Prüfbericht Kubernetes-Sicherheitsaudit

BSI IT-Grundschutz, Baustein APP.4.4 Kubernetes

> **Musterbericht — frei erfundenes Beispiel.** Auftraggeber, Cluster, Befunde und Zahlen sind vollständig fiktiv und keiner realen Umgebung entnommen. Der Bericht dient allein als Arbeitsprobe für Umfang, Tiefe und Form der Berichterstattung.

AUFTRAGGEBER	Muster-Kunde GmbH (frei erfunden)
PRÜFGEGENSTAND	`prod-cluster-01`, Produktion, selbstverwaltetes Kubernetes auf eigenen virtuellen Maschinen
BETRIEBSMODELL	Control Plane einschließlich etcd in Verantwortung des Auftraggebers; kein verwalteter Dienst
KUBERNETES-VERSION	1.30.6
NAMESPACES	`payments`, `portal`, `integration`
PRÜFUMFANG	Paket 2 — Standard-Audit, Anforderungen A1 bis A12
PRÜFMASSSTAB	BSI IT-Grundschutz-Kompendium, Baustein APP.4.4 Kubernetes, Edition 2023; CIS Benchmark Kubernetes v1.9.0
ERHEBUNGSZEITRAUM	14.09.2026 bis 25.09.2026
PRÜFER	Brendon Sutaj — CKS, CNCF Kubestronaut
BERICHTSSTAND	25.09.2026, Version 1.0
VERTRAULICHKEIT	Vertraulich — nur für den Auftraggeber bestimmt

Sutaj Services · Brendon Sutaj · St. Ingbert · brendon@sutajservices.de

1 · Management-Summary

ERGEBNIS IN EINEM SATZ

Die Plattform erfüllt 2 der 12 geprüften Anforderungen vollständig, 7 teilweise und 3 nicht — der Betrieb ist stabil und gut überwacht, die Zugriffs- und Netztrennung entspricht jedoch nicht dem Stand der Technik.

BEWERTUNGSÜBERSICHT

STUFE	GEPRÜFT	ERFÜLLT	TEILWEISE	NICHT ERFÜLLT	N. A.
Basis (MUSS)	5	0	3	2	0
Standard (SOLLTE)	7	2	4	1	0
Summe	**12**	**2**	**7**	**3**	**0**

DIE DREI WICHTIGSTEN FESTSTELLUNGEN

> **Drei Personengruppen haben unbegrenzte Rechte auf dem Produktionscluster.** Die Gruppen `dev-all`, `ops` und `ci-runner` sind über ClusterRoleBindings an `cluster-admin` gebunden — zusammen 31 Personen und ein Dienstkonto. Damit kann jede dieser Identitäten Secrets aller Namespaces lesen, Audit-relevante Objekte verändern und Workloads auf jedem Node starten. Eine Trennung zwischen Entwicklung und Produktionsbetrieb besteht technisch nicht.
> Anforderung A3 · Priorität hoch

> **Secrets liegen unverschlüsselt in etcd und im Konfigurations-Repository.** Für den Cluster ist keine `EncryptionConfiguration` aktiv; alle 148 Secrets sind im etcd-Snapshot im Klartext enthalten. Zusätzlich liegen in zwei Helm-Wertedateien Zugangsdaten zu einer Datenbank und zu einem Zahlungsdienstleister im Klartext in der Versionsverwaltung, mit Lesezugriff für 23 Personen.
> Anforderung A2 · Priorität hoch

> **Zwischen den Namespaces besteht keine Netztrennung.** Es sind keine NetworkPolicies definiert. Jeder Pod kann jeden anderen Pod des Clusters auf allen Ports erreichen, auch über Namespace-Grenzen hinweg. Ein kompromittierter Container im Portal erreicht damit unmittelbar die Zahlungsverarbeitung.
> Anforderung A7 · Priorität hoch

EMPFOHLENES VORGEHEN

Ohne Projektrahmen und kurzfristig umsetzbar sind drei Maßnahmen: die Verschlüsselung der Secrets at rest (M-01), die Rotation der im Repository offengelegten Zugangsdaten (M-02) und ein protokollierter Wiederherstellungstest für etcd (M-05) — zusammen **3 Personentage**.

Die beiden größten Posten brauchen eine Abstimmung mit Entwicklung und Betrieb: die Ablösung der `cluster-admin`-Bindungen samt der Wildcard-Rolle `portal-operator` durch rollenbezogene Rechte (M-03, 4 PT) und die Einführung von Default-Deny-Policies zwischen den Namespaces (M-04, 4 PT). Der Gesamtaufwand für alle Maßnahmen mit Priorität hoch und mittel beträgt **19 Personentage**; mit den Maßnahmen niedriger Priorität sind es 22,5.

