Security-Sorgenkind DevOps – wie schützen Unternehmen sich richtig?

Mittlerweile hat sich DevOps für viele Unternehmen zu einem Wettbewerbsvorteil entwickelt. Doch bereitet die Security vielen IT-Verantwortlichen noch immer Bauchschmerzen.

Von Jens Freitag, Security Specialist bei Tenable


Jens Freitag © tenable

Mit DevOps steht Unternehmen eine nützliche Methode zur Prozessverbesserung in Rahmen der Systemadministration und Softwareentwicklung zur Verfügung: Gemeinsame Tools in der Entwicklung, im IT-Betrieb und der Qualitätssicherung ermöglichen eine effizientere Zusammenarbeit. Zudem bieten sie mehr Stabilität und lassen sich gut skalieren. Produkte können so schneller auf den Markt kommen, Neuveröffentlichungen sind weniger fehlerhaft und Zeitfenster bis zur Behebung verkleinern sich. Unternehmen profitieren von besserer Softwarequalität sowie effizienterer Organisation.

Es ist nicht verwunderlich, dass es DevOps längst in die Unternehmen geschafft haben. Einer Umfrage zufolge nutzten 2017 bereits 56 Prozent der deutschen Unternehmen DevOps. Zur Technologie gehört jedoch auch die Sicherheit. Und hier hakt es noch. So fand die „2018 DevSecOps Community Survey“ heraus, dass knapp die Hälfte der Entwickler nicht genug Zeit für Security-Fragen haben – auch keine Lösungen oder Prozesse erarbeiten.

Hacker nutzen bereits die mangelnde DevOps-Cyberhygiene aus und schleusen Crypto-Mining-Malware über Docker Hub Backdoors, Kubernetes-Konten und ungepatchte Drupal-Webapplikationen ein. Zwar erfordern Angriffe noch sehr viel Rechenleistung, um Profit aus Kryptowährungen generieren zu können, doch bald wird es ihnen noch leichter fallen.

Die Sicherheitsexperten sollten sich das zu Herzen nehmen, das traditionelle Schwachstellenmanagement überdenken und neue Sicherheitsmethoden einführen, um auch DevOps-Prozesse in ihre IT-Sicherheitsmaßnahmen einzubeziehen. Tenable erklärt, was dafür erforderlich ist.

- **Kontinuierlich identifizieren und scannen**. Monatliche oder vierteljährliche Scans sind in der DevOps-Welt nicht ausreichend. Kontinuierliche Softwarebereitstellung bedeutet, dass sich die Umgebung ständig verändert. Aus diesem Grund sollten Unternehmen Cyberrisiken kontinuierlich identifizieren sowie bewerten und das über den gesamten Lebenszyklus der Softwareentwicklung hinweg – von der Bedarfsanalyse bis zum Einsatz. Nur so können Unternehmen vollständige Transparenz gewährleisten.
- **Sicherheitsmaßnahmen in DevOps-Prozesse integrieren**. Sicherheitstests und -kontrollen sollten ein integraler Bestandteil des Softwareentwicklungs-Lebenszyklus sein und in die Entwicklungspipeline integriert werden. Wieso Schwachstellen, Malware und

Fehlkonfigurationen nicht wie jede andere Art von Softwarefehler behandeln und so früh wie möglich beheben, bevor z. B. die Codequalität leidet?

- **Sicherheitsabläufe automatisieren**. Um die Skalierbarkeit und Geschwindigkeit von DevOps zu unterstützen, sollten Verantwortliche Sicherheitskontrollen programmgesteuert mit APIs in DevOps-Systeme einbinden und so die Vorteile der Automatisierung während des gesamten Entwicklungszyklus nutzen. Anstatt die Images anhand vordefinierter Security Gates manuell zu bewerten, können die Teams Sicherheitstests automatisch auslösen, um alle Build-Prozesse zu bewerten, wenn sie erstellt werden.

Der Markt bietet mittlerweile viele Lösungen, die Unternehmen dabei unterstützen. Cloud-Konnektoren tracken etwa kontinuierlich Asset-Veränderungen, um sicherzustellen, dass alle Cloud-Workloads bekannt sind und auf Schwachstellen untersucht werden. Dabei werden die Lösungen oft in CI/CD-Systeme (Continuous Integration and Continuous Delivery) integriert, um Schwachstellen und Malware schon während der Entwicklung zu beheben. Gut dokumentierte APIs ermöglichen es zudem, Sicherheitsscans zu automatisieren und Kontrollen innerhalb von Workflows zu integrieren. Für IT-Verantwortliche bedeutet dies, dass es durchaus Möglichkeiten gibt, etwas gegen ihre Bauchschmerzen zu unternehmen.