KubeOps

Sicherheits-Checkliste für Ihre Kubernetes-Infrastruktur

Der Leitfaden für mehr Sicherheit & Compliance

KubeOps

Sicherheits-Checkliste für Ihre Kubernetes-Infrastruktur

Herausforderungen in KRITIS-Unternehmen

Als Verantwortliche*r für IT-Sicherheit, insbesondere in kritischen Infrastrukturen (KRITIS), stehen Sie vor der Herausforderung, Kubernetes-Container-Systeme zu verwalten und gleichzeitig höchste Sicherheitsstandards einzuhalten. Angesichts der aktuellen Bedrohungslage und der zunehmenden Komplexität von IT-Umgebungen haben wir eine spezielle Checkliste entwickelt, die Ihnen hilft, die Sicherheit Ihrer Container-Infrastruktur systematisch zu bewerten und zu optimieren.

Sicherheitsstandards im Fokus

Basierend auf den aktuellen Sicherheitsstandards des Bundesamts für Sicherheit in der Informationstechnik (BSI), der NIS-Richtlinie (NIS 1) und der überarbeiteten NIS 2-Richtlinie führt Sie diese Checkliste durch wesentliche Sicherheitsaspekte von Kubernetes-Containern und erläutert deren Bedeutung. Sie unterstützt Sie dabei, Sicherheitslücken zu identifizieren, bewährte Verfahren umzusetzen und gesetzliche Anforderungen zu erfüllen.

Strategien für den sicheren Betrieb von Kubernetes-Containern

Unser Ziel ist es, IT-Verantwortliche dabei zu unterstützen, die Komplexität im IT-Betrieb zu reduzieren, steigende Sicherheits- und Compliance-Anforderungen zu erfüllen und Kubernetes-Anwendungen sicher und stabil aufzusetzen. Software-Lieferanten helfen wir dabei, sich auf die Entwicklung ihrer Applikationen zu konzentrieren, ohne zusätzliche Ressourcen in die Container-Infrastruktur investieren zu müssen, und ihre Kunden technisch so vorzubereiten, dass sie containerisierte Software oder Managed Services sicher einsetzen können.

Grundlegende Sicherheitsüberprüfung

Verwenden Sie ausschließlich distroless Container?

Verwenden Sie distroless Container, um die Angriffsfläche zu minimieren. Diese Container enthalten nur die notwendigste Laufzeitumgebung und entsprechen den Sicherheitsanforderungen des BSI Grundschutzes.

Sind Ihre Anwendungen vollständig statisch kompiliert?

Durch statische Kompilierung vermeiden Sie Probleme mit dynamischen Bibliotheken und erhöhen die Sicherheit, indem Sie Abhängigkeiten verringern. Dies wird von NIS 1 empfohlen.

Ist Ihr Image-Stack vollständig gehärtet?

Härtung des Image-Stacks schützt vor bekannten Schwachstellen und unautorisierten Änderungen. Dies ist ein Muss gemäß den Vorgaben des NIS 2.

Integrierte Paketverwaltung

Enthalten Ihre Pakete alle notwendigen Artefakte ohne externe Abhängigkeiten?

Selbstständige Pakete reduzieren Angriffsvektoren durch externe Abhängigkeiten und verbessern die Sicherheitslage, wie im BSI Grundschutz beschrieben.

Sind Ihre Pakete vollständig konfigurierbar, einschließlich der Verwendung von Helm-Charts?

Konfigurierbare Pakete ermöglichen eine flexible Anpassung und erhöhen die Sicherheit und Effizienz der Verwaltung, was von NIS 2 unterstützt wird.

Ist die Versionierung Ihrer Pakete eindeutig und nachvollziehbar?

Eindeutige Versionierung ist entscheidend für die Nachverfolgbarkeit und Verwaltung von Sicherheitsupdates, gemäß den Anforderungen des BSI Grundschutzes.