Bemerkenswert ist die Asymmetrie des Ergebnisses: Verfügbarkeit und Überwachung sind überdurchschnittlich gut gelöst, die Schutzmaßnahmen gegen seitliche Bewegung im Cluster fehlen

dagegen weitgehend. Das ist ein verbreitetes Muster bei Plattformen, die aus einem Verfügbarkeitsprojekt gewachsen sind.

> **EINORDNUNG DER ERGEBNISSE**
>
> Dieser Bericht ist ein **Beitrag zur technischen Dokumentation** des Auftraggebers: eine mit Rohdaten belegte Bewertung der Container-Plattform gegen den Baustein APP.4.4.
>
> Er ist **kein vollständiger Nachweis** der Pflichten aus dem BSIG. § 30 Absatz 2 BSIG umfasst zehn Maßnahmenbereiche, von denen mehrere — Vorfallbewältigung, Schulungen, Lieferantenmanagement, organisatorische Konzepte — über die Plattform hinausreichen und hier nicht geprüft wurden. Ob der Auftraggeber dem BSIG unterliegt und ob seine Dokumentation insgesamt ausreicht, entscheidet der Auftraggeber. Die Zuordnung der geprüften Anforderungen findet sich in Abschnitt 6.

2 · Prüfmethodik

VORGEHEN

1. Kickoff und Abgrenzung des Prüfgegenstands am 14.09.2026.
2. Lesende Erhebung über ein zeitlich befristetes Dienstkonto mit einer eigens angelegten ClusterRole (`get` / `list` auf RBAC-, Netz-, Workload- und Admission-Ressourcen). Die mitgelieferte Rolle `view` war nicht ausreichend, da sie Roles und RoleBindings nicht einschließt. Keine Leserechte auf Secrets — die Angaben zur Verschlüsselung at rest und das Secret-Inventar stellte der Auftraggeber bereit. Alle Abfragen sind in der Nachweismappe protokolliert.
3. Automatisierte Prüfläufe gegen den CIS Kubernetes Benchmark v1.9.0: kube-bench v0.9.3 für die Knoten- und Control-Plane-Prüfpunkte, kubescape v3.0 für die Policy-Prüfpunkte. kube-bench liest Konfigurationsdateien und Prozessinformationen der Knoten; das lesende Dienstkonto aus Schritt 2 umfasst diesen Zugriff nicht. Die Läufe hat deshalb der Auftraggeber selbst ausgeführt — auf einem Control-Plane-Knoten und zwei Worker-Knoten — und die vollständigen Ausgaben bereitgestellt (Nachweismappe N-01). Die Ausgaben sind unverändert übernommen; eine eigene Erhebung auf Knotenebene war nicht Gegenstand der Prüfung.
4. Auswertung der Konfigurations- und Pipeline-Definitionen aus dem GitOps-Repository.
5. Fachgespräche mit der Plattformverantwortlichen am 18.09.2026 und mit dem Lead Developer Portal am 19.09.2026.
6. Bewertung gegen die Anforderungen A1 bis A12 des Bausteins.
7. Abschlussworkshop am 25.09.2026.

BEWERTUNGSSCHEMA

BEWERTUNG	BEDEUTUNG
Erfüllt	Die Anforderung ist vollständig umgesetzt und der Nachweis liegt vor.
Teilweise erfüllt	Dem Grunde nach umgesetzt, aber Lücken im Umfang, in der Durchgängigkeit oder in der Dokumentation.
Nicht erfüllt	Nicht oder nur punktuell umgesetzt.
Nicht anwendbar	Greift für den Prüfgegenstand nicht. Begründung zwingend.

GRENZEN DER AUSSAGEKRAFT

Die Bewertung beschreibt den Zustand zum Erhebungszeitpunkt auf Grundlage der bereitgestellten Zugänge und Auskünfte. Die Erhebung erfolgte ausschließlich lesend. Es wurden keine Angriffstechniken angewendet und keine Schwachstellen ausgenutzt. Der Bericht ersetzt weder einen Penetrationstest noch einen fortlaufenden Sicherheitsbetrieb. Die Festlegung des Schutzbedarfs obliegt dem Auftraggeber.

Drei Bereiche beruhen auf Angaben des Auftraggebers und nicht auf eigener Erhebung: die Benchmark-Ausgaben der Knoten und der Control Plane, die Angabe zur Verschlüsselung at rest und das Secret-Inventar. Für diese Punkte ist die Bewertung nur so belastbar wie die bereitgestellte Ausgabe. Wo das für eine einzelne Anforderung tragend ist, steht es dort ausdrücklich.

