voicepoint | CLOUD

Voicepoint Cloud

Security Factsheet

Intelligentes, cloudbasiertes Diktieren

Die Voicepoint Cloud bietet eine sichere, cloudbasierte Diktatmanagement- und Spracherkennungslösung, die es Ärztinnen und Ärzten sowie Anwältinnen und Anwälten ermöglicht, die Patientengeschichte respektive rechtliche Fälle per Sprache zu dokumentieren. Hoher Aufwand für die Implementierung und den Betrieb einer eigenen Infrastruktur entfällt und die Applikationen sind direkt einsatzbereit - das spart Zeit für das IT-Personal und steigert die Produktivität und Effizienz der Ärzteschaft sowie die der Anwaltschaft. Weitere Informationen sowie die Vor- und Nachteile der Voicepoint Cloud finden Sie in unserem Voicepoint Cloud Factsheet oder auf unserer Website.

Sicherer Premium-Cloud-Anbieter

Voicepoint betreibt ihre Lösungen im Schweizer Datacenter von Microsoft Azure und wurde bei der Konzeption, der Architektur und der Implementierung eng von Microsoft Spezialisten begleitet.

Die von der Voicepoint Cloud benötigten Microsoft Azure Dienste des Datacenters in Zürich sind hochverfügbar und bieten konstante Betriebszeiten mit einer sehr hohen Verfügbarkeit.

Microsoft Azure erfüllt eine breite Palette von internationalen und branchenspezifischen Compliance-Standards. Eine detaillierte Übersicht sowie weitere Informationen der Microsoft Azure-Compliance finden Sie hier.

ISO 27001 Zertifizierung

Die wichtigsten branchenüblichen Standards werden durch unsere ISO 27001 Zertifizierung erfüllt, laufend erneuert und bieten ein höheres Schutzniveau für Informationssicherheit.

Sicheres und robustes Cloud-Angebot

Unsere Sicherheitspraktiken in Kombination mit unserer hochverfügbaren und redundanten Infrastruktur sorgen dafür, dass den Nutzern unsere performanten, sicheren Lösungen mit maximalem Komfort und standortunabhängig zur Verfügung stehen.

Sicherheit des Datacenters

Zusätzlich zur Kernsicherheit des Microsoft Azure Datacenters wendet Voicepoint viele branchenübliche Best Practices an, um die Kundendaten weiter zu schützen und die Sicherheit der angebotenen Lösungen insgesamt zu erhöhen.

Physischer Zugang: Der physische Zugang zum Datacenter wird mit zahlreichen fortschrittlichen Sicherheitstechniken gesichert. Zu den Datacentern von Microsoft Azure haben die Mitarbeiter von Voicepoint keinen physischen Zugang, was die Sicherheit zusätzlich erhöht.

Elektronischer Zugang: Voicepoint hält sich bei der Gewährung von elektronischem Zugang zum Datacenter zu Supportzwecken an die Vorgabe des «Minimum Need».

Multi-Faktor-Authentifizierung/Jumphost: Für den Zugriff auf das Microsoft Azure Management Portal ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich, die nur ausgewählten Mitarbeitenden zur Verfügung steht. Die jeweiligen Applikationsserver sind strengstens geschützt, wodurch der indirekte Zugriff auf die Systeme durch Jumphosts über ein spezielles VPN ermöglicht wird.

Patches und Updates: Die für die Voicepoint Cloud-Infrastruktur berechtigten Mitarbeiter von Voicepoint führen monatliche Windows-Updates der Umgebung durch. Aktualisierungen an den eingesetzten Applikationen oder an der Infrastruktur werden unabhängig der monatlichen Updates durchgeführt und vorgängig geplant. Die Anwender werden dementsprechend frühzeitig über Wartungsfenster informiert. Voicepoint behält sich vor, dringende Windows-Updates sowie dringende Applikationsupdates ausserhalb der geplanten monatlichen Wartungsfenster durchzuführen, um die Sicherheit zusätzlich zu erhöhen.

