AUTODESK CONSTRUCTION CLOUD™

Whitepaper zur Sicherheit

Inhalt

Einführung

Autodesk Construction Cloud® ist eine Cloud-basierte Projektmanagementplattform für Planungs- und Bauprojekte, deren Zweck die Verbesserung des Ablaufs des gesamten Projektlebenszyklus ist. Als sichere, Cloud-basierte Plattform bietet Autodesk Construction Cloud alle Vorteile der Zusammenarbeit im Planungs- und Baubereich, und schützt zugleich die Kundendaten. Autodesk Construction Cloud wurde anhand von Best Practices für Cloud-Software entwickelt und basiert auf Amazon Web Services (AWS), der weltweit führenden Cloud-Infrastruktur. Bei der Entwicklung unserer Services haben wir den Schwerpunkt auf Skalierbarkeit und Sicherheit gelegt, sodass wir unseren Kunden eine stabile und sichere Anwendung bieten können. Wir wissen, dass das Geschäft unserer Kunden von uns abhängt, und nehmen diese Verantwortung sehr ernst.

Zweck und Umfang dieses Dokuments

Dieses Dokument erläutert den Betrieb von Autodesk Construction Cloud, die Softwareentwicklung und die in der Umgebung implementierten Sicherheitsmaßnahmen.

DIESES DOKUMENT GILT FÜR:

Dieses Whitepaper gilt für alle Module und Services in Autodesk Docs, Autodesk Build (einschließlich PlanGrid Build), Autodesk Takeoff, Autodesk BIM Collaborate und Autodesk BIM Collaborate Pro (einschließlich Revit® Cloud Worksharing, Collaboration for Civil 3D® und Collaboration for Plant 3D®).

DIESES DOKUMENT GILT NICHT FÜR:

Dieses Whitepaper gilt nicht für Assemble, BuildingConnected, Pype, ACC Connect, BIM 360 Field, BIM 360 Glue, BIM 360 Plan, BIM 360 Ops und BIM 360 Team. Weitere Informationen zu den Sicherheitspraktiken für Autodesk-Produkte finden Sie im Autodesk Trust Center.

Cloud-Services

Das Cloud Services-Team* von Autodesk ist verantwortlich für die Ausarbeitung und Durchführung von Maßnahmen im Zusammenhang mit der Freigabe der Software, den Hardware- und Betriebssystem-Upgrades, der Überwachung des Systemzustands und allen weiteren Tätigkeiten, die zur Wartung und Pflege von Autodesk Construction Cloud notwendig sind.

* Die Begriffe „Cloud Services-Team“, „Cloud Infrastructure-Team“ und „Cloud Operations-Team“ beziehen sich auf dasselbe Team bei Autodesk.

Hohe Verfügbarkeit

Durch unsere Verpflichtung zu hoher Verfügbarkeit profitieren unsere Kunden von der vollen Leistungsfähigkeit von Autodesk Construction Cloud. Autodesk Construction Cloud ist auf höchste Verfügbarkeit ausgelegt. Dafür sorgen unter anderem redundante Systeme in der zugrunde liegenden Infrastruktur und die Verteilung der Rechenlast über eine skalierbare Anzahl von Instanzen. Das Autodesk Construction Cloud-System besteht aus mehreren Web- und Anwendungsservern, Systemen zur Verarbeitung von Hintergrundjobs und zur Erstellung von Berichten sowie Daten- und Dateispeichern.

- Jedes Autodesk-Rechenzentrum ist auf mehrere AWS-Regionen und Availability Zones (AZ) verteilt. Bei einer AZ handelt es sich um ein unabhängiges physisches Rechenzentrum innerhalb eines Gebiets. Durch die Nutzung mehrerer AZs sind Autodesk Construction Cloud-Anwendungen somit vor Ausfällen geschützt.
- Kunden, die in Autodesk Construction Cloud enthaltene Produkte nutzen, können ihre Autodesk Construction Cloud-Projektdaten wahlweise primär in Rechenzentren in den USA oder Europa speichern. Der primäre Speicherort für Projektdaten (auch als „abgedeckte Inhalte“ bezeichnet) ist das Rechenzentrum, in dem das Konto gehostet wird. Zu den Projektdaten gehören Projektdateien, Modelle, Zeichnungen, Datensätze, Bilder, Dokumente oder ähnliche Materialien, die vom Kunden oder von dessen berechtigten Benutzern in unserem Service übermittelt oder hochgeladen werden. Ebenfalls zu den Projektdaten gehören die aus dem Service basierend auf den eigenen Rohdaten

oder Informationen des Kunden generierten Ausgaben sowie die zugehörigen Metadaten der Projektdateien, die weder Binärdaten noch im Entwurfsobjekt selbst enthalten sind, z. B. persönliche Daten (Autorenname, E-Mail-Adressen usw.), Zeitstempel und Aktivitätsstream.

