aiio GmbH
Klausenerstraße 10a
39112 Magdeburg

Betrieb der Applikation

„aiio®“

Betriebs- und IT- Sicherheitskonzept

Version 3.0

Stand: 14.08.2025

1 Vorwort / Zweck dieses Dokuments

Dieses Dokument beschreibt die IT-Sicherheitsaspekte der Anwendungsarchitektur und insbesondere die nutzungsbezogenen Sicherheitsfeatures für das Produkt aiio.

Inhaltsverzeichnis

2 Autoren und Änderungen des Dokuments

Dokumentenhistorie

Datum	Änderung	Autor	Version
24.03.2023	Erste Version	Moser P.	1.0
31.05.2023	Ergänzung bzgl. Zusammenarbeit mit OpenAI	Moser P.	2.0
14.08.2025	Überarbeitung KI- Partner Einführung von APM und CNAAP Exportfunktionen ergänzt Präzisierung der Konzepte für Verschlüsselung und Notfallwiederherstellung	Moser P.	3.0

3 Beschreibung der Anwendung

aiio ist ein webbrowserbasiertes Modellierungstool, mit dem Prozesse gezeichnet und Verantwortlichkeiten zugeordnet werden können – im Team und in gewohnter Microsoft 365 Optik.

3.1 Leistungsbeschreibung

aiio ermöglicht die direkte Verlinkung von Dokumenten und Strukturen mit den Prozessschritten. Die Prozessaktualität wird durch einfache Feedbackmöglichkeiten gewährleistet. Kommentare zu Prozessen und Probleme an Prozessen können durch jeden Nutzer aktiv geteilt werden. Durch die Einbindung von aiio in Webbrowser oder MS Teams kann jederzeit auf die Informationen zugegriffen werden.
Aiio ermöglicht die Einbeziehung von KI-Unterstützung. Damit ist es möglich Potentiale zur Verbesserung der Prozesse zu erkennen.

3.2 Verantwortlichkeiten

Verantwortlich für den Betrieb des Rechenzentrums, in dem die Hosting- Umgebung gehostet ist, zeichnet:
Microsoft Ireland Operations, Ltd.
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

Verantwortlich für den Betrieb der Hosting- Umgebung ist:
aiio GmbH
Klausenerstraße 10a
39112 Magdeburg

Verantwortlich für den Betrieb des KI-Modells und der damit verbundenen Datenverarbeitung ist der jeweils vom Kunden gewählte Anbieter. Der Kunde kann zwischen den folgenden KI-Partnern wählen:

OpenAI, L.L.C., San Francisco, United States of America

Anthropic, PBC, San Francisco, United States of America

Google Cloud EMEA GmbH, mit Hosting-Standort in Frankfurt am Main (Region europe-west3), Deutschland.

3.3 Schulung der Anwender

Der Einstieg in aiio ist so einfach wie möglich gestaltet. Durch die Anlehnung an M365 fällt den Nutzern der Einstieg in die Bedienung leichter. Zusätzlich gibt es durch die aiio Academy die Möglichkeit sich selbst über die grundlegenden Funktionen zu informieren und dann mit aiio zu starten.

Auf Kundenwunsch können gegen Vergütung spezifische Anwenderschulungen gebucht werden. Der Schulungsbedarf wird individuell abgestimmt. Themenschwerpunkte können hierbei sein:

- Einführungen in aiio®
- Schulung in der Methodik Prozessmanagement
- Schulung in der Prozessmodellierung
- Einführung in bisher nicht genutzte Funktionen und Weiterentwicklungen von aiio®

Verantwortlich: Consulting Services der aiio GmbH

3.4 Weiterentwicklung

aiio unterliegt einer kontinuierlichen Weiterentwicklung. Die Vorgehensweise für das Entwicklerteam folgt im Wesentlichen dem Schema der agilen Softwareentwicklung an die Scrum-Methodik angelehnt.
Features bzw. die inhaltliche Ausrichtung der Weiterentwicklung folgen zu einem hohen Maß den Bedürfnissen der aiio®- Nutzer oder sie ergeben sich aus Markt- bzw. Regulierungsanforderungen.

