

Mehr Sicherheit in der Hybrid Cloud



Schützen Sie Ihr Unternehmen mit wichtigen cloudnativen Sicherheitsaspekten

/Flexible Optionen



Von Lucy Huh Kerner, Director, Security Global Strategy and Evangelism, Red Hat

Inhaltsverzeichnis



Kapitel 1

Bereitstellen einer
sicherheitsorientierten
Hybrid Cloud

03



Kapitel 3

Sicherheitsaspekt 1:

Beginnen Sie mit einer
starken Basis

08



Kapitel 5

Sicherheitsaspekt 3:

Schützen Sie Ihre
Hybrid Cloud mit
Automatisierung und
Management

15



Kapitel 2

Sicherheit ist ein Prozess
und kein Produkt

06



Kapitel 4

Sicherheitsaspekt 2:

Implementieren Sie eine
bewährte Softwarelieferkette
mit DevSecOps

11



Kapitel 6

Bereit für den Einstieg?

19

Kapitel 1

Bereitstellen einer sicherheitsorientierten Hybrid Cloud

Die Nutzung der Cloud erfreut sich einer wachsenden Beliebtheit. Aktuell geben 65 % der Organisationen an, dass sie die Cloud in großem Umfang nutzen, und 72 % der Unternehmen verfolgen eine Hybrid Cloud-Strategie.¹

Hybrid Cloud ist eine IT-Architektur, bei der die Portierbarkeit, die Orchestrierung und das Management von Workloads über 2 oder mehr vernetzte, aber separate Umgebungen zu einem gewissen Grad integriert sind, darunter Bare Metal-, Private Cloud-, Public Cloud- und virtualisierte Umgebungen. Mit einer Hybrid Cloud-Architektur können Sie Workloads in beliebigen vernetzten Umgebungen ausführen und Ressourcen aus diesen Umgebungen austauschbar verschieben und nutzen.



Durch den Einsatz von Hybrid Cloud-Umgebungen können Organisationen:



Infrastruktur, Plattformen, Anwendungen und Tools von verschiedenen Anbietern miteinander verbinden



Effizienz und Skalierbarkeit verbessern



Kosten senken



Agilität erhöhen



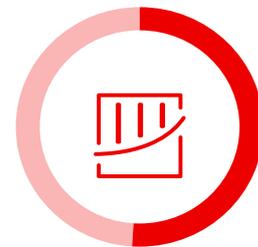
Datenplatzierung optimieren

¹ Flexera: „Flexera 2023 State of the Cloud Report“, März 2023.

Unabhängig davon, in welchem Umfang Sie Hybrid Cloud-Technologie aktuell nutzen – Sicherheit ist immer ein wichtiges Thema. Dabei bezeichnen 79 % der Unternehmen die Cloud-Sicherheit als eine Herausforderung.¹ Schwachstellen bei der Hybrid Cloud-Sicherheit entstehen normalerweise durch einen Verlust der Kontrolle über Ressourcen, einschließlich unberechtigter Public Cloud-Nutzung, fehlender Transparenz der Ressourcen, unangemessener Änderungskontrolle, schlechtem Konfigurationsmanagement, unwirksamen Zugriffskontrollen, menschlichen Fehlern und anderen Auslösern. Unbefugte Nutzende können diese Lücken ausnutzen, um sich Zugriff auf vertrauliche Daten und interne Ressourcen zu verschaffen, was sehr kostspielig sein kann.



Die durchschnittlichen globalen Kosten einer Datenpanne haben im Jahr 2023 mit **4,45 Millionen USD** ein neues Hoch erreicht, wobei **29,2 %** dieser Kosten auf Geschäftsverluste zurückgehen.²



51 %

der Unternehmen geben an, ihre Sicherheitsinvestitionen nach einer Datenpanne erhöhen zu wollen.²



¹ Flexera: „Flexera 2023 State of the Cloud Report“, März 2023.

² IBM Security: „Cost of a Data Breach Report 2023“, 2023.

Sowohl die durchschnittlichen Kosten pro Datensatz bei einer Datenpanne als auch die Zeit, die für die Eindämmung von Sicherheitsverletzungen benötigt wird, sind im Jahr 2023 angestiegen.² Indem Sie Ihre Methoden anpassen, um den Unterschieden zwischen einer On-Premise- und einer Cloud-Architektur Rechnung zu tragen, können Sie eine [sicherheitsorientierte Hybrid Cloud](#) bereitstellen, mit der Sie diese wachsenden Herausforderungen überwinden können. In diesem E-Book werden neue Ansätze und Aspekte für die Sicherheit Ihrer Hybrid Cloud erläutert.



**277
Tage**

durchschnittlicher Zeitraum zur Erkennung und Eindämmung einer Datenpanne im Jahr 2023²

**USD
1,02
Millionen**

Kosteneinsparungen, wenn die Erkennung und Eindämmung einer Datenpanne in maximal 200 Tagen erfolgt²

² IBM Security: „Cost of a Data Breach Report 2023“, 2023.

