# Kubernetes-Sicherheitsaudit nach BSI IT-Grundschutz APP.4.4

**Leistungsbeschreibung und Konditionen — Sutaj Services, Stand 30.10.2026**

## 1. Anlass beim Kunden

Das BSI-Gesetz in der Fassung vom 02.12.2025 (BGBl. 2025 I Nr. 301) ist am 06.12.2025 ohne allgemeine Übergangsfrist in Kraft getreten. § 30 Abs. 1 Satz 3 BSIG verlangt von betroffenen Einrichtungen wörtlich:

> „Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren."

Sechs der zehn Maßnahmenbereiche aus § 30 Abs. 2 BSIG berühren den Betrieb einer Container-Plattform:

| § 30 ABS. 2 BSIG | MASSNAHMENBEREICH |
|---|---|
| Nr. 3 | Backup, Wiederherstellung, Krisenmanagement |
| Nr. 4 | Sicherheit der Lieferkette |
| Nr. 5 | Schwachstellenmanagement und -offenlegung |
| Nr. 8 | Kryptografiekonzepte |
| Nr. 9 | Personalsicherheit, Zugriffskontrolle, Verwaltung von IKT-Systemen |
| Nr. 10 | Multi-Faktor- oder kontinuierliche Authentifizierung |

Das BSI führt für Kubernetes einen eigenen Prüfbaustein: **APP.4.4 Kubernetes**, Edition 2023, mit 21 numerierten Anforderungen. Er ist vom Baustein SYS.1.6 Containerisierung getrennt; SYS.1.6 nimmt Orchestrierung ausdrücklich aus seinem Anwendungsbereich aus und verweist für Kubernetes auf APP.4.4.

Dieses Audit liefert dazu einen **Beitrag zur technischen Dokumentation**: eine nachvollziehbare, mit Rohdaten belegte Bewertung der Container-Plattform gegen ein anerkanntes Prüfraster. Es deckt die Dokumentationspflicht nicht vollständig ab — die übrigen Maßnahmenbereiche aus § 30 Abs. 2 BSIG reichen über die Plattform hinaus (siehe Abschnitt 4).

## 2. Leistungsumfang entlang der 21 Anforderungen

### Stufe Basis — die fünf MUSS-Anforderungen (A1–A5)

| NR. | ANFORDERUNG | GEPRÜFT WIRD |
|---|---|---|
| A1 | Planung der Separierung der Anwendungen | Mandanten- und Anwendungstrennung, Namespace-Schnitt, dokumentierte Separierungsentscheidung |

| NR. | ANFORDERUNG | GEPRÜFT WIRD |
|---|---|---|
| A2 | Planung der Automatisierung mit CI/CD | Rollen- und Rechtekonzept der Pipelines, Absicherung von Kubernetes Secrets (Verschlüsselung at rest, External-Secrets/Sealed-Secrets-Nutzung, Leckage in Logs und Manifesten) |
| A3 | Identitäts- und Berechtigungsmanagement | Authentifizierung aller Zugriffe, keine anonymen administrativen Handlungen, RBAC nach Least Privilege, Auswertung von ClusterRoleBindings, Wildcard- und `cluster-admin`-Vergaben |
| A4 | Separierung von Pods | Trennung von Prozess- und Benutzer-IDs, IPC, Dateisystem und Netz inkl. Hostname; `hostPID` / `hostIPC` / `hostNetwork`, Pod Security Standards, Container-Runtime-Isolation |
| A5 | Datensicherung im Cluster | Sicherung von etcd, Persistent Volumes sowie Code- und Image-Registries; Wiederherstellbarkeit, Aufbewahrung, Verschlüsselung der Sicherungen |

### Stufe Standard — Stand der Technik (A6–A12)

| NR. | ANFORDERUNG | GEPRÜFT WIRD |
|---|---|---|
| A6 | Initialisierung von Pods | Init-Container, Beendigung laufender Prozesse, Startreihenfolge nur bei erfolgreicher Initialisierung |
| A7 | Separierung der Netze | Trennung von Administrations-, Control-Plane- und Anwendungsnetzen; Default-Deny zwischen Namespaces mit Whitelisting; Erreichbarkeit administrativer Ports nur aus dem Administrationsnetz; Berechtigung zur CNI- und Regelverwaltung |

