Docker-Container und -Hosts überwachen

Sicher am laufenden Band

Patrick Münch, Christoph Puppe

Sicherheitsprozesse zu automatisieren, ist ein zentraler Bestandteil von DevSecOps. Wichtig wird das vor allem im Rahmen von Continuous Integration und DevOps. Da dort häufig Container eingesetzt werden, müssen Produkte zur Automatisierung von Sicherheit damit umgehen können.

Früher war „Ich werde dich durch ein Shell-Script ersetzen“ eine freundliche Drohung gegenüber Administratoren, heute ist es die Arbeitsrealität in größeren Unternehmen. Automatisierung der Administration ist das Schlagwort, das als DevOps bekannt wurde. Das Gebot der Stunde ist nun die Erweiterung der Automatisierung auf die Sicherheit: DevSecOps. Einige Produkte erledigen dies speziell für das Trendthema Container und überwachen Docker-Container und -Hosts auf Sicherheitsprobleme. Ihr Fokus liegt dabei auf dem Erkennen von Schwachstellen in den Konfigurationen der Hosts und der Container über den gesamten Lebenszyklus hinweg.

Mit dem Siegeszug von Docker wird die Frage relevant, welche Container auf welchen Hosts laufen und welche Software diese Container enthalten. Es ist also notwendig, eine Übersicht über den gesamten Betrieb zu erstellen und diese in einer für die Administratoren verständlichen Form zu präsentieren. Dies erledigen die bekannten Verwaltungs- und Orchestrierungstools wie Mesos, Kubernetes oder Rancher. Die Frage, welche Versionsstände und Konfigurationen die Hosts und Container enthalten, beantworten die Tools für Sicherheitsbelange allerdings nicht ausreichend. Dass der Frontend-Container in Version 13 läuft, mag für den Betrieb ausreichen, für das Management der Verwundbarkeiten ist ein sehr viel detaillierterer Blick notwendig.

Diese Informationen zu sammeln, auszuliefern und zu verarbeiten, haben sich mehrere Sicherheitsmanagement-Tools vorgenommen. Ihr Ansatz ist dabei ähnlich: Aus einem mehr oder weniger automatisierten Erkennen der Hosts heraus erfolgt ein Scan der Container und deren Konfiguration. So erstellen die Programme einen Überblick der zu betrachtenden Assets und unterziehen sie mindestens einem Compliance-Check gegen den CIS Benchmark für Docker-Container. Aqua Sec geht in der im Februar 2017 vorgestellten Version 2.0 noch einige Schritte weiter.

Wichtig für alle DevSecOps-Werkzeuge ist die Einbettung in das Management über RESTful APIs. Nur damit können sie ihre Arbeit automatisiert verrichten. Ziel der DevSecOps ist wie bei DevOps, keine manuellen Schritte im Betrieb mehr zu benötigen. So kann die Administration den Betrieb vollständig in einer Testumgebung simulieren und dann ohne Veränderungen in die Produktion übertragen.