Kapitel 2

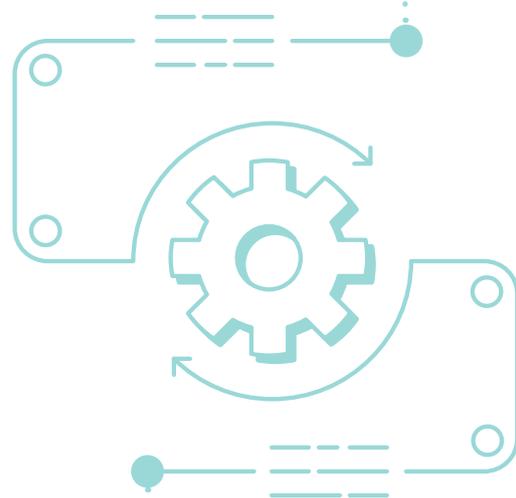
Sicherheit ist ein Prozess und kein Produkt

Effektive Sicherheit erfordert einen ganzheitlichen Ansatz, bei dem Personal, Prozesse und Technologien berücksichtigt werden. Die Bereitstellung sicherheitsorientierter Produkte und Tools alleine reicht nicht aus, um Ihre Infrastruktur, Ihre Cloud oder Ihr Unternehmen zu schützen. Sie sollten darüber hinaus Sicherheitsstrategien und -prozesse in Betracht ziehen, um die Fähigkeiten Ihrer Produkte zu maximieren und Risiken zu mindern.

Diese Strategien und Prozesse können laufend an neue Technologien, Bedrohungen und Anforderungen angepasst werden. Da Hybrid Cloud-Umgebungen keinen festgelegten Umfang haben, sind traditionelle Sicherheitsansätze ineffektiv und müssen angepasst werden.

Zentralisiertes Identitätsmanagement und Zugriffskontrolle sind für cloudzentrierte Sicherheitsansätze von großer Bedeutung. Dabei wird das Least Privilege-Prinzip verwendet, um Nutzenden nur die Zugriffsberechtigungen zu geben, die sie auch benötigen. Bei dieser Methode werden die aktuellen Zugriffsrechte der Nutzenden überprüft. Anschließend wird der Nutzer oder die Nutzerin neu eingestuft, um die richtige Zugriffsebene festzulegen.

Hybrid Cloud-Sicherheit erfordert außerdem eine mehrschichtige „Defense in Depth“-Sicherheitsstrategie. Dabei kommen die Funktionen der einzelnen Schichten in Ihrer Umgebung, wie Betriebssysteme, Container-Plattformen und Automatisierungstools, zum Einsatz.



Betriebssystem

Nutzen Sie integrierte Tools, mit denen Sie die Anforderungen für Sicherheits-Compliance erfüllen, physische Sicherheit implementieren, die Netzwerksicherheit verbessern, den Benutzerzugriff kontrollieren, Prozesse isolieren und die Datensicherheit erhöhen können. Hierzu gehören beispielsweise OpenSCAP, USBGuard, Security-Enhanced Linux® (SELinux), Identitätsmanagement und NBDE (Network Bound Disk Encryption).



Container-Plattform

Setzen Sie integrierte Funktionen innerhalb Ihrer Plattform und Kubernetes ein, um die Container-Sicherheit zu erhöhen. Hierzu gehören beispielsweise Pod-Sicherheitsrichtlinien, Kontrollen des Netzwerktraffics, Kontrollen für Cluster-Ingress und -Egress, rollenbasierte Zugriffskontrollen (Role-based Access Controls, RBACs), integrierte Zertifikatsverwaltung und Mikrosegmentierung des Netzwerks.



Automatisierungstools

Wählen Sie eine Automatisierungssprache und -plattform, die sämtliche Mitarbeitenden innerhalb Ihres Unternehmens, darunter Entwicklungs-, IT-Operations-, Sicherheits- und Compliance-Teams, leicht erlernen und anwenden können. Nutzen Sie Funktionen für Zugriffskontrolle, Protokollierung und Auditing.

Es ist außerdem wichtig, Ihre vorhandenen Sicherheitsprozesse und -tools zu überprüfen. Stellen Sie sicher, dass Sie die verfügbaren Features verwenden. Stellen Sie fest, ob eine Änderung oder Neukonfiguration der Einstellungen möglich ist, um den Schutz zu verbessern, oder ob neue Prozesse und Tools erforderlich sind.