3 · Basis-Anforderungen (MUSS)

APP.4.4.A1

TEILWEISE ERFÜLLT

Planung der Separierung der Anwendungen

Priorität Mittel · **Belegstelle** Nachweismappe N-01

FESTSTELLUNG

Der Cluster trennt die drei Fachanwendungen sauber über Namespaces, und die Namenskonvention ist konsistent. Produktion und Integrationstest laufen jedoch auf demselben Cluster und auf denselben Nodes: `integration` teilt sich mit `payments` fünf von sieben Worker-Nodes. Eine dokumentierte Entscheidung, warum dieses Separierungsniveau für den festgestellten Schutzbedarf ausreicht, liegt nicht vor; im Fachgespräch wurde die Zusammenlegung mit Lizenzkosten begründet.

BEWERTUNGSBEGRÜNDUNG

Der Baustein verlangt die *Planung* der Separierung, nicht ein bestimmtes Niveau. Die Trennung existiert und ist nachvollziehbar umgesetzt — es fehlt die begründete Festlegung, gegen die sich das Ergebnis prüfen lässt. Da die Zusammenlegung von Produktion und Test auf gemeinsamen Nodes eine bewusste Entscheidung sein kann, ist dies keine Nichterfüllung, aber auch keine vollständige.

EMPFEHLUNG

Separierungskonzept in zwei Seiten festhalten: welche Anwendungen welche Trennungsebene erhalten (Cluster, Node, Namespace), mit Begründung aus dem Schutzbedarf. Falls `payments` einen höheren Schutzbedarf hat als `integration`, ist A15 zu prüfen. Aufwand: 1 PT.

APP.4.4.A2

NICHT ERFÜLLT

Planung der Automatisierung mit CI/CD

Priorität Hoch · **Belegstelle** Nachweismappe N-02, N-05

FESTSTELLUNG

Drei Befunde:

- Für den Cluster ist keine `EncryptionConfiguration` aktiv. Alle 148 Secrets liegen im etcd-Snapshot im Klartext. Die Snapshots werden auf einem Objektspeicher abgelegt, auf den neun Personen Lesezugriff haben.
- In `charts/portal/values-prod.yaml` und `charts/payments/values-prod.yaml` stehen Zugangsdaten zu einer Datenbank und zu einem Zahlungsdienstleister im Klartext. Das Repository ist für 23 Personen lesbar; die Werte sind seit 19 Monaten in der Historie.
- Das Dienstkonto der Pipeline (`ci-runner`) ist über ein ClusterRoleBinding an `cluster-admin` gebunden (siehe A3).

Ein Rollen- und Rechtekonzept für die Pipelines existiert nicht in schriftlicher Form.

BEWERTUNGSBEGRÜNDUNG

Der Baustein verlangt ausdrücklich, dass Rollen- und Rechtekonzept sowie die Absicherung von Kubernetes Secrets Teil der Planung sein MÜSSEN. Beides fehlt.

Die Offenlegung der Zugangsdaten ist darüber hinaus datenschutzrechtlich zu bewerten; eine Meldepflicht folgt daraus nicht automatisch. Sie setzt zunächst voraus, dass überhaupt eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 DSGVO vorliegt. Liegt eine solche vor, ist die Meldung nach Artikel 33 Absatz 1 DSGVO der Regelfall: Sie erfolgt unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung dem Verantwortlichen bekannt wurde. Die Ausnahme ist eng gefasst — sie greift nur, wenn die Verletzung voraussichtlich **nicht** zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Zwei Punkte werden dabei häufig verwechselt. Das Risiko ist kein Merkmal, das positiv nachzuweisen ist, sondern der Ausnahmegrund, der zu begründen ist, wenn nicht gemeldet wird. Und die Frist beginnt mit dem Bekanntwerden, nicht mit dem Abschluss der eigenen Ermittlungen — Artikel 33 Absatz 4 DSGVO lässt ausdrücklich eine schrittweise Nachmeldung zu.

Zu prüfen ist durch den Auftraggeber daher: ob die betroffenen Konten Zugriff auf personenbezogene Daten eröffnen, ob ein unbefugter Zugriff stattgefunden hat oder nicht ausgeschlossen werden kann, und ob sich das Ausbleiben eines Risikos begründen lässt. Bleibt die Meldung aus, ist diese Begründung zu dokumentieren; die Dokumentationspflicht nach Artikel 33 Absatz 5 DSGVO besteht in jedem Fall.