Geschäftskontinuität und Redundanz von Rechenzentren

Autodesk hat einen Plan für die Geschäftskontinuität und einen Disaster-Recovery-Prozess auf der Basis von AWS Availability Zones (AZ) entwickelt. Im Einklang mit diesem Prozess wird Autodesk Construction Cloud in mehreren AWS Availability Zones (AZ) bereitgestellt. Jede AWS AZ befindet sich in einem separaten physischen Rechenzentrum, und die Daten werden zwischen den AZs repliziert. Als Teil der Bereitstellung in mehreren AWS AZs wurden redundante Stromversorgungen installiert, die einen Betrieb rund um die Uhr gewährleisten. Darüber hinaus stellen unterbrechungsfreie Stromversorgungen (USV) und Generatoren bei einem Ausfall eine langfristige Notstromversorgung sicher. Jedes AWS-Rechenzentrum ist über mehrere Anbieter mit dem Internet verbunden, um Verbindungsausfälle zu vermeiden.

Datenreplikation

Kundendaten werden zwischen Rechenzentren an verschiedenen Standorten repliziert. Die Replikation verringert das Risiko eines Datenverlusts oder einer Serviceverzögerung, falls ein Rechenzentrum ausfällt und auf ein anderes umgeschaltet werden muss. Daten werden in der Regel innerhalb von 15 Minuten repliziert. Darüber hinaus werden mindestens einmal täglich separate Datenbankbackups erstellt.

Sicherheit der physischen Infrastruktur

Autodesk Construction Cloud-Anwendungen werden in sicheren Rechenzentren ausgeführt, die sich im Besitz von Amazon AWS befinden und von Amazon AWS betrieben werden. Die AWS-Rechenzentren werden durch eine Reihe von Sicherheitsmaßnahmen vor unberechtigtem Zutritt und schädlichen Umwelteinflüssen geschützt.

- **Zugangskontrolle in den Liegenschaften:** Der Zutritt wird an allen Gebäudeeingängen durch professionelles Sicherheitspersonal mithilfe von Überwachungs- und Meldesystemen sowie anderen elektronischen Systemen kontrolliert. Der Zutritt zu den AWS-Rechenzentren durch befugtes Personal erfolgt mittels Multifaktor-Authentifizierung. Die Eingänge zu den Serverräumen sind durch Alarmsysteme gesichert, die bei einem gewaltsamen Öffnen oder Offenhalten der Türen eine entsprechende Reaktionskette anstoßen.
- **Videoüberwachung:** Die Zugangsbereiche zu den AWS-Serverräumen werden mithilfe von Videokameras überwacht. Das Videomaterial wird gemäß gesetzlichen Vorgaben gespeichert.
- **Brandschutz:** Die AWS-Rechenzentren sind mit Brandmelde- und Brandbekämpfungsanlagen ausgerüstet. Zu den Brandmeldeanlagen gehören Rauchmelder in den Bereichen, in denen Netzwerke, Mechanik und Infrastruktur untergebracht sind. Diese Bereiche sind außerdem mit Brandbekämpfungsanlagen ausgerüstet.
- **Klimaregelung:** Die AWS-Rechenzentren sind mit Anlagen ausgerüstet, die das Raumklima regeln und eine angemessene Betriebstemperatur für Server und andere Hardwarekomponenten sicherstellen, um das Risiko einer Überhitzung und eines Ausfalls von Services zu verringern. Temperatur und Luftfeuchtigkeit werden durch Personal und Anlagen überwacht und in angemessenen Bereichen gehalten.

Störfallmanagement

Autodesk Construction Cloud verfügt über eine Richtlinie für das Störfallmanagement mit Best Practices zur Behebung eventueller Störfälle. Der Störfallmanagementprozess basiert auf den Vorgaben der Information Technology Infrastructure Library (ITIL, Version 3). Der Schwerpunkt der Richtlinie für das Störfallmanagement von Autodesk Construction Cloud liegt auf der Aufzeichnung aller unternommenen Lösungsmaßnahmen und einer eingehenden Fehlerursachenanalyse mit dem Ziel, eine Wissensdatenbank mit direkt verwertbaren Vorgehensweisen aufzubauen. Der Zweck der Richtlinie besteht somit nicht nur in einer möglichst schnellen und wirksamen

Behebung von Störungen, sondern auch in der Sammlung und Weitergabe detaillierter Informationen zu Störfällen, um die Prozesse ständig zu verbessern und bei zukünftigen Störungen auf das gesammelte Wissen zurückgreifen zu können. Weitere Einzelheiten finden Sie im Autodesk Trust Center.