- 1** Erstellen Sie ein Inventory Ihrer aktuellen IT-Assets und -Tools.
- 2** Dokumentieren Sie Ihre vorhandenen Sicherheits- und Netzwerkarchitekturen, Richtlinien zur Cybersicherheit, Arbeitsprozesse sowie Qualifikationen und Kompetenzlücken.
- 3** Entwickeln Sie ein Bedrohungsmodell, und legen Sie Strategien für Risikotoleranz und -minimierung bei Verletzungen der Cybersicherheit fest.
- 4** Bewerten Sie Ihre Architekturen, Richtlinien und Prozesse, und ermitteln Sie Bereiche, in denen Änderungen erforderlich sind.
- 5** Beurteilen Sie Ihre aktuellen Tools und Assets dahingehend, ob sie Ihre aktualisierten Strategien und Prozesse unterstützen können. Dokumentieren und planen Sie, wie Sie Sicherheitslücken beseitigen können.

In den folgenden Abschnitten werden wichtige Aspekte der Hybrid Cloud-Sicherheit behandelt. Außerdem erhalten Sie Tipps zur Verbesserung Ihres Schutzes.



Kapitel 3

Sicherheitsaspekt 1

Beginnen Sie mit einer starken Basis

Warum ist das wichtig?

Wenn Ihre Workloads auf mehrere Umgebungen verteilt sind oder wenn Sie nicht geprüfte Open Source-Technologien in Ihrer Umgebung verwenden, kann es schwierig sein, die Schwachstellen zu identifizieren. Hinzu kommt, dass sich Risiken bei mehrschichtiger Sicherheit nicht so leicht mindern lassen, wenn diese nicht auf einer starken Sicherheitsbasis aufbaut. Die Verwendung von Open Source-Software direkt von Upstream Communities kann dazu führen, dass Sie Risiken und Lieferketten-Angriffen ausgesetzt sind, bei denen die Schwachstellen von Drittanbieter-Services und -Software ausgenutzt werden, um ein

Endziel zu gefährden. Diese Angriffe können verschiedene Formen annehmen, wie das Hijacking von Software-Updates und das Einschleusen von unerwünschtem Code in legitime Software. In den vergangenen 3 Jahren ist die Anzahl der Angriffe auf die Softwarelieferkette um durchschnittlich 742 % pro Jahr gestiegen.³ Deshalb ist es wichtig, Ihr Unternehmen mit einer einheitlichen, stabilen und sicherheitsorientierten Basis zu schützen.

Empfehlungen und Best Practices

Reduzieren Sie Sicherheitsrisiken in Ihrer Softwarelieferkette, indem Sie Open Source-Software von einem vertrauenswürdigen Open Source-Anbieter für Unternehmen nutzen, der während des gesamten Lifecycles der Software Unternehmenssupport bietet, wie Red Hat. Ein Anbieter von Open Source-Software für Unternehmen entwickelt seine Software mit einem robusten Sicherheitsprozess für die Softwarelieferkette, der unter anderem das Kuratieren von Open Source-Software für seine Kunden beinhaltet. Dadurch stellt er sicher, dass die Open Source-Software, die Kunden verwenden, vertrauenswürdig, resilient und sicher ist.

Zusätzlich ist es wichtig, kritische Anwendungen auf einer Plattform mit integrierten Sicherheitsfunktionen auszuführen. Diese bildet die

Sicherheitsbasis, auf der Kunden zuverlässig kritische Anwendungen ausführen, mehrschichtige Sicherheitsfunktionen integrieren sowie Compliance- und Sicherheitsautomatisierung implementieren können.

Mit einem resilienten, bewährten Betriebssystem wie [Red Hat® Enterprise Linux®](#), das für Stabilität und Sicherheit gehärtet wurde, machen Sie eine sicherheitsorientierte Basis für Anwendungen und Prozesse zur Priorität. Dadurch entsteht eine stabile Basis, mit der Sie zuverlässig kritische Anwendungen skalieren, Sicherheits-Compliance einhalten und neue Technologien einheitlich einführen können – in Bare Metal-, virtuellen, Container- und anderen Arten von Cloud-Umgebungen.



³ Sonatype: „9th Annual State of the Software Supply Chain“, 2023.

Red Hat Enterprise Linux ist die Basis für den Großteil des Red Hat Portfolios und ist aufgrund seiner integrierten Sicherheitsfunktionen das bewährte Betriebssystem vieler Unternehmen.

Red Hat Enterprise Linux bietet folgende Vorteile:



Mindern Sie mit integrierten Sicherheitsfunktionen wie Live-Kernel-Patching das Risiko einer Offenlegung von Daten oder Systemen. So können Sie Sicherheits-Patches anwenden, ohne dass ein Neustart oder eine Unterbrechung der Runtime erforderlich ist. Darüber hinaus gibt es weitere integrierte Sicherheitsfunktionen, wie z. B. das Erstellen von Allowlists für Anwendungen. Dabei wird ein Index genehmigter Anwendungen oder ausführbarer Dateien angegeben, die von bestimmten Nutzenden auf einem System ausgeführt werden dürfen. Mit [SELinux](#) können Sie detaillierte Kontrolle über Dateien, Prozesse, Nutzende, Anwendungen und mehr erhalten.