Verschlüsselung der Datenübertragung

Die Kommunikation zwischen den eingesetzten Client-Applikationen und den Voicepoint Cloud-Diensten wird zu jeder Zeit verschlüsselt. Dies gilt für den Stream der Audiodaten während der Spracherkennung sowie für die Übertragung jeglicher Daten innerhalb der Applikationen. Die Daten werden dabei über HTTPS unter Verwendung von TLS 1.3 mit einem AES 128/256-Bit-Chiffrieralgorithmus übertragen. Ältere und als unsicher definierte Algorithmen oder TLS-Versionen wurden deaktiviert.

Sicherheitsstandards und Übertragungsprotokolle werden als Reaktion auf neue Sicherheitsbedrohungen ständig weiterentwickelt. Aus diesem Grund überprüfen wir regelmässig unsere Dienste, damit sie den höchsten Standards für eine sichere Datenübertragung entsprechen. Die webbasierten Applikationen der Voicepoint Cloud erhalten routinemässig ein «A+»-Rating von Qualys SSL Labs, das eine eingehende Analyse der TLS-Endpunkte durchführt. Der Test prüft unter anderem die Stärke der Zertifikate, unterstützte TLS-Protokollversionen, unterstützte Chiffren und Schwachstellen in der Konfiguration.

Datenspeicherung und Weiterverwendung

Die Applikationsdaten werden in sogenannten «Storage Accounts» gespeichert, die nicht über das Internet zur Verfügung stehen und verschlüsselt sowie vor unberechtigten Zugriffen geschützt sind.

Diktate des Diktatmanagementsystems «Winscribe» werden verschlüsselt abgelegt und von den Anwendern der Client-Applikationen zur Diktatabschrift benötigt. In Winscribe werden Diktate solange aufbewahrt, bis diese transkribiert wurden. Danach werden die Diktate in einem anpassbaren Zeitraum gelöscht.

Standardmäßig werden Daten der Spracherkennungslösung «Dragon Medical One» bis zu einer Gesamtdauer von 50 Diktatstunden pro Benutzer aufbewahrt. Sobald dieses Limit erreicht ist, erfolgt automatisch die Löschung der ältesten Aufzeichnungen. Die erkannten Audio- und Textdaten der Spracherkennungslösung werden für den Adaptionsprozess zum Abgleich genutzt. Dies schliesst Korrekturen im Text mit ein, die vom Benutzer durchgeführt werden. Das System verwendet nur die Daten, die in der Audiodatei und im Text vorhanden sind, um akustische und sprachliche Anpassungen im Sprachprofil des Anwenders vorzunehmen.

Diese tragen zur Verbesserung der Spracherkennungsqualität bei. Wenn beispielsweise ein medizinischer Anwender diktiert: ‹Der Patient hat Herzrhythmusstörungen›, gibt es keine gespeicherten Audioinformationen, die diese Information mit einem individuellen Patienten in Verbindung bringen könnten. Die Übertragung der Daten über das Internet erfolgt verschlüsselt.

Hohe Verfügbarkeit und Service-Kontinuität

Die verwendeten Microsoft Azure-Dienste werden in unterschiedlichen Verfügbarkeitszonen («Availability Zones») bereitgestellt. Einige ältere Dienste nutzen noch die «Availability Sets». Dies ermöglicht das Erreichen einer hohen Verfügbarkeit, da ein Dienst in mehrere Verfügbarkeitszonen verteilt ist und sich dadurch in verschiedenen physischen Standorten und Einrichtungen befinden kann. Jede dieser Zonen ist mit einer eigenen Strom- und Netzwerkquelle ausgestattet, was die Auswirkungen von potenziellen Hardwarefehlern oder Standortstörungen verringert. Updates von Microsoft Azure werden jeweils nur in einer Verfügbarkeitszone eingespielt und beeinflussen somit nicht die Verfügbarkeit der Dienste in anderen Zonen.

