Red Hat

The State of Kubernetes Security Report: Ausgabe für 2024

Ausgabe 2024

Ein Bericht von Red Hat

Zusammenfassung

Cloudnative Technologien verändern den Ansatz von Organisationen beim Entwickeln, Bereitstellen und Skalieren von Anwendungen. Dank der inhärenten Skalierbarkeit, Agilität und Flexibilität der Cloud-Infrastruktur können Unternehmen die Markteinführung beschleunigen, die Effizienz steigern und die Innovation fördern. Da Cyberangriffe jedoch zunehmend raffinierter werden, sind robuste Sicherheitsmaßnahmen zum Schutz sensibler Daten, zum Schutz vor Verstößen und für die Compliance mit regulatorischen Standards in Hybrid Cloud-Umgebungen unerlässlich. Als Reaktion darauf investieren viele IT-Organisationen in moderne Sicherheitsplattformen und implementieren kollaborative, sicherheitsorientierte Prozesse, um kritische Systeme, Workloads und Daten zu schützen. Für nahezu 50 % der Unternehmen stellt die IT-Sicherheit eine der wichtigsten Finanzierungsaufgaben dar.[1]

Mit dem Schwerpunkt auf Container Workloads und Kubernetes befragten Red Hat und Illuminas weltweit Fachleute aus den Bereichen DevOps, Engineering und Sicherheit in Organisationen, darunter sowohl kleine Unternehmen als auch Großkonzerne. Basierend auf diesen Daten untersucht die Ausgabe 2024 des State of Kubernetes Security Report einige der häufigsten cloudnativen Sicherheitsherausforderungen und Geschäftsauswirkungen, mit denen Organisationen derzeit konfrontiert sind. Wir befassen uns mit den spezifischen Sicherheitsrisiken, die Unternehmen am meisten beunruhigen – einschließlich Vulnerabilities in der Softwarelieferkette und in der Anwendungs-Runtime – sowie mit den Strategien, die Unternehmen ergreifen, um diese Risiken zu minimieren. Wir identifizieren die Arten und Häufigkeiten von Sicherheitsvorfällen, die in Unternehmen in Kubernetes-Umgebungen auftreten. Wir betrachten die Verteilung der Kubernetes-Sicherheitsverantwortung auf Entwicklungs-, Sicherheits- und Operations-Teams, um die neuesten Trends beim Einführen von DevSecOps aufzuzeigen. Abschließend bieten wir eine Anleitung zur Risikoverringerung während des gesamten Anwendungs-Lifecycles.

Umfassende Container- und Kubernetes-Sicherheit ist zwar eine Herausforderung, kann Sie aber bei der Beschleunigung von Innovationen und der Schaffung von Mehrwert für Ihr Unternehmen unterstützen. Mithilfe der Ergebnisse unserer Umfrage können Sie Ihre eigene Kubernetes-Sicherheit bewerten, um Verbesserungsmöglichkeiten zu finden und Insights in die Reduzierung von Sicherheitslücken zu gewinnen. Durch kontinuierliches Optimieren Ihrer Sicherheitsmaßnahmen können Sie wichtige Unternehmensressourcen schützen und eine proaktive Sicherheitskultur schaffen, die Integrität und Resilienz Ihrer Infrastruktur und Anwendungen sicherstellt.

Lesen Sie weiter, um die 13 wichtigsten Ergebnisse der Umfrage zu erfahren.

*1 Bericht von Red Hat: „**2024 global tech trends**", Februar 2024.*

Über diesen Bericht

Für die Ausgabe für 2024 dieses Berichts sponserte Red Hat eine Umfrage unter 600 DevOps-, Technik- und Sicherheitsexperten in den USA, Großbritannien und der englischsprachigen Region Asien-Pazifik (APAC), um aufkommende Trends bei Containern, Kubernetes und cloudnativer Sicherheit zu ermitteln. Die Daten wurden durch 21-minütige Online- und Telefoninterviews mit Befragten aus Online-Panels und Datenbanken von Drittanbietern erhoben. Die Umfrage wurde im Dezember 2023 und Januar 2024 durchgeführt.

Profil der Befragten:

- IT-Fachleute, die sich mit Anwendungen, Plattformen, Infrastruktur, Operationen, Sicherheit oder Software-Architektur oder -Entwicklung beschäftigen
- Unternehmen mit mehr als 100 Beschäftigten
- Unternehmen, die über ein internes Entwicklungsteam für Anwendungen verfügen
- Unternehmen, die derzeit Container nutzen

Demografische Daten der Befragten

600
Antworten insgesamt

DevOps-Fachleute

Engineering-Fachleute

Sicherheits-fachleute

25 % 100–499 Beschäftigte
24 % 500–999 Beschäftigte
52 % mehr als 1.000 Beschäftigte

26 % Technologie
25 % Finanzdienst-leistungen
24 % Telekommunikation, Medien und Unterhaltung
26 % Andere Branchen

Wichtige Ergebnisse

Unsere Umfrage liefert erneut umfassende Informationen darüber, wie Unternehmen die Sicherheit von Kubernetes handhaben. Nachfolgend finden Sie die wichtigsten Punkte:

67 % der Unternehmen verzögerten oder verlangsamten das Deployment aufgrund von Kubernetes-Sicherheitsaspekten.

46 % der Unternehmen haben aufgrund eines Container- oder Kubernetes-Sicherheitsvorfalls Umsatz oder Kunden verloren.

42 % der Befragten nennen Sicherheit als wichtigen Aspekt bei Container- und Kubernetes-Strategien.

42 % der Befragten geben an, dass sich DevSecOps-Initiativen in ihrem Unternehmen in einem fortgeschrittenen Stadium befinden.

48 % der Unternehmen befinden sich in einem Frühstadium von DevSecOps-Initiativen, bei denen die Teams an gemeinsamen Richtlinien und Workflows arbeiten.

33 % der Befragten glauben, dass ihre bestehende Container- und Kubernetes-Sicherheitslösung die Entwicklung verlangsamt.

30 % der Befragten identifizierten Vulnerabilities als ihre größte Sorge in Bezug auf ihre Container- und Kubernetes-Umgebung.

Lesen Sie weiter, um mehr über diese Ergebnisse zu erfahren.

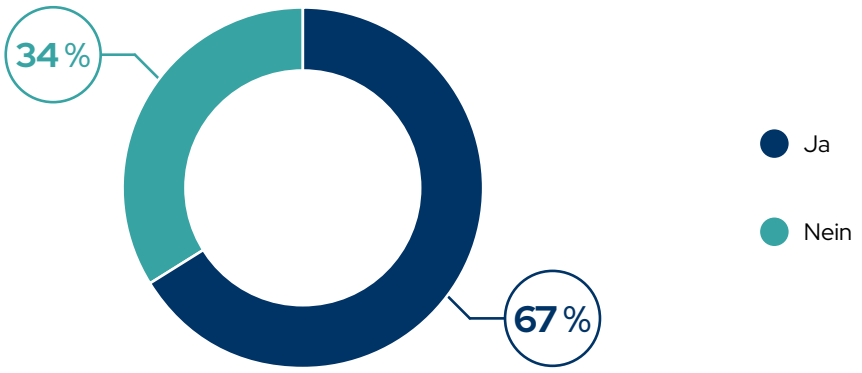
Ergebnis 1:

Sicherheitsprobleme beeinflussen die Geschäftsergebnisse

Sicherheitsprobleme zwangen 67 % der Unternehmen, das Deployment von Anwendungen zu verzögern oder zu verlangsamen.

Weltweit setzen Unternehmen cloudnative Technologien wie Kubernetes und auf Microservices basierende Architekturen ein, um das Entwickeln, Ausführen und Skalieren von Anwendungen zu transformieren. Während einige Unternehmen ihre gesamte neue Software als Microservices entwickeln, führen viele ein Refactoring bestehender Anwendungen mit containerbasierten Technologien durch. Unabhängig davon können Container die Entwicklungs- und Release-Zyklen beschleunigen und die Flexibilität beim Ausführen und Verwalten von Anwendungen in hybriden Umgebungen erhöhen. Jedoch kann unzulängliche Sicherheit während des gesamten Anwendungs-Lifecycles – von der Entwicklung bis zum Deployment und der Wartung – diese wichtigen Vorteile zunichte machen. Tatsächlich ergab unsere Umfrage, dass 67 % der Befragten das Deployment containerbasierter Anwendungen aufgrund von Sicherheitsbedenken verzögert oder verlangsamt haben.

Haben Sie schon einmal aufgrund von Container- oder Kubernetes-Sicherheitsbedenken das Deployment einer Anwendung in der Produktivumgebung verschoben oder verlangsamt?



F27. Haben Sie schon einmal aufgrund von Container- oder Kubernetes-Sicherheitsbedenken das Deployment einer Anwendung in der Produktivumgebung verschoben oder verlangsamt? Basisgröße: Gesamt = 600

Wegen Rundungen ist es möglich, dass Prozentwerte zusammengerechnet nicht 100 % ergeben.

