

Höchste Sicherheit für unbesorgtes und entspanntes Arbeiten



speechi
connect

Willkommen bei Speechi Connect, unserer SaaS-Plattform, bei der Sicherheit und Zuverlässigkeit im Mittelpunkt unserer Lösungen stehen.

Entdecken Sie die technischen und sicherheitsrelevanten Elemente, die unsere Lösung zu einer sicheren und leistungsstarken Wahl für alle Anwendungsfälle machen.



AUTHENTIFIKATION

Die Plattform nutzt IAM für eine sichere und einfache Authentifizierung, mit biometrischer Erkennung und Multi-Faktor-Authentifizierung, die internationalen Standards entspricht und Sicherheitsrisiken reduziert



SPEICHERUNG

Der Dienst bietet eine temporäre und sichere Speicherung, gewährleistet verschlüsselte Übertragungen ohne Datenpersistenz, entspricht internationalen Sicherheitsstandards, nutzt Server in Europa und löscht Daten automatisch am Ende jeder Sitzung.

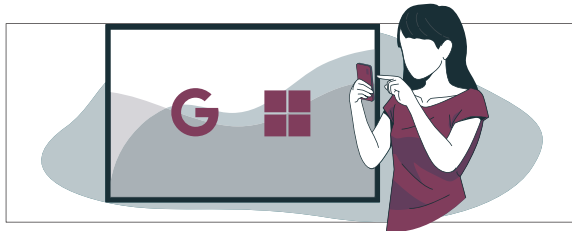


INFRASTRUKTUR

Das System wird durch eine moderne Firewall auf Anwendungsebene, eine rigorose Segmentierung der Infrastruktur, regelmäßige Sicherheitsprüfungen und eine kontinuierliche Überwachung geschützt, die einen optimalen Schutz vor Bedrohungen und die Einhaltung internationaler Sicherheitsstandards gewährleisten.

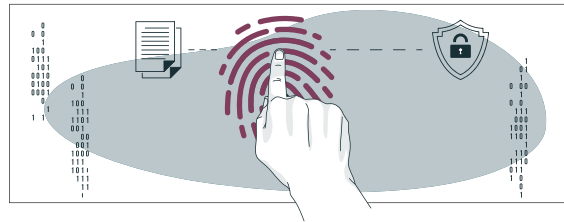
AUTHENTIFIZIERUNG

Unsere Speechi Connect-Plattform nutzt IAM (Identity and Access Management) für die Benutzerauthentifizierung und gewährleistet so ein hohes Maß an Sicherheit und Zuverlässigkeit. Speechi hat keine Kenntnis von Ihren Benutzerdaten und Passwörtern. Der Cloud-IAM-Dienst bietet mehrere Vorteile.



Einfache Anmeldung

Kompatibel mit den wichtigsten Identitätsanbietern wie **Google** und **Microsoft**.



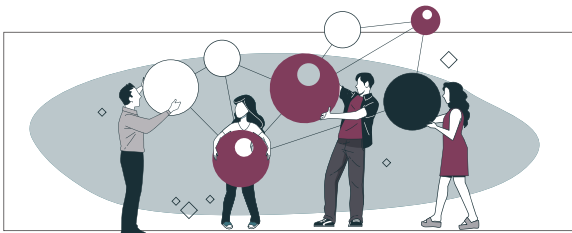
Biometrische Erkennung

Integration von **biometrischer Erkennung** für mehr Sicherheit und ein besseres Nutzererlebnis.



Multi-Faktor-Authentifizierung (MFA)

Optional eine **Zwei-Faktor-Authentifizierung** für einen besseren Schutz.



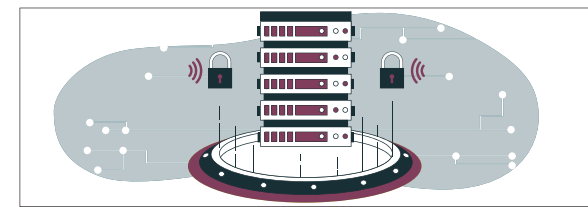
Skalierbarkeit

Unterstützt Millionen von Nutzern ohne Auswirkungen auf die Leistung.



Compliance und Sicherheit

Zertifiziert nach internationalen Sicherheitsstandards, einschließlich **DSGVO** und **HIPAA**.



Risikominderung

Durch die Nutzung eines spezialisierten und weltweit anerkannten Anbieters, werden die Sicherheitsrisiken, die mit der Verwaltung interner Zugangsdaten verbunden sind, kontrolliert und begrenzt.

