

MUSTERBERICHT, GEKÜRZT

AWS-Architektur-Review mit Kostencheck

Bericht zur AWS-Umgebung des Kundenportals
der Musterwerk GmbH

Auftraggeber	Musterwerk GmbH (fiktiv)
Geprüfte Umgebung	Kundenportal auf AWS, ein Account, Region Frankfurt (fiktiv)
Gebaut und betrieben von	Externer Dienstleister seit 2023 (fiktiv)
AWS-Rechnung	Rund 8.000 € im Monat, Durchschnitt der letzten sechs Monate
Stufe	Architektur-Review mit Kostencheck
Prüfer	Mark Joachim, tarienna GmbH
Stand	Oktober 2026

Dieser Bericht ist ein gekürztes Muster.

Auftraggeber, Umgebung, Dienstleister und alle Feststellungen sind frei erfunden. Ähnlichkeiten mit bestehenden Unternehmen oder Systemen sind nicht beabsichtigt. Der Bericht zeigt den Aufbau eines Berichts des AWS-Architektur-Reviews in Auszügen. Ein Bericht aus einem beauftragten Review enthält zu allen sieben Prüfpunkten sämtliche Feststellungen, die vollständige Maßnahmenliste, den vollständigen Kostenanhang und alle offenen Fragen.

1 Gesamteinschätzung

Bewertung **Gelb** Trägt den heutigen Betrieb, nicht den nächsten Ausfall

Die Umgebung ist für die heutige Nutzung passend gebaut. Die Bausteine sind angemessen, die Infrastruktur liegt als Code vor, und die öffentlichen Endpunkte sind geschützt.

Zwei Punkte würde ich vor allem anderen klären. Das Backup der Datenbank wurde seit der Inbetriebnahme nie zurückgespielt, und die Datenbank läuft in einer einzigen Verfügbarkeitszone. Fällt sie aus, steht das Portal, und niemand weiß, wie lange die Wiederherstellung dauert. Außerdem hält der Dienstleister als Einziger Administratorrechte und die Deployment-Kette läuft nur von seinem Rechner. Ein Wechsel des Dienstleisters wäre heute ein Risiko für den Betrieb.

Bei den Kosten liegen rund 1.200 € im Monat in Ressourcen, die niemand braucht, in einer fehlenden Reservierung und in Protokollen ohne Löschfrist. Über drei Jahre sind das rund 43.200 €, etwa 15 Prozent der Rechnung. Die Maßnahmen dafür sind in wenigen Tagen umgesetzt und stehen im Kostenanhang (Abschnitt 5).

2 Ampelübersicht

Nr.	Prüfpunkt	Ampel	Kernaussage
1	Sicherheit	Gelb	Endpunkte geschützt, Verschlüsselung aktiv. Zwei Nutzer ohne zweiten Faktor, Administratorrechte nur beim Dienstleister.
2	Zuverlässigkeit	Rot	Backup nie zurückgespielt, Datenbank in einer Verfügbarkeitszone, kein Alarm auf die Fehlerquote.
3	Kosten	Gelb	Rund 1.200 € im Monat vermeidbar: verwaiste Ressourcen, fehlende Reservierung, Protokolle ohne Löschfrist.
4	Betrieb	Gelb	Infrastruktur als Code vorhanden. Deployments nur vom Rechner des Dienstleisters, Abläufe nicht dokumentiert.
5	Architektur	Grün	Die Bausteine passen zur Aufgabe. Keine unnötige Komplexität, keine versteckten Abhängigkeiten.
6	Daten und Datenschutz	Gelb	Daten in Frankfurt. Zugriffsprotokolle mit personenbezogenen Daten ohne Löschfrist.
7	Zukunftsfähigkeit	Grün	Dienste aktuell, kein Baustein läuft aus. Der Weg zu KI-Funktionen auf AWS ist offen.

So ist die Ampel zu lesen

Grün

Kein wesentliches Risiko erkennbar.

Gelb

Es besteht ein Risiko, das sich mit überschaubarem Aufwand beheben lässt. Die Maßnahme steht in der Maßnahmenliste.