| NR. | ANFORDERUNG | GEPRÜFT WIRD |
|---|---|---|
| A8 | Absicherung von Konfigurationsdateien | Versionierung und Annotation aller Cluster-Konfiguration inkl. Erweiterungen; minimale Zugangsrechte auf die Verwaltungssoftware; gesonderte Einschränkung des Zugriffs auf Control-Plane-Konfiguration |
| A9 | Nutzung von Service-Accounts | Kein `default`-Service-Account in Pods und keine Rechte darauf; eigene Service-Accounts je Anwendung; `automountServiceAccountToken` dort deaktiviert, wo nicht benötigt; privilegierte Accounts nur für Control Plane; eigene Token je Automatisierungsprogramm |
| A10 | Absicherung der Automatisierungsprozesse | Pipelines mit minimalen Rechten; getrennte Prozesse je Benutzergruppe mit gruppenspezifischen Rechten |
| A11 | Überwachung der Container | Readiness- und Liveness-Checks je Container, aussagekräftige Prüflogik, angemessene Zeitspannen, Lösch- bzw. Neustartverhalten |
| A12 | Absicherung der Infrastruktur-Anwendungen | Registry, Automatisierung, Storage- und Konfigurationsverwaltung: personenbezogene und Service-Accounts, verschlüsselte Kommunikation auf allen Netzports, minimale Berechtigungen, Protokollierung von Änderungen, regelmäßige Datensicherung |

### Stufe Erhöhter Schutzbedarf (A13–A21)

Nur nach vorliegender Risikoanalyse des Kunden. Der Baustein bezeichnet diese Anforderungen ausdrücklich als „exemplarische Vorschläge", die Festlegung erfolgt im Rahmen der individuellen Risikoanalyse.

| NR. | ANFORDERUNG |
|---|---|
| A13 | Automatisierte Auditierung der Konfiguration (Freigabeliste und standardisierte Benchmarks, technische Durchsetzung im Cluster) |
| A14 | Verwendung dedizierter Nodes |

| NR. | ANFORDERUNG |
|---|---|
| A15 | Trennung von Anwendungen auf Node- und Cluster-Ebene |
| A16 | Verwendung von Operatoren |
| A17 | Attestierung von Nodes |
| A18 | Verwendung von Mikro-Segmentierung |
| A19 | Hochverfügbarkeit von Kubernetes |
| A20 | Verschlüsselte Datenhaltung bei Pods |
| A21 | Regelmäßiger Restart von Pods |

Der Baustein nennt in Abschnitt 4 als weiterführende Quellen den **CIS Benchmark Kubernetes** und **NIST SP 800-190**. Beide werden in Stufe Standard und Voll als technische Messlatte herangezogen.

---

## 3. Pakete, Aufwand und Preise

Alle Preise netto zzgl. 19 % USt., Festpreis, keine Tagessatzabrechnung.

### Paket 1 — Basis-Check (A1–A5)

**1.900 €** · 2 Personentage · Ergebnis innerhalb von 5 Arbeitstagen

Prüfung der **fünf** MUSS-Anforderungen, CIS-Benchmark-Lauf, Kurzbericht mit Ampelbewertung und Sofortmaßnahmen. Für Einstieg, Zweitmeinung oder einen einzelnen Cluster.

### Paket 2 — Standard-Audit (A1–A12) · *Empfehlung*

**4.500 €** · 4 Personentage · Ergebnis innerhalb von 10 Arbeitstagen

Vollständige Prüfung aller **zwölf** Basis- und Standard-Anforderungen (A1 bis A12), CIS-Benchmark-Auswertung, priorisierter Maßnahmenplan, Management-Summary und Abschlussworkshop. Dies ist der Umfang, der dem Stand der Technik nach BSI entspricht.

### Paket 3 — Vollaudit (A1–A21)

**7.900 €** · 7 Personentage · Ergebnis innerhalb von 15 Arbeitstagen

Zusätzlich die **neun** Anforderungen bei erhöhtem Schutzbedarf (A13 bis A21), insgesamt also einundzwanzig, Abgleich gegen die Risikoanalyse des Kunden, NIST SP 800-190, sowie Entwurf einer Admission-Policy-Baseline zur technischen Durchsetzung nach A13.

### Fristen

Die angegebenen Arbeitstage laufen ab der vollständigen Bereitstellung der vereinbarten Zugänge und Auskünfte nach Abschnitt 5, nicht ab Auftragserteilung. Konkrete Termine für Kickoff, Erhebung und Abschlussworkshop werden nach Vereinbarung festgelegt.