Verwenden Sie feste Referenzen über SHA-Keys, um Konsistenz sicherzustellen?

Feste Referenzen gewährleisten die Integrität der Pakete und verhindern Manipulationen. Dies entspricht den Best Practices von NIS 1.

Baseline-Level Sicherheitsmaßnahmen

Sind alle Parameter auf die höchste Sicherheitsstufe gesetzt?

Setzen Sie alle Parameter auf die höchste Sicherheitsstufe, um das Risiko von Sicherheitslücken zu minimieren, wie im BSI Grundschutz vorgeschrieben.

Haben Sie alle notwendigen betrieblichen Parameter integriert?

Vollständige Integration betrieblicher Parameter gewährleistet die Betriebsbereitschaft und Sicherheit der Infrastruktur. Dies ist eine Anforderung von NIS 2.

Ist Ihre Dokumentation vollständig und aktuell?

Eine aktuelle Dokumentation ist unerlässlich für die Nachvollziehbarkeit und den sicheren Betrieb, wie es der BSI Grundschutz fordert.

Sicherheitsangepasste Pakete

Haben Sie ungenutzten Code vollständig entfernt und sichere Codierungspraktiken angewendet?

Entfernen Sie ungenutzten Code, um die Angriffsfläche zu reduzieren und die Sicherheit zu verbessern. Dies ist gemäß den Vorgaben von NIS 1 erforderlich.

Nutzen Sie ConfigMaps und Secrets für alle Zugangsdaten und Zertifikate?

Nutzen Sie ConfigMaps und Secrets, um sensible Daten zu schützen und den Sicherheitsanforderungen von NIS 2 zu entsprechen.

Haben Sie Role-Based Access Control (RBAC) vollständig implementiert?

RBAC schützt vor unautorisiertem Zugriff und ist eine bewährte Sicherheitsmaßnahme gemäß BSI Grundschutz.

Wenden Sie Ingress Network Policies vollständig an?

Kontrollieren Sie den Netzwerkzugriff durch Ingress Network Policies, um die Sicherheit zu erhöhen. Dies ist eine Anforderung von NIS 1 und 2.

Lieferkettensicherheit

Verwenden Sie ausschließlich minimale Basis-Images, die nicht veraltet sind?

- Minimale Basis-Images reduzieren die Angriffsfläche und entsprechen den Empfehlungen von BSI Grundschutz und NIS 2.

Werden Ihre Container-Images vollständig aus Open Source Software erstellt?

- Erstellen Sie Ihre Container-Images aus Open Source Software, um Transparenz und Sicherheit zu erhöhen. Dies wird von NIS 1 gefordert.

Validieren Sie Ihre Container-Images vollständig durch Prüfsummen?

- Prüfsummenvalidierung stellt die Integrität der Images sicher und ist eine grundlegende Anforderung des BSI Grundschutzes.

Führen Sie tägliche Scans und die Entfernung kritischer Schwachstellen durch?

- Regelmäßige Vulnerabilities-Scans sind entscheidend für die frühzeitige Erkennung und Behebung von Schwachstellen gemäß NIS 2.

Betriebsbereitschaft

Sind Ihre Ingress- und Proxy-Server vollständig integriert?

- Integrierte Ingress- und Proxy-Server gewährleisten die sichere und effiziente Verwaltung des Datenverkehrs, wie im BSI Grundschutz empfohlen.

Nutzen Sie strukturierte Labels und umfassendes Monitoring vollständig?

- Vollständiges Labeling und Monitoring sind entscheidend für die Übersicht und Sicherheit der Infrastruktur, wie von NIS 1 gefordert.

Haben Sie Liveness- und Readiness-Probes vollständig implementiert?

- Health Checks sind unerlässlich für die Betriebsbereitschaft und Verfügbarkeit, wie im BSI Grundschutz und NIS 2 vorgeschrieben.

Folgen Sie vollständig den bewährten Praktiken für Skalierbarkeit und Unterstützung?

