Vom Risiko zur Resilienz: Sicherstellung der Kubernetes-Compliance

Executive Summary

Dieses Whitepaper „Vom Risiko zur Resilienz: Sicherstellung der Kubernetes-Compliance“ untersucht die sich entwickelnde Landschaft der Compliance für Unternehmen, die Kubernetes verwenden, eine Open-Source-Plattform, die die Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen automatisiert. Angesichts der zunehmenden Nutzung von Container-Technologie — laut Veeam-Report „Trends bei der Datensicherung 2024“ setzen 87 % der Unternehmen Container in der Produktion ein oder planen dies — sind strikte Compliance-Maßnahmen noch wichtiger geworden. Dies ist auf die Notwendigkeit zurückzuführen, die Risiken von Cyberangriffen zu mindern und sensible Daten, einschließlich personenbezogener Daten (PII) und Finanzdaten, zu schützen.

Dieses Whitepaper erläutert internationale Normen und Branchenstandards wie ISO/IEC 27001, FIPS 140-3 und das NIST Cybersecurity Framework (CSF). Diese machen deutlich, wie wichtig Compliance für den Schutz von personen- und unternehmensbezogenen Daten ist. Das Whitepaper befasst sich mit den Herausforderungen im Zusammenhang mit Open-Source-Tools wie Velero, die oft keine Compliance-Funktionalitäten und keine Integrationsunterstützung bieten, und zeigt die Vorteile der Einführung von Veeam Kasten *for Kubernetes*, einer robusten Lösung speziell für Kubernetes-Umgebungen.

Veeam Kasten, führende Kubernetes-Lösung für Datenschutz und Mobilität, bietet wichtige Compliance-spezifische Funktionen wie z. B. Richtlinienautomatisierung, granulare Datenwiederherstellung, verbessertes Monitoring und integrierten Cloud-Storage. Diese Funktionalitäten entsprechen nicht nur den gesetzlichen Vorgaben, sondern erhöhen auch die Datensicherheit. Letztendlich ist die Einführung kommerzieller Lösungen wie Veeam Kasten nicht nur ein Compliance-Mandat, sondern eine strategische Notwendigkeit, die es Unternehmen ermöglicht, die Data Governance, die operative Resilienz und ihre Wettbewerbsvorteile in einem komplexen regulatorischen Umfeld zu verbessern.

Einführung

Kubernetes hat sich schnell zur führenden Plattform für die Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen, virtuellen Maschinen (VMs) und KI/ML-Workloads entwickelt. Kubernetes ist eine leistungsstarke Open-Source-Lösung für die Container-Orchestrierung, die ursprünglich von Google entwickelt und im September 2014 veröffentlicht wurde. Seitdem hat sie sich zum Industriestandard für die Verwaltung von Cloud-nativen Anwendungen entwickelt, eine Position, die von GigaOm hervorgehoben wird. Laut Veeam-Report „Trends bei der Datensicherung 2024" gaben 52 % der Unternehmen an, Container bereits in der Produktion einzusetzen, während sich mindestens 35 % in der Planungs-/Bereitstellungsphase befinden. Das sind mindestens 87 % in den drei untersuchten Jahren. Der „Kubernetes in the Wild Report 2025" von Dynatrace unterstreicht die weit verbreitete Akzeptanz von Kubernetes und beschreibt es als das „Betriebssystem" der Cloud, basierend auf Produktionsdaten von Tausenden von Unternehmen weltweit. Im Zuge der fortlaufenden Weiterentwicklung von Kubernetes machen die verbesserten Funktionalitäten der Plattform für die Verwaltung Session-bezogener, dauerhafter Informationen deutlich, dass die Compliance mit regulatorischen Vorgaben im Geschäftsbetrieb immer wichtiger wird.

