Sicherheitslücken durch Fehlkonfigurationen vermeiden

Containerisierung

Container-Technologien haben die IT-Landschaft revolutioniert, doch viele Unternehmen unterschätzen die Sicherheitsrisiken. Besonders im öffentlichen Sektor und Finanzwesen können falsche Konfigurationen zu schwerwiegenden Compliance-Verstößen führen.

Die Containerisierung hat sich in den letzten Jahren als Standardtechnologie für moderne Anwendungsbereitstellung etabliert. Docker und Kubernetes dominieren dabei die Landschaft und ermöglichen es Unternehmen, Anwendungen schneller und effizienter zu entwickeln und zu betreiben. Doch dieser Fortschritt bringt neue Sicherheitsherausforderungen mit sich, die viele Organisationen noch nicht ausreichend erkannt haben.

Die häufigsten Sicherheitsfallen. Aufgrund jahrelanger Beratungserfahrung in verschiedenen Branchen zeigen sich im Bereich Security immer wiederkehrende Muster: Die meisten Sicherheitsvorfälle entstehen nicht durch ausgefeilte komplexe Angriffe, sondern durch grundlegende Fehlkonfigurationen. Besonders problematisch ist dabei das Ausführen von Containern mit Root-Privilegien. Viele Entwickler-Teams nutzen standardmäßig Root-Benutzer in ihren Container-Images, da dies zunächst weniger Konfigurationsaufwand bedeutet. Jedoch öffnet diese Praxis Angreifern bei einem erfolgreichen Container-Escape direkten Zugang zum Host-System.

Ein weiterer kritischer Punkt ist die unzureichende Netzwerksegmentierung. Container kommunizieren standardmäßig über ein gemeinsames Netzwerk, wodurch lateral bewegende Angriffe möglich werden. In einem kürzlich beobachteten Fall konnte ein Angreifer durch eine kompromittierte Webanwendung auf eine interne Datenbank zugreifen, da beide Container im selben Netzwerk-Namespace liefen und keine Netzwerk-Policies implementiert waren.

Die Verwendung von Base-Images unbekannter Herkunft stellt ein oft unterschätztes Risiko dar. Viele Entwickler-Teams laden Images direkt aus öffentlichen Registries herunter, ohne deren Inhalt zu überprüfen. Diese Images können kompromittiert sein und Malware enthalten oder veraltete Software-Versionen mit bekannten Sicherheitslücken nutzen. Ein systematisches Image-Scanning und die Verwendung vertrauenswürdiger Base-Images sind daher unerlässlich.

Kubernetes-spezifische Herausforderungen. Kubernetes als Container-Orchestrierungsplattform bringt zusätzliche Komplexität mit sich. Die Role Based Access Control (RBAC) wird häufig zu permissiv konfiguriert. Anstatt granulare Berechtigungen zu vergeben, erhalten Service-Accounts oftmals administrative Rechte, was einem Generalschlüssel für das gesamte System entspricht.

Auch das Secret Management wird in der Regel vielfach vernachlässigt. Sensitive Daten wie Passwörter oder API-Schlüssel werden in Umgebungsvariablen gespeichert oder als Plain-Text in ConfigMaps hinterlegt. Diese Informationen sind dann für jeden sichtbar, der Zugriff auf die entsprechenden Namespaces hat.

Die Admission Controller, die als Sicherheits-Gatekeeper fungieren sollten, werden in vielen Installationen deaktiviert oder nur unzureichend konfiguriert. Pod Security Standards (PSS), die gefährliche Konfigurationen verhindern können, finden heute noch nicht flächendeckende Anwendung.

Compliance-Anforderungen im Fokus. Für Unternehmen im öffentlichen Sektor und Finanzbereich verschärfen sich die Anforderungen durch regulatorische Vorgaben wie NIS2, DORA oder MaRisk. Die DSGVO verlangt Datenschutz by Design, was bei Containern bedeutet, dass Sicherheitsmaßnahmen bereits bei der Entwicklung implementiert werden müssen. Die IT-Grundschutz-Kompendien des BSI fordern explizit die Härtung von Container-Umgebungen und regelmäßige Sicherheitsüberprüfungen.

Im Finanzsektor müssen zusätzlich die Anforderungen der BaFin bezüglich der Auslagerung von IT-Dienst-

Illustration: © Valery Brozhinsky, Ink Drop | shutterstock.com

*/ Die meisten Sicherheitsvorfälle entstehen nicht durch ausgefeilte komplexe Angriffe, sondern durch grundlegende Fehlkonfigurationen. Besonders problematisch ist dabei das Ausführen von Containern mit Root-Privilegien.

leistungen beachtet werden. Container-Deployments in Cloud-Umgebungen können unter diese Regelungen fallen und erfordern entsprechende Risikobeurteilungen und Kontrollen.

Shift-Left-Security: Sicherheit von Anfang an. Die Implementierung einer umfassenden Container-Sicherheitsstrategie folgt dem bewährten »Shift-Left-Security«-Ansatz, bei dem Sicherheitsmaßnahmen bereits in den frühesten Phasen des Entwicklungsprozesses integriert werden. Anstatt Sicherheit erst kurz vor der Produktionsfreigabe, dem Go-Live, zu berücksichtigen, werden potenzielle Risiken bereits beim Code-Design und der Container-Erstellung identifiziert und behoben.