Vulnerability Assessment von Tenable

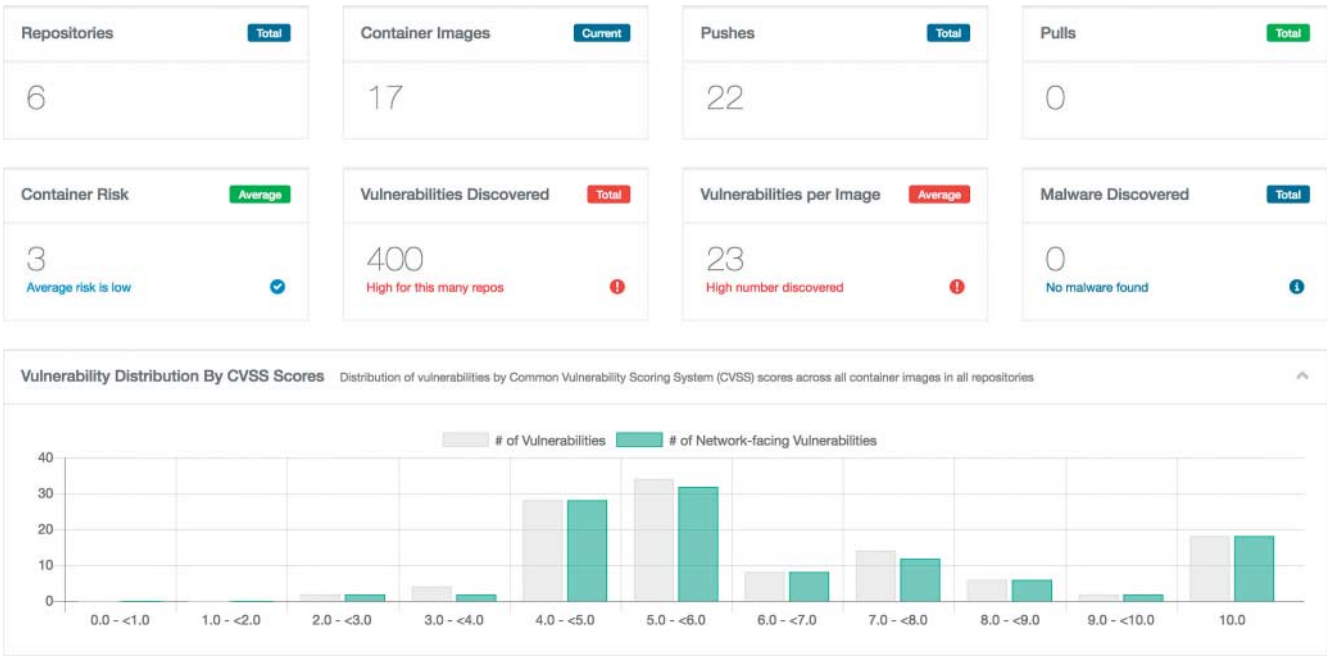
Von den Herstellern auf dem Markt weist Tenable die größte Erfahrung auf. Deren bekanntestes Produkt ist Nessus, das vor fast 20 Jahren das Vulnerability Assessment einführte. Tenable erweitert seit Anfang 2017 sein Portfolio um das auf Cloud und Container spezialisierte Tenable.io als Software-as-a-Service-Angebot. Es gibt zwar auch eine On-Premises-Variante, allerdings ist diese im Funktionsumfang stark eingeschränkt. Das neue Cloud-Angebot besteht aus drei Teilen:

1. Das Vulnerability Management verwaltet die gefundenen Schwachstellen in einer Webseite, stellt aber auch Schnittstellen zum Patch-Management und zu Ticketsystemen bereit.
2. Der Web Application Security Scanner (Dynamic Application Security Testing – DAST) stellt für Tenable ein neues Marktsegment dar, ist allerdings erst in einer geschlossenen Betaphase.
3. Das dritte Modul ist die Container Security, die sich in die Verwaltung der Container wie Kubernetes integriert (Continuous Integration and Continuous Deployment – CI/CD).

Damit hat Tenable.io alle Container ab dem Erstellen im Blick und nicht erst mit der Inbetriebnahme. Dieses Modul überwacht auch Hosts und Container auf Schwachstellen und Fehler in der Konfiguration, wie Abweichungen vom CIS Docker Benchmark.

Zusätzlich überwacht Tenable.io den Netzwerkverkehr. Ob dies als Ersatz für Intrusion Detection gedacht ist oder ob es um das Erkennen von Assets geht, ist jedoch nicht klar. Die Konfiguration der Hosts und Container sowie den Netzwerkverkehr erhält Tenable.io über Agenten auf den Hosts. Zwar ist auch ein Betrieb ohne diese möglich, das schränkt allerdings den Funktionsumfang ein.

Quelle: Tenable



Übersicht über die Ergebnisse der Überwachung auf Schwachstellen in der Konsole von Tenable.io (Abb. 1)

Da Nessus bereits heute über eine große Zahl von Checks auf Sicherheitslücken verfügt, kann Tenable auf eine ausgereifte Technik zurückgreifen. Dies bedeutet gegenüber den anderen Produkten einen erheblichen Vorteil, da die Firmen hinter den anderen hier vorgestellten Projekten alle weniger als zwei Jahre alt sind.

Wie gut die Integration in die CI/CD-Produkte ist, wird die Zeit zeigen. Da der Markt für die Orchestrierung von Docker noch im Aufbruch ist, sind hier Unregelmäßigkeiten und unerwartetes Verhalten zu befürchten.

Tenable.io enthält eine API zur Integration von Angeboten für Passwort- und Tokenverwaltung sowie Mobile Device Management. Es versucht, die gesamte IT zu umfassen – von Hosts zu mobilen Geräten, von Anwendungen bis hin zu Containern und Webseiten. Dieser Ansatz hat für den Anwender den Vorteil, dass eine einzelne Konsole den Überblick über den Sicherheitsstatus aller Assets gibt. Die Basis verfügt über einen hohen Reifegrad, lediglich die neuen Module müssen sich im Alltag noch bewähren.

