Cyber Security – Die Herausforderungen in 2024

DevSecOps erfordert eine Veränderung der Unternehmenskultur

Cloud Security umfasst die Sicherheitsmaßnahmen, die ergriffen werden müssen, um Cloud Computing zu schützen. DevSecOps ist ein wesentlicher Bestandteil der Cloud Security, der gewährleisten soll, dass Anwendungen und Systeme von Anfang an sicher sind.

Zu den Top-Herausforderungen gehört im Jahr 2024 zweifelsfrei das Thema Cloud Security respektive DevSecOps. Oftmals wird in den Unternehmen die Frage gestellt, wer hierfür eigentlich zuständig ist. Um es vorwegzunehmen, diese Frage lässt sich nicht pauschal für alle Unternehmen gleich beantworten. Cyber Security – quasi als Überbegriff – ist ein wichtiger Aspekt für Unternehmen, um Daten und Systeme vor Diebstahl, Beschädigung oder unbefugtem Zugriff zu schützen. Bei DevSecOps handelt es sich dagegen um einen Ansatz, der die Sicherheit in den Entwicklungsprozess integriert, um zu gewährleisten, dass Anwendungen und Systeme von Anfang an sicher sind. DevSecOps ist also ein wichtiger Bestandteil der Cyber Security, der einen wesentlichen Beitrag leistet, Schwachstellen in Anwendungen und Systemen zu identifizieren und zu beheben – im Idealfall noch bevor diese ausgenutzt werden können.

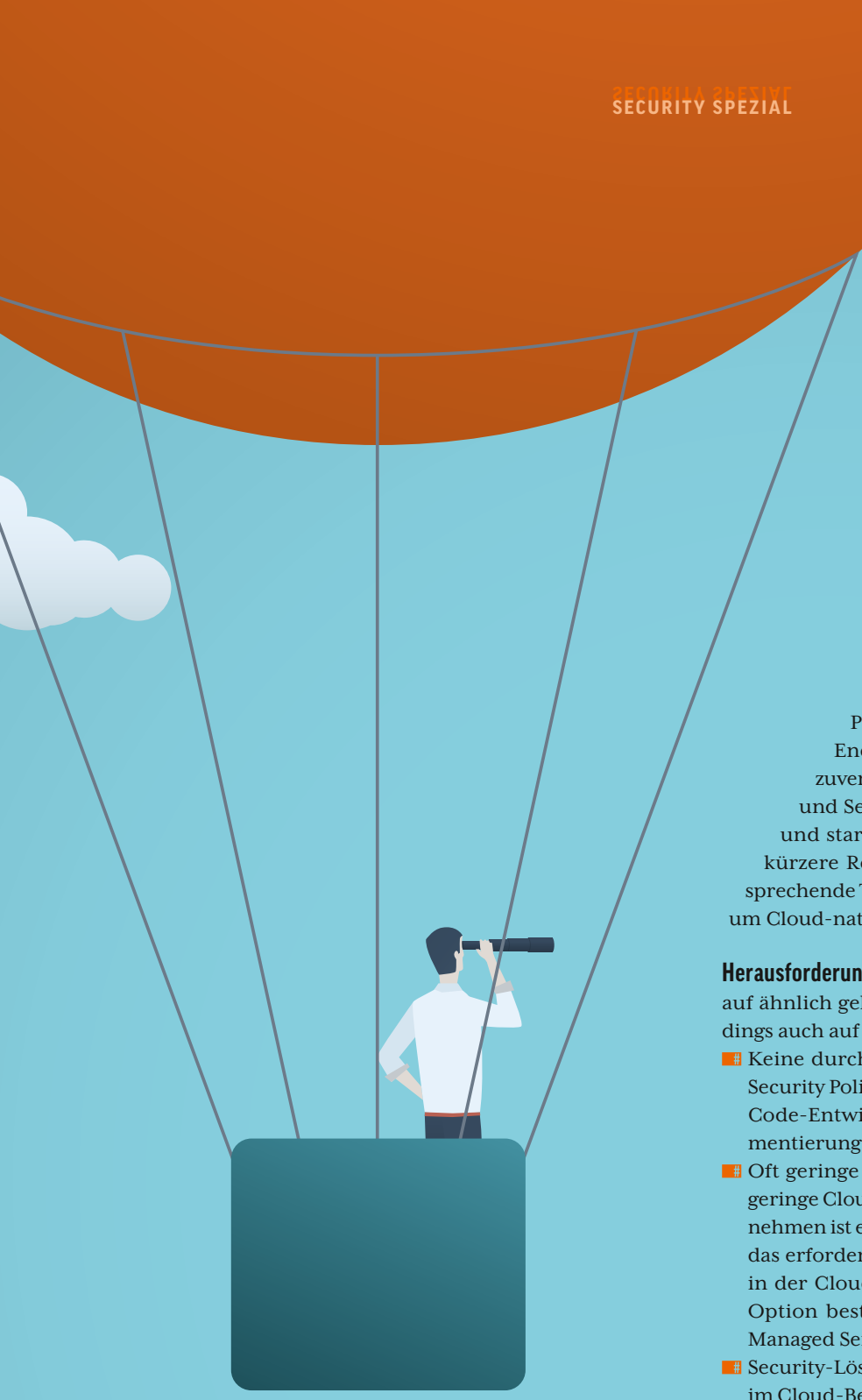
In der Regel finden Entwicklungen mittlerweile vorzugsweise in der Cloud statt, da es hier möglich ist, schnell und agil zu arbeiten. Allerdings ist es gerade in puncto Cloud wichtig, die Sicherheit ganzheitlich zu betrachten und entsprechend sensibel zu berücksichtigen. Bedenken hinsichtlich der Sicherheit von Cloud-Computing-Systemen sind sicherlich nicht ungerechtfertigt, da diese für Angriffe von Hackern durchaus anfällig sind. Cloud Security bezieht sich an dieser Stelle auf die Sicherheitsmaßnahmen, die ergriffen werden, um Cloud Computing zu schützen.

