/ MAURISEC.DE

FIELD NOTES / CHECKLIST 07

Kubernetes: Grenzen tatsächlich durchsetzen

PRUEFEN. BELEGEN. NACHHALTEN.

Prüfhilfe für autorisierte Cluster-Verantwortliche. Vor Änderungen Abhängigkeiten, Kubernetes-Version, Betriebssystem und CNI-Verhalten erfassen; zunächst in einer geeigneten Testumgebung prüfen.

Pruefbereich / Team:

Datum:

- [ ] **01 / Cluster, Namespaces, Workloads und Verantwortliche inventarisieren; öffentlich erreichbare Verwaltungszugänge prüfen und auf erforderliche Zugriffswege begrenzen.**

  Nachweis: Inventar, Netzfreigaben und dokumentierte Erreichbarkeitsprüfung von API, kubelet und etcd.

- [ ] **02 / RBAC nach Aufgaben beschränken; cluster-admin, Wildcards und Rechte für Rollenänderungen, Secrets oder Workload-Erstellung gezielt überprüfen.**

  Nachweis: Role-/Binding-Export und positive sowie negative Berechtigungstests für repräsentative Identitäten.

- [ ] **03 / Eigene ServiceAccounts je Anwendung verwenden; automatisch eingebundene API-Tokens deaktivieren, wenn der Workload sie nicht benötigt.**

  Nachweis: ServiceAccount-Zuordnung und geprüfte Pod-Spezifikationen ohne unnötige Token-Mounts.

- [ ] **04 / Nachweisen, dass das eingesetzte CNI die verwendeten NetworkPolicies tatsächlich durchsetzt; vorhandene Policies vollständig erfassen.**

  Nachweis: CNI-Dokumentation und reproduzierbare Verbindungsversuche statt lediglich vorhandener YAML-Dateien.

- [ ] **05 / Ingress und Egress schrittweise auf benötigte Verbindungen begrenzen; erforderliches DNS und Betriebsverkehr ausdrücklich berücksichtigen.**

  Nachweis: Verbindungsmatrix mit erlaubten und gesperrten Pfaden einschließlich benötigter TCP-/UDP-Verbindungen.

- [ ] **06 / Überlappende Freigaben prüfen: NetworkPolicies sind additiv. Eine breit erlaubende Policy wird durch eine zusätzliche Default-Deny-Policy nicht aufgehoben.**

  Nachweis: Gesamtauswertung der auf einen Pod wirkenden Regeln und negative Gegenproben.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 07

- [ ] **07 / Passende Pod-Security-Standards zunächst mit Warn-/Audit-Auswertung prüfen und kontrolliert durchsetzen; Ausnahmen begründen und terminieren.**

  Nachweis: Namespace-Konfiguration, Admission-Ergebnisse, Ausnahmeliste und Nachweis abgewiesener Test-Pods.

- [ ] **08 / Linux-Workloads soweit kompatibel ohne root, ohne Privilege Escalation und mit geeignetem Seccomp-Profil betreiben; zusätzliche Capabilities minimieren.**

  Nachweis: SecurityContext, Laufzeitprüfung und begründete Abweichungen für unvermeidbare Sonderfälle.

- [ ] **09 / Nicht benötigte Hostzugriffe und Cloud-Metadatenzugriffe unterbinden; Administrator-Aktionen und relevante Konfigurationsänderungen nachvollziehbar protokollieren.**

  Nachweis: Pod-/Netzprüfungen und auffindbare Audit-Ereignisse mit geschütztem Zugriff.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

In einem Test-Namespace die freigegebene Verbindungsmatrix prüfen: benötigte Verbindungen funktionieren, eine ausdrücklich gesperrte Verbindung scheitert.

GRENZEN UND VORAUSSETZUNGEN

NetworkPolicies ersetzen keine Anwendungsautorisierung und verschlüsseln Verkehr nicht automatisch. Wirkung und Sonderfälle hängen vom CNI und Netzpfad ab. Pod-Security-Anforderungen unterscheiden sich teilweise nach Betriebssystem und Version. Nicht ungeprüft Default-Deny in Produktion aktivieren; die Checkliste bescheinigt keine vollständige Cluster-Sicherheit.

PRIMAERQUELLEN / STAND 09.11.2026

Kubernetes: Security Checklist
kubernetes.io

Kubernetes: RBAC Good Practices
kubernetes.io

Kubernetes: Network Policies
kubernetes.io

Kubernetes: Pod Security Standards
kubernetes.io