3.5 Ansprechpartner und Supportadressen aiio

https://www.aiio.de/support über das Kontaktformular oder per E-Mail an support@aiio.de

Verantwortlich: Customer Success Service der aiio GmbH

Weitere Informationen zum Störungsmanagement sind unter Kapitel 7 zu finden.

4 Technische Beschreibung

Die gesamte aiio®-Anwendungsarchitektur beruht auf einer Kombination aus React (Frontend) und Django (Backend) angeschlossen an eine MySQL Datenbank.
Die gesamte Umgebung ist in einem vollständig virtualisierten Microsoft® Azure™ Tennant installiert.
Die gesamte Umgebung wird in einem Microsoft Azure Tennant gehostet, wobei ein Azure Kubernetes Cluster zum Hosting der Applikation genutzt wird.

4.1 Architektur

Die Umgebung stellt sich wie folgt dar:

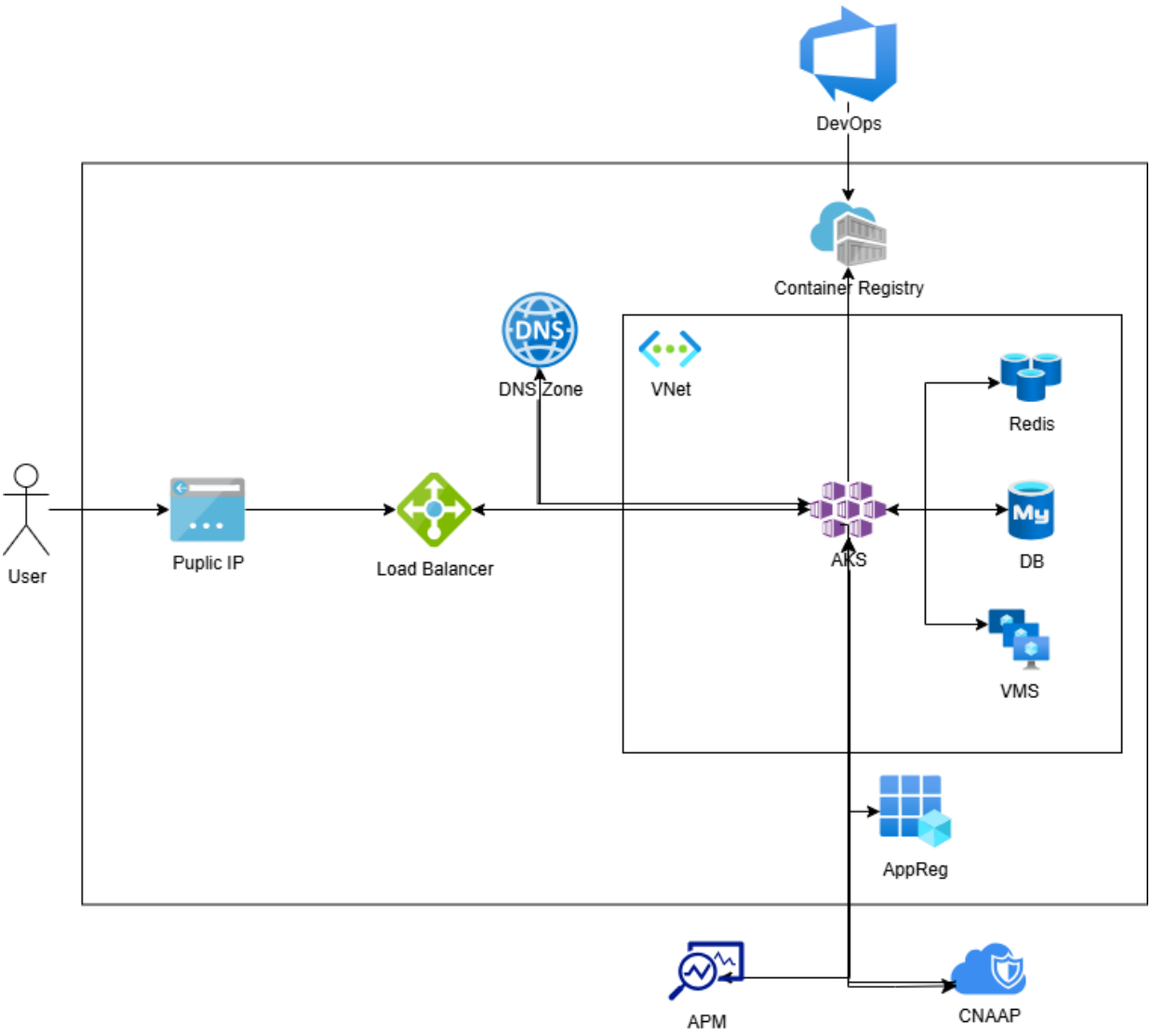

Abbildung 1 Schema aiio® Architektur

Um für alle Anwender größtmögliche Informationssicherheit zu gewährleisten, ist die Umgebung im Wesentlichen in 2 Bereiche segmentiert.
Das Hauptsegment umfasst ein virtuelles Netzwerk, das ein Azure Kubernetes Cluster und das dazugehörige Virtual Machine Scale Set beinhaltet. Ebenso befindet sich die MySQL Datenbank und der Redis Cache in diesem Netzwerk, auf das nur die Applikationen innerhalb des Clusters Zugriff haben.

Die Architektur wird im in einem speziell für aiio angelegten Tennant gehostet. Als einziger regulärer Zugriffspunkt auf die Applikation dient ein eine Public IP die über die DNS app.aiio.de erreichbar ist. Nutzer werden dann über einen Loadbalancer zu den Deployments innerhalb vom Cluster weitergeleitet.

Weiterer Zugriff ist nur über die aiio interne DevOps Plattform - für automatisierte Plattform Updates - oder ausgebildete Administratoren möglich.

Während des Betriebes stellt das Azure Kubernetes Cluster selbst konstant sicher, dass die Applikation lauffähig ist und bei hoher Last auch für jeden die Performance hält. Je nach Anzahl der Nutzer und Operationen wird sowohl die Datenbank als auch die Anzahl an virtuellen Maschinen skaliert. Sollten während des Betriebes Fehler oder sonstige wichtige Informationen auf Anwendungsebene auftreten, werden diese an einen spezialisierten Dienst für Application Performance Monitoring (APM) und Fehlerprotokollierung gemeldet.
