LISTICLE

Diese vier Best Practices sichern den DevSecOps-Erfolg

München, 22. Februar 2024 – Das DevOps-Prinzip hat sich für IT-Projekte als enorm wertvoll erwiesen: Entwickler und Administratoren brechen Wissenssilos auf und schaffen es mit den entsprechenden Methoden, die Zusammenarbeit zu verbessern. Wie DevOps-Teams nun auch den Sicherheitsaspekt integrieren und DevSecOps erfolgreich in die Praxis umsetzen, zeigt der IT-Dienstleister Consol anhand von vier goldenen Regeln.

Das Kunstwort DevOps setzt sich aus den Begriffen Development (Entwicklung) und Operations (IT-Betrieb) zusammen und bedeutet mehr als nur lose Kollaboration zwischen Codern und den Herrschern der IT-Systeme – im Gegenteil: DevOps steht für die Verschmelzung beider Bereiche zu einem gemeinsamen, holistischen Arbeitsbereich. Da der Sicherheitsaspekt in den vergangenen Jahren allerdings immer mehr an Bedeutung gewonnen hat, sollten DevOps-Teams auch Security tief und von Beginn an in den Softwareentwicklungs- und -auslieferungsprozess integrieren. Die folgenden vier Best Practices sind in diesem Zusammenhang essenziell:

1. Expertise und Sensibilität für Sicherheit aufbauen

Je später DevOps-Teams einen Fehler im Entwicklungs- und Auslieferungsprozess erkennen, desto teurer wird dessen Behebung und desto weitreichender sind die möglichen Sicherheitsfolgen. Daher ist es für DevOps-Teams extrem wichtig, möglichst frühzeitig ausreichende Maßnahmen für die Fehlererkennung zu ergreifen. Um diesen Ansatz in die Praxis umzusetzen, lehrt das DevSecOps-Prinzip, frühzeitig ein Bewusstsein für IT-Sicherheit im Team zu schaffen. Gleichzeitig müssen die Mitglieder Verantwortung für die Sicherheit ihres Produktes übernehmen und sich ihr ebenso verschreiben wie der einwandfreien Funktionalität ihrer Software. Auch bei der Planung der Architektur für das spätere Produkt sollten Sicherheitsaspekte bereits eine Rolle spielen. All das setzt, wie auch beim traditionellen Dev-Ops-Gedanken, einen kulturellen Wandel im gesamten Unternehmen voraus.

2. Konsequente Integration automatisierter Sicherheitsverfahren

Neben dem eher menschlichen Aspekt eines Umdenkens bei der Planung und Durchführung von Softwareprojekten, gibt es natürlich auch einen technischen und prozessualen Aspekt. DevSecOps-Teams sollten in allen Phasen des Entwicklungs- und CI/CD-Zyklus automatisierte Sicherheitsverfahren integrieren. Nur so können sie menschliche Fehler, die leider immer wieder passieren, vermeiden. Auch der Einsatz von Tools für die Quellcodeanalyse ist, neben automatisierten Tests, sinnvoll.

3. Risiken in der Softwarelieferkette identifizieren

Manchmal sind die größten Sicherheitsrisiken weder im Bereich Softwareentwicklung noch in der Auslieferung der fertigen Produkte zu finden, sondern in den verwendeten Bibliotheken. DevSecOps-Teams sollten daher die entsprechenden Frameworks, Tools und Libraries auf Bugs sowie Sicherheitslücken untersuchen – bestenfalls lassen sie das entsprechende Werkzeuge zur regelmäßigen Dependency-Analyse automatisch erledigen. Blackduck, Syft, Docker SBOM, Grype, Dependency-Check von OWASP sind nur einige wenige der bekannten Tools für diese Aufgabe. Besonders sinnvoll ist es, auf entsprechende Scanner zu setzen, die die verwendete Programmiersprache nativ unterstützen. Außerdem sollten Dev-
SecOps-Teams die Tools fest in die Continuous-Integration-/Continuous-Delivery-Pipeline integrieren. So stellen sie sicher, dass die Analysen auch wirklich regelmäßig stattfinden und die Ergebnisse immer aktuell sind.