Ergebnis 2:

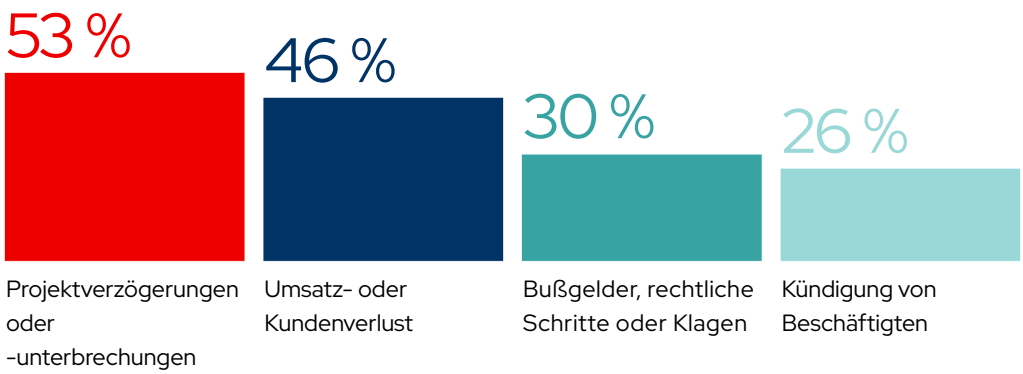
Sicherheitsverletzungen betreffen jeden

Sicherheitsvorfälle führen zu weitreichenden Konsequenzen, einschließlich der Kündigung von Beschäftigten und Umsatzeinbußen.

Die Auswirkungen von Container- und Kubernetes-Sicherheitsproblemen können weit über verzögerte Deployments von Anwendungen hinausgehen. 26 % der Befragten gaben an, dass ein Sicherheitsvorfall zur Entlassung von Beschäftigten führte, während 30 % berichteten, dass ihr Unternehmen infolge eines Vorfalls eine Geldstrafe zahlen musste. In solchen Situationen kann der Verlust wichtiger Fachkräfte, Kenntnisse und Erfahrungen die Geschäftsabläufe erheblich beeinträchtigen, während Geldstrafen und negative Publicity die Unternehmen finanziell stark belasten können.

46 % der Befragten gaben außerdem an, dass ihr Unternehmen infolge eines Sicherheitsvorfalls Umsatz- oder Kundenverluste erlitten hat. Sicherheitsverletzungen können das Unternehmenswachstum bremsen, wenn sich Projekte oder Produktveröffentlichungen aufgrund von Fehlerbehebungen verzögern. Sobald Kunden das Vertrauen in die Datenschutzfähigkeiten eines Unternehmens verlieren, wenden sie sich möglicherweise an Mitbewerber, die sicherere Praktiken anwenden.

Sind in den letzten 12 Monaten infolge von Container/Kubernetes-Sicherheits- oder Compliance-Problemen oder -Vorfällen eine der folgenden Auswirkungen auf Ihr Unternehmen aufgetreten?



F29. Sind in den letzten 12 Monaten infolge von Container/Kubernetes-Sicherheits- oder Compliance-Problemen oder -Vorfällen eine der folgenden Auswirkungen auf Ihr Unternehmen aufgetreten? Basisgröße: Gesamt = 600

Ergebnis 3:

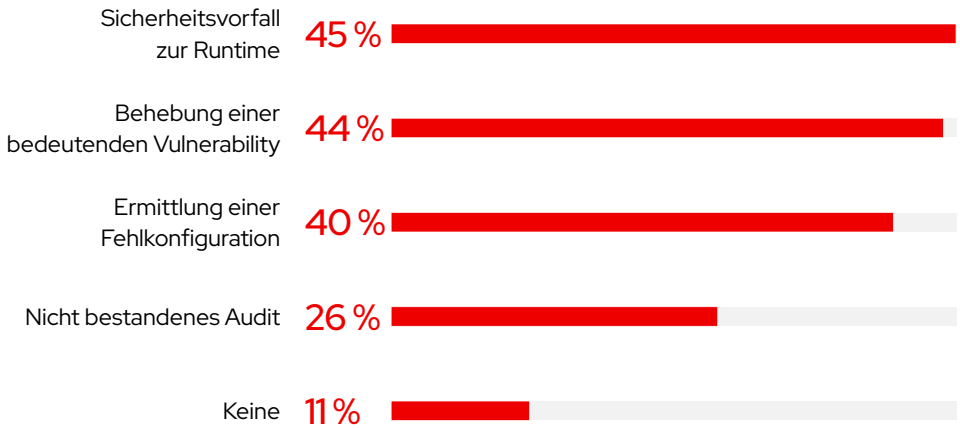
Sicherheitsvorfälle treten in sämtlichen Phasen des Lifecycles von Anwendungen auf

Nahezu 9 von 10 Unternehmen verzeichneten in den letzten 12 Monaten mindestens einen Container- oder Kubernetes-Sicherheitsvorfall.

Sicherheitsvorfälle sind nicht nur auf aktuell ausgeführte Anwendungen beschränkt. Vielmehr können sich Sicherheitsvorfälle im Zusammenhang mit Containern und Kubernetes auf alle Phasen des Anwendungs-Lifecycles auswirken. 45 % der Befragten gaben an, dass es in ihrem Unternehmen in den letzten 12 Monaten zu Problemen mit der Runtime gekommen ist. Fast ebenso viele (44 %) gaben an, dass sie Probleme in der Entwicklungs- und Deployment-Phase hatten und verwiesen dabei auf größere Vulnerabilities, die behoben werden mussten. Gleichzeitig gaben 40 % an, dass ihr Unternehmen Fehlkonfigurationen in ihren Container- oder Kubernetes-Umgebungen entdeckt hat, und 26 % berichteten, dass ihr Unternehmen ein Audit nicht bestanden hat.

Container und Kubernetes-Technologien können die Produktivität durch funktionsübergreifende Funktionen und vereinfachte Abläufe steigern. Kubernetes bietet zwar Mechanismen wie Netzwerkrichtlinien und RBAC (Role-based Access Control), um die Sicherheit in Ihrem Cluster zu erhöhen, doch einige Funktionen sind standardmäßig zu tolerant oder deaktiviert und erfordern eine zusätzliche Konfiguration, um ausreichenden Schutz zu bieten. Hinzu kommt, dass Sicherheitskontrollen wie **SELinux** zwar die Anwendungssicherheit deutlich erhöhen können, die Anpassung und Integration in eine operative Umgebung jedoch mitunter eine Herausforderung darstellt. Diese Schwierigkeiten treten häufig in Form von Sicherheitsvorfällen, Vulnerabilities und Fehlkonfigurationen in verschiedenen Phasen des Anwendungs-Lifecycles auf. Unsere Umfrageergebnisse zeigen, dass viele Unternehmen immer noch mit der komplexen Absicherung von containerbasierten Kubernetes-Umgebungen zu kämpfen haben. 89 % berichteten von mindestens einem Sicherheitsvorfall in den letzten 12 Monaten.

Welche Sicherheitsvorfälle oder -probleme hinsichtlich Container und/oder Kubernetes haben Sie in den letzten 12 Monaten erlebt?



F28. Welche Sicherheitsvorfälle oder -probleme hinsichtlich Container und/oder Kubernetes haben Sie in den letzten 12 Monaten erlebt?
Basisgröße: Gesamt = 600

Ergebnis 4:

Derzeitige Container-Sicherheitsstrategien sind problematisch

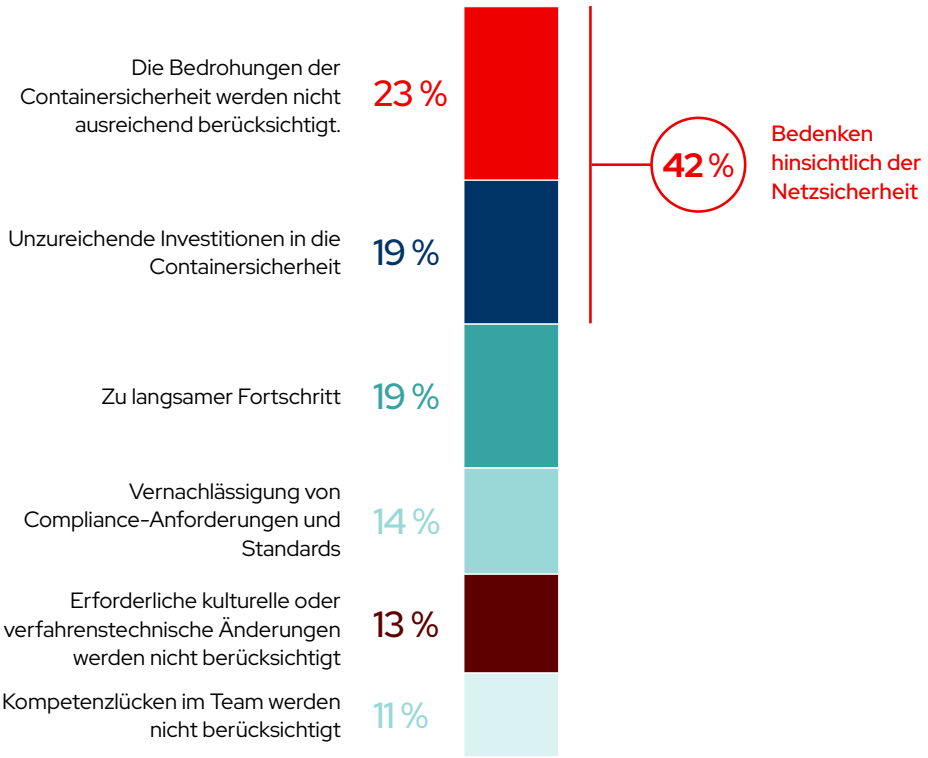
42 % der Befragten sind der Meinung, dass ihr Unternehmen nicht ausreichend in die Container-Sicherheit investiert oder sich mit den damit verbundenen Bedrohungen auseinandersetzt.