Rot

Es besteht ein wesentliches Risiko für den Betrieb. In der vorliegenden Form trägt dieser Punkt nicht.

So sind die Feststellungen gekennzeichnet

G

Geprüft. Ich habe die Aussage über den lesenden Zugang, mit einem Werkzeug von AWS oder in den Unterlagen nachvollzogen.

A

Angabe. Die Aussage beruht auf dem Gespräch mit dem Auftraggeber oder dem Dienstleister und wurde nicht überprüft.

3 Die Prüfpunkte im Einzelnen (Auszug)

Dieser Musterbericht zeigt drei der sieben Prüfpunkte mit einer Auswahl der Feststellungen. Ein Bericht aus einem beauftragten Review enthält zu jedem Prüfpunkt alle Feststellungen, die Einordnung und die zugehörigen Maßnahmen.

3.1 Sicherheit

Wer kommt an die Umgebung heran, und würde es jemand merken?

Bewertung**Gelb**

... Feststellungen und Einordnung sind im Musterbericht gekürzt.

3.2 Zuverlässigkeit

Was passiert, wenn ein Baustein ausfällt, und wie schnell läuft die Anwendung wieder?

Bewertung**Rot**

Feststellungen (Auszug)

G

Die Datenbank wird täglich automatisch gesichert, die Sicherungen werden sieben Tage aufbewahrt (Konfiguration des Datenbankdienstes).

A

Eine Wiederherstellung aus einer Sicherung wurde seit der Inbetriebnahme 2023 nie durchgeführt. Wie lange sie dauert, kann niemand sagen.

G

Die Datenbank läuft in einer einzigen Verfügbarkeitszone. Alarmer bestehen nur auf die Auslastung der Rechner, nicht auf die Fehlerquote oder die Antwortzeit des Portals (Konfiguration von Datenbank und Monitoring).

... Weitere Feststellungen sind im Musterbericht gekürzt.

Bedeutung für die Entscheidung

Hier liegt das größte Risiko. Eine Sicherung, die nie zurückgespielt wurde, ist eine Vermutung, kein Backup. Fällt die Datenbank aus, steht das Portal, bis jemand die Wiederherstellung zum ersten Mal unter Druck durchführt. Zwei Tage Stillstand kosten im Rechenbeispiel des Auftraggebers rund 32.500 €, die Wiederherstellungsprobe einen halben Tag.

3.3 Kosten

Wofür zahlt der Auftraggeber, und wie entwickelt sich die Rechnung mit dem Wachstum?

Bewertung **Gelb**

Feststellungen (Auszug)

- G** Rund 480 € im Monat entfallen auf Ressourcen ohne Verwendung, darunter eine Testumgebung aus dem Jahr 2024, nicht zugeordnete Datenträger und alte Schnappschüsse (Cost Explorer, Trusted Advisor, eigene Auswertung).
- G** Die Datenbank läuft seit zwei Jahren unverändert zum Standardtarif. Eine Reservierung über ein Jahr würde rund 520 € im Monat sparen (Preisliste, Nutzungsverlauf).
- G** Zugriffsprotokolle werden unbegrenzt aufbewahrt und kosten rund 200 € im Monat, Tendenz steigend (Konfiguration der Protokollgruppen, Cost Explorer).

... Weitere Feststellungen sind im Musterbericht gekürzt.

Ein Befund, der nicht umgesetzt wird

Das Werkzeug zeigt

Der Compute Optimizer empfiehlt, den Anwendungsserver um eine Größe zu verkleinern. Die Auslastung lag in den letzten 14 Tagen im Mittel bei 18 Prozent. Ersparnis laut Werkzeug rund 310 € im Monat.

Die Erfahrung liest

Das Werkzeug sieht 14 Tage. Im Nutzungsverlauf der letzten sechs Monate steigt die Auslastung an jedem Monatsende für zwei Tage auf über 85 Prozent, weil das Portal dann die Abrechnungen für alle Kunden erzeugt. Eine kleinere Instanz würde genau dann zu langsam, wenn die Kunden das Portal am dringendsten brauchen.