Angesichts der weiterhin gewaltig zunehmenden Einführung von Kubernetes und der Tatsache, dass immer mehr kritische Daten in Clustern verwaltet werden, wird Compliance zu einer unternehmenskritischen Notwendigkeit, insbesondere in regulierten Umgebungen. Dieses Whitepaper untersucht die wichtigsten Compliance-Anforderungen, die Organisationen bei der Einführung von Kubernetes berücksichtigen müssen.

Zunächst werden wir die verschiedenen Arten von Daten erörtern, die in Unternehmensanwendungen verwaltet werden, und sie mit den Schutzanforderungen in Einklang bringen. Wir werden darüber hinaus auch einige der wichtigeren Compliance-Anforderungen und die Richtlinien behandeln, denen ihre Verwendung unterliegt. Dann werden wir die Herausforderungen im Zusammenhang mit der Verwendung von Open-Source-Tools für den Datenschutz erörtern. Schließlich werden wir Ihnen zeigen, wie Veeam Kasten Unternehmen ein effektives und notwendiges Mittel an die Hand gibt, um die regulatorische Aufsicht und Governance effizient zu erfüllen.

52%

Prozentsatz der Unternehmen weltweit, die bis Ende 2024 die Containertechnologie eingeführt haben

90%

Anteil kommerzieller Plattformen wie Red Hat OpenShift am Markt für die Bereitstellung von Kubernetes-Plattformen.

Ermittlung von Anwendungsinformationen, die geschützt werden müssen

Vorschriften sind von entscheidender Bedeutung, um das Risiko von Cyberangriffen auf Unternehmen zu minimieren und den Schutz von persönlichen und Unternehmensdaten vor Diebstahl zu gewährleisten. Während die Verhinderung von Cyberangriffen ein wichtiger Schwerpunkt ist, befassen sich die Vorschriften mit einer viel breiteren Palette von Risiken, einschließlich der versehentlichen Offenlegung von Daten, Bedrohungen durch Insider, Bedenken hinsichtlich des Datenschutzes und rechtlicher oder vertraglicher Verpflichtungen.

Die Vorschriften zum Datenschutz und zur Sicherheit von Informationssystemen spielen eine wichtige Rolle bei der Bewältigung dieser Probleme. Für dieses Papier gehören zu den vorgeschriebenen Kategorien von Informationen:

- **Persönlich identifizierbare Informationen (PII):** Diese Datensätze enthalten Informationen zu Personen wie Namen, Adressen, Telefonnummern, E-Mail-Adressen, Identifikationsnummern und mehr. Personalakten sind Beispiele für Unterlagen, die diese sensiblen Daten enthalten.
- **Kundendaten:** Kundendaten umfassen alle Arten von Transaktionsaufzeichnungen und Kommunikation, die nicht nur die Beziehung zwischen Unternehmen und ihren Kunden schützen, sondern auch die Fähigkeit eines Unternehmens, seine Strategie umzusetzen.
- **Finanzdaten:** Die Vorschriften betreffen sensible Finanzdaten wie Bankkontodaten, Kredit- und Debitkarteninformationen und finanzielle Transaktionen.
- **Krankenakten:** Die Vorschriften betreffen auch den Schutz von medizinischen und anamnestischen Aufzeichnungen sowie von genetischen und biometrischen Daten.
- **Daten der Regierung:** Informationen, die von Regierungsbehörden erzeugt, verarbeitet oder kontrolliert werden - einschließlich klassifizierter Dokumente, Bürgerdaten, Daten zur nationalen Sicherheit und behördenübergreifender Kommunikation.

Die Vorschriften dienen in erster Linie dazu, die Sicherheit und den Schutz sensibler Informationen zu gewährleisten und sie vor unberechtigtem Zugriff, Missbrauch oder Diebstahl zu schützen. Unternehmen, die geschäftlich tätig sind, ob auf lokaler oder internationaler Ebene, sind dafür verantwortlich, diese Vorschriften zu befolgen und die geltenden Anforderungen zu erfüllen, wenn sie Geschäfte machen.