Patchmanagement

Das Cloud Services-Team befolgt die Autodesk-Richtlinie für das Patchmanagement, um eine effektive Bereitstellung der Patches zu gewährleisten. Die Suche nach neuen Patches und die Ausarbeitung von Listen zur Bereitstellung der Patches erfolgt nach Möglichkeit vollautomatisch. Diese Listen werden anschließend von autorisierten Cloud-Services-Mitarbeitern genehmigt. In der Autodesk Construction Cloud-Richtlinie für das Patchmanagement sind auch die Kriterien definiert, nach denen die Auswirkung eines Patches auf die Systemstabilität beurteilt wird. Wenn ein Patch potenziell größere Auswirkungen hat, führt das Cloud-Services-Personal vor der Bereitstellung des Patches sorgfältige Regressionstests durch. Die Bereitstellung von Patches auf Produktionssystemen wird vom Cloud Services-Team protokolliert. Die Qualitätssicherung umfasst automatisierte und manuelle Tests während des gesamten Entwicklungs- und Bereitstellungsprozesses.

Änderungsmanagement

Das Cloud Services-Team befolgt eine Richtlinie für das Änderungsmanagement, die folgende Prozesse und Verfahren vorsieht:

- **Änderungsanforderungen:** Alle Änderungen, die an den Systemen zur Unterstützung der Anwendung vorgenommen werden, unterliegen einem formalen Änderungsmanagementprozess und lassen sich über entsprechend abgezeichnete Tickets nachweisen.
- **Wiederherstellungspläne:** Das Cloud Services-Team erstellt vor der Bereitstellung einer Änderung detaillierte Wiederherstellungspläne, damit im Fall einer Serviceunterbrechung durch eine Änderung der ursprüngliche Systemzustand wiederhergestellt werden kann. Wiederherstellungspläne enthalten Skripte mit genauen Anweisungen zur Wiederherstellung des Systemzustands mit minimalen manuellen Schritten.

- **Definierte Wartungsfenster:** Das Cloud Services-Team legt Wartungsfenster für die geplante Wartung, Notfallwartung und erweiterte Wartung fest. Die geplante Wartung wird in Nebenzeiten angesetzt.
- **Testplan:** Das Cloud Services-Team definiert Tests zur Überprüfung der Verfügbarkeit sämtlicher Funktionen nach der Bereitstellung einer Änderung.
- **Staging-Umgebung:** In einer Staging-Umgebung wird das Layout des Produktionssystems gespiegelt. Alle Änderungen an der Produktionsumgebung werden zuerst in der Staging-Umgebung vorgenommen. Vor der Übernahme von Änderungen aus der Staging-Umgebung in die Produktionsumgebung werden umfangreiche Tests durchgeführt, darunter auch Funktionstests.
- **Testdurchführung:** Nach erfolgter Bereitstellung werden Tests durch das Cloud-Services-Team und das QS-Team für das Produkt durchgeführt. Damit wird sichergestellt, dass vor der Änderung als risikobehaftet bewertete Funktionen nach wie vor verfügbar sind.

Kapazitätsmanagement

Die Anforderungen von Autodesk Construction Cloud-Ressourcen können sich im Laufe der Zeit je nach Kundennachfrage ändern. Die Anforderungen von Autodesk Construction Cloud an die Cloud-Ressourcen werden von den Autodesk-Entwicklern anhand der Ressourcenauslastung und der Elastizität der Cloud-Infrastruktur umfassend analysiert. Die Auslastung der Ressourcen für Autodesk Construction Cloud wird in regelmäßigen Abständen für verschiedene Infrastrukturkomponenten erfasst. Neben physischen Geräten werden dabei auch virtuelle Instanzen, Speichermedien und Netzwerkgeräte berücksichtigt. Die Statistik der Auslastung wird zu Analysezwecken gespeichert und kann auch zur proaktiven Aufwärts- oder Abwärtsskalierung der virtuellen Instanzen abhängig von der Kundennachfrage herangezogen werden.

Leistung und Skalierbarkeit

Zur Sicherstellung hoher Verfügbarkeit werden während des gesamten Lebenszyklus der Softwareentwicklung Leistungs- und Belastungstests durchgeführt. Die aktuelle

und die historische Verfügbarkeit werden zusammen mit bevorstehenden geplanten Wartungsmaßnahmen im Autodesk Health Dashboard ausgewiesen (https://health.autodesk.com/).