Wenn Unternehmen Container-Umgebungen einführen, um Deployment und Skalierbarkeit von Anwendungen zu optimieren, müssen sie auch ihre Sicherheitsprozesse an diese dynamischen und verteilten Systeme anpassen. Kubernetes und Container führen neue Softwareebenen ein, die zu mehr Komplexität und zusätzlichen Sicherheitsrisiken für kritische Infrastrukturen führen können. Da es zunehmend mehr potenzielle Angriffspunkte für Cyber-Bedrohungen gibt, sind

robuste Sicherheitsmaßnahmen zum Schutz vor Vulnerabilities, unbefugtem Zugriff und Datenpannen erforderlich. Dennoch sind einige der Befragten skeptisch, was die Container-Strategie ihres Unternehmens angeht. Tatsächlich sind 23 % der Ansicht, dass die Strategie ihres Unternehmens Bedrohungen der Container-Sicherheit nicht ausreichend berücksichtigt. Weitere 19 % sind der Auffassung, dass die Investitionen in die Container-Sicherheit unzureichend sind.

Umfassende Container- und Kubernetes-Sicherheit beginnt mit dem Wissen um die Komplexität und die potenziellen Sicherheitsrisiken moderner Umgebungen. Durch das Implementieren von Kontrollen, die die Ebenen des Software-Stacks umfassen – einschließlich der zugrunde liegenden Infrastruktur, der Kubernetes Control Plane, des Netzwerks sowie der Container-Images und -Registries – können Sie beginnen, die Risiken für Ihre cloudnativen Anwendungen zu minimieren.

Was ist Ihre größte Sorge hinsichtlich der Container-Strategie Ihres Unternehmens?



F7. Was ist Ihre größte Sorge hinsichtlich der Container-Strategie Ihres Unternehmens? Basisgröße: Gesamt = 600

Wegen Rundungen ist es möglich, dass Prozentwerte zusammengerechnet nicht 100 % ergeben.

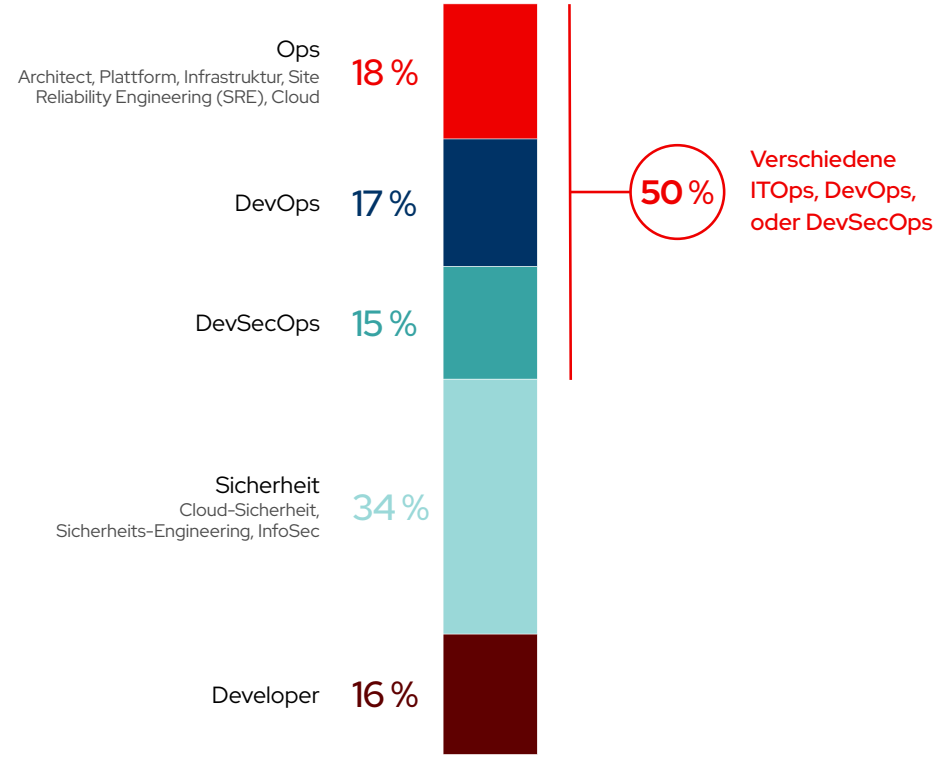
Ergebnis 5:

Die Verantwortung für die Sicherheit ist stark dezentralisiert

Nur ein Drittel der Befragten gibt an, dass ihre Sicherheitsteams für die Kubernetes-Sicherheit verantwortlich sind.

In vielen Unternehmen arbeiten mehrere Gruppen zusammen, um Workloads in containerbasierten Kubernetes-Umgebungen zu entwickeln und bereitzustellen. Unsere Umfrageergebnisse zeigen, dass es keine einzelne Rolle gibt, die für die Kubernetes-Sicherheit in Unternehmen verantwortlich ist.

Welche Rolle ist in Ihrem Unternehmen hauptsächlich für die Sicherheit von Containern und Kubernetes verantwortlich?



F9. Welche Rolle ist in Ihrem Unternehmen hauptsächlich für die Sicherheit von Containern und Kubernetes verantwortlich? Basisgröße: Gesamt = 600

Tatsächlich geben nur 34 % der Befragten an, dass Sicherheitsteams in ihrem Unternehmen die Hauptverantwortung für die Container- und Kubernetes-Sicherheit tragen. In 50 % der Unternehmen sind verschiedene Betriebsrollen, einschließlich ITOps, DevOps und DevSecOps, für die Sicherheit verantwortlich. Interessanterweise ist es in APAC-Organisationen wahrscheinlicher, dass ein DevSecOps Mitarbeiter die Hauptverantwortung trägt (21 %).

Durch fortschrittliche Kubernetes-Sicherheitstechnologien und -Prozesse können eine enge Zusammenarbeit zwischen verschiedenen Teams gefördert und Barrieren zwischen Domain-Fachleuten abgebaut werden. Entwicklungsteams können benutzerdefinierte Software, Open Source-Komponenten und Container-Images erstellen und integrieren. Sicherheitsfachleute können Richtlinien und Kontrollen für die Cluster-Ressourcen definieren und umsetzen. Zudem können Operations-Teams die Cluster-Infrastruktur, Zugriffskontrollen und Autorisierungsmechanismen verwalten – und das mit einer einheitlichen Sicherheitslösung.

Ergebnis 6:

DevSecOps-Praktiken sind in den verschiedensten Unternehmen weit verbreitet

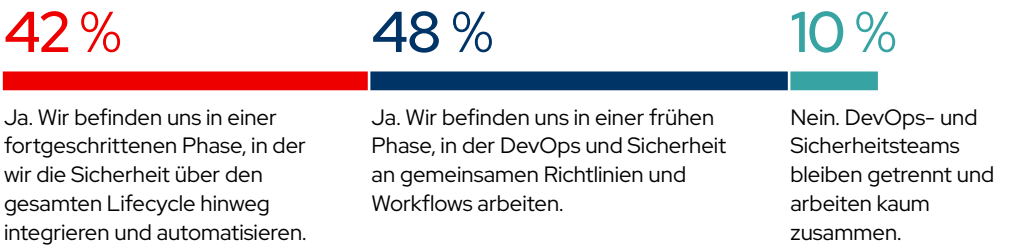
42 % der Befragten geben an, dass sich DevSecOps-Initiativen in ihrem Unternehmen in einem fortgeschrittenen Stadium befinden.

Unternehmen setzen weiterhin DevSecOps-Praktiken ein, um Sicherheitsrisiken früher in ihren Deployment-Prozessen für Container und Kubernetes zu erkennen und zu mindern. Tatsächlich sagen 42 % der Befragten, dass ihr Unternehmen die Sicherheit in den gesamten Anwendungs-Lifecycle integriert und automatisiert, indem es DevSecOps-Prozesse und -Tools wie automatisierte Tests, kontinuierliche Überwachung und Code Reviews einsetzt.

Gleichzeitig berichten 48 %, dass ihr Unternehmen den Wert von DevSecOps erkannt hat und sich in einem frühen Stadium der Einführung befindet, in dem Entwicklungs-, Operations- und Sicherheitsteams an gemeinsamen Richtlinien und Workflows arbeiten. Dies ist ein deutlicher Anstieg gegenüber dem letzten Jahr, als sich nur 39 %

der Befragten in dieser Phase befanden. Bei den verbleibenden 10 % der Unternehmen können getrennte DevOps- und Sicherheitsteams zu reaktiven Prozessen führen, die Vulnerabilities erst beim Deployment oder zur Runtime beheben. Dies führt zu einer geringeren Effizienz, Geschwindigkeit und Softwarequalität sowie zu einer langsameren Anwendungsbereitstellung.

Hat Ihr Unternehmen eine DevSecOps-Initiative?