Gestaltung der Compliance-Landschaft

Um eine solide Governance für Anwendungen mit sensiblen Informationen sicherzustellen, müssen die Datenschutzverantwortlichen einen umfassenden Plan aufstellen, der den gesetzlichen Vorschriften entspricht. Bei der Bewertung der gesetzlichen Vorschriften sollten je nach Unternehmensbereich branchenspezifische, regionale und internationale Gremien berücksichtigt werden. Mehrere wichtige gesetzliche Vorschriften spielen eine entscheidende Rolle in Bezug auf Datenschutz und Compliance. Im Folgenden finden Sie eine kategorisierte Aufschlüsselung der wichtigsten Compliance-Richtlinien:

Schutz sensibler Daten

Konzentriert sich auf den Schutz von persönlichen, finanziellen und gesundheitsbezogenen Informationen.

- **DSGVO (Datenschutz-Grundverordnung)**
  Gilt für die Daten von EU-Bürgern, auch wenn diese außerhalb der EU verarbeitet werden. Erfasst die Einwilligung, den Umgang mit Daten und die Benachrichtigung bei Verstößen.
- **HIPAA (Health Insurance Portability and Accountability Act)**
  US-amerikanisches Gesetz zum Schutz von persönlichen Gesundheitsinformationen (PHI). Verlangt Datenschutzerklärungen und Sicherheitsvorkehrungen für Gesundheitsdaten.
- **PCI DSS (Payment Card Industry Data Security Standard)**
  Wird vom PCI Security Standards Council für Organisationen vorgeschrieben, die mit Kreditkartendaten arbeiten. Stellt eine sichere Speicherung, Verarbeitung und Übertragung der Daten von Karteninhabern sicher.
- **DPAs (Data Protection Authorities)**
  Nationale Regulierungsbehörden wie das britische ICO setzen die DSGVO und lokale Datenschutzgesetze durch.

Sichere Entwicklung & Governance Frameworks

Leitlinien für den Aufbau sicherer Systeme und das Risikomanagement.

- **ISO/IEC 27001, 27701, 29100**
  Internationale Standards für Informationssicherheitsmanagement, Datenschutz-Frameworks und datenschutzfördernde Technologien.
- **NIST Cybersecurity Framework (CSF)**
  US-amerikanisches Framework mit Best Practices für die Identifizierung und Erkennung von Cybersecurity-Bedrohungen, den Schutz davor, die Reaktion darauf und die Wiederherstellung nach diesbezüglichen Vorfällen.

Datenschutz-Behörden (DPAs):

Die Datenschutzbehörden in den einzelnen EU-Ländern, darunter auch das britische Information Commissioner's Office (ICO), stellen Richtlinien für die Compliance mit der DSGVO zur Verfügung, um sicherzustellen, dass Unternehmen die notwendigen Anforderungen erfüllen. Es ist erwähnenswert, dass die ICO auch Datenschutzanforderungen und -richtlinien für den Schutz britischer Bürger festlegt, da das Vereinigte Königreich nicht mehr Mitglied der EU ist.

- **Adversarial Tactics, Techniques, and Common Knowledge (MITRE) ATT&CK**
  Die weltweit eingesetzte MITRE ATT&CK-Matrix hilft Unternehmen, Bedrohungen zu erkennen und zu analysieren und besser darauf zu reagieren. Dies ist ein wichtiger Schritt, um zu bewerten, wie gut ein Unternehmen auf Vorfälle und die Reaktion darauf vorbereitet ist.
- **FINRA (Financial Industry Regulatory Authority)**
  US-Regulierung für Wertpapierfirmen, mit indirekten Auswirkungen auf internationale Unternehmen, die mit US-Kunden Handel treiben.

Sichere Übertragung und kryptografische Standards

Stellt sicher, dass die Daten sicher übertragen und verschlüsselt werden.

- **FIPS 140-3 (Federal Information Processing Standard)**
  U.S.-Standard für kryptografische Module, die zum Schutz sensibler Informationen bei der Übertragung und Speicherung verwendet werden.