## Aufwandsaufschlüsselung Paket 2

| SCHRITT | PT |
|---|---|
| Kickoff, Scope-Festlegung, Zugangsklärung | 0,5 |
| Erhebung im Cluster (lesend), Benchmark-Läufe, RBAC- und NetworkPolicy-Auswertung | 1,0 |
| Bewertung gegen A1–A12, Rückfragen an Betrieb und Entwicklung | 1,0 |
| CIS-Benchmark-Auswertung, Priorisierung nach Risiko und Aufwand | 0,5 |
| Bericht, Nachweismappe, Management-Summary | 0,75 |
| Abschlussworkshop (90 Minuten) | 0,25 |
| **Summe** | **4,0** |

## Mengen und Zuschläge

- Enthalten: **ein** Cluster und bis zu **drei** Namespaces im Detail.
- Jeder weitere Cluster: +60 % des Paketpreises, da Control Plane und Infrastruktur erneut zu bewerten sind.
- Jeder weitere Namespace im Detail: +250 €.
- On-Premises-Plattformen ohne Managed Control Plane: +0,5 PT, Festzuschlag **+560 €**.
- Vor-Ort-Termin statt remote: +450 € pro Tag zzgl. Reisekosten.

  **Satz für Auditzuschläge: 1.125 € je Personentag.** Das ist der im Standard-Audit

  enthaltene Tagessatz. Für Zuschläge im Umfang eines halben Personentags gilt ein gerundeter

  Festzuschlag von **560 €**; rechnerisch wären es 562,50 €, der Betrag ist bewusst abgerundet

  und wird nicht je Fall neu gerechnet. Der Satz von 980 €/PT gilt ausschließlich für

  Umsetzungsunterstützung und wird für Auditzuschläge nicht herangezogen.

## Anrechnung auf ein Umsetzungsprojekt

Bis zu **1.900 €** des Auditpreises werden auf die erste Rechnung angerechnet, wenn innerhalb von **30 Tagen** nach Berichtsübergabe ein Umsetzungsprojekt von mindestens **zehn Personentagen** beauftragt wird. Die Anrechnung erfolgt einmalig je Auftraggeber und ist nicht auszahlbar.

## Folgeleistungen (optional)

- **Nachprüfung** nach Umsetzung, gleicher Prüfumfang, Delta-Bericht: **1.500 €** (Paket 2).
- **Jahresnachweis**: zwei Nachprüfungen pro Jahr plus Fortschreibung der Nachweismappe, **3.900 €/Jahr**.
- Umsetzungsunterstützung nach Aufwand: **980 €/Personentag**.

---

## 4. Ergebnisartefakte

Der Kunde erhält nach Abschluss:

1. **Prüfbericht** mit einer Zeile je geprüfter Anforderung und der Bewertung *erfüllt / teilweise erfüllt / nicht erfüllt / nicht anwendbar*, jeweils mit Begründung und Belegstelle.
2. **Nachweismappe** mit den Rohdaten der Erhebung: ausgeführte Kommandos, Zeitstempel, Benchmark-Ausgaben, Konfigurationsauszüge. Damit ist jede Bewertung für einen Dritten nachvollziehbar und der Bericht hält einer Rückfrage stand.
3. **Maßnahmenplan**, priorisiert nach Risiko und Umsetzungsaufwand, mit geschätztem Aufwand je Maßnahme.
4. **Management-Summary**, zwei Seiten, adressiert an die Geschäftsleitung.
5. **Zuordnungstabelle** APP.4.4-Anforderung → § 30 Abs. 2 BSIG, damit sich die Ergebnisse in eine vorhandene Dokumentation einordnen lassen.
6. **Abschlussworkshop**, 90 Minuten, remote, mit Betrieb und Entwicklung.

Lieferform: PDF und Markdown. Die Nachweismappe zusätzlich als Dateisammlung.

### Aufbewahrung und Löschung der Nachweismappe

Die Nachweismappe enthält die Rohdaten der Erhebung und ist damit das schutzbedürftigste der gelieferten Artefakte. Dafür gelten folgende Regeln:

- **Inhalt.** Secret-Werte, Token, Schlüssel und Zugangsdaten werden nicht aufgenommen. Dokumentiert wird jeweils der Befund, nicht der Inhalt. Personenbezogene Daten werden auf das Notwendige beschränkt; Gesprächsnotizen führen die Rolle statt des Namens, sofern der Auftraggeber nichts anderes wünscht.
- **Übergabe** erfolgt verschlüsselt.
- **Aufbewahrungsdauer auf meiner Seite.** Die Frist wird im Kickoff vereinbart und im Erhebungsprotokoll der Nachweismappe festgehalten. Nach Ablauf wird die Mappe einschließlich aller Arbeitskopien gelöscht. Wird keine abweichende Frist vereinbart, richtet sie sich nach der Vorgabe des Auftraggebers.
- **Auf Wunsch** erfolgt die Löschung unmittelbar nach Übergabe und Abnahme des Berichts. Für Rückfragen und eine spätere Nachprüfung steht die Mappe dann nicht mehr zur Verfügung.
- Bericht, Management-Summary und Maßnahmenplan sind davon unberührt und verbleiben beim Auftraggeber.