Security Management mit Aqua Security

Das Start-up Aqua Security gewann Ende 2016 eine Finanzierung von 9 Millionen US-Dollar. Seine Software aqua bettet sich wie Tenable.io in CI/CD ein, um Sicherheitsfunktionen darin wahrzunehmen. Die Anwendung läuft als Container auf allen involvierten Hosts und hat Zugriff auf die notwendigen Daten wie die Konfiguration des Hosts und der Container oder deren Datenverkehr. Neben den Checks gegen den CIS Benchmark bringt es eigene Profile mit, gegen die es die Konfiguration abgleicht. Laut Hersteller verfügt aqua über 5 Millionen Signaturen für Verwundbarkeiten. Das erscheint etwas hoch, hier muss die Praxis zeigen, was von diesen Angaben zu halten ist.

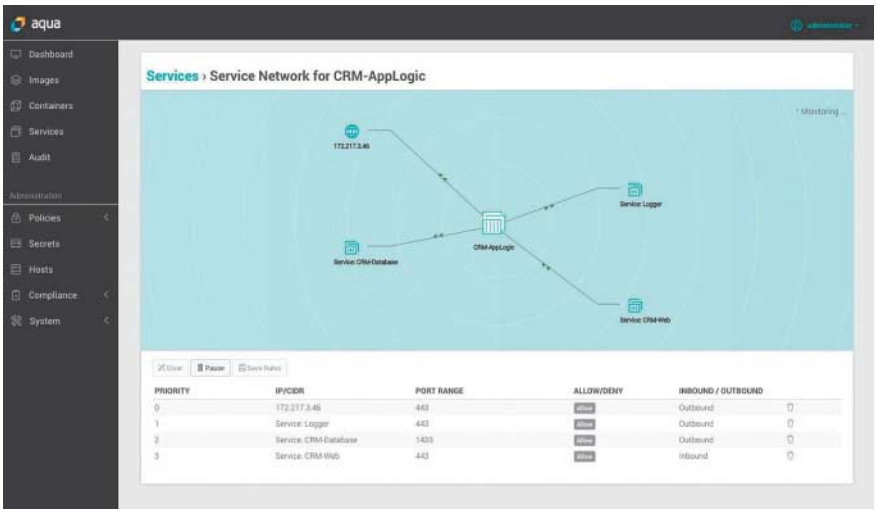
aqua untersucht unter anderem die Software in den Containern. Ob es so weit geht wie etwa Black Duck, das Verwundbarkeiten in Open-Source-Bibliotheken sucht, ist nicht erkennbar. Auch erfordern Signaturen viele Jahre Einsatz auf vielen Systemen, um hohe Qualität gewährleisten zu können. Hier hat ein neuer Hersteller einiges nachzuholen.

Die Software von aqua verwaltet Docker-Images inklusive digitaler Signaturen. So kann sie ungenehmigt veränderte Images erkennen und diese sperren. Sie bietet einen Lernmodus, bei dem sie den Netzverkehr der Container aufzeichnet und über einen Agenten ein Firewall-Profil erstellt (siehe Abbildung 2). Dies ist ein interessanter Ansatz, den man sich auch für andere Bereiche wünschen würde, wie beim Filtern von Kernel-API-Aufrufen (seccomp Profile) oder Capabilities (SELinux). Zudem kann aqua seit Version 1.2 bestimmtes Verhalten der Container unterbinden, etwa Port-Scans oder Fork-Bombs. Hier geht der Hersteller in Richtung einer Firewall, die das Verhalten der Software beobachtet und einschränkt.

Identity and Access Management (IAM) ist für Container eher ein Fremdwort. Docker besitzt Standardeinstellungen, die sich mit einem sicheren Betrieb nicht vertragen. Wer möchte, kann Authentifizierungsmodule selbst einbinden und Regeln erstellen. In aqua eingebaut ist ein eigenes Management der Benutzer mit Role Based Access Control (RBAC). Es integriert sich in vorhandene Benutzerverzeichnisse auf Basis von

X-TRACT

- DevSecOps erweitert die automatisierte Administration im Rahmen von DevOps um sicherheitsrelevante Aspekte.
- Im Bereich DevOps nehmen Container eine immer wichtigere Rolle ein und müssen deshalb bei DevSecOps berücksichtigt werden.
- Mehrere Produkte untersuchen Container und Hosts auf Sicherheitslücken und können automatisiert Gegenmaßnahmen einleiten. Ihre Ansätze reichen dabei vom Abfangen der Kernel-API-Calls bis zur Netzwerkanalyse.



