Möglichkeit zur Entwicklung und Durchsetzung von Cybersicherheitsrichtlinien in diesen Umgebungen über das gleiche Management-Framework zu finden.

Um dieses Ziel zu erreichen, hat Palo Alto Networks in diesem Jahr Twistlock, Entwickler einer Container-Sicherheitsplattform, sowie PureSec, Anbieter einer Lösung zur Sicherung serverloser Computing-Frameworks, übernommen. Palo Alto Networks hat bereits Millionen in die Entwicklung eines Prisma-Frameworks investiert, um die Steuerung der Cybersicherheit von bestehenden monolithischen Anwendungsumgebungen zu automatisieren. Heute wird die Prisma-Plattform kontinuierlich erweitert, um auch cloudnative Computing-Anwendungen auf Basis von Containern und serverlosen Computing-Frameworks zu unterstützen.

Dadurch wird Prisma zur bislang umfassendsten Lifecycle-Management-Plattform für Cybersicherheit.

FAZIT

Wie immer steht es ausgesprochen gut und zugleich schlecht um die Cybersicherheit. In vielerlei Hinsicht war ihre Gewährleistung noch nie so komplex wie heute, zumal auch die IT-Umgebungen immer heterogener werden. Gleichzeitig zieht aber auch das Tempo der Innovationen im Bereich der Cybersicherheit an.

Die wichtigste Sicherheitsentscheidung, die jede Organisation in den kommenden Monaten treffen muss, betrifft die Auswahl eines Anbieters, der nicht nur die Tools und das Know-how besitzt, um bestehende Umgebungen schützen zu können, sondern auch sichere neue Anwendungsumgebungen bietet, da sich die Entwickler trotz der anfänglichen Sicherheitsbedenken vieler Unternehmen verstärkt innovativen Plattformen zuwenden.

Wenn Sie mehr darüber erfahren möchten, wie Sie diese Umgebungen schützen können, besuchen Sie *www.paloaltonetworks.com/cloud-security*


PRISMA™
BY PALO ALTO NETWORKS