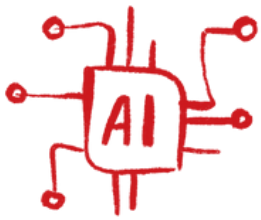
KI im geschützten Raum: Sichere OpenAI-Implementierung für ein multinationales Unternehmen im Bereich Bürotechnologie

Künstliche Intelligenz (KI) ist kein Hype-Thema mehr, sondern gehört zur Grundausstattung zukunftsfähiger Unternehmen. Das sieht auch unser Kunde so, ein führender Hersteller im Bereich Bürotechnologie, und will künftig auf das Potenzial von ChatGPT setzen. Bei der Implementierung gab es klare Prioritäten: **Sicherheit** und **Compliance** standen von Anfang an im Fokus.



Für dieses Projekt holte das Unternehmen Cloutomate an Bord. Unsere Aufgabe bestand darin, eine **interne Demo-Anwendung** auf Basis des **Azure OpenAI Services** bereitzustellen, die nicht nur höchsten Sicherheitsstandards genügt, sondern auch flexibel genug ist, um in Zukunft **Unternehmensdaten und Anwendungen** zu integrieren.

Herausforderungen auf dem Weg zur sicheren OpenAI-Integration

Jedes Projekt bringt seine eigenen Herausforderungen mit sich – bei unserem Kunden drehte sich neben Sicherheit und Compliance alles um eine **nahtlose technische Integration**. Unser Ziel: eine Lösung, die in diesen Bereichen keine Kompromisse zulässt.

1. Sicherheit

OpenAI sollte in der Cloud bereitgestellt werden – in einer geschützten Umgebung, die höchsten Sicherheitsanforderungen entspricht. Anders als in der Standard-konfiguration bei Azure wurde deshalb sichergestellt, dass der Service nicht öffentlich zugänglich ist, sondern nur in einer abgeschotteten Umgebung betrieben wird.

2. Technische Komplexität der Integration

Die Implementierung des Azure OpenAI Services in Kombination mit einer Webanwendung in einer Private Cloud erforderte technisches Feingefühl und präzise Planung. Die Netzwerkarchitektur wurde speziell angepasst, um die Zugriffspunkte gezielt zu kontrollieren und alle internen Sicherheitsrichtlinien einzuhalten.

3. Interne Authentifizierung und Zugriffskontrolle

Ein weiteres Anliegen war die Implementierung eines zentralen Authentifizierungs-systems. Nur ausgewählte Benutzergruppen sollten Zugang zum OpenAI Dienst erhalten. Um unautorisierten Zugriff zuverlässig zu verhindern waren spezielle Maßnahmen und Konfigurationen sowie manuelle Anpassungen erforderlich.

Um das Projekt gezielt auf die Anforderungen des Technologieunternehmens abzustimmen und sicherzustellen, dass alle Vorgaben von Anfang an berücksichtigt werden, starteten wir mit intensiven Workshops. Dabei haben wir sowohl technische und betriebliche Anforderungen als auch rechtliche Rahmenbedingungen aufgenommen.

Maßgeschneiderte Sicherheitsarchitektur: Isolierte Bereitstellung und Schutzmaßnahmen

Basierend auf den Anforderungen haben wir eine **maßgeschneiderte Architektur** entwickelt, die den sicheren Betrieb des Azure OpenAI Service in einer **abgeschotteten Umgebung** ermöglicht. Wir haben den Azure **OpenAI Service über Private Endpoints** abgesichert, sodass der Dienst ausschließlich über das **interne Netzwerk** erreichbar ist und öffentliche Zugriffe vollständig ausgeschlossen sind. Ein **Azure Virtual Network (VNet)** isolierte den Datenfluss innerhalb der Cloud-Infrastruktur und verhindert konsequent jede Verbindung über das öffentliche Internet. Ein **Reverse Proxy**, der auf einem Kubernetes-Cluster eingerichtet ist, steuert zusätzlich den Zugang zu den **OpenAI-Services**. Er verschlüsselt alle Anfragen und prüft sie auf potenziell unerlaubte Zugriffe, wodurch eine sichere und effiziente Weiterleitung der Daten zwischen externen Anfragen und dem OpenAI-Dienst gewährleistet wird.

Sichere Bereitstellung – aber bitte einfach für die Nutzer

Trotz der technischen Komplexität war unser Ziel klar: Die Lösung sollte für die Nutzer **einfach und unkompliziert** sein. Der OpenAI-Dienst wurde deshalb als **benutzerfreundliche Web-App** im Azure App Service bereitgestellt, vollständig über private Netzwerke abgesichert und durch eine benutzerdefinierte Domäne geschützt. So können die internen Teams sicher auf die ChatGPT-Demo zugreifen und erste Erfahrungen sammeln.

Verwaltet wird der Zugriff auf den Dienst zentral mit **Microsoft Entra ID (Azure AD)**. **Role-Based Access Control (RBAC)** ermöglicht es, die Benutzerrechte granular zu definieren, sodass nur autorisierte Benutzergruppen und ausgewählte Mitarbeitende auf die Anwendung zugreifen können. Die Authentifizierungsrichtlinien von **Microsoft 365** haben wir nahtlos integriert, um den Login-Prozess zu vereinheitlichen und die Sicherheit zusätzlich zu erhöhen. Spezielle Firewall-Regeln beschränken den Zugang zudem auf autorisierte interne IP-Adressen, und Netzwerk-Sicherheitsgruppen wurden eingerichtet, um den Datenfluss zwischen den Ressourcen innerhalb des VNets gezielt zu kontrollieren.

Verschlüsselte Kommunikation & automatisches Zertifikatsmanagement

Für die **verschlüsselte Kommunikation** sorgt ein automatisches Zertifikats-management mithilfe des **Cert-Managers und Let‘s Encrypt**. Das Zertifikat wird automatisch durch das Kubernetes-Cluster bereitgestellt und verwaltet, sodass alle Verbindungen zur Web-App sicher über HTTPS laufen. Dadurch wird die Datenübertragung kontinuierlich verschlüsselt, ohne dass manueller Aufwand für die Nutzer entsteht.

Intelligente Content Filtering für sichere Inhalte

Intelligente Content-Filter stellen zudem sicher, dass die generierten Inhalte stets den Qualitäts- und Sicherheitsstandards des Kunden entsprechen. Sie erkennen und entfernen automatisch unangemessene Inhalte wie beleidigende Sprache, Gewalt oder Fehlinformationen.

Flexibel, sicher und bereit für die Zukunft

Der Bürotechnologie-Hersteller kann den **Azure OpenAI Service** nun sicher und effizient nutzen, um intern Erfahrungen mit KI zu sammeln – und das alles in einer **Compliance-konformen** Umgebung. Die Lösung ist nicht nur für den aktuellen Einsatz optimiert, sondern bietet auch **flexiblen Raum für zukünftige Erweiterungen**, wie die **Anbindung von SAP-Daten**, und ist darauf ausgelegt, mit den **wachsenden Anforderungen** des Unternehmens Schritt zu halten.