- Best Practices gewährleisten eine skalierbare und unterstützte Umgebung. Dies wird von NIS 2 empfohlen.

Mindestanforderungen bei der Auslieferung

Ist die Dokumentation der verwendeten Tools und Systembibliotheken vollständig?

Vollständige Dokumentation ist unerlässlich für die Nachvollziehbarkeit und Wartung, wie es der BSI Grundschutz vorschreibt.

Führen Sie einen vollständigen Schwachstellenscan vor der Auslieferung durch und protokollieren die Ergebnisse?

Schwachstellenscans vor der Auslieferung stellen sicher, dass keine bekannten Schwachstellen vorhanden sind. Dies ist eine Anforderung von NIS 1.

Beseitigen Sie alle kritischen Schwachstellen vollständig vor der Auslieferung?

Vollständige Schwachstellenbeseitigung minimiert das Risiko von Sicherheitsvorfällen, wie es der BSI Grundschutz und NIS 2 fordern.

Prüfanforderungen bei Erhalt

Validieren Sie die Härtungsmaßnahmen vollständig durch das Vier-Augen-Prinzip?

Validierung durch das Vier-Augen-Prinzip stellt sicher, dass die Sicherheitsmaßnahmen korrekt umgesetzt wurden. Dies ist eine Best Practice gemäß NIS 1.

Arbeiten Sie die Checkliste zur Validierung vollständig ab?

Vollständige Abarbeitung der Checkliste stellt sicher, dass alle Sicherheitsanforderungen erfüllt sind, wie es der BSI Grundschutz empfiehlt.

Dokumentieren Sie alle Abweichungen vollständig und erarbeiten Lösungsansätze?

Dokumentation von Abweichungen und Lösungsansätzen gewährleistet die kontinuierliche Verbesserung der Sicherheitsmaßnahmen, wie es NIS 2 verlangt.

Passen Sie vollständig an und validieren erneut?

Erneute Validierung nach Anpassungen stellt sicher, dass die Sicherheitsmaßnahmen wirksam sind. Dies wird vom BSI Grundschutz empfohlen.

Resümee und Handlungsempfehlungen

Diese Checkliste unterstützt Sie dabei, die Sicherheit Ihrer KRITIS-Infrastruktur systematisch zu bewerten und kontinuierlich zu verbessern. Durch die Umsetzung der aufgeführten Sicherheitsmaßnahmen sichern Sie Ihre Container-Infrastruktur effektiv gegen aktuelle und zukünftige Bedrohungen ab. So gewährleisten Sie eine robuste und widerstandsfähige IT-Umgebung, die den hohen Anforderungen an kritische Infrastrukturen gerecht wird.

Sichere KRITIS-Infrastruktur mit angepassten Lösungen

Lassen Sie uns bei einem kostenlosen Beratungstermin über Ihre aktuelle Kubernetes-Nutzung und die Herausforderungen bei der Verwaltung und Sicherung Ihrer Container-Infrastruktur sprechen. Gemeinsam eruieren wir Ihre technologischen und betrieblichen Anforderungen und zeigen Ihnen auf, wie unser Managed Kubernetes Service (MKS) Ihnen helfen kann, eine hochsichere, stabile und effiziente IT-Infrastruktur zu gewährleisten. Dabei beantworten wir auch gerne Ihre spezifischen Fragen und erarbeiten passende Handlungsmöglichkeiten für Ihre Situation. So unterstützen wir Sie dabei, Ihre Ziele zu erreichen und Ihre KRITIS-Infrastruktur optimal zu sichern.

Sie haben Fragen?
Nehmen Sie Kontakt zu uns auf!

Ihre Vorteile auf einen Blick:

- Gegenseitiges Kennenlernen
- Fokus auf Engpassanalyse
- Erste Lösungsvorschläge
- Zielsetzung für die Zukunft

www.kubeops.net
info@kubeops.net
+49 7433 93724 90

Zum kostenlosen Erstgespräch