Für die übergreifende Sicherheitsüberwachung der Cloud-Infrastruktur und die proaktive Erkennung von Bedrohungen wird zusätzlich eine Cloud-Native Application Protection Platform (CNAPP) eingesetzt (siehe 4.2).

Für die Architektur werden folgende Services verwendet:
Azure Kubernetes Cluster
Azure Database for MySQL flexible server (MySQL Version 5.7)
Azure Cache for Redis (Redis Version 6.0)
Virtual Machine Scale set (Image: AKSUbuntu-2204gen2containerd-202505.14.0)
Azure Container Registry
Dienst für Application Performance Monitoring (APM)
Cloud-Native Application Protection Platform (CNAPP)
DNS Zone

Die Updates der Services erfolgen automatisch durch den Einsatz von Azure.
Die Auswirkungen von Updates dieser Komponenten werden in einer Testumgebung überprüft, bevor die Updates in das Live-System eingespielt werden.

4.2 Betriebsbeschreibung

Der Betrieb der Umgebung funktioniert in aller Regel vollautomatisch und ohne Benutzereingriffe, es sei denn, es kommt zu Fehlern, die Benutzereingriffe durch die verwaltenden Personen erfordern.
Die Betriebsbereitschaft wird den verwaltenden Personen mittels integrierten Monitorings (s. Abb.2) angezeigt. Im Fehlerfall werden die verwaltenden Personen per E-Mail zusätzlich sofort informiert. Das Monitoring gehört zum Standardumfang der Microsoft® Azure™ Umgebung.
Ergänzend dazu wird der Betrieb durch zwei spezialisierte Ebenen abgesichert: Ein Dienst für Application Performance Monitoring (APM) und Fehlerprotokollierung überwacht kontinuierlich die Anwendungsleistung und meldet umgehend Fehler oder Engpässe. Dies wird ergänzt durch eine führende Cloud-Native Application Protection Platform (CNAPP), welche die Umgebung proaktiv schützt, indem sie rund um die Uhr Cloud-Fehlkonfigurationen, Schwachstellen und aktive Bedrohungen analysiert und bei sicherheitskritischen Vorfällen alarmiert.
Die Überwachung der Betriebsbereitschaft der Umgebung obliegt ausschließlich speziell dafür ausgebildetem Fachpersonal der aiio GmbH.