EMPFEHLUNG

- `EncryptionConfiguration` mit AES-GCM aktivieren und alle Secrets durch Neuschreiben umschlüsseln. Aufwand: 1 PT.
- Die beiden offengelegten Zugangsdatensätze **rotieren**, nicht nur entfernen — sie sind in der Git-Historie und müssen als kompromittiert gelten. Aufwand: 1 PT zuzüglich Koordination mit dem Zahlungsdienstleister.

- Secrets aus den Wertedateien in ein Secret-Management überführen (External Secrets oder Sealed Secrets). Aufwand: 2 PT.
- Rechtekonzept der Pipeline schriftlich festlegen, gemeinsam mit der Umsetzung aus A3 und A10.

APP.4.4.A3

NICHT ERFÜLLT

Identitäts- und Berechtigungsmanagement bei Kubernetes

Priorität Hoch · **Belegstelle** Nachweismappe N-03

FESTSTELLUNG

Drei ClusterRoleBindings binden an `cluster-admin`:

BINDING	SUBJEKT	UMFANG
`dev-all-admin`	Gruppe `dev-all`	24 Personen
`ops-admin`	Gruppe `ops`	7 Personen
`ci-runner-admin`	ServiceAccount `ci/ci-runner`	Dienstkonto

Zusätzlich existiert die ClusterRole `portal-operator` mit `apiGroups: ["*"]`, `resources: ["*"]`, `verbs: ["*"]`, gebunden an zwei Dienstkonten. Die Anbindung an den Identitätsanbieter über OIDC ist korrekt konfiguriert, anonyme Zugriffe auf die API sind deaktiviert (`--anonymous-auth=false`, belegt durch die vom Auftraggeber bereitgestellte kube-bench-Ausgabe zu Prüfpunkt 1.2.1, Nachweismappe N-01). Eine periodische Überprüfung der vergebenen Rechte findet nicht statt; die letzte dokumentierte Durchsicht datiert von 2023.

BEWERTUNGSBEGRÜNDUNG

Die Authentifizierung ist sauber gelöst, die Autorisierung nicht. Der Baustein verlangt, dass Benutzende NUR die unbedingt notwendigen Rechte erhalten. 31 Personen mit unbegrenzten Clusterrechten auf einem Produktionssystem erfüllen das nicht, unabhängig von der Vertrauenswürdigkeit der Beteiligten: Die Rechte überleben jeden Rollenwechsel und jede Kompromittierung eines einzelnen Kontos.

EMPFEHLUNG

- Vier rollenbezogene ClusterRoles definieren (Entwicklung lesend, Entwicklung schreibend je Namespace, Plattformbetrieb, Notfallzugang) und die drei bestehenden Bindungen ersetzen. Aufwand: 2 PT.
- Den Notfallzugang als gesondertes, protokolliertes Verfahren ausgestalten statt als Daueranspruch.
- `portal-operator` auf die tatsächlich genutzten Ressourcen einschränken; die benötigten Rechte lassen sich aus den Audit-Logs der letzten 30 Tage ableiten. Aufwand: 1 PT.
- Die drei bezifferten Positionen aus A3 und A10 — ClusterRoles 2 PT, `portal-operator` 1 PT, Dienstkonten je Zielumgebung 1 PT — sind in Maßnahme M-03 mit zusammen 4 PT zusammengefasst.
- Halbjährliche Rechteüberprüfung als wiederkehrenden Termin etablieren.

APP.4.4.A4

TEILWEISE ERFÜLLT

Separierung von Pods

Priorität Mittel · **Belegstelle** Nachweismappe N-04

FESTSTELLUNG

Die Pod Security Standards sind clusterweit aktiv, aber in den drei geprüften Namespaces auf `privileged` gesetzt — also auf die Stufe ohne Einschränkung. Im Einzelnen:

- 4 von 61 Pods laufen mit `hostNetwork: true`, davon 3 Infrastrukturkomponenten (Ingress, CNI, Node-Exporter) mit nachvollziehbarer Begründung und ein Anwendungs-Pod im Namespace `integration` ohne erkennbaren Grund.
- 2 Pods laufen mit `privileged: true`, beide Infrastruktur.
- 38 von 61 Pods laufen als `root` (kein `runAsNonRoot`), darunter alle Anwendungs-Pods in `payments`.
- Kein Pod setzt `readOnlyRootFilesystem`.
- `hostPID` und `hostIPC` werden nirgends verwendet.

BEWERTUNGSBEGRÜNDUNG

Die groben Isolationsbrüche sind weitgehend vermieden, und die vorhandenen sind bei der Infrastruktur sachlich begründet. Die Trennung der Benutzer-IDs ist jedoch faktisch nicht umgesetzt: Ein Prozess, der als `root` im Container läuft, ist bei einem Ausbruch aus der Container-Grenze privilegiert auf dem Node. Der Baustein nennt die Trennung von Benutzer-IDs ausdrücklich als Mindestumfang.