4. Team-Mitglieder weiterbilden

Zu guter Letzt sollten DevSecOps-Teams kontinuierlich ihre Sicherheitsexpertise steigern und ihre Sinne schärfen. Das beginnt mit regelmäßigen Security-Trainings, in denen sie sich über aktuelle Bedrohungen und entsprechende Maßnahmen weiterbilden. Außerdem sollten sie sich von Expertinnen und Experten auf dem Gebiet in Schulungen über Best Practices in Sachen IT-Sicherheit aufklären lassen und ihre Prozesse auf den Prüfstand stellen. Oft sind nämlich auch eingefahrene und starre Workflows Gift für den Lebenszyklus einer Software. Und auch die anhaltende Recherche zu aktuellen Sicherheitsvorfällen und typischen Fallstricken bei deren Behebung sollte zum kleinen Einmaleins von DevSecOps-Teams gehören.

„Wie auch bei DevOps ist der Erfolg von DevSecOps maßgeblich von den Methoden und dem spezifischen Fachwissen der Teammitglieder abhängig“, erklärt Dr. Christoph Ehlers,

Leiter DevOps bei Consol. „Zwar gibt es wichtige Tools, die den sicheren Software-Delivery-Prozess unterstützen, ultimativ ist DevSecOps aber eben vor allem eine Frage der richtigen Arbeits- und Unternehmenskultur."

Weitere Informationen unter: https://www.consol.de/it-services/devops/

Dieses Listicle und Bildmaterial sind abrufbar unter www.pr-com.de/companies/consol.

Über Consol

Die Consol Consulting & Solutions Software GmbH mit Hauptsitz in München begleitet seit mehr als 35 Jahren lokale und internationale Unternehmen mit passgenauen IT-Lösungen durch den gesamten Software-Lifecyle. High-End-IT-Beratung, agile Software-Entwicklung sowie Betrieb und Support sind die Eckpfeiler des Portfolios, das Consol unter Anwendung von modernsten Technologien ständig erweitert. Dazu zählen Open Source-Projekte wie Quarkus, OpenShift oder Tekton. Das Unternehmen entwickelt und vertreibt auch die Software Consol CM, eine Plattform zur Digitalisierung von Geschäftsprozessen. Bei der Umsetzung der Digitalisierungsstrategien seiner Kunden macht Consol IT-Umgebungen und Geschäftsprozesse fit für die Herausforderungen von morgen. Mit den Leitmotiven Exzellenz und höchste Qualität folgt Consol dem Ziel, Businesses weiter voranzubringen. Dabei fokussiert Consol Bereiche wie Cloud-native, Container, Microservice-Architekturen oder IT Automation.

Consol ist Red Hat Premier Partner und NGINX Preferred Partner. Strategische Partnerschaften bestehen außerdem zu AWS und Microsoft Azure. Zu den Kunden zählen Großunternehmen wie Haribo, Daimler oder Vodafone. Aktuell beschäftigt Consol rund 260 Mitarbeiter an seinen Standorten München, Düsseldorf, Wien, Krakau, Dubai sowie San Francisco.

Weitere Informationen unter https://www.consol.de, https://cm.consol.de und https://blog.consol.de.

Pressekontakt

ConSol Consulting & Solutions Software GmbH
Isabel Baum
St.-Cajetan-Straße 43
D-81669 München
Fon: +49-89-45841-101
E-Mail: Isabel.Baum@consol.de
Web: https://www.consol.de und https://cm.consol.de

PR-COM GmbH
Nicole Oehl
Sendlinger-Tor-Platz 6
D-80336 München
Fon: +49-89-59997-758
E-Mail: nicole.oehl@pr-com.de
Web: www.pr-com.de