Die Systemarchitektur der Voicepoint Cloud in Microsoft Azure bietet über die Verfügbarkeitszonen hinweg die folgenden Hochverfügbarkeitsmerkmale:

- Vollständig redundante Netzwerkinfrastruktur, einschliesslich Loadbalancer und Switches
- Mehrere redundante Applikationsserver
- Hochverfügbare und sichere Datenablage
- Redundante SQL-Datenbankserver-Cluster

Voicepoint ist bestrebt, die Service-Kontinuität hochzuhalten und die Hochverfügbarkeit regelmässig zu überprüfen und bei Bedarf zu erweitern und zu verbessern.

Umgang mit dem US CLOUD Act

Der CLOUD Act ist ein amerikanisches Gesetz, das US-Behörden den Zugriff auf gespeicherte Daten von amerikanischen Unternehmen gewährt, auch wenn diese Daten nicht in der USA liegen. Für weitere Informationen und zum Umgang mit dem US CLOUD Act verweist Voicepoint an dieser Stelle auf den Beitrag «US CLOUD Act: Warum er Cloud-Projekte nicht verhindern sollte» von David Rosenthal, Rechtsanwalt und Partner der Kanzlei VISCHER AG.

Des Weiteren weist Voicepoint auf das «Microsoft Commitment Summary» hin. Microsoft hat seine «Online Service Terms» im April 2023 mit einem «Data Protection Addendum (DPA)» erweitert. Dabei verpflichtet sich Microsoft, in seinen Verträgen die Anforderungen des schweizerischen Datenschutzgesetztes, Berufsgeheimnis und Amtsgeheimnis zu den Produkten und Services einzuhalten. Weitere Informationen diesbezüglich kann Voicepoint auf Anfrage zur Verfügung stellen.

Schweizer Engagement

Als Schweizer Unternehmen verinnerlicht die Voicepoint AG die schweizerischen Werte und achtet auch bei der Bereitstellung ihrer Dienste auf den «swiss-made»-Faktor. Seit der Einführung der Schweizer Rechenzentren kann sich zudem auch die schweizerische Niederlassung von Microsoft (Microsoft Schweiz GmbH) zu den Schweizer Hosting-Anbietern zählen, wodurch Voicepoint den «swiss-made»-Faktor weiterhin anbieten kann. Als Schweizer Lösungsanbieter stellt Voicepoint die Installation, die Wartung und den Support eigenständig bereit, ohne direkten Einfluss und Zugriff von Drittanbietern.

Übersicht zur Datensicherheit von Microsoft Azure

Netzwerksicherheit

Werden branchenübliche Firewalls eingesetzt? Wo werden diese eingesetzt? Wie werden diese aktuell gehalten? Wird administrativer Zugriff zur Firewall und zu anderen Geräten nur durch sichere Kanäle oder direkten Zugriff erlaubt?	Voicepoint verwendet redundante und unterbrechungsfreie Linux-basierte Loadbalancer-VMs der Firma loadbalancer.org mit integrierter Web-Application-Firewall. Die VMs werden innerhalb des Microsoft Azure Datacenters in einem «Availability Set» betrieben, deren Aktualisierungen der Software sowie der Sicherheitsrichtlinien vollständig automatisiert sind. Diese Loadbalancer-VMs sind der Dreh- und Angelpunkt der Verbindung zwischen externen Zugriffen und den Cloud-internen Netzwerken. Für die Verwaltung steht eine Web-Oberfläche mit separater Authentifizierung zur Verfügung, die für das autorisierte Personal nur über eine mit MFA gesicherte VPN-Verbindung erreichbar ist.
Welche Protokolle und Ports werden für die Kommunikation erlaubt?	Alle Client-Applikationen und Smartphone-Apps übertragen Daten via HTTPS Port 443, gesichert durch TLS 1.3 mit einer 128/256-bit AES Verschlüsselung.
Gibt es formale Verfahren für die Reaktion auf Vorfälle? Werden sie regelmässig getestet?	Prozesse für Vorfälle sind implementiert und beinhalten spezifische Verfahren zur Klassifizierung des Schweregrads und der Behandlung von Vorfällen, die die Verfügbarkeit oder Sicherheit der Lösungen betrifft.