SPEICHERUNG

Sichere temporäre Speicherung

Speechi Connect bietet eine temporäre Speicherung, um den sicheren Austausch zwischen Ihren Geräten und den interaktiven Displays zu erleichtern. Dieses System hat zahlreiche Vorteile.



Sicherer Austausch

Die Daten werden sicher übertragen, ohne Spuren auf den Servern zu hinterlassen.



Keine Datenpersistenz

Nach Verwendung werden keine Daten gespeichert, wodurch das Risiko von Datenlecks oder unberechtigtem Zugriff minimiert.



Standardmäßige SSE-Verschlüsselung

Die Daten werden mit dem AES-256-Algorithmus verschlüsselt, wodurch ein robuster Schutz der Daten im Ruhezustand gewährleistet wird. Die Speicherung auf AWS S3 profitiert außerdem von der SSE-S3-Verschlüsselung (Server-Side Encryption mit verwalteten Schlüsseln), die auf demselben AES-256-Standard mit vom Speicherserver verwalteten Verschlüsselungsschlüsseln basiert..



Datenverschlüsselung während der Übertragung

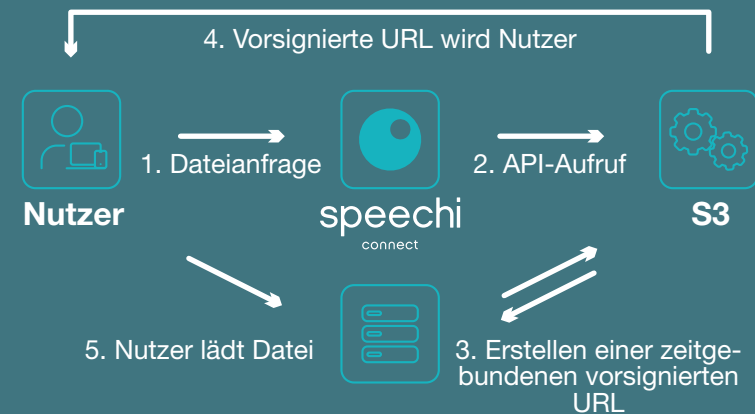
Um die Daten während der Übertragung zu sichern, werden diese beim Austausch mithilfe von Transport Layer Security (TLS 1.3) verschlüsselt.



Zertifizierung und Compliance

Unsere Speicherserver verfügen über zahlreiche Sicherheits- und Compliance-Zertifizierungen, darunter PCI-DSS, HIPAA/HITECH, FedRAMP, SEC Rule 17-a-4, FISMA, und erfüllen die EU-Datenschutzrichtlinie.

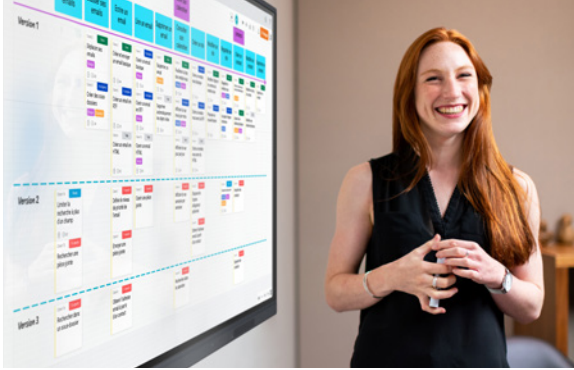
Kein direkter Zugang zu persönlichen und Unternehmensdaten



Unsere Plattform ist dafür konzipiert, Ihre Privatsphäre und vertrauliche Daten zu schützen. So stellen wir sicher, dass es keinen direkten Zugriff auf die persönlichen Daten oder Unternehmensdaten der Nutzer gibt. Diese strikte Trennung schützt Ihre Informationen vor Angriffsversuchen.

Keine Datei geht durch unser Backoffice, weder bei der Übertragung von Daten von Ihren Geräten auf das interaktive Display noch beim Abrufen Ihrer Arbeit vom interaktiven Display auf Ihre Geräte.

Wir verwenden ein System mit vorsegnierten URLs und die Datenübertragung ist mit TLS 1.3 verschlüsselt.



Normgerechte Speicherung in Europa

Wir verpflichten uns zur Einhaltung der strengen europäischen Datenschutzbestimmungen. Unsere SaaS-Server befinden sich in Europa, und zwar in Deutschland, Frankreich, der Schweiz, und Irland, und garantieren:

- **Vollständige Einhaltung der DSGVO** und der Datenschutzrichtlinien der Europäischen Union.
- Hohe Leistung und Verfügbarkeit durch eine robuste und skalierbare Infrastruktur.