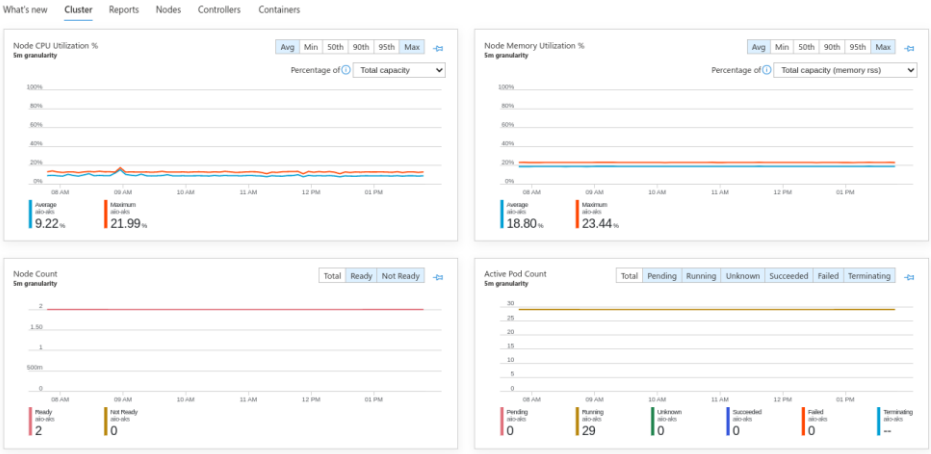

Abbildung 2 Darstellung Monitoring Übersicht

4.3 Voraussetzungen

Voraussetzung für die Nutzung von aiio® ist eine abgeschlossene Leistungsvereinbarung. Besondere technische Voraussetzungen existieren nicht.
aiio® kann über jeden handelsüblichen Büro-PC-Arbeitsplatz, der über eine Internetverbindung verfügt, genutzt werden.

4.4 Interne Schnittstellen

Die internen Standardschnittstellen zwischen den einzelnen Architekturbereichen, sind unter 4.1 „Architektur“ erklärt.

4.5 Externe Schnittstellen

Über eine API werden Daten an den vom Kunden gewählten KI-Anbieter (OpenAI, Anthropic oder Google) übermittelt. Dabei werden keine personenbezogenen Daten übermittelt. Die übermittelten Daten werden nicht zum Training oder zur Verbesserung der Modelle und Services des jeweiligen Anbieters verwendet. Mit allen KI Anbieter wurden entsprechende DPA´s vereinbart.
Zusätzlich verfügt aiio® über eine eigene API-Schnittstelle, die Kunden und Partnern einen programmatischen Zugriff auf die Plattform ermöglicht. Diese Schnittstelle kann beispielsweise zur Integration in Drittsysteme oder für benutzerdefinierte Auswertungen genutzt werden. Der Zugang zur API ist für Kunden ab dem "Excellence Modus" möglich.

4.6 Physische Sicherheit

Die durch aiio gewährleistete Sicherheit der Applikation ist in der Anlage 1 „aiio-TOM“ beschrieben. Die Anwendung selbst wird auf der Cloud-Plattform Microsoft Azure betrieben, wodurch Microsoft für die physische Sicherheit der zugrundeliegenden Rechenzentrumsinfrastruktur verantwortlich ist.

Microsoft stellt die Einhaltung modernster Sicherheits- und Compliance-Standards durch ein umfassendes System von Kontrollen und regelmäßigen Audits sicher. Die jeweils gültigen

Zertifizierungen, Audit-Berichte und Nachweise zur physischen Sicherheit werden von Microsoft zentral und aktuell im Microsoft Trust Center zur Verfügung gestellt.