Sofern die Erhebung personenbezogene Daten berührt, ist vor Beginn ein Vertrag über die Auftragsverarbeitung nach Artikel 28 DSGVO zu schließen.

### Einordnung der Ergebnisse

Der Bericht ist ein **Beitrag zur technischen Dokumentation** des Auftraggebers: eine nachvollziehbare, 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, die weit über die Container-Plattform hinausreichen — etwa Vorfallbewältigung, Schulungen, Lieferantenmanagement und organisatorische Konzepte. Welche Anforderungen den Auftraggeber treffen und ob seine Dokumentation insgesamt ausreicht, entscheidet der Auftraggeber; das Audit deckt davon den plattformtechnischen Ausschnitt ab.

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

---

## 5. Mitwirkung des Kunden

Erforderlich, sonst verschiebt sich der Liefertermin:

### Cluster-Zugang

Die mitgelieferte Standard-ClusterRole `view` **reicht nicht aus**. Die Kubernetes-Dokumentation hält dazu fest: *„Allows read-only access to see most objects in a namespace. It does not allow viewing roles or role bindings."* Genau diese Objekte sind aber Gegenstand der Anforderungen A3, A9 und A10.

Benötigt wird deshalb eine eigens angelegte, rein lesende ClusterRole mit `get` und `list` auf:

| BEREICH | RESSOURCEN |
|---|---|
| `rbac.authorization.k8s.io` | `roles`, `rolebindings`, `clusterroles`, `clusterrolebindings` |
| Kern-API | `pods`, `services`, `serviceaccounts`, `configmaps`, `namespaces`, `nodes`, `persistentvolumes`, `persistentvolumeclaims`, `resourcequotas`, `limitranges` |
| `apps`, `batch` | `deployments`, `statefulsets`, `daemonsets`, `replicasets`, `jobs`, `cronjobs` |
| `networking.k8s.io` | `networkpolicies`, `ingresses` |
| `admissionregistration.k8s.io` | `validatingwebhookconfigurations`, `mutatingwebhookconfigurations` |
| `storage.k8s.io`, `apiextensions.k8s.io` | `storageclasses`, `csidrivers`, `customresourcedefinitions` |
| `policy` | `poddisruptionbudgets` |

Ein fertiges Manifest liefere ich zum Kickoff mit. Die Rolle wird zeitlich befristet gebunden und nach Abschluss der Erhebung wieder entfernt.

### Secrets — bewusst ohne Zugriff

Leserechte auf `secrets` fordere ich **nicht** an. Kubernetes kann Metadaten und Inhalt nicht getrennt freigeben: Wer Secrets listen darf, liest ihre Werte mit. Die beiden Prüfungen aus A2 führt deshalb der Auftraggeber selbst durch und stellt mir die Ausgabe zur Verfügung:

- Ist eine `EncryptionConfiguration` aktiv (Verschlüsselung at rest)?
- Inventar der Secrets je Namespace, nur Name, Typ und Alter — ohne Werte.

### Benchmark-Läufe und Control Plane

Die lesende Rolle reicht genau so weit wie die Kubernetes-API. Ein Teil der Prüfpunkte des CIS Benchmark liegt außerhalb davon: kube-bench bewertet die Konfiguration von Control Plane und Knoten, indem es auf dem jeweiligen Knoten Konfigurationsdateien und Prozessinformationen liest. Das setzt Zugriff auf das Betriebssystem voraus, in Teilen mit erhöhten Rechten. Auch die Ausführung als Pod im Cluster ändert daran nichts: Der Lauf braucht dann Host-Pfade und Host-Prozessinformationen. **Diesen Zugriff fordere ich nicht an.**

Daraus ergeben sich drei Fälle, die vor dem Kickoff festzulegen sind:

| FALL | WER ERHEBT | WIE DER BERICHT DAMIT UMGEHT |
|---|---|---|
| Knoten im Zugriff des Auftraggebers | Der Auftraggeber führt kube-bench aus und stellt die vollständige Ausgabe bereit | Ausgabe geht unverändert in die Nachweismappe, gekennzeichnet als Angabe des Auftraggebers |
| Begleitete Sitzung | Ein Administrator des Auftraggebers führt die Läufe aus, ich protokolliere mit | wie oben, zusätzlich mit Zeitstempel und Teilnehmenden |
| Verwaltete Control Plane | Niemand — der Anbieter betreibt die Master-Knoten | Die betroffenen Prüfpunkte werden als **nicht unabhängig prüfbar** ausgewiesen |