Sicherheitsmaßnahmen für den Betrieb von Autodesk Construction Cloud

Autodesk setzt verschiedene Sicherheitsmaßnahmen für die Autodesk Construction Cloud-Produkte ein, um unbefugte Zugriffe auf die Konten und Daten von Kunden zu verhindern.

- **Hintergrundprüfungen:** Autodesk verlangt (gegebenenfalls) Hintergrundprüfungen von Mitarbeitern, bevor diese Zugang zu den Rechenressourcen und zugrunde liegenden Systemen von Autodesk Construction Cloud erhalten.
- **Zugriffsmanagement:** Autodesk hat Richtlinien und Prozesse für das Zugriffsmanagement festgelegt. Diese Richtlinien und Prozesse betreffen die Bereitstellung von Konten, die Beschränkung des Zugriffs auf Informationen und Systeme von Autodesk auf ausschließlich den für die Ausführung der zugewiesenen Aufgaben erforderlichen Umfang und den zeitnahen Zugriffsentzug. Die Autodesk-Richtlinien für das Zugriffsmanagement werden mindestens einmal jährlich durch das Autodesk-Sicherheitsteam überprüft.
- **Testdurchführung:** Nach erfolgter Bereitstellung werden Tests durch das Cloud Services-Team und das für das Produkt zuständige QS-Team durchgeführt. Damit wird sichergestellt, dass vor der Änderung als risikobehaftet bewertete Funktionen nach wie vor verfügbar sind.
- **Administrative Funktionen:** Die administrativen Tools von Autodesk Construction Cloud bieten Administratoren eine flexible Möglichkeit zur Verwaltung von Benutzern, rollenbasierten Berechtigungen und anderen Zugriffskontrollen für Endbenutzer.
- **Redundante Technologien:** Redundante Technologien wie Lastverteiler und geclusterte Datenbanken reduzieren mögliche Störungen.

Entwicklung von Autodesk Construction Cloud

Das Entwicklungsteam von Autodesk Construction Cloud ist für das Konzipieren, Implementieren und Testen der Autodesk Construction Cloud-Anwendungen verantwortlich. Konzeption, Codierung, Test und Wartung von Autodesk Construction Cloud sind Teil eines Softwareentwicklungsprozesses mit entsprechenden Sicherheitsmaßnahmen.

Während der Konzeption erstellen Softwarearchitekten detaillierte Konzeptdokumente von Anwendungsfällen, die genau auf Funktionalität und Skalierbarkeit geprüft werden. Die Konzeptionsphase basiert auf einem Prozess zur Anwendungsentwicklung, bei dem Architekten und Softwareentwickler gemeinsam die Anwendungsfälle im Hinblick auf Funktionalität, Skalierbarkeit und Leistung analysieren.

Bei der Implementierung überprüfen Entwickler und Architekten gemeinsam den erstellten Code, um eventuelle Abweichungen von den Entwicklungsanforderungen für die Autodesk Construction Cloud-Anwendungen zu ermitteln.

Der gesamte während des Prozesses erstellte Code wird getestet, integriert und im Rahmen der QS geprüft. Neue Versionen gelten erst als vollständig, nachdem die Abnahmekriterien durch das Qualitätssicherungspersonal geprüft wurden.

Als Teil des Entwicklungslebenszyklus führt das Performance-Team von Autodesk Construction Cloud während der Entwicklungszyklen Belastungstests durch, bei denen Änderungen mit negativen Auswirkungen auf die Performance frühestmöglich erkannt werden können.

Mitarbeiterschulung

Autodesk bietet allen internen und externen Mitarbeitern regelmäßig Schulungen zu allgemeinen Informationen, Sicherheitsrichtlinien und zur Sensibilisierung für die Sicherheitsmaßnahmen an. Darüber hinaus wird vorausgesetzt, dass alle Mitarbeiter den Verhaltenskodex des Unternehmens lesen, verstehen und einen entsprechenden

Schulungskurs absolvieren. Der Verhaltenskodex verlangt von allen Mitarbeitern ein rechtlich und ethisch einwandfreies Geschäftsgebaren sowie Integrität und Respekt gegenüber Kollegen, Kunden, Partnern und Mitbewerbern des Unternehmens.

