Technische Dokumentation

Version: 2.2 vom 01.06.2026

Slideroom GmbH
Gewerbepark Cité 4
76532 Baden-Baden

Tel.: 07221 40 37 633
info@slideroom.de
www.slideroom.de

Grenke Bank AG
IBAN: DE21 2013 0400 0060 3067 27
BIC: GREB DEH1 XXX

USt-IdNr. DE367213821
Amtsgericht Mannheim
HRB 750 207

Geschäftsführer:
Christian Vollmer
Maximilian Supper

Management Summary für IT-Abteilungen und Sicherheitsverantwortliche

1. Hosting, Infrastruktur & Compliance

- **Hosting** ausschließlich in Microsoft Azure / Germany West Central
  → erfüllt deutsche Datenschutzanforderungen & DSGVO.
- **Moderne Architektur:** Kotlin/Spring Boot Backend, Vue.js Frontend, PostgreSQL, Azure Blob Storage, Nginx Reverse Proxy.
- **Serverzugriffe** ausschließlich via SSH-Key-Authentifizierung
  (nur CTO + Vertretung).
- **Getrennte Entwicklungs-, Test- und Produktivumgebungen**

2. Datenschutz & Sicherheit (DSGVO Art. 25 & 32)

Vertraulichkeit

- **Vollständige Mandantenfähigkeit** (strikte logische Trennung der Kundendaten)
- **Rollenbasierte Zugriffskontrolle** (Admin/User)
- **Keine unbefugten Entwicklerzugriffe** (Need-to-Know-Prinzip)
- **Physische Sicherheit** durch Microsoft Azure (Videoüberwachung, Zutrittskontrollen)

Pseudonymisierung

- **Alle Dateien werden pseudonymisiert gespeichert**
  → keine inhaltsbezogene Suche möglich
- **Analysedaten** nur anonymisiert/pseudonymisiert (Opt-in)

Integrität

- **Dateiintegrität** durch Checksummen
- **Kommunikation** ausschließlich über HTTPS/TLS

Verfügbarkeit

- **Backups** alle 4 Stunden, Wiederherstellbarkeit jederzeit möglich
- **Soft-Delete & Versionierung** von Dateien
- **Redundante Azure-Infrastruktur**; Disaster-Recovery-Plan in Vorbereitung

KI-Verarbeitung

- **Funktionen mit künstlicher Intelligenz** basieren auf Microsoft Azure AI Foundry und Azure OpenAI (GPT-5-mini)
- **Verarbeitung erfolgt über Data Zone Standard** (EU)
- **Prompts, Eingaben und Modellantworten** werden ausschließlich innerhalb der europäischen Microsoft Azure Data Zone verarbeitet.
- **Übermittelte Inhalte** werden nicht zum Training oder zur Verbesserung der zugrundeliegenden KI-Modelle verwendet.

3. Authentifizierung & Autorisierung

- **Microsoft Single Sign-On (OAuth2)** vollständig integriert
- **Alternative Login-Option:** E-Mail + Passwort (mit starken Anforderungen)
- **Mehrfaktor-Authentifizierung (MFA)** optional
- **Tokens in Secure** / HttpOnly / SameSite = Strict Cookies
- **Tokens** sind gerätegebunden → Schutz gegen Token-Theft
- **Session-Timeouts** klar definiert (5 Minuten / 1 Tag / 1 Jahr)

4. Datenverarbeitung & Datenspeicherung

Welche Daten werden verarbeitet?

- **Benutzerdaten:** Name, E-Mail, gehashte Passwörter
- **Login- & Gerätedaten:** für Session-Handhabung
- **Dateien & Präsentationen:** mandantenisoliert, pseudonymisiert

Wo werden Daten gespeichert?