Ein **Content Delivery Network (CDN)** ist nativ in unsere Plattform integriert, sodass eine Nutzeranfrage vom CDN-Netz an den vom Nutzer nächstgelegenen Server weitergeleitet wird und so die Latenzzeit minimiert wird.



Datenverschlüsselung

Die Sicherheit der auf unserer Plattform gespeicherten Daten wird durch fortschrittliche Verschlüsselungsmechanismen gewährleistet:

- **SSE-KMS-Verschlüsselung** (Server Side Encryption mit Key Management Service): Alle gespeicherten Daten werden verschlüsselt und sind über einen eindeutigen Chiffrierschlüssel lesbar. Ohne diesen Chiffrierschlüssel sind die Daten nicht lesbar.
- Schlüsselverwaltung: Die **Schlüssel** werden durch die Verwendung eines unabhängigen Schlüsselverwaltungssystems gesichert.
- Sichere Übertragung: Die Daten werden über **sichere Protokolle (TLS/SSL)** übertragen, um ein Abfangen zu verhindern



Löschung der Daten am Ende der Sitzung

Wir gewährleisten die Vertraulichkeit und Sicherheit Ihrer Aktivitäten, indem wir alle Spuren Ihrer Sitzung löschen, wenn Sie das interaktive Display verlassen:

- **Löschung von Notizen:** Alle Notizen, die auf dem interaktiven Display erstellt wurden, werden am Ende der Arbeitssitzung automatisch gelöscht.
- **Browserverlauf:** Der Verlauf der besuchten Websites sowie Anmeldedaten und Passwörter, die Sie eventuell während der Sitzung eingegeben haben, werden automatisch gelöscht.
- **Heruntergeladene Dateien:** Auch heruntergeladene Dateien werden am Ende der Sitzung gelöscht, um eine ungewollte Speicherung zu vermeiden.

INFRASTRUKTUR

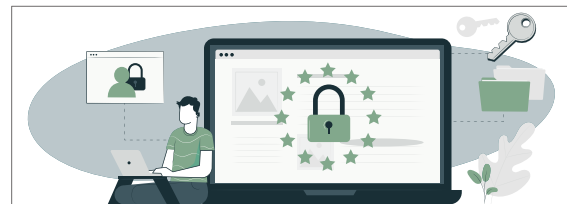
Anwendungsfirewall

Unsere Speechi Connect-Plattform ist durch eine **fortschrittliche Anwendungsfirewall** geschützt, die eine zusätzliche Sicherheitsebene gewährleistet. Diese Firewall auf Anwendungsebene bietet zahlreiche Vorteile.



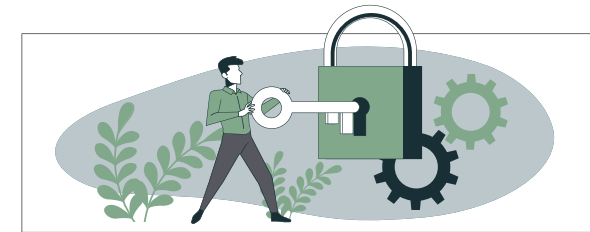
Schutz vor Angriffen

Angriffsversuche werden blockiert, auch SQL-Injection-Angriffe, Cross-Site-Scripting (XSS) und andere gängigen Bedrohungen.



Kontinuierliche Überwachung

Die Echtzeitanalyse des Netzwerkverkehrs erkennt und verhindert verdächtiges Verhalten, begrenzt Anfragen pro IP innerhalb eines definierten Zeitraums und sperrt bekannte böstartige IPs.

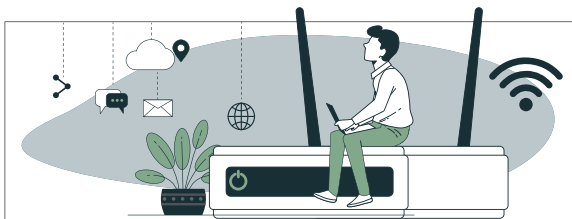


OWASP

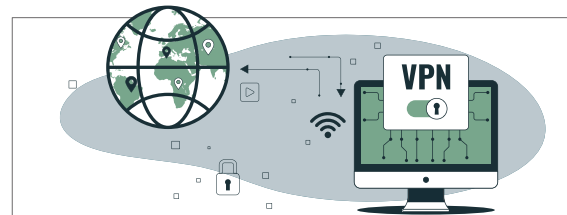
Entspricht den vom Open Web Application Security Project (OWASP) empfohlenen Regeln und hält somit internationale Sicherheitsstandards ein, um zum Schutz sensibler Daten beizutragen.