EMPFEHLUNG

- Pod Security Standards in `payments` und `portal` auf `baseline`, perspektivisch `restricted` heben, zunächst im `warn`- und `audit`-Modus. Aufwand: 1 PT.
- `runAsNonRoot` für die Anwendungs-Pods setzen; der Aufwand liegt bei den Images, nicht beim Cluster. Aufwand: 2 PT verteilt auf die Anwendungsteams.
- `hostNetwork` beim Anwendungs-Pod in `integration` entfernen oder begründen und dokumentieren.

APP.4.4.A5

TEILWEISE ERFÜLLT

Datensicherung im Cluster

Priorität Hoch · **Belegstelle** Nachweismappe N-06

FESTSTELLUNG

OBJEKT	SICHERUNG	AUFBEWAHRUNG	VERSCHLÜSSELT	LETZTER TEST
etcd	täglich 02:00	30 Tage	ja	**keiner dokumentiert**
PV `payments`	täglich	14 Tage	ja	03/2026
PV `portal`	**keine**	—	—	—
Image-Registry	**keine**	—	—	—
Konfigurations-Repo	gespiegelt	unbegrenzt	ja	—

BEWERTUNGSBEGRÜNDUNG

Die Sicherung existiert für die wesentlichen Objekte und ist automatisiert, zwei vom Baustein ausdrücklich genannte Objekte fehlen jedoch: die Datenhaltung der Image-Registry und die Volumes des Portals. Gravierender ist das Fehlen eines Wiederherstellungstests für etcd — eine ungetestete Sicherung ist eine Annahme, kein Nachweis.

EMPFEHLUNG

- Wiederherstellungstest für etcd auf einem Testcluster durchführen und protokollieren; danach halbjährlich wiederholen. Aufwand: 1 PT.
- Sicherung der Portal-Volumes aufnehmen. Aufwand: 0,5 PT.
- Registry-Datenhaltung in die Sicherung aufnehmen oder dokumentieren, dass alle Images reproduzierbar neu gebaut werden können und wie lange das dauert. Aufwand: 0,5 PT.

4 · Standard-Anforderungen (SOLLTE)

APP.4.4.A6

ERFÜLLT

Initialisierung von Pods

Belegstelle Nachweismappe N-04

FESTSTELLUNG

Alle sieben Pods mit Initialisierungsbedarf nutzen eigene Init-Container. Die Hauptcontainer starten ausschließlich nach erfolgreichem Abschluss; bei Fehlschlag bleibt der Pod in `Init:Error`. Datenbankmigrationen laufen als eigene Jobs, nicht als Init-Container — sachgerecht, da sie nicht bei jedem Pod-Start wiederholt werden dürfen.

BEWERTUNGSBEGRÜNDUNG

Anforderung vollständig umgesetzt. Keine Maßnahme erforderlich.

APP.4.4.A7

NICHT ERFÜLLT

Separierung der Netze bei Kubernetes

Priorität Hoch · **Belegstelle** Nachweismappe N-07

FESTSTELLUNG

Im gesamten Cluster ist **keine einzige NetworkPolicy** definiert. Das CNI unterstützt sie. Daraus folgt: Jeder Pod erreicht jeden anderen Pod auf allen Ports, über Namespace-Grenzen hinweg. Stichprobe bestätigt: aus einem Pod in `portal` ist der PostgreSQL-Port 5432 des Datenbank-Pods in `payments` erreichbar.

Das Administrationsnetz ist von den Anwendungsnetzen getrennt, und der API-Server ist nur über das Administrationsnetz und einen Bastion-Zugang erreichbar — das ist korrekt gelöst. Die Verwaltung des CNI ist auf die Gruppe `ops` beschränkt.

BEWERTUNGSBEGRÜNDUNG

Der Baustein verlangt bei mehreren Anwendungen auf einem Cluster ausdrücklich, dass zunächst **alle** Netzverbindungen zwischen Namespaces untersagt und nur benötigte gestattet werden. Das Gegenteil ist der Fall. Die saubere Trennung des Administrationsnetzes verhindert den Zugriff von außen, nicht die seitliche Bewegung innerhalb des Clusters — und genau darauf zielt die Anforderung.

EMPFEHLUNG

- Default-Deny-Policy je Namespace einführen, zunächst in `integration`, um die tatsächlich benötigten Verbindungen zu ermitteln. Aufwand: 1 PT.
- Erforderliche Verbindungen als explizite Policies ergänzen; die Beziehungen lassen sich aus den Metriken des bereits laufenden Service-Mesh-Proxys ableiten. Aufwand: 2 PT.
- Ausrollen auf `portal` und `payments` nach Messung. Aufwand: 1 PT.