Die Compliance mit diesen Vorschriften ist entscheidend, um den Datenschutz und die Cybersicherheit bei Kubernetes-Bereitstellungen sicherzustellen. Die Berücksichtigung der Vorschriften trägt zum Schutz sensibler Daten, zur Einhaltung von Branchenstandards und zur Wahrung der Sicherheit und des Datenschutzes in Bereitstellungsumgebungen bei.

Die Compliance-Lücken von Open-Source Datenschutz-Tools

Open-Source-Tools werden zwar häufig eingesetzt, um Kosten zu senken, aber sie erfüllen häufig nicht die Compliance-Anforderungen des Unternehmens. Velero, eine Kubernetes-native Open-Source-Lösung, wird häufig von Unternehmen eingesetzt, die Kubernetes-basierte Anwendungsplattformen erforschen. Es fehlen jedoch die robusten Compliance-, Automatisierungs- und Governance-Funktionen, die Unternehmen benötigen. Tools wie Velero haben eine Schlüsselrolle bei der frühen Einführung von Kubernetes gespielt, da sie einen flexiblen Einstiegspunkt für Tests und Entwicklung bieten. Wenn Kubernetes-Workloads jedoch skaliert werden, um globale Aktivitäten und hochgradig regulierte Umgebungen zu unterstützen, weisen diese Tools oft Einschränkungen auf, was erweiterte Funktionen, Benutzerfreundlichkeit und die für die moderne Datensicherung und die Compliance erforderliche Enterprise-Funktionalität anbelangt. Im Folgenden finden Sie drei wichtige Überlegungen, die Sie anstellen sollten, wenn Sie entscheiden, ob Sie Open-Source-Lösungen in Ihren Werkzeugkasten aufnehmen oder nicht.

1. **Eingeschränkte Compliance-spezifische Features:** Open-Source-Tools wie Velero für Kubernetes priorisieren von der Community getätigte Investitionen, die möglicherweise nicht mit den dringendsten Compliance-Anforderungen Schritt halten. Möglicherweise fehlen ihnen integrierte Funktionalitäten wie Prüfprotokolle, Zugriffssteuerungen oder Reporting-Funktionen, die für die Compliance unerlässlich sind.

2. **Mangel an offizieller Unterstützung (einschließlich Dokumentation):** Nicht-kommerzielle Lösungen sind auf den Support der Community angewiesen, die möglicherweise nicht so schnell reagiert wie offizielle Support-Teams. Außerdem kann das Fehlen einer kontrollierten Benutzerdokumentation die Suche nach umfassenden und aktuellen Anleitungen erschweren, da die Ressourcen über verschiedene Community-Foren und Wiki-Seiten verstreut sind.

3. **Herausforderungen bei der Integration:** Kubernetes verfügt über ein umfangreiches Ökosystem von Anwendungen, Distributionen, Speichern und Services im Bereich Sicherheit. Bei der Verwendung von Open-Source-Tools werden Integrationen mit anderen Komponenten möglicherweise nicht gründlich getestet. Dies erschwert einen nahtlosen Übergang zu einer alternativen Infrastruktur — im Rahmen einer geplanten Migration oder als Reaktion auf Ausfallzeiten infolge von Katastrophen wie beispielsweise einem Cyberangriff.

4. **Ressourcenbedarf zur Sicherstellung der Compliance:** Um die Grenzen von Open-Source-Tools bei der Erfüllung von Compliance-Anforderungen zu überwinden, müssen Unternehmen in umfassende Tests, eine detaillierte Dokumentation und eine unabhängige Überprüfung investieren, um sicherzustellen, dass diese Tools mit den spezifischen gesetzlichen Standards übereinstimmen. Dies erfordert oft zusätzliche Ressourcen für die Entwicklung, Anpassung und den laufenden Support, was die anfänglichen Kosteneinsparungen durch die Verwendung von Open-Source-Lösungen zunichte machen kann.