4.7 Speicherorte

Grundsätzlich werden alle Kundendaten auf Servern innerhalb der Europäischen Union gespeichert. Eine Ausnahme kann die optionale Nutzung von KI-Funktionen darstellen, bei der je nach Anbieterwahl eine Datenübertragung in ein Drittland stattfinden kann.

4.8 Datenexport

Aiio stellt verschiedene Möglichkeiten für den Export von Daten zur Verfügung.

- PDF-Export für Prozesse und Prozessgrafiken
- SVG-Export für Organigramme
- CSV oder Excel-Export für Prozessliste, Anforderungen, Ressourcen, Standorte und Mitarbeiter
- API-Schnittstelle

5 Installation und Konfiguration

Um einem neuen Kunden seine aiio®-Instanz verfügbar zu machen, bedarf es keiner Neuinstallation einer Umgebung. Ein Nutzer des Kunden besucht die aiio Applikation und kann selbst ein Testsystem mithilfe einen Button Clicks initiieren. Dabei werden nötige Einträge automatisch in die Datenbank eingepflegt, wodurch der Nutzer nach kurzer Zeit ein einsatzfähiges aiio benutzen kann.

6 Anwendungsbetrieb und Sicherheit

Im Rahmen des Anwendungsbetriebs hat der aiio®-Kunde keine Aufgaben.
Der Anwendungsbetrieb erfolgt wie unter Abbildung 1 Schema aiio® Architektur beschrieben in aller Regel vollautomatisch.
Die für den Betrieb notwendigen VM sind 24/7 aktiv. Die Sicherheit der Anwendung beruht auf den Standards der Microsoft®-Azure™-Technologie.

6.1 Rollen- und Rechteverwaltung

Die für aiio® erforderlichen Rollenzuweisungen und Benutzerrechte folgen einem festgelegten Schema.

aiio® stellt hierfür mehrere vordefinierte Benutzerrollen mit spezifischen Berechtigungsstufen zur Verfügung. Die Verwaltung und Zuweisung dieser Rollen an die jeweiligen Nutzer obliegt dem Kunden und wird durch einen oder mehrere benannte aiio Executive Nutzer des Kunden in der Anwendung selbst vorgenommen.

Da sich die genauen Berechtigungen dieser Rollen mit der Weiterentwicklung der Software ändern können, wird auf eine statische Auflistung in diesem Dokument verzichtet. Die jeweils aktuelle und detaillierte Beschreibung der einzelnen Rollen ist auf der offiziellen aiio®-Webseite im Bereich der Preis- und Leistungsbeschreibung einsehbar.

6.2 Autorisierung/Authentifizierung

Für die Benutzerauthentifizierung wird komplett auf die Microsoft Authentication Library (MSAL) gesetzt. Hierbei wird der Kunde beim Besuch von aiio sofort aufgefordert, sich mit seinem Microsoft Entra ID Account anzumelden. Dieser Account gehört zum Tennant des Kunden.
Alle sicherheitsrelevanten Funktionen, wie die Durchsetzung von Passwortrichtlinien oder Multi-Faktor-Authentisierung, werden dabei von Microsoft Entra ID bereitgestellt und verwaltet. aiio erhält von den Microsoft-Servern lediglich eine Bestätigung, dass es sich um einen validen Nutzer des Kunden-Tennants handelt. Dies stellt sicher, dass Benutzer ihre gewohnte Unternehmensidentität für einen nahtlosen und sicheren Zugriff auf aiio verwenden. Alle Tennant internen Informationen (z.B. andere Nutzer, SharePoint Dateien) sind dann nur dem angemeldeten Nutzer sichtbar, sofern dieser die Rechte im Kunden-Tennant besitzt.

6.2.1 Single Sign-on „SSO“

Die Authentifizierung über Microsoft Entra ID ermöglicht ein nahtloses Single Sign-on (SSO) Erlebnis. Ist ein Benutzer bereits in seiner Arbeitsumgebung, beispielsweise im Browser oder innerhalb von Microsoft Teams, bei seinem Microsoft-Konto angemeldet, wird er bei aiio® automatisch und ohne erneute Eingabe seiner Zugangsdaten authentifiziert.