APP.4.4.A8

TEILWEISE ERFÜLLT

Absicherung von Konfigurationsdateien

Priorität Mittel · **Belegstelle** Nachweismappe N-08

FESTSTELLUNG

Die Anwendungskonfiguration ist vollständig versioniert und wird über GitOps ausgerollt; Änderungen sind nachvollziehbar und mit Freigaben versehen. Die Konfiguration der Control Plane und der Cluster-Erweiterungen liegt dagegen außerhalb der Versionsverwaltung und wurde laut Auskunft manuell gepflegt. Schreibrechte auf das Konfigurations-Repository haben 14 Personen, ohne Unterscheidung zwischen Anwendungs- und Plattformkonfiguration.

BEWERTUNGSBEGRÜNDUNG

Für den größeren Teil des Umfangs ist die Anforderung erfüllt. Der Baustein verlangt jedoch, dass Zugriffsrechte auf die Konfiguration der Control Plane besonders sorgfältig vergeben und eingeschränkt werden — eine Unterscheidung, die hier weder im Repository noch in den Rechten existiert.

EMPFEHLUNG

Control-Plane- und Erweiterungskonfiguration in ein eigenes Repository mit engerem Berechtigungskreis überführen und ebenfalls über GitOps ausrollen. Aufwand: 2 PT.

APP.4.4.A9

TEILWEISE ERFÜLLT

Nutzung von Kubernetes Service-Accounts

Priorität Mittel · **Belegstelle** Nachweismappe N-03

FESTSTELLUNG

6 von 23 Deployments laufen unter dem `default`-Service-Account des jeweiligen Namespace. Dem `default`-Account sind keine zusätzlichen Rechte eingeräumt — insoweit korrekt. `automountServiceAccountToken` ist bei 19 von 23 Deployments aktiv, obwohl laut Auskunft nur 4 Anwendungen die Kubernetes-API ansprechen. Privilegierte Accounts sind auf Control-Plane-Pods und zwei Operatoren beschränkt.

BEWERTUNGSBEGRÜNDUNG

Der kritische Teil — keine Rechte auf dem `default`-Account — ist erfüllt. Zwei Teilanforderungen sind es nicht: eigene Service-Accounts je Anwendung und kein Token-Zugriff für Pods, die keinen benötigen. Ein eingehängtes Token ist bei einer Container-Kompromittierung der erste Baustein einer Rechteausweitung.

EMPFEHLUNG

- `automountServiceAccountToken: false` als Vorgabe setzen und nur für die vier API-nutzenden Anwendungen aktivieren. Aufwand: 0,5 PT.
- Eigene Service-Accounts für die sechs Deployments anlegen. Aufwand: 0,5 PT.

APP.4.4.A10

TEILWEISE ERFÜLLT

Absicherung von Prozessen der Automatisierung

Priorität Hoch · **Belegstelle** Nachweismappe N-09

FESTSTELLUNG

Die Pipelines laufen über ein einziges Dienstkonto mit `cluster-admin` (siehe A2 und A3). Eine Trennung nach Benutzergruppen besteht nicht: Dieselbe Pipeline-Identität rollt nach `integration` und nach `payments` aus. Positiv: Die Freigabe für Produktionsausrollungen erfordert eine Zustimmung im Repository durch eine zweite Person, und diese Prüfung lässt sich technisch nicht umgehen.

BEWERTUNGSBEGRÜNDUNG

Das Vier-Augen-Prinzip auf der Prozessebene ist vorhanden und wirksam, die technische Rechtetrennung fehlt. Der Baustein verlangt, dass unterschiedliche Gruppen durch **eigene Prozesse** mit jeweils nur den notwendigen Rechten arbeiten.

EMPFEHLUNG

Je Zielumgebung ein eigenes Dienstkonto mit auf den jeweiligen Namespace begrenzten Rechten. Umsetzung gemeinsam mit A3; der Aufwand von 1 PT ist in Maßnahme M-03 enthalten und dort nicht erneut zu rechnen.

APP.4.4.A11

ERFÜLLT

Überwachung der Container

Belegstelle Nachweismappe N-04

FESTSTELLUNG

Alle 61 Pods definieren Readiness- und Liveness-Checks. Stichprobe über acht Anwendungen: Die Checks prüfen fachliche Verfügbarkeit, nicht nur den Prozess — der Zahlungsdienst meldet `not ready`, wenn die Datenbankverbindung fehlt. Die Zeitspannen sind je Dienst unterschiedlich gesetzt und plausibel begründet. Neustartverhalten über `restartPolicy: Always` und Backoff ist korrekt.