Q25. Hat Ihr Unternehmen eine DevSecOps-Initiative? Basisgröße: Gesamt = 600

Ergebnis 7:

Kubernetes-Umgebungen führen zu neuen Sicherheitsherausforderungen

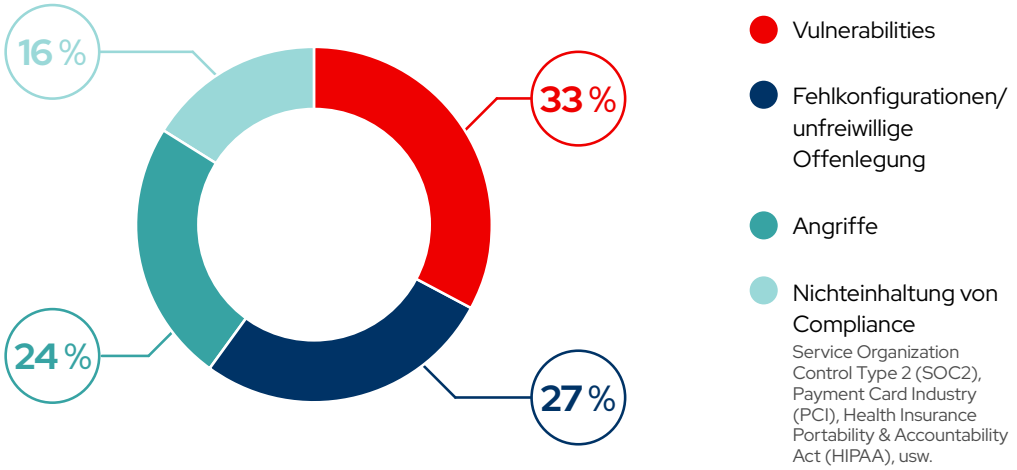
60 % der Befragten sorgen sich um Vulnerabilities, Fehlkonfigurationen und Gefährdungen in ihren Container- und Kubernetes-Umgebungen.

Das Beseitigen von Vulnerabilities in komplexen, dynamischen Kubernetes- und Container-Umgebungen kann schwierig sein. Da Container Host-Ressourcen wie Betriebssystem-Kernel gemeinsam nutzen, kann eine einzelne Vulnerability in einem Container mehrere Container betreffen. Außerdem kann eine Vulnerability in einem Host selbst sämtliche auf dem System installierten Container beeinträchtigen. Die Befragten sind sich dieser Herausforderung eindeutig bewusst, denn 33 % sind am meisten über Vulnerabilities in ihrer Container- und Kubernetes-Umgebung besorgt.

Eine der größten Sorgen von 27 % der Befragten ist, dass falsch konfigurierte Komponenten, einschließlich Basis-Images, Libraries und Abhängigkeiten, zu kritischen Sicherheitsproblemen für komplette Umgebungen führen können. Wenn diese Komponenten nicht ordnungsgemäß validiert und gewartet werden, können sie als potenzielle Angriffspunkte dienen und die Integrität und Vertraulichkeit wichtiger Anwendungen und sensibler Daten gefährden.

Diese Bedenken sind zwar berechtigt, können aber durch gründliche Sicherheitsverfahren entkräftet werden. Die Implementierung automatischer, kontinuierlicher Sicherheitsscans kann Ihnen beispielsweise dabei helfen, häufige Vulnerabilities zu erkennen und zu beheben und die korrekte Konfiguration sicherheitsrelevanter Komponenten zu sicherzustellen.

Über welches der folgenden Risiken für Ihre Container- und Kubernetes-Umgebungen sind Sie am meisten besorgt?



F10. Über welches der folgenden Risiken für Ihre Container- und Kubernetes-Umgebungen sind Sie am meisten besorgt? Basisgröße: Gesamt = 600

Ergebnis 8:

Organisationen befassen aktiv sich mit risikoreichen Themen

Fehlerhafter Code, ungeschützte sensible Daten, mangelhafte Netzwerksicherheit und unentdeckte Malware stellen die größten Sicherheitsrisiken dar.

Insgesamt gesehen gibt es für die Unternehmen kein einzelnes Hauptrisiko, sondern sie sind fast gleichermaßen besorgt über eine Vielzahl potenzieller Probleme. Angefangen bei Programmierfehlern (36 %) und der Preisgabe sensibler Daten (34 %) bis hin zu mangelhafter Netzwerksicherheit (32 %) und unentdeckter Malware (32 %) zeigen diese Sicherheitsrisiken die Notwendigkeit umfassender Strategien zur Minderung von Vulnerabilities und zum Schutz vor Cyberbedrohungen. Eine umfassende Analyse von Kubernetes- und Containerkomponenten kann Vulnerabilities und Fehlkonfigurationen aufdecken und Ihnen helfen, gezielte Fehlerbehebungsmaßnahmen in Ihrer Containerumgebung zu implementieren. Robuste, auf die Anforderungen der Anwendung abgestimmte Sicherheitsmaßnahmen können Risiken wirksam mindern, sensible Daten schützen und Bedrohungen abwehren. Benutzerfreundliche Sicherheitskontrollen, die in den gesamten Anwendungs-Lifecycle integriert sind, können die Compliance verbessern und das Risiko menschlicher Fehler verringern.

Die Ergebnisse unserer Umfrage zeigen, dass Unternehmen aktiv daran arbeiten, risikoreiche Probleme in ihren Container- und Kubernetes-Umgebungen zu reduzieren. Tatsächlich konzentriert sich mehr als die Hälfte der befragten Unternehmen auf alle potenziell risikoreichen Sicherheitsprobleme. Gleichzeitig befassen sich 66 % der Unternehmen mit Bedrohungen im Zusammenhang mit exponierten vertraulichen Daten, mangelhafter Netzwerksicherheit, überprivilegierten Containern und ungenutzten Komponenten.

Welche der folgenden Punkte gelten in Ihrem Unternehmen als besonders risikoreich?		Mit welchen der folgenden risikoreichen Themen befassen Sie sich in Ihrem Unternehmen? (Unter denen, die die jeweiligen Bedenken äußern.)
36 %	Programmierfehler	63 %
34 %	Offengelegte/ungeschützte sensible Daten	66 %
32 %	Schwache Netzwerksicherheit	66 %
32 %	Nicht erkannte Malware	64 %
31 %	Ungepatchte Fehler	64 %
27 %	Verwendung von unsicheren/nicht vertrauenswürdigen Repositories	56 %
26 %	Ungeeignete Zugriffskontrollen Identity Access Management (IAM) und Role-based Access Control (RBAC)	52 %
26 %	Beibehaltene unsichere Standardkonfigurationen	56 %
25 %	Container mit zu vielen Berechtigungen	66 %
25 %	Vorhandensein bekannter behebbarer Vulnerabilities	53 %
24 %	Erhöhte Angriffsfläche durch ungenutzte eingesetzte Komponenten	66 %
23 %	Veraltete, ungescannte oder nicht überprüfte Images	59 %
23 %	Ungeschützte Netzwerkports	53 %

F13. Welche der folgenden Punkte gelten in Ihrem Unternehmen als besonders risikoreich? Basisgröße: Gesamt = 600

F14. Mit welchen der folgenden risikoreichen Themen befassen Sie sich in Ihrem Unternehmen? Basisgröße: Unter denjenigen, die jedes Anliegen anführen = 139–213

Ergebnis 9:

Sicherheitsprobleme können schwerwiegende Folgen haben

Mehr als die Hälfte der Unternehmen stellte fest, dass in ihren Umgebungen nicht autorisierte Prozesse ausgeführt wurden.

Viele risikoreiche Sicherheitsprobleme – vom unbefugten Ausführen von Prozessen (45 %) über das Offenlegen sensibler Daten (43 %) bis hin zu Ransomware (41 %) – beschäftigen die Befragten. Dies zeigt, wie wichtig der Schutz vor verschiedenen Bedrohungen ist, welche die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Systemen gefährden können. Das unbefugte Ausführen von Prozessen stellt ein erhebliches Risiko dar und ermöglicht es böswilligen Akteuren, Systeme zu infiltrieren, Operationen zu stören und auf sensible Informationen zuzugreifen. Die Offenlegung sensibler Daten gibt Anlass zur Sorge über die Compliance und die finanziellen und rufschädigenden Auswirkungen von Datenpannen. Dazu können Ransomware-Angriffe zu erheblichen Unterbrechungen und finanziellen Verlusten für Unternehmen führen.

Diese Bedenken sind berechtigt. Hinsichtlich der einzelnen Sicherheitsprobleme, die wir in unserer Umfrage identifiziert haben, haben mehr Befragte tatsächliche Erfahrungen mit diesen Problemen als sich Sorgen darüber gemacht haben. Beispielsweise war die größte Sorge das unbefugte Ausführen von Prozessen, das von 45 % der Befragten genannt wurde. Allerdings berichteten 52 % der Befragten, dass in ihrem Unternehmen allein in den letzten 12 Monaten unzulässige Prozesse ausgeführt wurden. Noch größer ist diese Diskrepanz bei unbefugtem Zugriff auf interne Cloud-Ressourcen, DoS-Angriffen, kompromittierten Zugangsdaten und unbefugten Lateral Movements. 11–15 % mehr Unternehmen haben Erfahrungen mit diesen risikoreichen Problemen, als sich Sorgen darüber gemacht haben.

Welche der folgenden risikoreichen Themen bereiten Ihnen die größten Sorgen?