DevSecOps und Cloud Security. Die beiden Begriffe DevSecOps und Cloud Security sind also eng miteinander verbunden. DevSecOps ist ein wichtiger Bestandteil der Cloud Security. Es gibt jedoch einige Herausforderungen für den Einsatz von DevSecOps in Unternehmen. Eine große Herausforderung besteht darin, dass DevSecOps ein recht neuer Ansatz ist und viele Unternehmen bisher noch Schwierigkeiten haben, diesen so zu implementieren, dass eine enge Zusammenarbeit zwischen Entwicklern, Sicherheitsteams und Betriebsteams stattfindet. Die Unternehmenssicherheit soll erhöht werden, gleichzeitig darf die Security die Entwicklungsprozesse aber nicht verlangsamen. Die größte Herausforderung besteht jedoch darin, dass DevSecOps in der Regel auch eine Veränderung der Unternehmenskultur erfordert.

Bei der Umsetzung von DevSecOps gilt es, zunächst ein gemeinsames Verständnis für die Problemstellung zu schaffen. Dadurch lassen sich am besten die beschriebenen organisatorischen Herausforderungen in Unternehmen und Behörden angehen und letztendlich auch lösen. Selbstverständlich sind hier auch die Security-Hersteller gefragt, Lösungen sowohl für aktuelle als auch für zukünftige Sicherheitsanforderungen in der Cloud bereitzustellen.

Die IT-Sicherheit hat sich in den letzten Jahren aufgrund der Umstellung auf Cloud-native Technologien und infolge moderner Entwicklungsansätze wie Infrastructure as Code (IaC), CI/CD-Pipelines, Container, serverlose Funktionen und

Illustration: © Jozef Micic | shutterstock.com



Kubernetes stark verändert. Herkömmliche Sicherheitskonzepte und -tools, die für On-Premises-Rechenzentren und lokal installierte Endgeräte entwickelt wurden, bieten oft keinen zuverlässigen Schutz für Cloud-native Anwendungen und Services. Dies hat zu dynamischen, kurzlebigen und stark automatisierten Umgebungen geführt, die kürzere Release-Zyklen erfordern. Daher ist eine entsprechende Transformation der IT-Sicherheit erforderlich, um Cloud-native Anwendungen und Services abzusichern.

Herausforderungen für DevSecOps. Die Security-Teams stoßen auf ähnlich gelagerte Probleme wie bei On-Premises, allerdings auch auf neue Herausforderungen und Risiken:

- Keine durchgängige Security-Strategie beziehungsweise Security Policy für die gesamte Cloud-Umgebung – von der Code-Entwicklung bis hin zum Workload bei der Implementierung von DevSecOps.
- Oft geringe Security-Expertise in den Cloud-Teams und geringe Cloud-Expertise in den Security-Teams. Für Unternehmen ist es wichtig, sicherzustellen, dass ihre Teams über das erforderliche Know-how verfügen, um die Sicherheit in der Cloud-Umgebung zu gewährleisten. Eine weitere Option besteht darin, sich diese Security-Expertise als Managed Service extern zu beziehen.
- Security-Lösungsanbieter erweitern ihr Portfolio, um sich im Cloud-Bereich zu positionieren und treten in den Wettbewerb mit den großen Hyperscalern. Hier gilt es, zu bewerten, welche Lösungen angeboten werden und ob es Vorteile bringt, weiter auf die bisher bekannten Security-Anbieter zu setzen. Beispielsweise weil ein einheitliches Management für On-Premises und in der Cloud Vorteile bietet. Vielleicht auch, weil man den Hyperscaler, dem man seine Daten anvertraut, lieber von einem anderen Anbieter kontrollieren lassen möchte. In vielen Fällen ist die Qualität der Produkte, die der Hyperscaler liefert, aber auch gut genug, oder man hat die Security-Lösung im Rahmen von Bundels, die der Hersteller liefert, lizenztechnisch bereits eingekauft.

> Cloud Security Posture Management (CSPM) kann ein wichtiger Bestandteil einer Cloud-basierten Sicherheitsarchitektur werden, wenn dieses professionell in die eigenen Prozesse eingebunden wird.