BEWERTUNGSBEGRÜNDUNG

Anforderung vollständig umgesetzt, und zwar über das Übliche hinaus. Keine Maßnahme erforderlich.

APP.4.4.A12

TEILWEISE ERFÜLLT

Absicherung der Infrastruktur-Anwendungen

Priorität Mittel · **Belegstelle** Nachweismappe N-10

FESTSTELLUNG

Geprüft wurden Image-Registry, GitOps-Controller und Storage-Provisionierer gegen die fünf vom Baustein genannten Punkte. Die Secret-Verwaltung ist nicht bewertet: Ohne Leserechte auf Secrets lagen dafür keine eigenen Erhebungsdaten vor.

KRITERIUM	REGISTRY	GITOPS	STORAGE
Personen- und Dienstkonten getrennt	ja	ja	ja
Verschlüsselte Kommunikation auf allen Ports	**nein** (intern HTTP)	ja	ja
Minimale Berechtigungen	teilweise	**nein** (siehe A3)	ja
Protokollierung von Änderungen	**nein**	ja	ja
Regelmäßige Datensicherung	**nein** (siehe A5)	ja	ja

BEWERTUNGSBEGRÜNDUNG

Vollständig erfüllt ist die Anforderung nur beim Storage-Provisionierer. Der GitOps-Controller erfüllt vier der fünf Punkte, nicht aber die minimale Rechtevergabe: Er arbeitet über dasselbe Dienstkonto mit `cluster-admin`, das in A3 und A10 beanstandet ist. Die Registry fällt in drei von fünf Punkten durch und ist zugleich das Infrastrukturelement mit der größten Hebelwirkung: Wer dort schreiben kann, bestimmt, was im Cluster läuft. Das berührt unmittelbar die Lieferkettensicherheit nach § 30 Absatz 2 Nummer 4 BSIG.

EMPFEHLUNG

- TLS für die clusterinterne Kommunikation zur Registry aktivieren. Aufwand: 0,5 PT.
- Push-Protokollierung aktivieren und in die bestehende Log-Auswertung aufnehmen. Aufwand: 0,5 PT.
- Datensicherung aufnehmen, gemeinsam mit A5.
- Perspektivisch: Signaturprüfung der Images beim Ausrollen, Voraussetzung für A13.

5 · Anforderungen bei erhöhtem Schutzbedarf

Für den Prüfgegenstand wurde vom Auftraggeber kein erhöhter Schutzbedarf festgestellt. Die Anforderungen A13 bis A21 des Bausteins waren daher nicht Gegenstand dieser Prüfung.

> **Hinweis.** Falls für `payments` ein erhöhter Schutzbedarf festgestellt wird, sind insbesondere A13 (automatisierte Auditierung gegen Benchmarks mit technischer Durchsetzung), A15 (Trennung auf Node- und Cluster-Ebene) und A18 (Mikro-Segmentierung) zu betrachten. Die dafür nötigen Vorarbeiten — NetworkPolicies aus A7 und Signaturprüfung aus A12 — stehen ohnehin an.

6 · Zuordnung zu § 30 Absatz 2 BSIG

APP.4.4	BEWERTUNG	§ 30 ABS. 2 BSIG
A1 Separierung der Anwendungen	Teilweise	Nr. 1 · Nr. 9
A2 CI/CD und Secrets	**Nicht erfüllt**	Nr. 5 · Nr. 8 · Nr. 9
A3 Identitäts- und Berechtigungsmanagement	**Nicht erfüllt**	Nr. 9 · Nr. 10
A4 Separierung von Pods	Teilweise	Nr. 9
A5 Datensicherung im Cluster	Teilweise	Nr. 3
A6 Initialisierung von Pods	Erfüllt	Nr. 5
A7 Separierung der Netze	**Nicht erfüllt**	Nr. 9
A8 Konfigurationsdateien	Teilweise	Nr. 5 · Nr. 9
A9 Service-Accounts	Teilweise	Nr. 9
A10 Automatisierungsprozesse	Teilweise	Nr. 5 · Nr. 9
A11 Überwachung der Container	Erfüllt	Nr. 2 · Nr. 3
A12 Infrastruktur-Anwendungen	Teilweise	Nr. 3 · Nr. 4 · Nr. 8 · Nr. 9

Betroffene Maßnahmenbereiche mit Lücken: Nr. 3 (Aufrechterhaltung des Betriebs), Nr. 4 (Lieferkette), Nr. 5 (Erwerb, Entwicklung, Wartung), Nr. 8 (Kryptografie), Nr. 9 (Zugriffskontrolle), Nr. 10 (Multi-Faktor-Authentifizierung).