Automatisieren Sie den Datenschutz in großem Umfang und halten Sie ihn mithilfe von integrierten Sicherheitsfunktionen wie zum Beispiel Network Bound Disk Encryption aufrecht, mit der sie das Entsperren verschlüsselter Systeme ohne die Verwaltung von Verschlüsselungsschlüsseln automatisieren können. Zusätzlich können Sie sich mit den systemweiten Verschlüsselungsrichtlinien darauf konzentrieren, Ihre Daten zu schützen, und außerdem Compliance-Anforderungen mit systemweiten, konsistenten und benutzerdefinierten Verschlüsselungseinstellungen erfüllen und so Ihre standortspezifischen Richtlinienanforderungen erfüllen.



Erfüllen Sie Compliance-Anforderungen und optimieren Sie Audits. Red Hat Enterprise Linux bietet integriertes Compliance-Scanning und Fehlerbehebung mit OpenSCAP, mit der Sie Konfigurations- und Schwachstellenscans auf einem lokalen System durchführen und die Compliance mit einer Vielzahl von Branchensicherheitsstandards überprüfen können.

Mit dem grundlegenden Sicherheitsansatz von Red Hat Enterprise Linux bieten die darauf aufbauenden Produkte, wie **Red Hat OpenShift**, eine umfassende Verteidigung für Container und Kubernetes. Red Hat weitet die Sicherheitsfunktionen im Stack auf die Kubernetes-Komponenten aus. Ebenso können Unternehmen mit den integrierten Sicherheitsfunktionen von **Red Hat Ansible Automation Platform** Sicherheits- und Compliance-Automatisierung in großem Umfang implementieren.



Taktische Schritte

Führen Sie bei Ihrem Einstieg in die Hybrid Cloud-Sicherheit folgende Schritte aus:



Wechseln Sie zu handelsüblichen Versionen.

Migrieren Sie Ihre Open Source-Software direkt aus Upstream Open Source-Projekten zu vertrauenswürdigen, **handelsüblichen Versionen**. Diese Versionen sind getestet und validiert, um das Risiko von Bugs und Sicherheitslücken zu reduzieren. Außerdem bieten sie oft Support auf Unternehmensniveau, mit dem Sie schnell Sicherheits-Patches und Anleitungen zum Konfigurieren Ihrer Software im Hinblick auf Sicherheit erhalten. Mit der Open Source-Software von einem vertrauenswürdigen Open Source-Anbieter für Unternehmen können Sie sicherstellen, dass die Software mit einem robusten Sicherheitsprozess für die Softwarelieferkette entwickelt wurde und Sie Unternehmenssupport für den gesamten Lifecycle der Software erhalten. Diese Faktoren tragen dazu bei, dass Unternehmen Open Source-Software nutzen und gleichzeitig Sicherheitsrisiken mindern können.



Wählen Sie eine Plattform mit integrierten Sicherheitsfunktionen.

Es ist wichtig, sich für eine Plattform (beispielsweise ein Betriebssystem, eine Container-Anwendungsplattform oder eine Automatisierungsplattform) mit integrierten Sicherheitsfunktionen zu entscheiden. Diese bildet die Sicherheitsbasis, auf der Kunden zuverlässig kritische Anwendungen ausführen, mehrschichtige Sicherheitsfunktionen integrieren sowie Compliance- und Sicherheitsautomatisierung in großem Umfang implementieren können.



Implementieren Sie Sicherheit in Ihrem gesamten Technologie-Stack.

Nachdem Sie eine grundlegende Sicherheitsbasis geschaffen haben, sollten Sie sicherstellen, dass die Technologien, die auf dieser Basis ausgeführt werden, ebenfalls diese Sicherheitsvorteile aufweisen und sie gemeinsam eine mehrschichtige Sicherheit bieten.



Kapitel 4

Sicherheitsaspekt 2

Implementieren Sie eine bewährte Softwarelieferkette mit **DevSecOps**

Warum ist das wichtig?

Im Jahr 2023 wurden 12 % der Datenpannen durch einen Angriff auf die Softwarelieferkette ausgelöst.² Die Verwendung nicht geprüfter Open Source-Software direkt von Upstream Communities kann dazu führen, dass Sie Sicherheitsverletzungen und Lieferketten-Angriffen ausgesetzt sind, bei denen die Schwachstellen von Drittanbieter-Services und -Software ausgenutzt werden, um ein Endziel zu gefährden. Diese Angriffe können verschiedene Formen annehmen, wie das Hijacking von Software-Updates und das Einschleusen von unerwünschtem Code in legitime Software.

Isolierte Sicherheitsansätze führen häufig zu Sicherheitslücken und doppeltem Aufwand, weil die Sicherheit bei Anwendungsentwicklung und Infrastrukturbereitstellung leicht in den Hintergrund gerät. Bei zunehmender Entwicklungsgeschwindigkeit und Bereitstellungsflexibilität wird es immer wichtiger, die Sicherheit im gesamten Prozess zu berücksichtigen.