- **PostgreSQL (Azure):** strukturierte Daten (verschlüsselt)
- **Azure Blob Storage:** Dateien, nur für autorisierte Benutzer zugänglich, versioniert + Checksummen

5. Betrieb, Monitoring & Updates

- **Testsystem:** automatisiertes Deployment; Produktivsystem: manuell/kontrolliert
- **Azure Monitoring & Alerts**, Application Insights (nur bei Opt-in)
- **Automatische Sicherheitsupdates** für OS und Komponenten
- **Vollständige Protokollierung** aller administrativen Zugriffe

6. Technische Sicherheitsmaßnahmen

- **HTTPS/TLS + HSTS und MFA-Unterstützung**
- **CSRF- & XSS-Schutz** durch Frameworks + Validierung
- **SQL-Injection-Schutz** (Hibernate/JPA)
- **Rate Limiting** gegen Missbrauch
- **Geplante Integration** von Azure DDoS Protection
- **Regelmäßige Aktualisierung** aller Bibliotheken & Security Dependencies
- **Strikte Beschränkung** administrativer Schnittstellen

7. Risikoübersicht & Gegenmaßnahmen

Risiko	Schutzmaßnahmen
Unbefugter Zugriff	SSO, MFA, starke Passwörter, Token-Security
Datenmanipulation	Checksummen, HTTPS/TLS
Datenverlust	Backups alle 4 Stunden, Versionierung
DDoS	Rate Limiting + geplante Azure DDoS Protection
Web-Angriffe (XSS, SQLi)	Framework-basierte Security + Validierung
Fehlkonfiguration	Getrennte Umgebungen, Best Practices

Zusammenfassung

slideroom wurde speziell für den professionellen Unternehmenseinsatz entwickelt und erfüllt höchste Anforderungen an Datenschutz, Informationssicherheit, Compliance und die verantwortungsvolle Nutzung von Künstlicher Intelligenz. Die Plattform orientiert sich konsequent an den Vorgaben des EU AI Acts, der DSGVO sowie etablierten Best Practices für Enterprise-Software und Microsoft-basierte IT-Infrastrukturen. slideroom verfolgt dabei einen **„Security, Privacy & Compliance by Design"-Ansatz.** Datenschutz, Informationssicherheit und regulatorische Anforderungen werden bereits bei der Entwicklung neuer Funktionen berücksichtigt und kontinuierlich überprüft.

EU AI Act & verantwortungsvolle KI-Nutzung

Die in slideroom integrierten KI-Funktionen dienen ausschließlich der Unterstützung von Anwendern, beispielsweise bei Textoptimierungen, Übersetzungen, Formulierungsvorschlägen oder Designempfehlungen. Die KI trifft dabei keine automatisierten Entscheidungen mit rechtlicher oder vergleichbarer Wirkung auf Personen.

Alle KI-generierten Inhalte werden dem Nutzer transparent angezeigt und können jederzeit geprüft, angepasst oder verworfen werden. Die finale Entscheidung verbleibt stets beim Anwender. Dadurch werden zentrale Anforderungen des EU AI Acts hinsichtlich Transparenz, menschlicher Kontrolle und verantwortungsvoller KI-Nutzung erfüllt.

slideroom beobachtet die laufende Weiterentwicklung des EU AI Acts kontinuierlich und passt Prozesse sowie technische Maßnahmen bei Bedarf an neue regulatorische Anforderungen an.

Datenschutz & DSGVO

slideroom erfüllt höchste technische und organisatorische Datenschutzanforderungen für den Unternehmenseinsatz.

Zu den wesentlichen Datenschutzmaßnahmen gehören:

- DSGVO-konforme Datenverarbeitung
- Berücksichtigung von „Privacy by Design“ und „Privacy by Default“
- Pseudonymisierte Speicherung personenbezogener Daten
- Datensparsame Verarbeitung nach dem Need-to-Know-Prinzip
- Verschlüsselte Datenübertragung mittels aktueller TLS-Standards
- Verschlüsselte Datenspeicherung („Encryption at Rest“)
- Klare Mandantentrennung zwischen Kundenorganisationen
- Rollen- und Berechtigungskonzepte
- Unterstützung von Auftragsverarbeitungsverträgen (AVV)

Informationssicherheit

slideroom wurde für den sicheren Betrieb in Unternehmensumgebungen entwickelt und verfügt über eine mehrschichtige Sicherheitsarchitektur.

Dazu gehören unter anderem:

- Getrennte Entwicklungs-, Test- und Produktivumgebungen
- Mehrstufige Zugriffsschutzmechanismen
- Regelmäßige Sicherheitsupdates und Wartungsprozesse
- Backup- und Wiederherstellungsstrategien
- Protokollierung sicherheitsrelevanter Vorgänge
- Mandantenfähige Systemarchitektur
- Schutz vor unbefugten Zugriffen und Datenmanipulationen
- Kontinuierliche Überwachung kritischer Systemkomponenten

Microsoft-Integration & Enterprise Readiness

slideroom ist speziell für Microsoft-basierte Unternehmensumgebungen konzipiert und lässt sich nahtlos in bestehende IT-Landschaften integrieren.