Quelle: Aqua Security

Eine Besonderheit bei aqua ist die Erkennung von Netzwerkverkehr. Firewall-Regeln erstellt die Software halb automatisch (Abb. 2).

Active Directory oder LDAP und ermöglicht es, den Zugriff auf einzelne Container oder Gruppen von Containern über Rollen zu regeln. Gruppenbildung für die Benutzer ist an die Definition von Anwendungen und Services geknüpft. Die Aktionen der Benutzer fließen wie alle anderen Vorkommnisse in die Protokollierung mit ein.

Aqua Sec hat mit seinem Angebot in kurzer Zeit ein interessantes Produkt auf den Markt gebracht, das einige neue Funktionen einführt, die bei bekannteren Herstellern nicht vorhanden sind.

Security Management mit Twistlock

Auch Twistlock agiert erst seit weniger als zwei Jahren auf dem Markt. Das gleichnamige Sicherheitsprodukt ist on Premises oder als SaaS verfügbar. Es ähnelt in einigen Punkten den bereits vorgestellten Produkten. Zusätzlich überwacht die Software die Nutzung der Kernel-API durch die Container und erstellt automatisch Profile. Abweichungen meldet sie und kann den Container isolieren oder ganz abschalten. Standards wie Checks gegen den CIS Benchmark, Überwachung des Netzwerkverkehrs und Untersuchung der Container sind enthalten. Die Software überwacht und schränkt die Nutzung von Container-Registries ein, indem sie sich in die CI/CD-Pipelines einhängt. Wieder besteht der Ansatz darin, alle Container zu überwachen, also Entwicklungsumgebungen zu scannen und mit einer hinterlegten Policy abzugleichen. Softwarestände vergleicht das Programm im Container auf allen Ebenen, aber wie bei aqua ist nicht klar, ob es die gleiche Prüftiefe wie spezialisierte Werkzeuge erreicht.

Twistlock ermöglicht ebenfalls IAM. Zusätzlich zu AD und LDAP bietet es Authentifizierung via SAML. Die Zugriffssteuerung integriert sich in die Docker-Tools und zusätzlich in Kubernetes. Regeln nach RBAC kann es nicht nur auf Gruppen von Containern und Benutzern anwenden, sondern auch einzelne Funktionen der API für Benutzer freigeben oder sperren.

Alle Aktionen der Benutzer sind in den Protokollen enthalten. Diese lassen sich über *syslog* und API in Werkzeuge zur Auswertung integrieren. Hosts überwacht Twistlock nicht auf sichere Konfiguration, aber über Intels Cloud Integrity Technology (CIT) kann es die Integrität der Hard- und Firmware sowie des Hypervisors prüfen.

Auch hier hat ein Start-up in kurzer Zeit ein spannendes Produkt auf den Markt gebracht. Es bietet die gängigen Features, aber auch einzigartige Funktionen.

Netzwerksicherheit mit NeuVector

NeuVector ist der jüngste Teilnehmer in dem sich schnell entwickelnden Markt. Erst im Februar 2017 stellte der Hersteller sein Produkt vor. Der Fokus liegt auf dem Beobachten des Netzwerkverkehrs und dem Absichern der Container über dynamische Firewall-Regeln, die auch innerhalb eines Hosts (East-West Traffic) greifen. aqua hat übrigens umgehend eine ähnliche Funktion in seine Plattform eingebaut. Beide beobachten allerdings nicht die Kernel-API-Nutzung der Container wie Twistlock. NeuVector verspricht dafür zusätzlich eine Überwachung des Netzwerkverkehrs auf Distributed-Denial-of-Service-Angriffe und andere Angriffe über das Netzwerk. Inwieweit es eine Web-Application-Firewall oder ein Intrusion-Detection-System (IDS) ersetzen kann, muss die Praxis zeigen. Diese Aspekte der Netzwerksicherheit sind komplex in der Konfiguration und ein derartiges Angebot muss mit einer großen Zahl von Anwendungen klarkommen.