Welche der folgenden risikoreichen Probleme sind in Ihrem Unternehmen in den letzten 12 Monaten aufgetreten? (Unter denen, die die jeweiligen Bedenken äußern.)

F15. Welche der folgenden risikoreichen Themen bereiten Ihnen die größten Sorgen? Basisgröße: Gesamt = 600

F16. Welche der folgenden risikoreichen Probleme sind in Ihrem Unternehmen in den letzten 12 Monaten aufgetreten? Basisgröße: Unter denjenigen, die sämtliche Bedenken anführen = 189–270

Ergebnis 10:

Risikomanagement ist entscheidend für Softwarelieferketten

44 % der Befragten halten Software Vulnerabilities für den risikoreichsten Aspekt von Softwarelieferketten. Dies entspricht einem Anstieg von 9 % gegenüber dem Vorjahr.

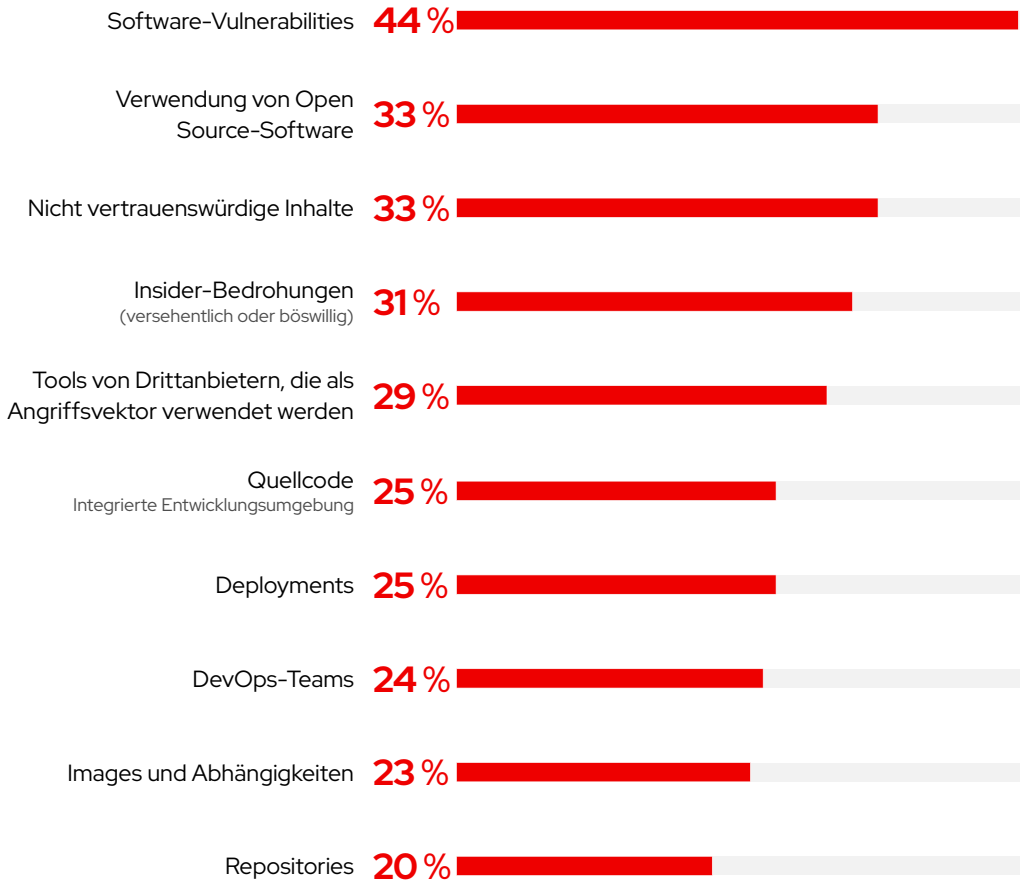
Die Sicherung von Softwarelieferketten kann aufgrund ihrer inhärenten Komplexität und globalen Reichweite eine Herausforderung darstellen. In Lieferketten wird häufig Software von verschiedenen kommerziellen Anbietern und Open Source-Projekten integriert, so dass es von entscheidender Bedeutung ist, die Integrität, Authentizität und Sicherheit der einzelnen Komponente zu gewährleisten.

Wir baten die Befragten, die risikoreichsten Aspekte von Softwarelieferketten zu nennen. Software Vulnerabilities (44 %), Open Source-Software (33 %) und nicht vertrauenswürdige Inhalte (33 %) rangieren in sämtlichen Unternehmen an der Spitze. Das ist sinnvoll, denn diese Aspekte können jeweils schwerwiegende Folgen haben. Software Vulnerabilities können zu Sicherheitsvorfällen wie Datenpannen und dem Ausführen von Malware führen. Open Source-Software muss ordnungsgemäß überprüft, gescannt und gewartet werden, um das Risiko des Auftretens neuer Vulnerabilities zu verringern. Nicht vertrauenswürdige Inhalte können zudem die Systemintegrität gefährden und unbefugten Zugriff ermöglichen.

Vor allem die Bedenken über Software Vulnerabilities stiegen um 9 % von 35 % im Jahr 2023 auf 44 % in diesem Jahr. Noch höher, nämlich auf 51 %, stuften die Befragten aus der Technologiebranche die Vulnerabilities ein. Wir stellten außerdem fest, dass die Befragten aus kleinen Unternehmen Insider-Bedrohungen überdurchschnittlich hoch einstuften, nämlich mit 36 % gegenüber 31 % insgesamt.

Unternehmen können diesen Herausforderungen mit einem umfassenden Ansatz für die Sicherheit der Softwarelieferkette begegnen, der strenge Lieferantenbewertungen, sicherheitsorientierte Coding-Methoden und eine kontinuierliche Überwachung der Softwareabhängigkeiten umfasst. Durch Priorisieren der Sicherheit in sämtlichen Phasen der Softwarelieferkette können Sie Risiken minimieren, sich vor Cyber-Bedrohungen schützen und die Integrität der Software für Ihre Nutzenden und Stakeholder gewährleisten.

Welche Sicherheitsaspekte der Softwarelieferkette stellen das größte Risiko dar?



F30. Welche Sicherheitsaspekte der Softwarelieferkette stellen das größte Risiko dar? Basisgröße: Gesamt = 600

Ergebnis 11:

Bedenken hinsichtlich der Sicherheit in der Softwarelieferkette sind berechtigt

57 % der Unternehmen entdeckten in den letzten 12 Monaten anfällige Anwendungskomponenten in ihrer Softwarelieferkette.

Die Sicherheit der Softwarelieferkette trägt dazu bei, die Integrität, Vertraulichkeit und Verfügbarkeit während des gesamten Anwendungs-Lifecycles sicherzustellen. Mit robusten Sicherheitsmaßnahmen können Unternehmen das Angriffsrisiko in der Lieferkette, den unbefugten Zugriff und Datenpannen mindern, um digitale Ressourcen zu schützen und das Vertrauen von Kunden und Stakeholdern zu erhalten.

Die Befragten äußerten jedoch viele Bedenken hinsichtlich der Sicherheit der Softwarelieferketten ihrer Unternehmen, darunter anfällige Anwendungskomponenten (37 %), unzureichende Zugriffskontrollen (32 %) und unsichere Container-Images (32 %). Wie bei den allgemeinen Sicherheitsaspekten (**Ergebnis 9**) sind diese Bedenken gerechtfertigt. Nahezu jedes in der Umfrage identifizierte Problem wurde von mehr als der Hälfte aller befragten Unternehmen beobachtet, wobei anfällige Anwendungskomponenten, mangelnde Automatisierung und fehlende SBOMs (Software Bills of Materials) bei fast 60 % der Unternehmen eine Rolle spielen.

Darüber hinaus gab es mindestens 1,5 Mal mehr Organisationen, die Erfahrungen mit den einzelnen Problemen machten als die, die darüber besorgt waren. Die vier am wenigsten besorgniserregenden Probleme – fehlende SBOMs, Schwächen in der CI/CD-Pipeline (Continuous Integration/Continuous Deployment), Schwächen in der Versionskontrolle und unsichere IaC-Templates (Infrastructure as Code) – traten bei mehr als doppelt so vielen Unternehmen auf als der Anzahl, die hinsichtlich dieser Probleme besorgt waren.