Dieser Paradigmenwechsel bedeutet konkret, dass Entwickler schon während der Programmierung Sicherheits-Linting-Tools verwenden, die unsichere Code-Patterns erkennen. Static Application Security Testing (SAST) wird direkt in die integrierte Entwicklungsumgebung (IDE) eingefügt, sodass Sicherheitsprobleme in Echtzeit sichtbar werden. Es ist ratsam, Container-Images automatisiert in der CI/CD-Pipeline auf Schwachstellen zu scannen – idealerweise mit mehreren verschiedenen Scanning-Tools, um unterschiedliche Arten von Vulnerabilities abzudecken.

Lokale, verifizierte Image Registries bilden das Fundament einer sicheren Container-Supply-Chain. Anstatt Images direkt aus öffentlichen Registries zu verwenden, sollten Organisationen private Registries mit definierten Verifikationsprozessen implementieren. Registry Security stellt häufig einen Schwachpunkt in Kubernetes-Projekten dar, der übersehen wurde – ungesicherte Registries können Angreifern direkten Zugang zur gesamten Container-Infrastruktur ermöglichen. Image-Signierung und rollenbasierte Zugriffskontrolle sind daher unerlässlich.

Der Shift-Left-Ansatz reduziert nicht nur die Kosten für Sicherheitskorrekturen erheblich. Ein Fehler, der in der Entwicklung behoben wird, kostet nicht nur etwa 100-mal weniger als derselbe Fehler in der Produktion, sondern erhöht auch die Akzeptanz bei Entwicklungs-Teams, da Sicherheit nicht als nachgelagerter Blocker, sondern als integraler Bestandteil des Entwicklungsprozesses wahrgenommen wird.

Netzwerk-Policies sind unerlässlich für die Mikrosegmentierung. Jeder Container sollte nur mit den Services kommunizieren können, die für seine Funktion notwendig sind. Service-Mesh-Technologien ergänzen die Netzwerksicherheit durch automatische Verschlüsselung der Service-zu-Service-Kommunikation und granulare Traffic-Policies. Sie bieten erweiterte Sicherheitsfunktionen, die über Standard-Kubernetes-Network-Policies hinausgehen, einschließlich Mutual TLS (mTLS) für Zero-Trust-Kommunikation und detailliertes Monitoring des Netzwerkverkehrs zwischen Mikroservices.

Runtime-Sicherheit durch spezialisierte Monitoring-Tools ermöglicht die Erkennung anomaler Aktivitäten in laufenden Containern. Diese Lösungen können beispielsweise warnen, wenn ein Container unerwartet Netzwerkverbindungen aufbaut oder auf Dateisystembereiche zugreift, die normalerweise nicht verwendet werden.

Empfehlungen für die Praxis. Organisationen sollten eine Zero-Trust-Architektur implementieren, bei der jede Komponente standardmäßig als nicht vertrauenswürdig betrachtet wird. Dies bedeutet konkret: Minimale Berechtigungen für alle Container, Verschlüsselung der Kommunikation zwischen Services und kontinuierliche Überwachung aller Aktivitäten.

Die Implementierung von Pod-Security-Standards sollte schrittweise erfolgen, beginnend mit dem »Restricted«-Profil für neue Workloads. Bestehende Anwendungen lassen sich graduell migrieren, um Betriebsunterbrechungen zu vermeiden.

Regelmäßige Penetrationstests und Sicherheitsaudits sind besonders wichtig, da sich die Container-Landschaft schnell entwickelt und permanent neue Angriffsvektoren entstehen. Die Zusammenarbeit zwischen Entwicklungs-, Operations- und Sicherheitsteams ist dabei entscheidend für den Erfolg.

Professionelle Unterstützung bei der Umsetzung. Angesichts der Komplexität von Container-Sicherheit setzen viele Unternehmen auf externe Expertise. Spezialisierte IT-Dienstleister und Managed Service Provider wie Controlware bieten gezielten Support durch umfangreiche Services – beispielsweise den Kubernetes Security-Checkup, bei dem bestehende Installationen systematisch auf Sicherheitslücken überprüft werden. Solche Assessments decken typischerweise RBAC-Fehlkonfigurationen, unsichere Pod-Spezifikationen und Compliance-Gaps auf.

Für Organisationen, die ihre Kubernetes-Umgebungen nicht vollständig selbst betreiben möchten, bieten Managed Services eine hervorragende Alternative. Dabei übernehmen erfahrene IT-Teams die operative Verantwortung für Cluster-Management, Security-Updates und Monitoring, während die internen IT-Teams sich auf die Anwendungsentwicklung konzentrieren können.

Ohne Frage bieten Container-Technologien enormes Potenzial für Effizienzsteigerungen und Innovationen. Doch nur durch eine durchdachte Sicherheitsstrategie können Unternehmen diese Vorteile nutzen, ohne sich neuen Risiken auszusetzen. Die Investition in Container-Sicherheit ist nicht nur technisch notwendig, sondern mittlerweile auch regulatorisch gefordert und geschäftskritisch für den langfristigen Erfolg digitaler Transformationsprojekte.

Jörg Bechtel,
Teamlead Competence Center
DevOps & Automation,
Controlware GmbH

www.controlware.de
blog.controlware.de