Auf dem hart umkämpften Markt von heute haben Unternehmen die Möglichkeit, diese Herausforderungen ganz zu umgehen. Sie können sich für eine konsistentere und bewährte Lösung entscheiden, die derartige Investitionen überflüssig macht.

Wie unterstützt Veeam Kasten die Compliance -Anforderungen?

Die Führungsrolle von Veeam wird durch die Spitzenplatzierung im GigaOm Radar for Kubernetes Data Protection bestätigt. Dabei wurde Veeam als Leader und Outperformer ausgezeichnet — ein Beweis für die Innovationskraft, die Bereitschaft für den Einsatz in Unternehmen und die operative Exzellenz.

Mit der zunehmenden Verbreitung von Kubernetes - insbesondere durch hybride Compute-Plattformen wie Red Hat OpenShift und SUSE Rancher Prime - müssen Unternehmen ihre Datenschutzstrategien mit den sich entwickelnden Compliance-Vorgaben in Einklang bringen. Veeam Kasten wurde speziell für diese Anforderungen entwickelt und bietet eine richtliniengesteuerte, überprüfbare und widerstandsfähige Architektur, die die Einhaltung von Vorschriften unterstützt, ohne die Agilität zu beeinträchtigen.

Mithilfe von wichtigen Compliance-Funktionen können die Kubernetes-Plattformteams den Datenschutz und die Datenverwaltung verbessern und so ihre Sicherheitslage mit Veeam Kasten stärken:

- **Datenschutz:** FIPS 140-3-konforme Verschlüsselung für Daten bei der Übertragung und bei der Speicherung, integriertes Schlüsselmanagement und unveränderlicher, durch ein Air-Gap getrennter Speicher, um die strengen Anforderungen an die Vertraulichkeit und Integrität der Daten zu erfüllen.
- **Richtlinienbasierte Automatisierung:** Durchsetzung von Schutzrichtlinien durch Kubernetes-eigene Konstrukte und Infrastructure as Code, Ermöglichung wiederholbarer, überprüfbarer Workflows im Einklang mit Frameworks wie ISO/IEC 27001 und NIST CSF.
- **Granulare Datenwiederherstellung:** Unterstützung von Wiederherstellungen auf Namespace- und Anwendungsebene mit der Möglichkeit, vollständige Umgebungszustände wiederherzustellen. Dies ist wichtig für den Nachweis der Wiederherstellbarkeit und Resilienz bei Compliance-Audits.
- **Zugriffssteuerung und RBAC:** Implementierung einer fein abgestuften, Namespace-bezogenen rollenbasierten Zugriffssteuerung (RBAC), um das Prinzip der geringsten Rechte durchzusetzen und die Anforderungen der Identitäts-Governance zu unterstützen.
- **Monitoring und Reporting:** Möglichkeit der Integration in mehrere SIEMs, um Echtzeit-Compliance-Scans durchzuführen und vor nicht autorisierten Änderungen zu warnen und so die Anforderungen an ein kontinuierliches Monitoring zu erfüllen.
- **Sichere Entwicklung:** Kasten ist ISO/IEC 27001-konform und über Iron Bank verfügbar. Die Plattform hält sich an sichere Praktiken für den Entwicklungslebenszyklus sowie an DoD-konforme Standards für die Container-Härtung.

- **Transparenz und Aufbewahrungsüberwachung:** Bietet eine zentrale Benutzeroberfläche für die Verwaltung von Backup-Richtlinien, Aufbewahrungszeitplänen und Audit-Protokollen und sorgt so für Transparenz und Nachvollziehbarkeit für Compliance-Teams.
- **Integrierter sicherer Cloud-Storage:** Sorgen Sie dafür, dass Ihre Daten an einem sicheren Ort landen mit Veeam Data Cloud Vault. Diese Integration bietet eine vollständig verwaltete, stets unveränderliche, verschlüsselte und logisch durch ein Air-Gap getrennte Cloud-Storage-Ressource mit All-inclusive-Preisen pro TB.