Über welche der folgenden Sicherheitsprobleme in der Softwarelieferkette ist Ihr Unternehmen am meisten besorgt?	Welche der folgenden Sicherheitsprobleme mit der Softwarelieferkette sind in Ihrem Unternehmen in den letzten 12 Monaten aufgetreten? (Unter denen, die die jeweiligen Bedenken äußern.)
Schwachstellen bei Anwendungskomponenten	37 % / 57 %
Unzureichende Zugriffskontrollen	32 % / 52 %
Unsichere Container Images	32 % / 49 %
Fehlende Auditierbarkeit	31 % / 54 %
Fehlende Automatisierung	30 % / 59 %
Inkonsistente Richtliniendurchsetzung	27 % / 54 %
Fehlende Software Bill of Materials (SBOM) oder Provenienz	26 % / 58 %
Schwachstellen in CI/CD-Pipelines (Continuous Integration/Continuous Deployment)	25 % / 56 %
Schwächen bei der Versionskontrolle	22 % / 51 %
Unsichere IaC-Templates (Infrastructure as Code)	18 % / 49 %

F32. Über welche der folgenden Sicherheitsprobleme in der Softwarelieferkette ist Ihr Unternehmen am meisten besorgt? Basisgröße: Gesamt = 600

F33. Welche der folgenden Sicherheitsprobleme mit der Softwarelieferkette sind in Ihrem Unternehmen in den letzten 12 Monaten aufgetreten? Basisgröße: Unter denjenigen, die sämtliche Bedenken anführen = 107–233

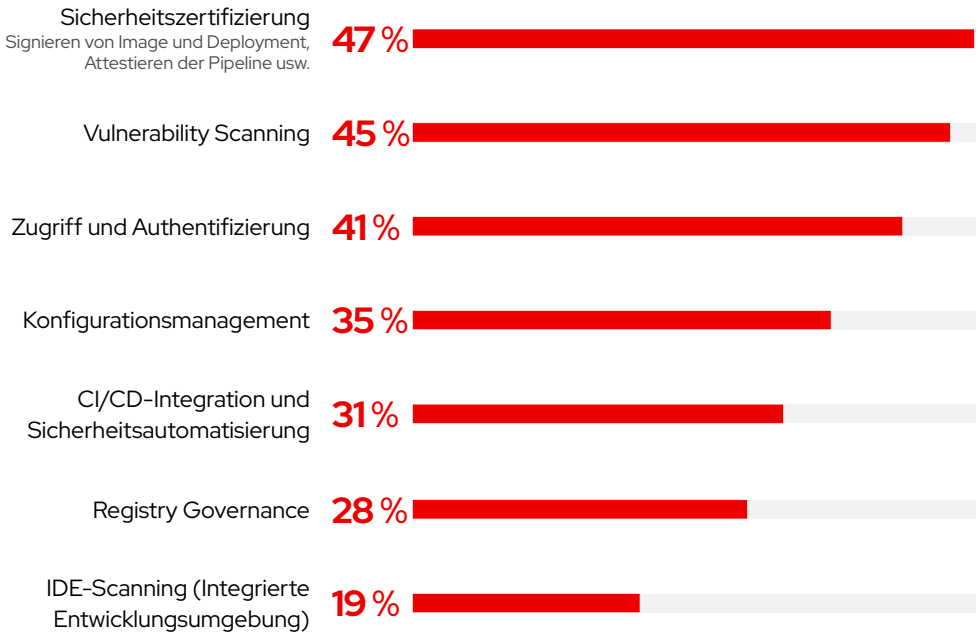
Ergebnis 12:

Tools und Prozesse unterstützen die Sicherheit der Softwarelieferkette

Fast die Hälfte der Befragten betrachtet die Sicherheitszertifizierung als eine wichtige Kontrolle der Softwarelieferkette.

Unternehmen minimieren Vulnerabilities und schützen kritische Softwarelieferketten mit einer Vielzahl moderner Sicherheitstools und -technologien, darunter Sicherheitszertifizierung (47 %), Vulnerability Scanning (45 %) sowie Zugriffs- und Authentifizierungsmechanismen (41 %). Durch Überprüfen der Herkunft, der Authentizität und der Compliance mit Sicherheitsstandards der einzelnen Softwarekomponenten hilft Ihnen die Sicherheitszertifizierung bei der Gewährleistung

Welche der folgenden Aspekte sind am wichtigsten, wenn es um die Sicherheit der Softwarelieferkette geht?



F31. Welche der folgenden Aspekte sind am wichtigsten, wenn es um die Sicherheit der Softwarelieferkette geht? (Bitte wählen Sie bis zu 3 der wichtigsten Aspekte aus.) Basisgröße: Insgesamt = 600

der Integrität und Vertrauenswürdigkeit von Anwendungen. Mit Vulnerability Scans können Sie Sicherheitsrisiken proaktiv vor dem möglichen Missbrauch begegnen, da potenzielle Schwachstellen und Vulnerabilities in Ihrer Softwarelieferkette identifiziert und behoben werden. Mit Zugriffs- und Authentifizierungsmechanismen wie Multifaktor-Authentifizierung (MFA) und RBAC können Sie das Risiko des unbefugten Zugriffs auf sensible Softwarekomponenten und Daten verringern.

Ergebnis 13:

Unternehmen nutzen Open Source Tools für Kubernetes-Sicherheit

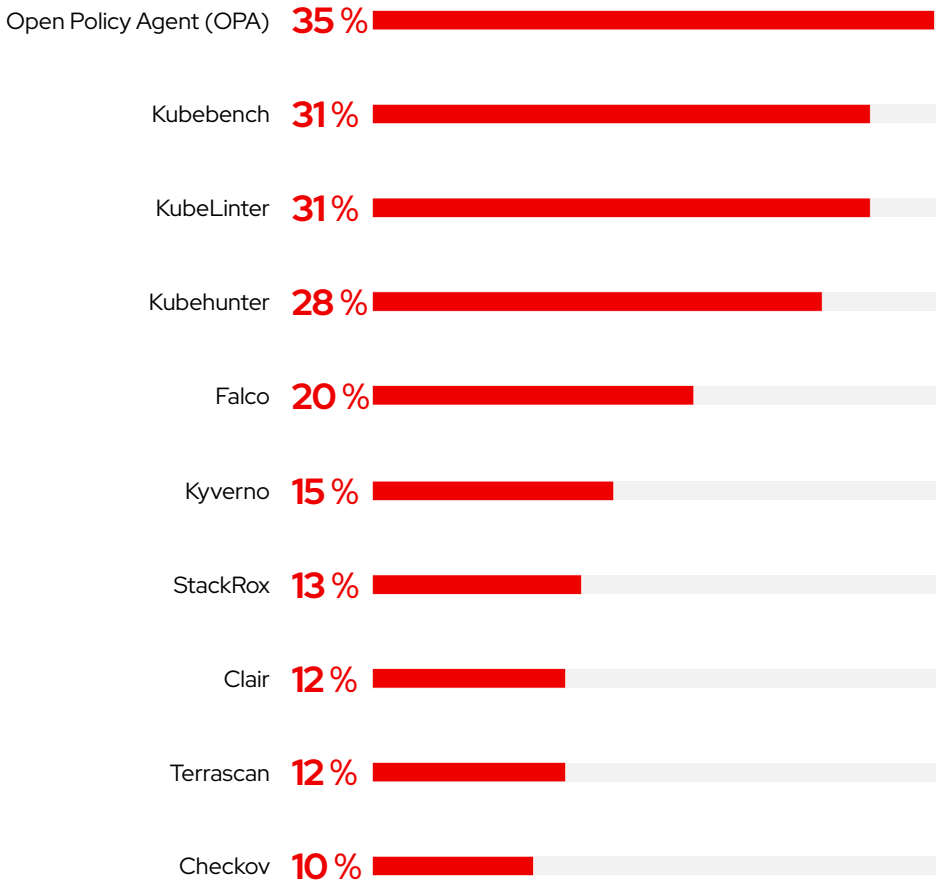
Open Policy Agent, Kube-bench und KubeLinter sind beliebte Open Source Kubernetes-Sicherheitstools.

Ein umfassendes IT-Ökosystem von Open Source Tools – mit fortschrittlichen Technologien, die von engagierten Mitwirkenden entwickelt wurden – bietet eine Vielzahl von Sicherheitslösungen für Container und Kubernetes-Umgebungen. Die befragten Unternehmen verlassen sich auf viele dieser Open Source-Sicherheitstools, um ihre cloudnativen Anwendungen zu schützen:

- 35 % vereinfachen die Richtlinienverwaltung mit **Open Policy Agent**, einem Toolset und Framework für einheitliche Richtlinien in verschiedenen cloudnativen Stacks.
- 31 % überprüfen die Sicherheit des Kubernetes-Deployments mittels **CIS Kubernetes Benchmark** mit **Kube-bench**.
- 31 % stellen mit **KubeLinter**, einem statischen Analyse-Tool für Kubernetes-YAML-Dateien und Helm-Diagramme sicher, dass Anwendungen die Best Practices einhalten.
- 28 % identifizieren Sicherheitsprobleme in Kubernetes-Clustern und cloudnativen Umgebungen mithilfe von **Kube-hunter**, einem Sicherheitstest- und Scan-Tool.

Insgesamt verwenden Unternehmen durchschnittlich 2,1 sicherheitsrelevante Open Source-Tools in ihren Kubernetes-Umgebungen.

Welche der folgenden Open Source-Tools verwenden Sie für die Kubernetes-Sicherheit?



F20. Welche der folgenden Open Source-Tools verwenden Sie für die Kubernetes-Sicherheit? Basisgröße: Gesamt = 600

Verbessern Ihrer Container- und Kubernetes-Sicherheit

Container und Kubernetes können Entwicklung und Deployment von Anwendungen in Hybrid Cloud-Umgebungen beschleunigen. Durch das Integrieren sicherheitsorientierter Prozesse und Technologien in den gesamten Lifecycle können Sie Anwendungen schützen, ohne die Entwicklung zu verlangsamen oder die operative Komplexität zu erhöhen. Sichern Sie sensible Daten, geistiges Eigentum und Kundeninformationen. Erfüllen Sie die gesetzlichen Anforderungen von Unternehmen, Branchen und Behörden. Stellen Sie Business Continuity sicher. Erhalten Sie das Vertrauen der Kunden aufrecht. Senken Sie die Kosten für verspätete Fehlerbehebungen.