6.2.2 Multi Faktor Authentisierung

aiio® selbst implementiert keine eigene Multi-Faktor-Authentifizierung, sondern integriert sich vollständig in die Sicherheitsarchitektur des Kunden. Alle in Microsoft Entra ID vom Kunden konfigurierten Authentifizierungsrichtlinien, insbesondere die Pflicht zur Nutzung von MFA, werden bei der Anmeldung an aiio automatisch und ohne Umwege erzwungen. Der Kunde behält somit die volle Kontrolle über die Sicherheit des Anmeldeprozesses.

6.3 Datensicherung

Die Datensicherung erfolgt vollautomatisch durch täglich durchgeführte Datenbank-Backups, welche für 30 Tage aufbewahrt werden. Die Überwachung des Prozesses ist sichergestellt.

Um ein Höchstmaß an Sicherheit zu gewährleisten, werden die Backups geo-redundant gespeichert. Das bedeutet, sie werden automatisch von der primären Region (Westeuropa) in eine geografisch getrennte Partnerregion von Azure repliziert. Diese Vorgehensweise schützt die Daten vor einem unwahrscheinlichen, aber möglichen Ausfall einer gesamten Rechenzentrumsregion und stellt die Wiederherstellbarkeit im Katastrophenfall sicher.

6.4 Änderungsmanagement

Änderungen/Anpassungen am Produkt aiio® folgen im Wesentlichen dem Entwicklungsschema, wie es in Abschnitt 3.4 ausgeführt ist.
Die Anpassungen am Produkt werden in unregelmäßigen Zeitabständen ausgerollt. Diese iterativen Änderungen werden den Kunden nahtlos zur Verfügung gestellt. Für die Kunden entsteht hierbei kein Aufwand. Über relevante Änderungen werden die Kunden informiert.

Zur Behebung akuter Fehlersituationen werden nach Ermessen der aiio GmbH Hot Fixes vorgenommen.

6.5 Löschkonzept

Alle Daten können in erster Linie vom Kunden selbst bei Bedarf gelöscht werden.
Sicherungsdateien aus der automatischen Datensicherung werden nach 30 Tagen gelöscht (siehe 6.3).
Die Vorgehensweise beim Löschen ist durch eine verbindlich zu verwendende Handlungsanweisung definiert.
Nach dem Löschen erhält der Kunde ein Löschprotokoll.
Sicherungsdateien können auf Anforderung auch vor Ablauf gelöscht werden.
Bei Vertragsbeendigung werden die Daten des ausscheidenden Mandanten spätestens bei Deinstallation des Mandanten gelöscht. Auf Anordnung des Mandanten können die Daten zum Vertragsende sofort gelöscht werden.

6.6 Mandantentrennungskonzept

Das Mandantentrennungskonzept wird sichergestellt, in dem jeder Datensatz innerhalb der Datenbank einem Tennant zugewiesen ist. Bei API-Anfragen wird die Tennant Information automatisch dem angemeldeten Nutzer entnommen und eine Filterung auf allen Datensätzen angewandt. Die Tennant Information sind von den Microsoft Authentifizierungsservern ausgestellt, und können somit nicht verändert werden.

6.7 Verbindungssicherheit

Die Webserver sind nur mittels Zertifikats und verschlüsselter Verbindung (SSL) durch die Anwender und mit der festgelegten Authentifizierung erreichbar. Wurde ein Mandant abgeschaltet (Vertragsende o.ä.) werden alle Zugänge gesperrt und die Mandantschaft ist nicht mehr zugänglich.

6.8 Verschlüsselungskonzept (Kommunikation, Datenspeicherung)

Unser Verschlüsselungskonzept schützt Daten sowohl während der Übertragung (in Transit) als auch im Ruhezustand (at Rest).

Verschlüsselung im Ruhezustand (at Rest): Alle virtuellen Festplatten der VMs sowie deren Backups und Snapshots nutzen die Azure Storage Service Encryption (SSE). Dabei werden alle Daten automatisch mit einem von Microsoft verwalteten 256-Bit-AES-Schlüssel verschlüsselt, bevor sie auf die Speichermedien geschrieben werden. Dies stellt sicher, dass die ruhenden Daten auf der physischen Ebene geschützt sind.