Empfehlungen und Best Practices

Um einen sicherheitsorientierten Ansatz für ihre Softwarelieferkette einzuführen, sollten Sie zuerst eine DevSecOps-Mentalität entwickeln. Bei einer DevSecOps-Mentalität arbeiten Anwendungsentwicklungs-, IT-Operations und Sicherheitsteams zusammen, um die Sicherheit der Softwarelieferkette im gesamten Infrastruktur- und Softwareentwicklungs-Lifecycle (SDLC) zu implementieren. Dieser Prozess findet dabei auf einer unternehmensgehärteten Open Source-Basis in einer Hybrid Cloud statt.

² IBM Security: „Cost of a Data Breach Report 2023“, 2023.

DevSecOps automatisiert die Integration von Sicherheit in den verschiedenen Phasen des Softwareentwicklungs-Lifecycles vom ursprünglichen Design über Integration, Tests, Deployment bis hin zur Softwarebereitstellung.

Die Einführung eines DevSecOps-Prozesses bietet folgende Vorteile:

- ▶ Unterstützung von IT- und Sicherheitsteam bei der Bewältigung von Herausforderungen im Bereich Personal, Prozesse und Technologien
- ▶ Verbesserte Effizienz, Konsistenz, Wiederholbarkeit und Zusammenarbeit
- ▶ Reduktion von menschlichen Fehlern, wodurch Risiken gemindert werden



Mit DevSecOps wird Sicherheit zur gemeinsamen Verantwortung, die von Anfang an in den Ablauf integriert ist. Anstatt nur ein einziges, separates Team zu haben, das für das Festlegen der Sicherheitsrichtlinien verantwortlich ist, arbeiten Mitarbeitende aus Sicherheits-, Entwicklungs- und Operations-Teams zusammen und sorgen so für Transparenz, geben Feedback und tauschen Erfahrungen aus. Mit diesem Ansatz können Sicherheitsprozesse von Anfang an bei der Anwendungsentwicklung und Infrastrukturbereitstellung integriert werden, was den Schutz erhöht.

Teams, die Unternehmensanwendungen und neue Softwarefunktionen für ihre Organisationen entwickeln, müssen ihre Sicherheitslage signifikant verbessern und mentale Belastungen verringern. Sicherheit muss im kompletten Lifecycle der Softwareentwicklung implementiert werden. Beim Programmieren wird dies durch integrierte Anwendungs-Sicherheitschecks erreicht, um Fehler früh im Lifecycle zu entdecken und so längere Ausfallzeiten zu reduzieren. In der Entwicklung werden Systeme mithilfe von sicherheitsorientierten CI/CD-Workflows (Continuous Integration/Continuous Delivery) geschützt. Und bei der Bereitstellung und Ausführung geschieht dies durch Golden Path-Vorlagen, Schwachstellenanalysen, Artefaktsignaturen, Zertifizierungen, Datenherkunft, Richtliniendurchsetzungspunkte und SBOMs (Software Bill of Materials).

Weiterhin ist es notwendig, eine Strategie zu entwickeln, um sicherzustellen, dass die Open Source-Technologien, die Ihre Teams verwenden, aus zuverlässigen Quellen stammen, dass sie fortlaufend auf automatisierte Weise gepatcht werden und dass bei der Konfiguration immer die Sicherheit an erster Stelle steht. Bevorzugen Sie außerdem den Einsatz unternehmenssicherer Open Source-Lösungen, die den entsprechenden Support für den gesamten Lifecycle bieten.

Wenn Sie unternehmensgerechte Open Source-Angebote wie die von Red Hat nutzen, profitieren Sie von den über 30 Jahren Erfahrung, die Red Hat hinsichtlich der Sicherheit der Open Source-Softwarelieferkette seiner Produkte hat. Zusätzlich benötigen Unternehmen Lösungen, mit denen sie ihre Vielzahl an Kubernetes-Clustern bereitstellen, managen und schützen sowie ihre Anwendungen in großem Umfang entwickeln, modernisieren und bereitstellen können.

Red Hat OpenShift Platform Plus ist eine einheitliche Plattform, die Red Hat OpenShift, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Quay und Red Hat OpenShift Data Foundation enthält. Die Plattform unterstützt Unternehmen beim sicheren Entwickeln, Modernisieren und Bereitstellen von containerisierten Anwendungen in großem Umfang in Kubernetes. Multi Cluster-Sicherheit, Compliance, Anwendungs- und Datenmanagement sorgen für Konsistenz in der gesamten Softwarelieferkette.

Taktische Schritte

Führen Sie bei der Implementierung von DevSecOps und Verbesserungen der Sicherheit in der Softwarelieferkette folgende Schritte aus:



Fangen Sie klein an, und expandieren Sie.