Nicht durch diesen Baustein abgedeckt: § 30 Absatz 2 Nummer 7 — grundlegende Schulungen und Sensibilisierungsmaßnahmen. Der Abschlussworkshop deckt davon nur den plattformbezogenen Teil ab. Nummer 2 nur teilweise, soweit sie über die technische Erkennung hinaus organisatorische Vorfallbewältigung verlangt.

7 · Maßnahmenplan

NR.	MASSNAHME	ANF.	PRIORITÄT	PT	EMPFOHLEN BIS
M-01	Secrets at rest verschlüsseln und umschlüsseln	A2	Hoch	1,0	sofort
M-02	Offengelegte Zugangsdaten rotieren	A2	Hoch	1,0	sofort
M-03	`cluster-admin`-Bindungen und Wildcard-Rolle durch Rollen ersetzen, Dienstkonten je Zielumgebung	A3, A10	Hoch	4,0	4 Wochen
M-04	Default-Deny und Policies je Namespace	A7	Hoch	4,0	6 Wochen
M-05	Wiederherstellungstest etcd, protokolliert	A5	Hoch	1,0	4 Wochen
M-06	Secrets in Secret-Management überführen	A2	Mittel	2,0	Quartalsende
M-07	Pod Security Standards auf `baseline`	A4	Mittel	1,0	Quartalsende
M-08	Registry: TLS, Protokollierung, Sicherung	A12, A5	Mittel	1,5	Quartalsende
M-09	Token-Automount abschalten, eigene SAs	A9	Mittel	1,0	Quartalsende
M-10	Control-Plane-Konfiguration in eigenes Repo	A8	Mittel	2,0	Quartalsende
M-11	Portal-Volumes in die Sicherung aufnehmen	A5	Mittel	0,5	Quartalsende
M-12	`runAsNonRoot` für Anwendungs-Pods	A4	Niedrig	2,0	nach Bedarf
M-13	Separierungskonzept dokumentieren	A1	Niedrig	1,0	nach Bedarf
M-14	Halbjährliche Rechteüberprüfung etablieren	A3	Niedrig	0,5	nach Bedarf
Gesamtaufwand Priorität hoch und mittel				**19,0**	

Ohne Projektrahmen umsetzbar: M-01, M-02 und M-05 — zusammen 3,0 Personentage. Die Spalte *Empfohlen bis* nennt davon unabhängig die empfohlene Frist.

8 · Nachweismappe

Separat übergeben, verschlüsselt, 11 Ablagen entsprechend der Berichtsstruktur. Jede Bewertung in diesem Bericht verweist über die Belegstelle auf die zugehörigen Rohdaten: ausgeführte Kommandos mit Zeitstempel, Benchmark-Ausgaben, Konfigurationsauszüge und Gesprächsnotizen.

> Secret-Werte, Token und Zugangsdaten sind nicht enthalten. Dokumentiert ist jeweils der Befund, nicht der Inhalt — die in A2 genannten Zugangsdaten sind in der Nachweismappe als Fundstelle und Zeitpunkt vermerkt, die Werte selbst nicht. Für die Prüfung standen keine Leserechte auf Secrets zur Verfügung; die Angaben zur Verschlüsselung at rest, das Secret-Inventar und die Benchmark-Ausgaben der Knoten hat der Auftraggeber bereitgestellt.

Löschfrist nach Vereinbarung: 12 Monate nach Übergabe.

9 · Rechtliche Hinweise

Dieser Bericht ist eine technische Bewertung des Prüfgegenstands gegen den BSI-Baustein APP.4.4 Kubernetes. Er stellt **keine Rechtsberatung** dar. Ob und in welchem Umfang der Auftraggeber den Pflichten des BSIG unterliegt, welchen Schutzbedarf er festlegt und welche Anforderungen für ihn verbindlich sind, entscheidet der Auftraggeber.

Der Bericht ist **kein Zertifikat** und **kein Testat**. Er ist weder ein Audit nach ISO/IEC 27001 noch eine Zertifizierung auf Basis IT-Grundschutz noch eine Prüfung nach § 39 BSIG.

Die Erhebung erfolgte ausschließlich lesend. Es wurden keine Konfigurationen verändert und keine Schwachstellen ausgenutzt.

Der Bericht ist vertraulich und ausschließlich für den Auftraggeber bestimmt. Eine Weitergabe an Dritte — ausgenommen Aufsichtsbehörden, Wirtschaftsprüfer und Kunden im Rahmen von Lieferkettennachweisen — bedarf der schriftlichen Zustimmung.

Sutaj Services · Brendon Sutaj · St. Ingbert · brendon@sutajservices.de