Verschlüsselung der Kommunikation (in Transit): Jegliche Kommunikation zwischen dem Endnutzer und der aiio-Anwendung ist durch TLS 1.2 oder höher gesichert. Ebenso ist die gesamte interne Kommunikation zwischen den verschiedenen Diensten innerhalb des Azure Kubernetes Clusters und zu den Datenbanken durch TLS-Verbindungen verschlüsselt.

6.9 Protokollierung

Alle Vorgänge auf der Datenbank, dem Azure Kubernetes Cluster und den dazugehörigen VM's werden in den Azure Standard-Event logs protokolliert. Ein spezialisierter Dienst für Application Performance Monitoring (APM) wird verwendet, um anwendungsinterne Fehler und Leistungsprobleme zu überwachen und zu protokollieren
Unsere CNAPP-Plattform erfasst und analysiert sicherheitsrelevante Ereignisse über alle Cloud-Ressourcen hinweg, erkennt Anomalien im Verhalten von Workloads und identifiziert potenzielle Bedrohungen.

6.10 Notfallkonzept

Grundsätzlich ist ein Ausfall des Systems unwahrscheinlich. Der Azure Kubernetes Cluster überprüft konstant, ob das Deployment des Front- oder Backends fehlerfrei läuft. Sollte dies nicht sein, probiert es selbstheilend eine weitere Instanz der Applikation zu starten. Konstante Health-Checks durch unseren APM-Dienst und kontinuierliche Bedrohungsanalysen durch unsere CNAPP-Plattform stellen sicher, dass das Fachpersonal bei sicherheitskritischen Vorfällen, Leistungsproblemen oder Anomalien sofort alarmiert wird.

Im Falle eines schwerwiegenden Ausfalls der Datenbank wird die Wiederherstellung aus dem zuletzt verfügbaren, geo-redundanten Backup eingeleitet (siehe Abschnitt 6.3). Während dieses Wiederherstellungsprozesses ist mit einer vorübergehenden Nichtverfügbarkeit der Anwendung (Downtime) zu rechnen. Die Möglichkeit der Wiederherstellung ist durch die geo-redundante Ablage jedoch mit höchster Wahrscheinlichkeit sichergestellt.

Bei Datenverlust oder Dateninkonsistenz greift das Sicherungskonzept (siehe 6.3).

6.11 Zertifizierungen und KI Compliance

6.11.1 Zertifizierungen der Infrastruktur

Die aiio-Anwendung wird auf der Cloud-Plattform Microsoft Azure betrieben. Die Sicherheit und Compliance der zugrundeliegenden Infrastruktur wird durch Microsoft gewährleistet und durch zahlreiche, von unabhängigen Dritten geprüfte, Zertifikate und Testate belegt.

Dazu gehören grundlegende Normen wie die ISO/IEC 27001 (Informationssicherheit) und ISO/IEC 27701 (Datenschutz) sowie das für den deutschen Markt relevante C5-Testat des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Um die Aktualität dieser Nachweise sicherzustellen und auf die Beilage potenziell veralteter Dokumente zu verzichten, verweist aiio auf das Microsoft Trust Center. Dort stellt Microsoft alle gültigen Zertifikate und Audit-Berichte zentral zur Verfügung.

Die aiio GmbH selbst unterhält keine eigene formale Zertifizierung, sichert den Betrieb der Applikation jedoch durch die in diesem Dokument und den Technisch-Organisatorischen Maßnahmen (TOM, siehe Anlage 1) beschriebenen Prozesse und Kontrollen ab

6.11.2 Umgang mit KI-Anbietern und vertragliche Grundlagen

Die aiio GmbH verfolgt die Entwicklungen rund um den EU AI Act aktiv und hat eine klare Strategie, um die Konformität sicherzustellen.

Sorgfältige Anbieterauswahl:
Wir setzen ausschließlich auf marktführende KI-Anbieter (siehe 3.2), die sich ihrerseits zur Einhaltung des EU AI Acts verpflichtet haben. Wir verlassen uns auf die Zusicherungen dieser Anbieter, dass ihre Basismodelle die Anforderungen an "General Purpose AI Models" (GPAI) erfüllen.