Physische Sicherheit

Was sind die wichtigsten physischen Sicherheits- und Business-Continuity-Merkmale Ihres Rechenzentrums?	Das Microsoft Azure Datacenter bietet umfangreiche elektronische und physische Sicherheitsmassnahmen. Unsere Datacenter-Konfiguration wird mit «Availability Sets» bereitgestellt, sodass eine konstant hohe Verfügbarkeit der Hardware gewährleistet werden kann.
Wer (inkl. Mitarbeiter des Datacenters, Voicepoint-Mitarbeiter oder Lieferanten) hat physischen Zugang zu den Servern?	Nur autorisiertes Personal hat Zugang zur physischen Einrichtung, der strikt eingeschränkt und regelmässig überprüft wird.

Systemsicherheit

Sind die Dateiberechtigungen nur auf der Basis von «Minimum Need» festgelegt?	Der Zugriff auf Dateien ist auf Basis von «Minimum Need» ausgelegt und ist auf die entsprechenden Dienstkonten und berechtigten Mitarbeiter eingeschränkt, die Zugriff darauf benötigen.
Sind auf allen Systemen, die kritische Informationen speichern oder verarbeiten, Audit-Logs implementiert? Werden Root-Befehle protokolliert? Welche Prozesse werden verwendet, um den Zugriff auf Geräte und Protokolle zu kontrollieren?	Alle eingesetzten Applikationen beinhalten eigenständige Log- oder Audit-Mechanismen. Die Systemprotokollierung erfolgt über die Windows Ereignisanzeige, die die Protokollierung von Sicherheits-, System- und Applikationsereignissen erlaubt. Zugriffe werden regelmässig geprüft und bei Bedarf angepasst. Zusätzlich werden Zugriffe und Änderungen im Microsoft Azure Portal protokolliert.
Wie wird die Integrität und Verfügbarkeit der Dienste und Applikationsserver überwacht?	Die Systemüberwachung ist vorhanden und nutzt intern entwickelte und branchenübliche Tools. Dabei werden unter anderem die Microsoft Azure-spezifischen Dienste für Alerts und das Monitoring eingesetzt.
Wurden nicht benötigte Dienste und Anwendungen auf den Applikationsservern deaktiviert?	Ja, es werden nur notwendige Dienste und Anwendungen auf den Servern installiert und betrieben.
Werden weitere Sicherheitsmechanismen verwendet?	Ja, für die übergreifende Sicherheit der Infrastruktur wird zusätzlich das Microsoft Azure Security Center eingesetzt, das jeweils die aktuellsten Sicherheitserkenntnisse und Sicherheitsmassnahmen prüft und dabei den Schweregrad einschätzt. Diese werden regelmässig von Voicepoint überprüft und bei Bedarf angewendet. Auf den Applikationsservern steht zudem jeweils der Windows Defender zur Verfügung, der als Antivirus fungiert und Rückmeldungen zum Microsoft Azure Defender sendet.

Web-Sicherheit

Wurden nicht benötigte HTTP-Module oder Erweiterungen auf den Applikationsservern deaktiviert?	Ja, auf unseren Applikationsservern werden nur die benötigten HTTP-Module und Erweiterungen verwendet.
Hat das Konto, unter dem Webdienste ausgeführt werden, Administratorrechte auf den Applikationsservern?	Für jede angebotene Applikation steht ein eigenes Dienstkonto zur Verfügung. Jeder Webdienst wird daher unter einem eigenen Dienstkonto ausgeführt. Die Rechte des Dienstkontos sind auf das erforderliche Minimum reduziert.
Wurden unsichere TLS-Versionen und Ciphers deaktiviert?	Ja, auf den Applikationsservern sowie auch auf der gesamten Umgebung wurden ältere und unsichere TLS-Versionen (<TLS 1.2) und Ciphers deaktiviert. Neue, unsichere Ciphers oder TLS-Versionen werden regelmässig mithilfe von Qualys SSL Labs geprüft und allfällig deaktiviert.