Wählen Sie für den Anfang ein einzelnes Projekt aus. Unterstützen Sie Experimente und iterative, kontinuierliche Verbesserungen zur Feinabstimmung und Optimierung Ihres Prozesses. Feiern Sie Ihre Erfolge und zeigen Sie auf, wie Ihre Bemühungen anderen in Ihrer Organisation nachweislich nutzen können.



Legen Sie klare, vereinbarte Ziele und Fristen fest.

Transparenz ist dabei äußerst wichtig. Stellen Sie sicher, dass alle beteiligten Personen mit den Zielen und Fristen für das Projekt vertraut und einverstanden sind.



Bilden Sie Ihr Personal übergreifend aus.

Entwickeln Sie Lernpfade zu Sicherheit, Infrastruktur und Entwicklung, die regelmäßig aktualisiert werden und allen Teammitgliedern zur Verfügung stehen.



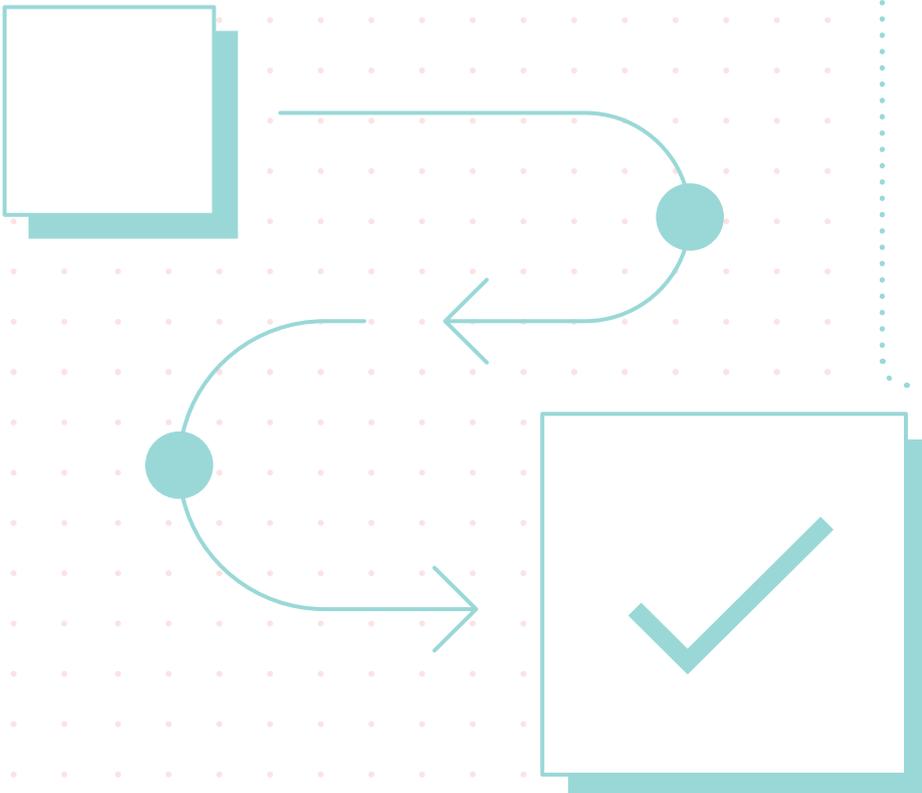
Bilden Sie eine Arbeitsgruppe für Sicherheit.

Bilden Sie ein integriertes, bereichsübergreifendes Team zur Definition von Use Cases und Strategien für die Sicherheit. Lernen Sie von anderen. Nutzen Sie die Erkenntnisse anderer Unternehmen.



Implementieren Sie mit einer einheitlichen Anwendungsplattform Sicherheit im gesamten Lifecycle der Softwareentwicklung.

Sicherheit muss im kompletten Lifecycle der Softwareentwicklung implementiert werden. Beim Programmieren wird dies durch integrierte Anwendungs-Sicherheitschecks erreicht, um Fehler früh im Lifecycle zu entdecken und so längere Ausfallzeiten zu reduzieren. In der Entwicklung werden Systeme mithilfe von sicherheitsorientierten CI/CD-Workflows (Continuous Integration/Continuous Delivery) geschützt. Und bei der Bereitstellung und Ausführung geschieht dies durch Golden Path-Vorlagen, Schwachstellenanalysen, Artefaktsignaturen, Zertifizierungen, Datenherkunft, Richtliniendurchsetzungspunkte und SBOMs (Software Bill of Materials).



Kapitel 5

Sicherheitsaspekt 3

Schützen Sie Ihre Hybrid Cloud mit Automatisierung und Management

Warum ist das wichtig?

Fehlkonfigurationen und unzureichende Änderungskontrolle stellen eine große Sicherheitsbedrohung dar.⁴ Durch Fehlkonfigurationen werden Systeme anfällig für Angriffe. Die Änderungskontrolle ist wichtig für die Erfassung von Daten darüber, wer eine Konfiguration geändert hat, wann die Änderung stattfand und was im Laufe eines Systemlebenszyklus geändert wurde.