Die Plattform bietet unter anderem:

- Single Sign-on (SSO) über Microsoft Entra ID (Azure AD)
- Automatische Benutzer- und Gruppenverwaltung über Microsoft Entra Connect Sync
- Direkte Integration in Microsoft PowerPoint
- Zentrale Benutzerverwaltung für IT-Administratoren
- Einfache Skalierung von Pilotprojekten bis zum unternehmensweiten Rollout
- Minimalen Betriebs- und Administrationsaufwand auf Kundenseite

Hosting & Datenstandort

Der Betrieb von slideroom erfolgt ausschließlich innerhalb der Microsoft Azure Cloud in Deutschland.

Wesentliche Merkmale:

- Hosting in deutschen Microsoft Azure-Rechenzentren
- Datenhaltung ausschließlich innerhalb Deutschlands
- Moderne Cloud-Infrastruktur auf Enterprise-Niveau
- Hohe Verfügbarkeit, Skalierbarkeit und Ausfallsicherheit
- Regelmäßige Sicherungen und Disaster-Recovery-Konzepte

Fazit

slideroom bietet Unternehmen eine sichere, datenschutzkonforme und zukunftssichere Plattform für die Nutzung von KI direkt in Microsoft PowerPoint. Durch die Kombination aus DSGVO-konformer Datenverarbeitung, Hosting in deutschen Azure-Rechenzentren, moderner Sicherheitsarchitektur, mandantenfähigem Betrieb, Microsoft-SSO-Integration sowie der konsequenten Berücksichtigung der Anforderungen des EU AI Acts erfüllt slideroom höchste Anforderungen an Datenschutz, Informationssicherheit und Compliance im Unternehmensumfeld.

Einleitung

Diese Dokumentation beschreibt die Architektur, Sicherheit und den Betrieb des PowerPoint Add-Ins slideroom.

Hinweis: Diese Dokumentation wird regelmäßig aktualisiert, um Änderungen an der Architektur, Sicherheitsmaßnahmen und anderen relevanten Informationen zu berücksichtigen. Eine Überprüfung und Aktualisierung erfolgt mindestens jährlich oder nach bedeutenden Änderungen an der Applikation.

Übersicht der Applikation

- **Name der Applikation:** slideroom
- **Technologie-Stack:** Vue.js mit TypeScript im Frontend, Kotlin mit Spring Boot im Backend, Deployment via Gradle. Nginx als Reverse Proxy.

Technische Dokumentation

1. Architektur

Präsentationsverarbeitung

- **Präsentationsdateien** werden zur Analyse und Verarbeitung an einen dedizierten Worker-Service übergeben
- Der Worker nutzt **Aspose.Slides for Java** zur Verarbeitung von Microsoft PowerPoint-Dateien (.pptx)
- Der Dienst wird innerhalb der von slideroom betriebenen Microsoft-Azure-Infrastruktur als Azure App Job in der Region **Germany West Central** ausgeführt
- **Sämtliche Verarbeitungsschritte** erfolgen innerhalb der eigenen Infrastruktur von slideroom. Eine Übermittlung von Präsentationsinhalten an externe Verarbeitungsdienste oder Drittanbieter findet nicht statt
- Die **Verarbeitung** umfasst unter anderem die Analyse von Präsentationen, die Extraktion relevanter Metadaten sowie weitere für die Funktionalität der Anwendung erforderliche Verarbeitungsschritte

- **Datenbank:** PostgreSQL für strukturierte Daten und Microsoft Blob Storage für Dateispeicherung.
- **Protokolle:**
  - **HTTPS** zur sicheren Kommunikation
  - **REST API** zwischen Frontend und Backend sowie Nutzung der externen REST APIs von Pexels und Pixabay (optional wählbar für Benutzer).

2. Sicherheitsmaßnahmen (gem. Art. 32 DSGVO)

2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Physische Sicherheit / Zutrittskontrolle

- **Hosting** in Azure-Rechenzentren in Deutschland. Höchster Sicherheitsstandard durch Azure.
- **Keine unbefugten Personen vor Ort:** Zutritt nur für autorisierte Personen.
- **Alarm- und Videoüberwachungssysteme** durch den Cloud-Anbieter.