Segmentierung der Infrastruktur

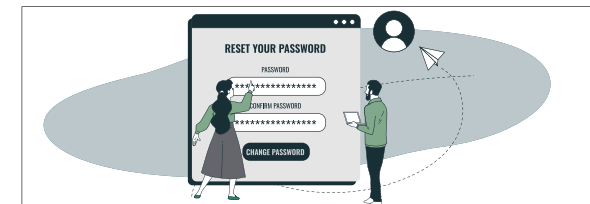
Zur Gewährleistung einer optimalen Sicherheit unserer Infrastruktur wenden wir eine strenge Segmentierung an.



Die Verwendung von **VLANs** (Virtual Local Area Networks) isoliert verschiedene Teile des Netzwerks und Umgebungen und verringert so das Risiko der Verbreitung von Bedrohungen.



VPNs (Virtual Private Networks) sorgen für sichere und private Verbindungen. Sicherheitsgruppen öffnen nach dem Least-Privilege-Prinzip nur die benötigten Datenströme.



Der Zugriff auf die Infrastruktur wird durch **IAM-Systeme** kontrolliert, die sicherstellen, dass nur autorisierte Nutzer und Abteilungen auf die benötigten Ressourcen zugreifen, wodurch der Schutz von Infrastruktur und Daten gestärkt wird.



Überwachung und Warnungen

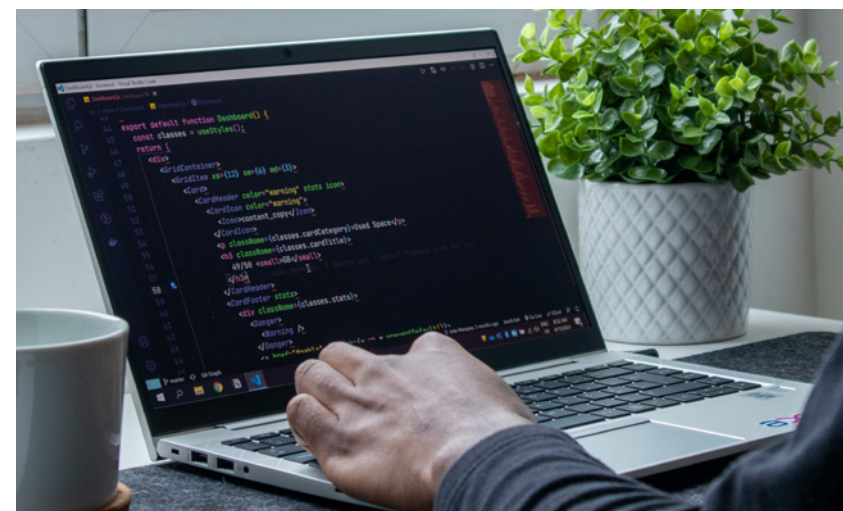
Die Überwachung und Warnmeldungen der Plattform werden rund um die Uhr von einem Cloud Observability-Dienst bereitgestellt, der sowohl Server als auch Daten abdeckt.

Diese Lösung ermöglicht es uns, Anomalien und Störungen schnell zu erkennen und darauf zu reagieren, wodurch eine optimale Verfügbarkeit und Leistung garantiert wird.

Prüfung der Anwendungssicherheit

Unsere Codebasis sowie unsere Bibliotheken werden regelmäßig von einem automatisierten Drittanbieterdienst geprüft. Diese Automatisierung ermöglicht die Erkennung bekannter Bugs und Schwachstellen und sorgt so für optimale Sicherheit.

Neben der automatisierten Prüfung führen wir auch regelmäßige manuelle Überprüfungen des Codes und Penetrationstests durch, um potenzielle Schwachstellen zu identifizieren, bevor sie zu einem Problem werden. Mit diesen Maßnahmen sorgen wir für einen kontinuierlichen und proaktiven Schutz unserer Anwendung.



Unsere SaaS-Plattform Speechi Connect wurde entwickelt, um eine sichere Arbeitsumgebung zu bieten, die höchsten Standards entspricht.

Durch die Kombination aus modernster Technologie und strengen Sicherheitsmechanismen sorgen wir dafür, dass Ihre Daten geschützt sind und Sie sich unbesorgt auf Ihr Geschäft konzentrieren können. Wenden Sie sich für weitere Informationen gerne an uns.