Entscheidung

Nicht verkleinern. Die Einsparung steht deshalb nicht im Kostenanhang. Stattdessen empfehle ich zu prüfen, ob die Abrechnung in einen eigenen, zeitlich begrenzten Prozess ausgelagert werden kann. Erst dann greift die Empfehlung des Werkzeugs gefahrlos.

Bedeutung für die Entscheidung

Die vermeidbaren Kosten sind nicht dramatisch, aber sie sind sicher und mit wenigen Ta-

gen Aufwand zu heben. Der Kostenanhang beziffert die drei Maßnahmen und ihren Aufwand.

3.4 Betrieb

Kann das Team des Auftraggebers die Umgebung ohne den Dienstleister betreiben?

Bewertung **Gelb**

Feststellungen (Auszug)

- G** Die Infrastruktur liegt vollständig als Code vor und entspricht dem Zustand im Account (Vergleich von Code und Konfiguration).
- A** Deployments laufen ausschließlich vom Arbeitsrechner eines Mitarbeiters des Dienstleisters aus. Eine automatisierte Pipeline gibt es nicht.
- G** Administratorrechte im Account hat nur eine Rolle, die der Dienstleister annimmt. Beim Auftraggeber gibt es keinen Nutzer mit diesen Rechten (Rechteübersicht, IAM Access Analyzer).

... Weitere Feststellungen sind im Musterbericht gekürzt.

Bedeutung für die Entscheidung

Die Umgebung ist gut gebaut, aber der Auftraggeber besitzt sie nicht wirklich. Ohne den Dienstleister kann heute niemand ein Deployment ausführen oder ein Problem im Account beheben. Das lässt sich mit einer Pipeline im Account des Auftraggebers und einer eigenen Administratorrolle mit zweitem Faktor in wenigen Tagen ändern. Der Dienstleister bleibt dabei an Bord, nur nicht mehr als einziger Schlüsselhalter.

3.5 Architektur

Passen die Bausteine zur Aufgabe, oder zahlt der Auftraggeber für Komplexität, die niemand braucht?

Bewertung **Grün**

... Feststellungen und Einordnung sind im Musterbericht gekürzt.

3.6 Daten und Datenschutz

Wo liegen die Daten, wer greift darauf zu, und wann werden sie gelöscht?

Bewertung **Gelb**

... Feststellungen und Einordnung sind im Musterbericht gekürzt.

3.7 Zukunftsfähigkeit

Trägt die Architektur die nächsten drei Jahre, oder blockiert sie das nächste Vorhaben?

Bewertung **Grün**

... Feststellungen und Einordnung sind im Musterbericht gekürzt.

4 Maßnahmenliste (Auszug)

Die Maßnahmen sind nach Dringlichkeit sortiert. Aufwand und Nutzen sind Schätzungen für die Umsetzung durch das Team des Auftraggebers oder seinen Dienstleister.

Nr.	Maßnahme	Priorität	Aufwand	Nutzen
1	Wiederherstellung der Datenbank aus einer Sicherung proben und die Dauer dokumentieren	Hoch	0,5 Tage	Ausfallzeit wird bekannt, Backup wird belastbar
2	Datenbank auf zwei Verfügbarkeitszonen umstellen	Hoch	1 Tag	Ausfall einer Zone trifft das Portal nicht mehr
3	Eigene Administratorrolle beim Auftraggeber mit zweitem Faktor einrichten	Hoch	0,5 Tage	Auftraggeber ist handlungsfähig ohne den Dienstleister
4	Deployment-Pipeline im Account des Auftraggebers aufsetzen	Mittel	2 Tage	Deployments unabhängig von einem Rechner

... Weitere Maßnahmen sind im Musterbericht gekürzt.

5 Kostenanhang (Auszug)

Die Einsparungen beruhen auf den Rechnungen der letzten sechs Monate und der Preisliste von AWS zum Zeitpunkt des Reviews. Ob sie eintreten, hängt von der Umsetzung ab.