Zugangskontrolle

- **Keine unbefugte Systembenutzung:** sichere Passwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung.
- **Verschlüsselung von Datenträgern** auf den Entwicklungs- und Administrationsgeräten.
- **Für unsere Infrastruktur:** SSH nur mit Schlüssel-Authentifizierung (nur CTO und Vertretung).

Zugriffskontrolle

- **Rollenbasierte Zugriffskonzepte** innerhalb der Anwendung (aktuell User/Admin) pro Organisation.
- **Entwickler-/Mitarbeiterzugriff** auf Infrastruktur nur für notwendige Wartung (Need-to-know-Prinzip).
- **Protokollierung** sämtlicher Zugriffe auf administrative Systeme.

Trennungskontrolle

- **Getrennte Verarbeitung** von Daten verschiedener Mandanten (Mandantenfähigkeit).
- **Separate Entwicklungs-, Test- und Produktivumgebungen** (Sandboxing).

2.2 Pseudonymisierung (Art. 32 Abs. 1 lit. a; Art. 25 Abs. 1 DSGVO)

- **Hochgeladene Dateien** werden pseudonymisiert gespeichert, sodass keine gezielte Suche nach Inhalten möglich ist.
- **Personenbezogene Daten** werden nur mit separaten Referenzen (IDs) verknüpft.
- Wenn möglich und sinnvoll, werden **Daten in der Datenbank pseudonymisiert**.
- **Analytics Tools** bekommen (sofern zugestimmt) nur pseudonymisierte Issue Reports.

2.3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- **Sichere Übertragung über HTTPS/TLS**
- **Für Dateien werden Checksummen erstellt** die dann beim Abruf überprüft werden um eine Manipulation zu verhindern.

2.4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

- **Schutz gegen Datenverlust und Ausfälle**: regelmäßige Backups (alle 4 Stunden) mittels Azure Backup.
- **Firewall, Virenschutz, USV** in Azure-Infrastruktur.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- **Geplante Disaster-Recovery-Strategie** (in Entwicklung).
- **Rollback-Mechanismen** durch regelmäßige Backups.
- **Versionierung** und Soft-Delete auf Dateiebene.

2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

- **Regelmäßige Kontrollen** der Datenverarbeitungsprozesse, Dokumentation und Anpassung an aktuelle DSGVO-Anforderungen.

Incident-Response-Management

- **Meldung von Sicherheitsvorfällen** an Mandanten und schnelle Reaktion gemäß definierten Prozessen.

2.6 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- **Standardmäßig minimale Datenerhebung**, Opt-in für erweiterte Analysen.

Auftragskontrolle

- **Keine Weitergabe oder Verarbeitung** ohne Weisung des Auftraggebers (Auftraggeber = Benutzer innerhalb der Organisation).
- Streng geregelte Auswahl etwaiger Subdienstleister (z. B. Cloud-Provider).

3. Datenfluss und Verarbeitung

Erhobene Daten

- **Personenbezogene Daten:** Name, E-Mail und Passwort (sicher gespeichert). Durch die notwendige Zugehörigkeit zu einer Organisation ist indirekt auch die Firmenzugehörigkeit bekannt.
- **Nutzungsdaten:** Login-Zeiten und Geräteinformationen über die Laufzeit der Session. Optional Opt-in für Seitenaufrufe und Klickverhalten (pseudonymisiert).
- **Dateien und Inhalte:** Hochgeladene Präsentationen und Medien und Metadaten.

Datenspeicherung

- **PostgreSQL:** Strukturierte Benutzerdaten und Metadaten. Passwörter und sensible Daten werden verschlüsselt gespeichert.
- **Microsoft Blob Storage:** Medieninhalte und Präsentationen, zugänglich nur für autorisierte Benutzer. Zusätzlich werden die Dateien vor der Ablage pseudonymisiert sodass nicht gezielt nach Inhalten gesucht werden kann. Gegen Manipulation der Dateien werden Checksummen berechnet und gespeichert.