- Entwickler lehnen häufig zusätzliche Security-Kontrollen ab: Dies geschieht natürlich nicht aus Fahrlässigkeit, sondern weil sie der Meinung sind, dass dadurch die Entwicklungsgeschwindigkeit beeinträchtigt wird. Es ist wichtig, dass Unternehmen die Sicherheit in den Entwicklungsprozess integrieren, ohne die Geschwindigkeit der Entwicklung maßgeblich zu beeinträchtigen.
- Unterschiedliche Security-Verantwortliche arbeiten parallel an der Behebung von Problemen respektive von Incidents: Hier gilt es, zunächst Transparenz herzustellen und Incidents zentral auszuwerten. Zudem sollten unterschiedliche Teams eng zusammenarbeiten, um sicherzustellen, dass Security Incidents schnell und effektiv behandelt werden. Auch hier kann ein externer Security Service – den Controlware für Cloud-Umgebungen anbietet – hilfreich sein.

Im Nachfolgenden nehmen wir die Gefahr von Cyberangriffen auf Software-Entwicklungspipelines etwas genauer unter die Lupe und skizzieren hier konkrete Lösungsansätze.

Cyberangriffe auf die Software-Entwicklungspipeline. Die Zunahme von Cyberangriffen auf Software-Entwicklungspipelines ist schon deshalb nachvollziehbar, da die Verbreitung beziehungsweise Nutzung von Cloud-Technologien gestiegen ist und sich Angriffe sehr effizient durchführen lassen. Ein Beleg hierfür sind die vielen Berichterstattungen über Sicherheitsvorfälle innerhalb der letzten Monate in der Fachpresse. Aufgrund der erhöhten Komplexität und der benötigten Ressourcen waren Angriffe dieser Art zunächst eher staatlichen Akteuren oder höchst professionellen Angreifern mit umfangreichem Fachwissen und finanziellen Mitteln vorbehalten. Nach dem Vorbild des Randsomware-as-a-Service-Modells, das sich gewinnbringend auch an Angreifer ohne tiefgreifendes Know-how verkaufen lässt, besteht mittlerweile durchaus die Möglichkeit, dass spezialisierte Akteure hier ebenfalls aktiv werden und verstärkt Software-Entwicklungspipelines infiltrieren. Dies erfordert zwar ein hohes Maß an zielgerichteten Kenntnissen in Technologien wie Jenkins, GitLab, GitHub und Kubernetes – »richtig« umgesetzt, lässt sich dieses Wissen aber profitabel an Käufer im Dark Web oder an andere Kanäle lukrativ »vermarkten«.

Lösungsansätze. Öffentliche Auftraggeber und die Privatwirtschaft werden nicht umhinkommen, etablierte, scheinbar vertrauensvolle Kommunikationsbeziehungen neu zu bewerten. Nicht nur der Benutzerzugriff im Allgemeinen, sondern auch der Zugriff auf Daten wird verstärkt überprüft werden müssen. Gerade die Einführung der sogenannten Zero-Trust-Strategie sehen hier viele Experten als einen wichtigen Faktor.

Ein funktionierendes Schwachstellenmanagement ist an dieser Stelle unbedingt hervorzuheben. Auch wenn das Thema nicht neu ist, erlebt es gerade eine Renaissance. Ein funktionierendes, strategisches Vulnerability Management (VM) beinhaltet weit mehr als nur das Scannen von PCs, Anwendungen und Infrastrukturkomponenten. Essenzielle Aufgaben wie das Scannen von Container-Images und die Überprüfung von Programmcode gehören ebenfalls dazu. Der Log4j-Vorfall hat Sicherheitsverantwortlichen wieder einmal deutlich gemacht, wie wichtig es ist, einen Überblick über die unterschiedlichen Komponenten der eingesetzten Software zu haben. Nur so lässt sich schnell eine potenzielle Betroffenheit ermitteln. Ohne Frage müssen wir uns zukünftig darauf einstellen, dass Angriffe auf bekannt gewordene Sicherheitslücken immer schneller stattfinden.

Cloud Security Posture Management (CSPM) kann ein wichtiger Bestandteil einer Cloud-basierten Sicherheitsarchitektur werden, wenn dieses professionell in die eigenen Prozesse eingebunden wird. Es hilft Unternehmen dabei, ihre Cloud-Ressourcen sicher zu konfigurieren und bereitzustellen. Externe CSPM-Lösungen bieten in der Regel eine bessere Sichtbarkeit auf Cloud-Assets eines Unternehmens, ihre Sicherheitslage und etwaige Risiken oder Schwachstellen als die Hyperscaler selbst. Dies ist vor allem bei einer Multi-Cloud-Strategie der Fall. CSPM-Lösungen bieten auf Wunsch auch automatisierte Abhilfemaßnahmen für Sicherheitsprobleme. Die Integration von CSPM in eine umfassende Sicherheitsstrategie ist mitentscheidend, um zu garantieren, dass Cloud-native Anwendungen und Services sicher sind.

Mario Emig, Head of Information Security Business Development, Controlware GmbH

www.controlware.de
blog.controlware.de