Im Folgenden finden Sie 3 Tipps zum Erhöhen der Sicherheit Ihrer cloudnativen Umgebungen.

1 Verwenden Kubernetes-nativer Sicherheitskontrollen

Kubernetes-native Sicherheit nutzt deklarative Daten und native Kontrollen zum Schutz Ihrer Container-Workloads.

- Analysieren Sie die in Kubernetes verfügbaren deklarativen Daten, um risikobasierte Insights in Konfigurationsmanagement, Compliance, Segmentierung und Vulnerabilities zu gewinnen.
- Vereinfachen und beschleunigen Sie die Analyse und Fehlerbehebung, indem Sie dieselbe Infrastruktur und Kontrolle für Entwicklung und Sicherheit nutzen.
- Reduzieren Sie operative Reibungen durch Sicherheitsautomatisierung und Skalierung.

2 Erweiterte Sicherheit über den gesamten Anwendungs-Lifecycle

Ein Fokus auf Sicherheit in sämtlichen Phasen des Anwendungs-Lifecycles unterstützt Sie beim frühzeitigen Erkennen und Beseitigen potenzieller Vulnerabilities und verringert so das Risiko von Datenpannen, Cyberangriffen und einer Beeinträchtigung des Vertrauens der Nutzenden.

- Integrieren Sie bewährte DevSecOps-Praktiken und interne Kontrollen in die Konfigurationsprüfungen innerhalb Ihrer Sicherheitsplattform.
- Automatisieren Sie Sicherheitsbewertungen der Kubernetes-Konfiguration mit Ihrer Container- und Kubernetes-Plattform.

3 Einführen von Tools, die DevSecOps-Praktiken unterstützen

Die richtigen Sicherheitstechnologien und -lösungen können die Zusammenarbeit zwischen Ihren Entwicklungs-, Sicherheits- und Operations-Teams verbessern.

- Nutzen Sie Ihre Container- und Kubernetes-Plattform, um Risikobeurteilungen durchzuführen und Sicherheitskontrollen für Ihre Umgebungen bereitzustellen.
- Führen Sie Tools ein, die Vulnerabilities in aktiven Deployments identifizieren und erklären können, um sicherheitsorientierte Praktiken zu verstehen und anzuwenden.

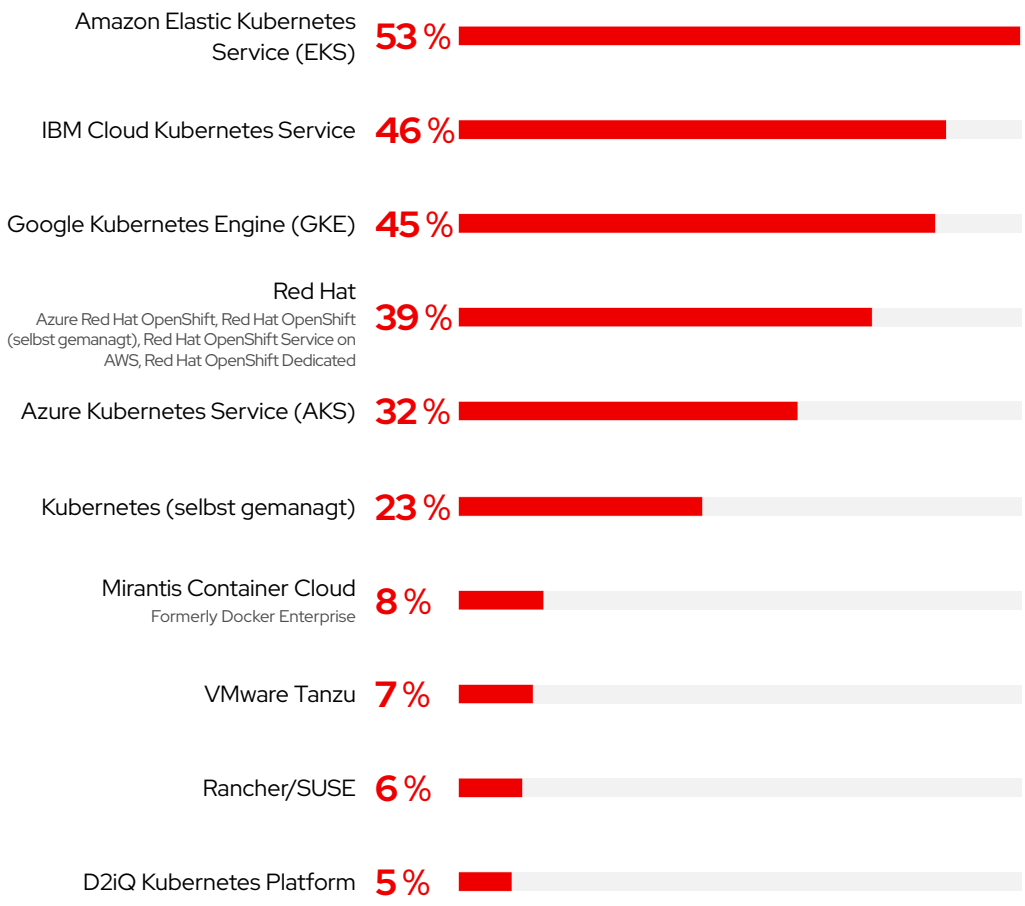
Über die Befragten

In diesem Abschnitt finden Sie weitere Einzelheiten über die Befragten und ihre Organisationen.

Einführung von Kubernetes

Die meisten Befragten nutzen Kubernetes in der Produktion, wobei cloudbasierte Kubernetes-Lösungen die beliebtesten Plattformen sind.

Welche Kubernetes-Plattform nutzen Sie zur Orchestrierung Ihrer Container?

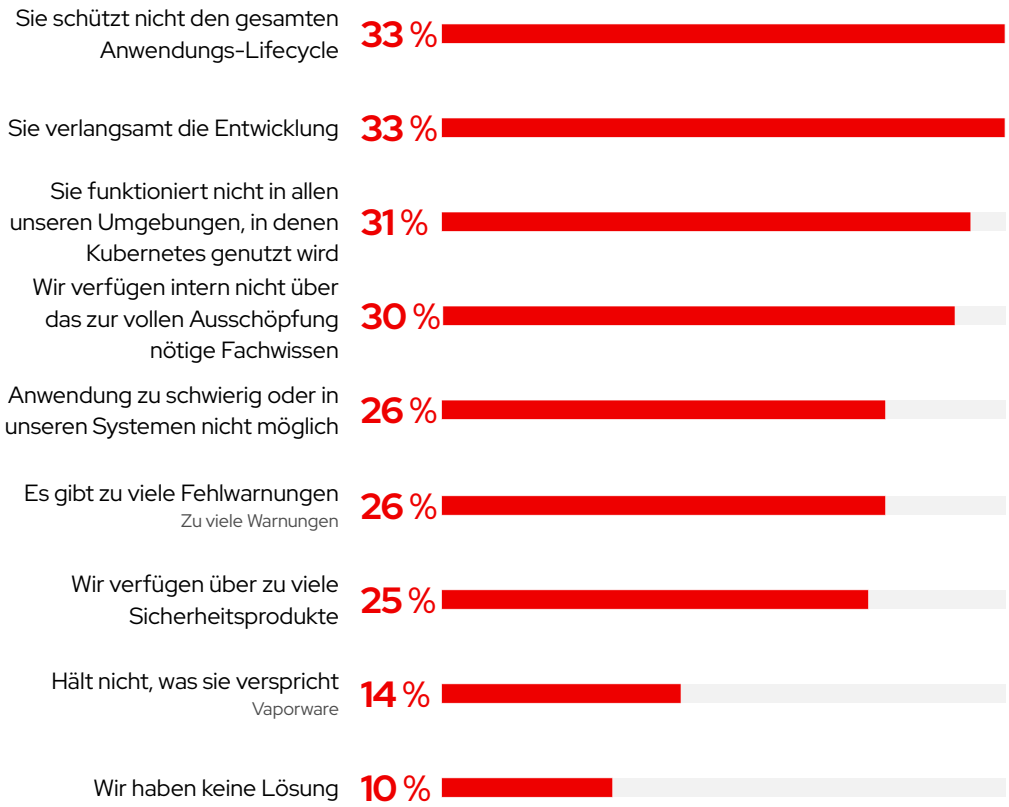


F3. Welche Kubernetes-Plattform nutzen Sie zur Orchestrierung Ihrer Container? Basisgröße: Diejenigen, die Kubernetes verwenden = 390

Verbreitete Hauptprobleme

Mangelnde Sicherheit für den gesamten Lifecycle und ein langsames Deployment werden im Zusammenhang mit den aktuellen Kubernetes-Sicherheitslösungen am häufigsten beklagt.

Welche sind die größten Problempunkte im Zusammenhang mit Ihrer aktuellen Kubernetes-Sicherheitslösung?