Mithilfe von Automatisierung, Management und KI können Sie tägliche Betriebsabläufe optimieren und von Anfang an Sicherheit in Prozesse, Anwendungen und Infrastruktur integrieren. Eine unternehmensweite Automatisierungs- und Managementstrategie unterstützt Sie dabei, menschliche Fehler zu reduzieren, sorgt für Geschwindigkeit, Konsistenz, Wiederholbarkeit und bietet die Möglichkeit, Verifizierungen und Audits durchzuführen. Zusätzlich hilft eine zentralisierte Automatisierungs- und Managementstrategie, die Sicherheit und Compliance zu verbessern, indem sie Unternehmen dabei unterstützt, Sicherheit von Anfang an und über den gesamten Lifecycle hinweg in die Anwendungsentwicklung und IT-Operationen zu integrieren. So können diese erfolgreich DevSecOps-Praktiken implementieren. Tatsächlich kann die Implementierung von Automatisierung, Management und KI in Sicherheitsprozessen die durchschnittlichen Kosten einer Datenpanne um durchschnittlich 39,3 % senken. Dennoch haben nur 28 % der Unternehmen diese Maßnahmen umgesetzt.²

² IBM Security: „Cost of a Data Breach Report 2023“, 2023.

⁴ Cloud Security Alliance: „Top Threats to Cloud Computing: Pandemic 11 Deep Dive“, Oktober 2023.

Empfehlungen und Best Practices

Implementieren Sie eine unternehmensweite Automatisierungs- und Managementstrategie, um mit den dynamischen Anforderungen für Sicherheit, Risiken und Compliance mitzuhalten. Durch die Einführung einer konsistenten Automatisierungs- und Managementstrategie für Ihre Hybrid Cloud können Sie erhöhte Agilität, Wiederholbarkeit, Konsistenz und ein vereinfachtes Auditing erreichen.

Eine einheitliche Automatisierungs- und Managementstrategie senkt das Risiko für Fehlkonfigurationen und manuelle Fehler innerhalb Ihres Unternehmens. Automatisierung und Management optimieren und erhöhen die Konsistenz von Infrastrukturmanagement, Anwendungsentwicklung und Sicherheitsprozessen zur Verbesserung von Schutz, Compliance und Änderungskontrolle. Dies bietet Ihnen folgende Vorteile:



Sorgen Sie für eine einheitliche Konfiguration der Ressourcen gemäß zuvor genehmigter Richtlinien und eine proaktive Wartung mit wiederholbaren Arbeitsschritten über den gesamten Lebenszyklus hinweg.



Ermitteln Sie schnell Systeme, die Patches oder eine Neukonfiguration benötigen.



Optimieren Sie das Patching und Änderungen von Systemeinstellungen anhand festgelegter Baselines und einheitlich für eine große Anzahl von Systemen.



Vereinfachen Sie Auditing und Fehlerbehebung mit automatisch erfassten Aktivitätsprotokollen.



Mithilfe von Identitätsmanagement und Zugriffskontrollen für Automatisierungsplattform und Prozesse stellen Sie sicher, dass nur autorisierte Mitarbeitende Automatisierungsaufgaben ausführen können. Wählen Sie eine Automatisierungsplattform, die alle Mitarbeitenden in Ihrem Unternehmen verwenden können. Mit der Auswahl einer Plattform in einer gängigen, leicht zu erlernenden Automatisierungssprache können Sie folgende Punkte verbessern:



Transparenz: Alle Mitarbeitenden sind über den Inhalt der automatisierten Aufgaben informiert.



Wiederholbarkeit: Eine leicht zugängliche Plattform und Sprache ermöglicht allen autorisierten Mitarbeitenden eine effektive und effiziente Nutzung der Automatisierung.



Zusammenarbeit: Die Automatisierungsaufgaben können innerhalb Ihres Unternehmens gemeinsam genutzt werden. So können andere Teams von bereits ausgeführten Aufgaben profitieren und doppelten Aufwand vermeiden.



Auditing: Mehrere Mitarbeitende können Automatisierungsaufgaben verifizieren und Protokolle für das Auditing anzeigen.

Unternehmen verlassen sich auf IT-Automatisierung zur Gewährleistung der Sicherheit in immer komplexeren Betriebsumgebungen, Anwendungen, Sicherheitsabläufen und Hybrid Cloud-Umgebungen. **Red Hat Ansible Automation Platform** ist eine End-to-End-Automatisierungsplattform und bietet Ihnen ein konsistentes Unternehmens-Framework für die Entwicklung und den Betrieb von IT-Automatisierung in großem Umfang, wobei die Sicherheit im Vordergrund steht. Die Lösung hilft Ihnen dabei, Ihre Effizienz zu verbessern, die Produktivität zu erhöhen sowie Risiken und Ausgaben zu kontrollieren. Weiterhin können Teams damit konsistent Sicherheit und Compliance im gesamten Unternehmen auf wiederholbare Art und Weise automatisieren. [Zertifizierte Automatisierungsinhalte](#) und der Rund-um-die-Uhr-Unternehmenssupport von Red Hat ermöglichen zusätzlich eine koordinierte Reaktion auf Bedrohungen.