Veeam Kasten bietet nicht nur dieselben Funktionalitäten wie Open-Source-Alternativen, sondern übertrifft diese sogar. Die Lösung bietet eine umfassende, kommerzielle Kubernetes-Plattform für Backup und Wiederherstellung und verfügt über eine robuste Suite von Datenmanagement-Tools.

Schlussfolgerung

Da Unternehmen zunehmend auf Kubernetes für ihre Cloud-nativen Anwendungen setzen, wird die Notwendigkeit einer robusten Compliance immer wichtiger. In diesem Whitepaper werden die kritischen Compliance-Anforderungen für den Umgang mit sensiblen Daten - von personenbezogenen Daten bis hin zu Finanzdaten des Unternehmens - erläutert und die besonderen Herausforderungen untersucht, die Open-Source-Tools bei der Einhaltung dieser Vorschriften mit sich bringen.

In einem Umfeld, in dem Cyberangriffe an der Tagesordnung sind und die gesetzlichen Bestimmungen immer strenger werden, können Unternehmen mit umfassenden Lösungen wie Veeam Kasten ihre Datenschutzstrategien effektiv verwalten und gleichzeitig die Compliance-Vorgaben für Backups und Speicher erfüllen. Mit einer Reihe von Compliance-spezifischen Features — von automatisierter Richtliniendurchsetzung bis hin zu fortschrittlichem Monitoring und Reporting — ist Veeam Kasten ein strategischer Verbündeter für Kubernetes-Plattformteams, da es einen sicheren, konformen Betrieb in verschiedenen regulatorischen Umgebungen ermöglicht.

Die Wahl der richtigen Tools für den Datenschutz ist nicht nur eine Frage der Kosteneffizienz. Es handelt sich vielmehr um eine strategische Entscheidung mit Auswirkungen auf die Resilienz und Glaubwürdigkeit eines Unternehmens. Durch den Einsatz von Veeam Kasten können Unternehmen die Komplexität der Compliance selbstbewusst meistern, ihre sensiblen Daten schützen und die betriebliche Integrität in einem zunehmend regulierten und wettbewerbsorientierten Umfeld aufrechterhalten. Der Übergang von reinen Open-Source-Lösungen zu einem hybriden Ansatz mit kommerziellen Tools stellt eine Verpflichtung zu hervorragender Data Governance dar, die Unternehmen nicht übersehen können. Das ist echte Datenresilienz.

Über Veeam Software

Veeam®, der absolute Weltmarktführer im Bereich Datenresilienz, ist der Ansicht, dass jedes Unternehmen in der Lage sein sollte, nach einer Unterbrechung des Geschäftsbetriebs mit Gewissheit und Kontrolle über alle seine Daten weiterzuarbeiten, wann und wo immer es diese benötigt. Veeam bezeichnet dies als maximale Ausfallsicherheit, und wir arbeiten kontinuierlich daran, innovative Lösungen zu entwickeln, mit denen unsere Kunden diese Zielvorgabe erreichen. Die Lösungen von Veeam sind speziell darauf ausgerichtet, die Datenresilienz durch Daten-Backup, Datenwiederherstellung, Datenportabilität, Datensicherheit und Datenintelligenz zu erhöhen. Mit Veeam können Verantwortliche im IT- und Sicherheitsbereich darauf vertrauen, dass ihre Anwendungen und Daten in allen Umgebungen, ob in der Cloud, virtuell, physisch, SaaS oder Kubernetes, sicher und jederzeit verfügbar sind. Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 550.000 Kunden, darunter 68 % der Global 2000-Unternehmen, die auf Veeam vertrauen, um einen zuverlässigen Geschäftsbetrieb zu gewährleisten. Maximale Ausfallsicherheit beginnt mit Veeam. Weitere Informationen finden Sie unter www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.

Weitere Informationen:
veeam.com