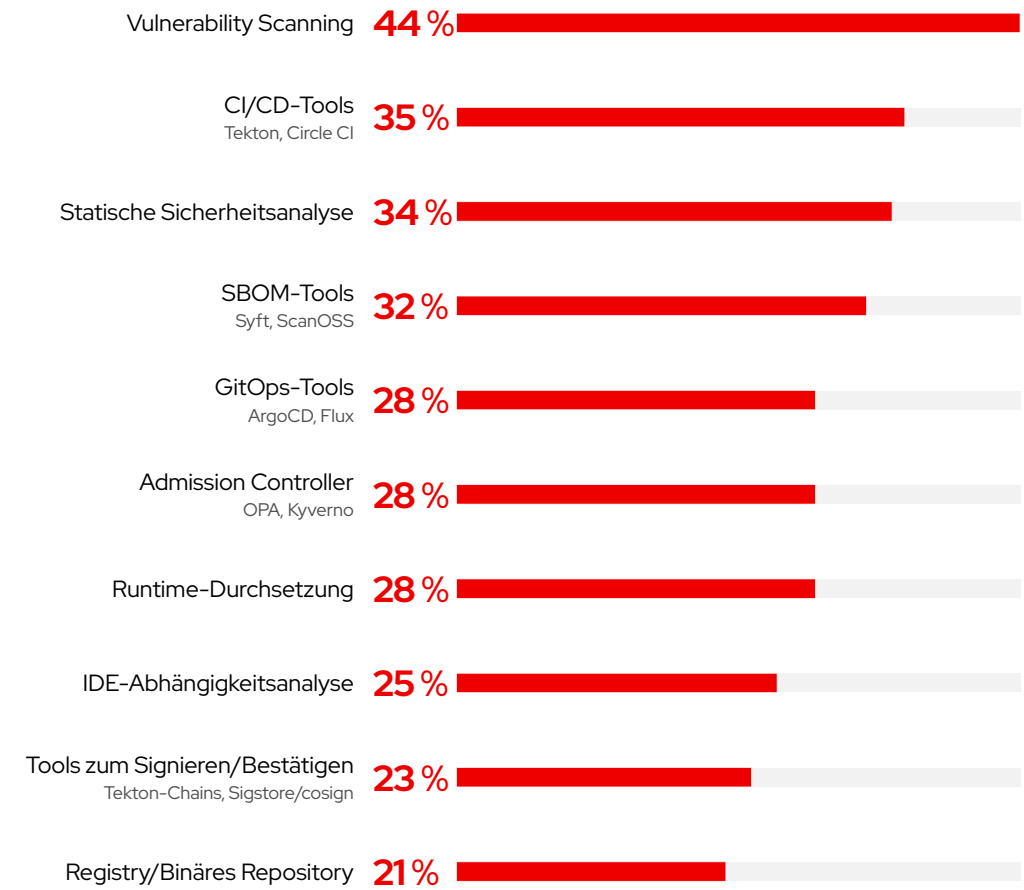


F26. Welche sind die größten Problempunkte im Zusammenhang mit Ihrer aktuellen Kubernetes-Sicherheitslösung? (Bitte wählen Sie bis zu 3 der Hauptprobleme aus.) Basisgröße: Insgesamt = 600

Sicherheits-Tools für die Lieferketten

Vulnerability-Scanner sind das am häufigsten verwendete Sicherheitstool, gefolgt von CI/CD, statischer Sicherheitsanalyse und SBOM-Tools. Unternehmen verwenden durchschnittlich 3 Sicherheitstools für ihre Softwarelieferketten.

Welche der folgenden Arten von Sicherheitstools verwenden Sie für Ihre Softwarelieferkette?

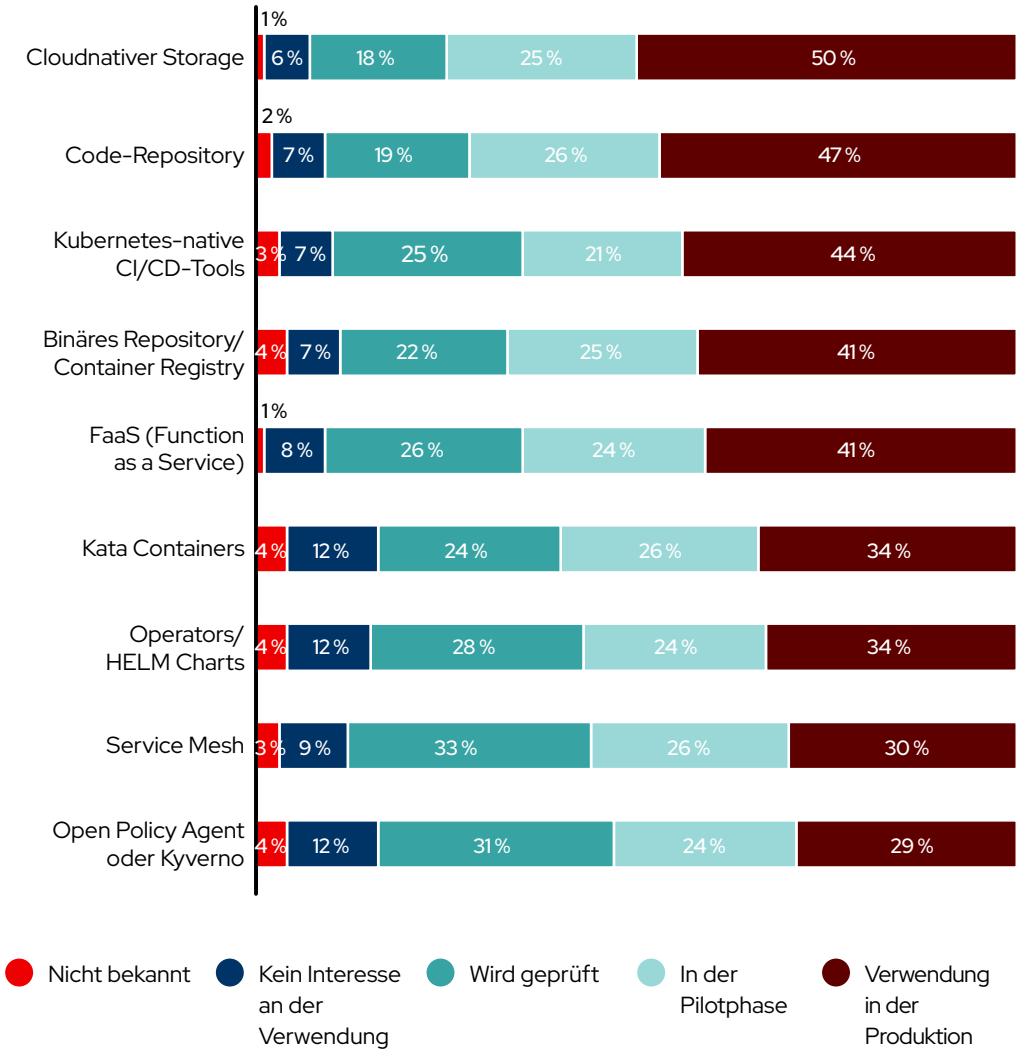


F22. Welche der folgenden Arten von Sicherheitstools verwenden Sie für Ihre Softwarelieferkette? Basisgröße: Gesamt = 600

Sonstige cloudnative Technologien

Kubernetes-native CI/CD-Tools gehören zu den am häufigsten verwendeten Arten cloudnativer Technologien.

Welche anderen cloudnativen Technologien erwägen oder nutzen Sie derzeit?



F6. Welche anderen cloudnativen Technologien erwägen oder nutzen Sie derzeit? Basisgröße: Gesamt = 600

Wegen Rundungen ist es möglich, dass Prozentwerte zusammengerechnet nicht 100 % ergeben.

Erste Schritte mit Red Hat Advanced Cluster Security für Kubernetes

Red Hat® Advanced Cluster Security for Kubernetes ist eine Kubernetes-native Sicherheitsplattform, mit der Sie cloudnative Anwendungen mit mehr Sicherheit entwickeln, bereitstellen und ausführen können. Mit Red Hat Advanced Cluster Security können Sie containerisierte Kubernetes-Workloads in den wichtigsten Public Cloud-Umgebungen und Hybrid Cloud-Plattformen schützen. Dazu gehören Red Hat OpenShift, Amazon Elastic Kubernetes Service (EKS), Microsoft Azure Kubernetes Service (AKS) und Google Kubernetes Engine (GKE).

Minimieren des operativen Risikos

Überwachen, erfassen und werten Sie Events auf Systemebene aus, beispielsweise das Ausführen von Prozessen, Netzwerkverbindungen und -flüsse sowie das Erweitern von Berechtigungen, um böswillige Aktivitäten wie aktive Malware, unbefugten Zugriff, Intrusionen und Lateral Movement zu erkennen.

Erhöhen der DevSecOps-Produktivität

Integrieren Sie Red Hat Advanced Cluster Security in Ihre CI/CD-Pipelines und Image Registries, um anfällige und falsch konfigurierte Images schnell zu beheben – direkt in Entwicklungsumgebungen – mit Echtzeit-Feedback und Warnmeldungen.

Schützen der Kubernetes-Infrastruktur

Stellen Sie sicher, dass Ihre Kubernetes-Infrastruktur durch kontinuierliche Scans anhand von CIS-Benchmarks und anderen bewährten Sicherheitspraktiken gehärtet und geschützt bleibt.

Vereinbaren Sie einen Termin für eine persönliche Demo von Red Hat Advanced Cluster Security for Kubernetes, die auf Ihr Unternehmen und Ihre Anforderungen abgestimmt ist.

Red Hat