Maßnahme	Einsparung je Monat	Aufwand
Testumgebung aus 2024, nicht zugeordnete Datenträger und alte Schnappschüsse löschen	480 €	1 Tag
Reservierung für die Datenbank über ein Jahr abschließen	520 €	0,5 Tage
Löschfrist für Zugriffsprotokolle setzen, ältere Protokolle archivieren	200 €	0,5 Tage
Summe	1.200 €	2 Tage

... Weitere Posten sind im Musterbericht gekürzt.

Über drei Jahre entsprechen die drei Posten rund 43.200 €, bei einer Rechnung von 8.000 € im Monat etwa 15 Prozent. Nicht enthalten ist die Verkleinerung des Anwendungsservers aus Abschnitt 3.3, weil sie den Monatsabschluss gefährden würde.

6 Offene Fragen (Auszug)

Diese Fragen sollte der Auftraggeber intern oder mit seinem Dienstleister klären, bevor er die Maßnahmen beauftragt.

1. Welche Ausfallzeit des Portals ist für das Geschäft tragbar, und ist der Aufwand für zwei Verfügbarkeitszonen dafür angemessen?
2. Wer beim Auftraggeber übernimmt die eigene Administratorrolle, und wie wird der zweite Faktor verwahrt?
3. Welche Löschfrist für Zugriffsprotokolle ist mit dem Datenschutzbeauftragten abgestimmt?
4. Lässt sich die Abrechnung am Monatsende in einen eigenen Prozess auslagern, damit der Anwendungsserver kleiner werden kann?

... Weitere offene Fragen sind im Musterbericht gekürzt.

7 Grundlagen und Grenzen des Reviews

Grundlagen

- Ein rein lesender Zugang zum Account des Auftraggebers über eine eigene Rolle, die nach dem Review entfernt wurde
- Die Werkzeuge von AWS (Cost Explorer, Trusted Advisor, IAM Access Analyzer, Compute Optimizer) und eigene Skripte über die AWS CLI
- Architekturunterlagen und die Rechnungen der letzten sechs Monate
- Ein Gespräch von zwei Stunden mit den Verantwortlichen des Auftraggebers für Anwendung und Betrieb

Grenzen

- Das Review beruht auf lesendem Zugang, Unterlagen und Gesprächen. Es ist kein Penetrationstest und keine Quellcode-Analyse der Anwendung.
- Einsparungen sind Schätzungen auf Basis der letzten sechs Monate und der Preisliste von AWS zum Zeitpunkt des Reviews. Ob sie eintreten, hängt von der Umsetzung ab.
- Das Review ersetzt keine Rechtsberatung, auch nicht beim Datenschutz. Es benennt Befunde und Fragen, die mit dem Datenschutzbeauftragten zu klären sind.
- tarienna hat nichts in der Umgebung geändert. Alle Befunde sind so dokumentiert, dass der Auftraggeber oder sein Dienstleister sie nachvollziehen und umsetzen kann.

Unabhängigkeit

- Die Vergütung hängt nie vom Ergebnis ab, auch nicht von der Höhe der gefundenen Einsparungen.
- tarienna erhält keine Provisionen von AWS, von Dienstleistern oder von Werkzeuganbietern.
- Der Bericht empfiehlt keine Umbauten, die tarienna anschließend selbst verkaufen will. Eine Umsetzung durch tarienna wäre ein getrenntes Angebot.
- Bestehende Geschäftsbeziehungen zum Dienstleister des Auftraggebers legt tarienna vor der Beauftragung offen.
- Umgebungen, die tarienna selbst gebaut oder maßgeblich mitgebaut hat, prüft tarienna nicht im Review.

Dieser Bericht ist ein gekürztes Muster mit frei erfundenem Auftraggeber, frei erfundener Umgebung und frei erfundenem Inhalt. Informationen zum AWS-Architektur-Review mit Kostencheck stehen unter www.tarienna.eu/aws-architektur-review/.