Datenverarbeitung

- **Benutzerregistrierung und Authentifizierung:** Per Email/Passwort oder Microsoft SSO. Passwortverarbeitung durch Spring Security und verschlüsselte Speicherung des Hashes.
- **Dateiverwaltung:** Dateien können innerhalb der Applikation hochgeladen, gespeichert und abgerufen werden.
- **Analyse und Monitoring:** Seitenaufrufe und Klickverhalten (Opt-in), anonymisierte oder pseudonymisierte (wenn zugestimmt) Fehlerberichte und Logs zur Verbesserung der Anwendung.

3.1 KI-gestützte Funktionen und Datenverarbeitung

Eingesetzte KI-Dienste

- **Für KI-gestützte Funktionen** nutzt slideroom Microsoft Azure AI Foundry sowie den Azure OpenAI Service.
- **Als Sprachmodell** wird aktuell GPT-5-mini eingesetzt.

Hosting und Datenverarbeitung

- **Die KI-Dienste** werden innerhalb der Microsoft-Azure-Infrastruktur betrieben.
- **Die Verarbeitung** erfolgt über die Bereitstellungsoption Data Zone Standard (EU).
- **Prompts, Eingaben und Modellantworten** werden ausschließlich innerhalb der europäischen Microsoft Azure Data Zone verarbeitet.
- **Eine Verarbeitung im Rahmen der KI-Inferenz außerhalb der EU Data Boundary findet nicht statt.**

Datenschutz und Verwendung der Eingaben

- **Inhalte, die im Rahmen der KI-Funktionen verarbeitet werden** (z. B. Texte, Präsentationsinhalte oder Benutzereingaben), werden ausschließlich zur Bearbeitung der jeweiligen Anfrage verwendet.
- **Übermittelte Inhalte** werden nicht zum Training, zur Verbesserung oder zur Weiterentwicklung der zugrunde liegenden KI-Modelle verwendet.
- **Es erfolgt keine Verwendung von Kundendaten** für Lern- oder Trainingszwecke durch slideroom.
- **KI-Funktionen werden ausschließlich über Dienste von Microsoft Azure OpenAI umgesetzt.** Es erfolgt keine direkte Nutzung öffentlich zugänglicher KI-Dienste oder Consumer-Angebote.

Technische und organisatorische Maßnahmen

- **Zugriff auf KI-Funktionen** erfolgt ausschließlich für authentifizierte Benutzer innerhalb der jeweiligen Organisation.
- **Berechtigungsprüfung** erfolgt entsprechend der rollenbasierten Zugriffskontrolle der Anwendung.
- **Übertragung aller Daten** erfolgt verschlüsselt über HTTPS/TLS.
- **Verarbeitung von KI-Anfragen** erfolgt innerhalb der Sicherheits- und Compliance-Rahmenbedingungen des Microsoft Azure OpenAI Service.

4. Authentifizierung und Autorisierung

Authentifizierung

- **E-Mail und Passwort:** Passwortanforderungen (mind. 8 Zeichen, mit Sonderzeichen, Zahl und Großbuchstaben).
- **Microsoft SSO:** Über OAuth2. Nach Anmeldung erfolgt Token- und Sessionverarbeitung wie bei E-Mail-Authentifizierung. Die Sessioninfos von Microsoft werden nur zum Abruf von Benutzerdaten verwendet (bei der Registrierung) und zur Authentifizierung des Users und dann verworfen.
- **Mehrfaktor-Authentifizierung (MFA):** Kann optional aktiviert werden: entweder per E-Mail-Verifizierung oder TOTP (Authenticator-App). Organisationsrichtlinien, damit Administratoren MFA innerhalb einer Organisation erzwingen können, sind geplant.

Sicherheitsmechanismen

- **Token-Sicherheit:** Tokens zur Sessionzuordnung werden in HTTP-Only Cookies gespeichert (Secure, HttpOnly und SameSite=Strict).

- **Gerätebindung der Tokens:** Interne Mechanismen binden Tokens an das jeweilige Gerät.
- **Session-Management:** Session-Timeouts für „Angemeldet bleiben“ (1 Jahr) oder ohne (1 Tag). Auth-Cookies 5 Minuten, für den Refresh-Token („Angemeldet bleiben“) 1 Jahr, sonst "Session".