Risikominimierung in der Anwendung:
Die in aiio implementierten KI-Funktionen dienen der Prozessanalyse und -optimierung, der Prozesszusammenfassung und dem Zusammenfassen von Prozessänderungen für die Versionierung. Nach unserem Verständnis fallen diese Anwendungsfälle nicht in eine der Hochrisikokategorien des AI Acts.

Unabhängig davon haben wir folgende Schutzmaßnahmen implementiert:

- Datenschutz:
  Es werden keine personenbezogenen Daten an die KI-Dienste übermittelt.

- Kundensouveränität:
  Die KI-Funktionen sind standardmäßig deaktiviert und müssen vom Kunden aktiv eingeschaltet werden. Der Kunde kann die Funktionen zudem jederzeit wieder deaktivieren.
  Der Kunde behält die Hoheit durch die Wahl des Anbieters und kann dessen spezifische Datenschutz- und Compliance-Zusagen bewerten. Bei Anbietern mit Hosting-Standort in der EU (z.B. Google in Frankfurt) wird die Datenresidenz zusätzlich gestärkt.

- Transparenz:
  Die Nutzung von KI-Funktionen ist für Anwender stets klar ersichtlich.

Mit den von uns verwendeten KI-Anbietern haben wir entsprechende Data Processing Agreements vereinbart. Um die Aktualität zu gewährleisten, werden diese Dokumente nicht als statischer Anhang beigefügt. Alle relevanten und stets aktuellen Verträge zur Auftragsverarbeitung mit den KI-Anbietern sind auf der aiio-Webseite einsehbar.

6.12 Prüfungsmöglichkeit des Auftraggebers

Dem Auftraggeber stehen die gemäß Art. 28 DSGVO (Auftragsverarbeitung) zugesicherten Prüfrechte in vollem Umfang zu.
Weitere, aus anderen regulatorischen Vorschriften, etwa Zertifizierungsanforderungen oder speziellen, für den Kunden geltenden Rechtsvorschriften sich ergebende Prüfrechte (z.B. WPO, SGB o.ä.) gestehen wir insofern zu, als das eine etwa geplante Prüfung mit einer ausreichenden Vorlaufzeit von 4-6 Wochen, in einer Art und Weise durchgeführt wird, dass sie den Geschäftsbetrieb der aiio GmbH nicht gefährdet.
Unangekündigte Prüfungen sind nicht statthaft.

6.13 Ausstiegskonzept

Bei Vertragsbeendigung besteht für den Kunden das uneingeschränkte Recht auf die Herausgabe oder sofortige Datenlöschung gemäß Art 28 DSGVO. Das Kündigungsrecht von Seiten des Kunden unterliegt den vertraglich vereinbarten Bestimmungen.

7 Störungsmanagement Applikation

Störungen werden vom automatischen Monitoring (s. Abb. 2) der aiio® Umgebung in der Regel schon erkannt, bevor sie Auswirkungen auf unsere Kunden haben können.
Dies verschafft aiio die Möglichkeit auf Störungen innerhalb der Umgebung unverzüglich[1] zu reagieren.

Störungen, die sich während der Nutzung durch den Kunden ergeben oder während dieser erkannt werden, sind an die unter 3.5 angegebenen Supportadressen zu melden.
Die Dauer der Behebung richtet sich nach den vertraglich festgelegten SLA.

7.1 Verfügbarkeit und Ablauf

Die Supporteinheiten der aiio GmbH sind von Montag bis Freitag zu den üblichen Geschäftszeiten verfügbar.
Über den Stand der Behebung von Störungen wird der Meldende jeweils informiert.

7.2 Vertragsbestimmungen und Auftragsverarbeitung

Es gelten die in der Leistungsvereinbarung enthaltenen Bestimmungen.
Die mit aiio vertraglich vereinbarten Leistungen, Hosting, Betrieb und Support der Umgebung und Anwendung sind als Auftragsverarbeitung im Sinne des Art. 28 DSGVO zu betrachten.

[1] Entsprechend der vertraglich vereinbarten SLA

8 Anlagen

Anlage 1 „aiio-TOM“, Katalog der technischen und organisatorischen Maßnahmen

9 Abbildungsverzeichnis