Red Hat Ansible Automation Platform automatisiert Konfigurationsmanagement, Patching und Fehlerbehebung und ermöglicht es Unternehmen, automatisierte Sicherheitsprozesse zu managen und so bösartigen Attacken einen Schritt voraus zu sein. Zusätzlich kann Red Hat Ansible Automation Platform als [Integrationspunkt](#) für Sicherheitslösungen fungieren. Dazu zählen Inhalte zertifizierter Partner wie [CyberArk](#), [IBM](#) und [Palo Alto Networks](#), mit denen Nutzende die Verwaltung und Integration einer breiten Palette externer Sicherheitstechnologien automatisieren können.



Taktische Schritte

Beachten Sie folgende Punkte beim Einstieg in die Sicherheitsautomatisierung.



Beginnen Sie mit einem einzelnen Projekt.

Versuchen Sie nicht, alle Aufgaben auf einmal zu automatisieren. Wählen Sie für den Anfang eine begrenzte Anzahl an Aufgaben aus.



Wählen Sie Routineaufgaben aus.

Automatisieren Sie Aufgaben, die wiederholt ausgeführt werden, wie Konfigurationsmanagement, Verwaltung von Softwarepaketen und Patches, Erkennung und Beseitigung von Sicherheitslücken sowie Durchsetzung von Richtlinien.



Messen, anpassen und wiederholen.

Arbeiten Sie iterativ bei der Bereitstellung von Automatisierungen, messen Sie die Ergebnisse, und passen Sie die Automatisierungen entsprechend an.



Bereiten Sie sich auf eine Erweiterung vor, indem Sie eine End-to-End-Automatisierungsplattform zur Skalierung nutzen.

Stellen Sie sicher, dass die Automatisierungen verifiziert und auditiert sind und gemeinsam genutzt werden können, sodass andere Teams innerhalb Ihres Unternehmens von den Ergebnissen und der Skalierung mit einer End-to-End-Automatisierungsplattform für Unternehmen profitieren können.

Kapitel 6

Bereit für den Einstieg?

Die Sicherheit der Hybrid Cloud ist eine Verantwortung, die sich Unternehmen teilen. Unabhängig davon, in welchem Umfang Sie Hybrid Cloud-Technologie aktuell nutzen – Red Hat kann Sie bei der Bereitstellung einer sicherheitsorientierten Hybrid Cloud unterstützen.

Das Red Hat Portfolio mit produktionsgerechter Open Source-Software enthält integrierte Sicherheitsfunktionen, mit denen Sie die Tools und Plattformen zur Bewältigung aktueller und zukünftiger Sicherheits- und Compliance-Herausforderungen erhalten. Red Hat bietet auch unternehmensgerechten Support, praxisorientiertes Training und Experten-Services, mit denen Sie Ihre Hybrid Cloud-Umgebung effizienter und sicherer entwickeln und ausführen können.



[Mehr über das Sicherheitskonzept von Red Hat für die Hybrid Cloud erfahren](#)

In den folgenden Ressourcen erhalten Sie weitere Informationen zum Ansatz von Red Hat für Sicherheit und Compliance in der Hybrid Cloud.

- ▶ [Überblick über Hybrid Cloud-Sicherheit](#)
- ▶ [Bewertung der Hybrid Cloud-Sicherheit](#)
- ▶ [Sicherheitsansätze für Hybrid Cloud-Umgebungen](#)
- ▶ [Verbesserung der Hybrid Cloud-Sicherheit](#)

Über Lucy Huh Kerner, Director, Security Global Strategy and Evangelism, Red Hat

Lucy Huh Kerner ist verantwortlich für die Entwicklung und die Technologie- und Markteinführungsstrategie im Bereich Sicherheit für Red Hat und das gesamte weltweite Red Hat Portfolio. Darüber hinaus engagiert sie sich bei der Erstellung und Bereitstellung sicherheitsbezogener technischer Inhalte für den praktischen Einsatz, für Kunden, Partner, Analysten und die Presse. Außerdem ist sie als Vortragende bei zahlreichen Veranstaltungen und Sicherheitskonferenzen vertreten. Lucy blickt auf mehr als 20 Jahre Berufserfahrung als Software und Hardware Development Engineer sowie als Solutions Architect und Global Security Analyst zurück. Im Rahmen dieser Tätigkeit arbeitete sie an verschiedenen Aspekten der Sicherheit.

EUROPA, NAHOST,
UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

f facebook.com/redhatinc
t @RedHatDACH
in linkedin.com/company/red-hat

de.redhat.com