NeuVector soll sowohl den Container als auch den Host auf Sicherheitslücken untersuchen. Nach welchen Standards es dabei vorgeht oder ob es den CIS Benchmark mit betrachtet, bleibt unklar. Es bietet weniger Integration in die CI/CD-Umgebungen als die Konkurrenz und beschränkt sich auf das Ausliefern des eigenen Containers in die Umgebungen. Außerdem bietet es keine Überwachung der Registries, so wie dies Twistlock und aqua tun. Protokollierung

Anbieterübersicht

	Tenable.io	aqua	Twistlock	NeuVector	InSpec + dev-sec.io
Website	tenable.io	aquasec.com	twistlock.com	neuvector.com	github.com/dev-sec/cis-docker-benchmark
-Wertung	⊕ lange Erfahrung ⊕ umfasst die ganze IT	⊕ untersucht Software in Containern ⊕ verwaltet Docker-Images samt Signaturen ⊕ erstellt über Lernmodelle Firewall-Regeln ⊖ kurz auf dem Markt	⊕ IAM per SAML und für Kubernetes ⊕ auch Überwachung der Kernel-API ⊖ kurz auf dem Markt ⊖ keine Überwachung der Host-Konfiguration	⊕ einzige Lösung mit Rancher-Integration ⊕ 30 fertige Policies im Lieferumfang ⊖ sehr kurz auf dem Markt	⊕ Profile zum Einbinden in Konfigurationsmanagementsysteme ⊕ schnelle Integration dank menschen- und maschinenlesbarer Policies ⊖ kurz auf dem Markt ⊖ wenig Funktion

erfolgt auch über *syslog*, es integriert sich damit nahtlos in vorhandene Überwachung.

Compliance-Check mit InSpec und dev-sec.io

Wer seine Container manuell verwaltet oder ein Konfigurationsmanagement wie Chef, Ansible oder Puppet einsetzt, kann mit dem CIS Docker Profile von dev-sec.io die Sicherheitseinstellung des Docker Daemon und die Konfigurationen der Docker-Container gegen den CIS Benchmark prüfen. Das Profil basiert auf InSpec aus der Toolchain von Chef.

InSpec ist ein Open-Source-Testing-Framework für Infrastrukturen in einer menschen- und maschinenlesbaren Sprache für Compliance, Security und andere Policy-Anforderungen. Es bietet eine einfache Integration automatisierter Tests, die die Einhaltung der Richtlinien in jedem Stadium von Deployment-Pipeline oder Produktion überprüfen. So hilft es, die in Dokumenten verankerten Anforderungen wie den CIS Benchmark in „Compliance as Code“ zu überführen.

Durch den Fokus auf Lesbarkeit lassen sich die einzelnen Tests, die in Profilen zusammengefasst sind, von allen beteiligten Personen einfach lesen und sofort auf den Systemen ausführen. Zusätzlich zum Scannen eines Hosts kann InSpec einen Docker-Container über die Docker-API inspizieren. Während des Überprüfens laufender Container sind deswegen keine Änderungen am Inhalt erforderlich. Auch Patchstände und Konfigurationen von Systemen und Anwendungen lassen sich mit den dev-sec.io-Profilen prüfen.

InSpec lässt sich in bestehende Datacenter-Infrastrukturen integrieren. Chef Compliance ist das kommerzielle Produkt zu InSpec und bietet ein Dashboard zur Verwaltung der Infrastruktur sowie deren Compliance-Profile.

Fazit

Automatisierung der IT-Sicherheit als Teil des DevOps erlauben verschiedene Produkte. Auch wenn die Anbieter teilweise noch sehr jung sind, ist dies ein guter Start, der es in Zukunft ermöglichen wird, einen hohen Grad an Automatisierung der Sicherheit in einem automatisierten Betrieb zu erreichen. Da die Nachfrage groß genug für mehrere Hersteller ist, kann man davon ausgehen, dass alle Produkte eine realistische Chance haben, auf genügend Umgebungen zu reifen. Der Markt wird sich sicherlich noch eine Weile dynamisch bewegen, auch weil zu erwarten ist, dass die großen Namen des Schwachstellenmanagements wie Qualys das Segment für sich entdecken. (jab)

Patrick Münch

ist IT-Security Consultant bei der SVA, Berater zu IT-Sicherheitskonzepten und DevOps-/DevSec-Strategien sowie Penetrationstester.

Christoph Puppe

ist Security Consultant bei der SVA, seit 17 Jahren Vollzeit in der IT-Sicherheit aktiv, Audit-Teamleiter, IS-Revisor, Mitautor der Grundschutzkataloge und ehemaliger Penetrationstester.

Alle Links: www.ix.de/ix1705078