Sicherheit der berechtigten Personen

Wie werden Anmeldedaten der berechtigten Personen behandelt?	Jeder berechtigte Voicepoint-Mitarbeiter verwendet einen persönlichen, mit MFA geschützten, systemübergreifenden Benutzer. Die Mitarbeiter werden dabei in unterschiedliche Verwaltungsrollen eingeteilt. Für den reinen Anwendungssupport berechtigte Mitarbeiter haben keinen direkten Zugang zu den einzelnen Applikationsservern oder Komponenten der Infrastruktur. Ein spezielles «Joiners-Movers-Leavers»-Konzept ist vorhanden und wird angewendet. Somit kann Voicepoint sicherstellen, dass nur berechtigte Mitarbeiter auf die für sie freigegebenen Dienste zugreifen können. Die Rolle des Systemadministrators wird dabei auf ein Minimum beschränkt, damit der Betrieb bei allfälligen Mitarbeiterausfällen gewährleistet werden kann.

Sicherheit der Applikationen

Werden die Daten bei der Übertragung über öffentliche Netzwerkverbindungen verschlüsselt?	Die Kommunikation zwischen Client-Anwendungen und Voicepoint Cloud-Diensten wird über HTTPS übertragen, gesichert durch TLS 1.3 mit einer 128/256-bit AES Verschlüsselung.
Werden irgendwelche Daten lokal auf dem Gerät oder Computer gespeichert (Diktatmanagement)?	Bei der Verwendung der Client-Anwendungen für die Diktatmanagementlösung werden in den lokalen Applikationsdaten des Anwenders Ordner für applikationsspezifische Einstellungen und Logdateien angelegt. Für die Zwischenspeicherung, den flüchtigen Zugriff auf Serverdaten und Diktatentwürfe wird zusätzlich ein sogenanntes «User-WorkingDirectory» verwendet, das wahlweise standardmässig lokal pro Benutzer oder auf einer zentralen Ablage des Kunden eingerichtet werden kann. Originaldiktate von mobilen Diktiergeräten werden nach dem Download lokal beim Kunden abgelegt, bis sie durch den automatischen Archivierungszyklus entfernt werden. Ein gewünschtes Datenbackup dieser Dateien obliegt dem Kunden.
Werden irgendwelche Daten lokal auf dem Smartphone gespeichert?	Beim Einsatz der Smartphone-App für die Diktatmanagementlösung werden temporäre Diktatdaten auf dem Gerät gespeichert. Die Audio-Dateien werden dabei mit einem automatisch generierten Sicherheitsschlüssel auf dem Smartphone verschlüsselt. Weitere Informationen bezüglich der Sicherheit im Winscribe Professional Smartphone App kann auf Anfrage bereitgestellt werden. Bei der Smartphone-Lösung PowerMic Mobile werden keine Diktatdaten gespeichert, da diese App lediglich als Mikrofonersatz dient.
Werden irgendwelche Daten lokal auf dem Gerät oder Computer gespeichert (Spracherkennung)?	Die entsprechenden Spracherkennungsclients streamen Audiodaten in Echtzeit an die sichere Serverumgebung zur Verarbeitung der Spracherkennung. Die Aufbewahrung des erkannten Textes, der vom Spracherkennungsserver zurückgegeben wird, liegt in der Verantwortung der Zielanwendung und des Anwenders.

Zusätzliche Informationen

Weitere Informationen zur Voicepoint Cloud finden Sie auf unserer Website.
Gerne steht Ihnen das Voicepoint Team auch persönlich über das Kontaktformular oder telefonisch unter 044 933 39 39 beratend zur Seite.

Versionsstand: September 2023

Voicepoint AG Schellerstrasse 14 CH-8620 Wetzikon
044 933 39 39 info@voicepoint.ch www.voicepoint.ch