Autorisierung

- **Rollenbasierte Zugriffskontrolle:** Admin und User-Rollen; zukünftige Erweiterung geplant. Rollen und Berechtigungen sollen vom Administrator verwaltet werden können.
- **Berechtigungsprüfung:** Zugriffskontrolle bei jeder Anfrage; Prinzip des geringsten Privilegs.

5. Infrastruktur

Hosting-Umgebung

- **Cloud-Plattform:** Microsoft Azure in der Region Germany West Central für deutsche Datenschutzbestimmungen.

Netzwerkarchitektur

- **Virtuelles Netzwerk (VNet):** Eine VM, keine Segmentierung, NSG für Traffic-Kontrolle.
- **Load Balancer:** Aktuell nicht vorhanden, geplant für zukünftige Skalierung.

Sicherheitsmaßnahmen für VMs

- **Betriebssystem:** Ubuntu.

- **Zugriffskontrolle:** SSH-Zugriff mit Schlüssel-Authentifizierung, nur für Administratoren (CTO und Vertretung).

Verfügbarkeit und Skalierbarkeit

- **Skalierung:** Aktuell vertikal, horizontale Skalierung und Load Balancer bei wachsender Last geplant.

CI/CD-Prozesse

- **Build-Prozess:** Jenkins für Builds und Integration; nur Netzwerkzugriff intern.
- **Deployment:** Manuelles Deployment auf Produktivsystem, Testsystem wird automatisch deployed.

Backup und Disaster Recovery

- **Backups:** Alle 4 Stunden durch Azure-Backup-Mechanismen.
- **Wiederherstellung:** Rollback bei Problemen durch regelmäßige Backups möglich.
- **Disaster Recovery Plan:** Geplant für zukünftige Implementierung.

6. Betrieb und Wartung

Updates und Deployment

- **Update-Prozesse:** Nach Bedarf; ausführliche Tests auf einem Testsystem vor Deployment. Unit- und UI-Tests werden beim Build ausgeführt.

Überwachung und Monitoring

- **Monitoring-Tools:** Azure Alerts, Bugtracking (Azure Application Insights) (Opt-In für Benutzer möglich).
- **Alarmierung:** Administrator wird bei kritischen Zuständen umgehend informiert.

Zugriffskontrolle und Berechtigungsmanagement

- **Administrative Zugriffe:** Streng kontrolliert, nur CTO und Vertretung.
- **Protokollierung:** Alle Zugriffe werden zur Nachvollziehbarkeit protokolliert.

Wartung und Sicherheitsupdates

- **Patch-Management:** Automatische Updates für Betriebssystem und Anwendungsspezifisches.
- **Sicherheitsmeldungen:** Administrator verfolgt Sicherheitsupdates regelmäßig (mindestens monatlich). Zusätzlich wird auf Sicherheitshinweise seitens Azure umgehend reagiert.

7. Risiken und Maßnahmen

- **Unautorisierter Zugriff auf Benutzerdaten:** MFA, HTTPS-Verschlüsselung, Passwort-Hashes mit Salt, Begrenzung von Login-Versuchen.
- **Cross-Site Scripting (XSS):** XSS-Schutz durch serverseitige Validierung der Eingaben. Browserseitig werden Escapemechanismen von vue.js verwendet.
- **Schwache Passwortsicherheit:** Passwortanforderungen und -feedback, optional MFA.
- **Man-in-the-Middle (MitM) Angriffe:** HTTPS mit TLS, HSTS für HTTPS-Erzwingung, regelmäßige Erneuerung der Zertifikate.
- **SQL-Injection:** Verwendung von JPA/Hibernate mit parametrisierten Queries, Serverseitige Validierung.

- **Distributed Denial of Service (DDoS):** Rate Limiting, geplante Nutzung von Azure DDoS Protection Services (Firewall).
- **Sicherheitslücken in Drittanbieter-Bibliotheken:** Regelmäßige Aktualisierung und Sicherheitsaudits für externe Abhängigkeiten.
- **Datenverlust:** Regelmäßige Backups und geplante Implementierung eines Disaster Recovery Plans.
- **Fehlkonfiguration der Server:** Anwendung von Best Practices, geplante Verwendung von IaC-Tools.
- **Unautorisierter Zugriff auf Administrationsschnittstellen:** Beschränkter Zugriff auf Admin-Funktionen und Implementierung von MFA für Administratoren.