Zum dritten Fall ausdrücklich: Bei einer verwalteten Control Plane kann der Benchmark-Lauf auch vom Auftraggeber nicht durchgeführt werden, weil die Master-Knoten nicht in seinem Zugriff stehen. An die Stelle des Laufs treten dann die Angaben, die der Anbieter in Konsole oder Dokumentation bereitstellt. Wo die Verantwortung beim Anbieter liegt, benennt der Bericht die Anbieterverantwortung und was der Auftraggeber von dort beibringen sollte. Er stellt dem Auftraggeber **keine Lücke** in Rechnung, die er gar nicht schließen kann.

Dasselbe gilt sinngemäß für einzelne Angaben zum API-Server, etwa `--anonymous-auth` oder die Konfiguration des Audit-Logs: Bei selbst betriebener Control Plane genügt Leserecht auf die Konfigurationsdateien oder der Auszug aus dem Benchmark-Lauf, bei verwalteter Control Plane tritt die Angabe des Anbieters an diese Stelle.

Welcher Fall vorliegt und welche Prüfpunkte damit entfallen, steht im Bericht im Abschnitt „Grenzen der Aussagekraft" und je Anforderung in der Belegstelle.

### Weitere Mitwirkung

- Lesender Zugriff auf die Pipeline-Definitionen und das Konfigurations-Repository.
- Benennung einer fachlich auskunftsfähigen Ansprechperson für Betrieb und für Entwicklung.
- Sofern vorhanden: Schutzbedarfsfeststellung, Netzplan, bestehende Risikoanalyse.
- Bei Produktivsystemen: Freigabe für die lesenden Erhebungsläufe.

Alternativ zu eigenen Zugängen ist eine **begleitete Sitzung** möglich: Ein Administrator des Auftraggebers führt die Abfragen aus, ich protokolliere mit. Das kostet einen halben Personentag mehr, Festzuschlag **+560 €**, und wird gesondert vereinbart.

---

## 6. Abgrenzung

Ausdrücklich **nicht** Gegenstand dieser Leistung:

- **Keine Rechtsberatung.** Ob und in welchem Umfang der Kunde dem BSIG unterliegt, welchen Schutzbedarf er festlegt und welche Anforderungen für ihn verbindlich sind, entscheidet der Kunde. Das Audit liefert eine technische Bewertung gegen ein Prüfraster, keine Rechtsauskunft.
- **Keine Zertifizierung und kein Testat.** Dies ist kein Audit nach ISO 27001, keine Zertifizierung auf Basis IT-Grundschutz und keine Prüfung nach § 39 BSIG. Es wird kein Zertifikat ausgestellt.
- **Kein vollständiger BSIG-Nachweis.** Der Bericht deckt den plattformtechnischen Ausschnitt ab, nicht die organisatorischen Maßnahmenbereiche des § 30 Absatz 2 BSIG (siehe Abschnitt 4, Einordnung der Ergebnisse).

- **Keine Änderungen am System.** Die Erhebung erfolgt ausschließlich lesend. Es werden keine Konfigurationen verändert, keine Workloads neu gestartet und keine Agenten dauerhaft installiert.
- **Kein Penetrationstest, kein Red Teaming, keine Exploit-Ausnutzung.**
- **Kein Review des Anwendungscodes** und keine Prüfung der in den Containern betriebenen Fachanwendungen.
- **Baustein SYS.1.6 Containerisierung** (26 Anforderungen) ist nicht enthalten und wird separat angeboten.
- **A13–A21** sind nur in Paket 3 und nur insoweit enthalten, als der Kunde einen erhöhten Schutzbedarf festgestellt hat.
- **Keine Vollständigkeitsgarantie.** Das Audit bewertet den Zustand zum Erhebungszeitpunkt auf Basis der bereitgestellten Zugänge und Auskünfte. Es ersetzt keinen fortlaufenden Sicherheitsbetrieb.

### Vertragliche Grundlage

Diese Leistungsbeschreibung stellt den Leistungsumfang dar. Sie ist **kein verbindliches Angebot**; eine Beauftragung kommt erst mit einem Einzelvertrag zustande.

Haftung, Gewährleistung und Vertraulichkeit werden im Einzelvertrag geregelt.