Autodesk-Mitarbeiter müssen die Unternehmensrichtlinien in Bezug auf Vertraulichkeit, Geschäftsethik, angemessene Nutzung und professionelle Standards befolgen. Neue Mitarbeiter müssen eine Vertraulichkeitserklärung unterzeichnen. Bei der Einarbeitung neuer Mitarbeiter wird die Bedeutung der Vertraulichkeit und des Datenschutzes von Kundendaten hervorgehoben.

Bei der Implementierung von Best Practices für die Sicherheit arbeitet jedes Entwicklungsteam eng mit einem dedizierten Sicherheitsbeauftragen zusammen. Für die Sicherheitsbeauftragen sind gesonderte Schulungen verpflichtend. Außerdem bietet Autodesk allen Entwicklern Schulungen zum Thema „Sichere Entwicklungslebenszyklen“ an. Alle Entwickler können die (ISC)^2 Software Security Practitioner-Zertifizierung erwerben.

Darüber hinaus bietet Autodesk allen Mitarbeitern regelmäßig verschiedene Übungen und informelle Treffen an, darunter auch regelmäßige Phishing-Übungen.

Sicherheitsmaßnahmen für die Autodesk Construction Cloud-Produkte

Autodesk Construction Cloud verfügt über integrierte Sicherheitsfunktionen, mit denen Kunden detaillierte Richtlinien für das Identitäts- und Zugriffsmanagement erstellen können. Mit den Sicherheitstools von Autodesk Construction Cloud können die Administratoren und Benutzer des Kunden das Eigentum ihrer Arbeitsbereiche und Dokumente verwalten sowie Berechtigungen zur Freigabe festlegen.

Authentifizierung und Verschlüsselung während der Übertragung

Für den Zugriff auf Autodesk Construction Cloud sind Zugangsdaten bestehend aus Benutzer-ID und Kennwort erforderlich. Die Zugangsdaten werden im Netzwerk

sicher übertragen und nur als Hash mit Salt (Anhängung einer zufällig gewählten Zeichenfolge) gespeichert.

Die sichere Kommunikation zwischen Clients und den Backend-Services erfolgt über einen verschlüsselten Kanal. Die Services werden regelmäßig mit branchenführenden Tools gescannt, um durchgehend höchste Standards zu gewährleisten. Die Services unterstützen Verbindungen über TLS 1.2 (Transport Layer Security) mit sicheren Chiffrensammlungen (Cipher Suites).

Verschlüsselung im Ruhezustand

Alle von Kunden in Autodesk Construction Cloud hochgeladenen Dateien werden verschlüsselt in der Cloud gespeichert. Bei der Speicherlösung kommt 256-Bit Advanced Encryption (AES-256) zum Einsatz, eine der stärksten verfügbaren Blockverschlüsselungen. Der gesamte Prozess aus Verschlüsselung, Schlüsselverwaltung und Entschlüsselung wird im Rahmen des bestehenden Auditprozesses regelmäßig intern überprüft.

Administrative Kontrollen

Autodesk Construction Cloud stellt Kundenadministratoren Sicherheitsfunktionen zur Erstellung von Richtlinien für das Identitäts- und Zugriffsmanagement zur Verfügung.

- **Benutzerbereitstellung:** Administratoren können Benutzer erstellen und deaktivieren.
- **Rollenbasierte Sicherheit:** Mithilfe von Rollen in Autodesk Construction Cloud können Administratoren die Zugriffskontrollebenen anpassen und den Zugriff individuell einschränken. Eine Rolle besteht aus verschiedenen Berechtigungen für Daten und Funktionen in Abhängigkeit vom Tätigkeitsbereich.
  Indem sich Berechtigungen auf Rollenbasis flexibel zuweisen lassen, befolgt Autodesk Construction Cloud das Prinzip der geringsten Privilegien. Dieses Prinzip besagt, dass jeder Benutzer nur Zugriff auf die Daten und Funktionen erhalten soll, die zur Erfüllung der zugeteilten Aufgaben benötigt werden.

Benutzerkontrolle

Benutzer können mit Ausnahme administrativer Einschränkungen den Zugriff auf Elemente, Berichte und Dateien kontrollieren, deren Eigentümer sie sind. Mithilfe von Dateiversionierung können Benutzer außerdem frühere Versionen von Dateien wiederherstellen, die sie an Elemente im Arbeitsbereich angehängt haben.

Standards zur Identitätsföderation

Autodesk Construction Cloud unterstützt Single Sign-On (SSO) bei Kundensystemen für alle Benutzer.

Sicherheit in der Cloud

Unser dediziertes Autodesk Security-Team konzentriert sich ausschließlich auf die Sicherheit der Autodesk Construction Cloud-Umgebung. Die Zuständigkeiten umfassen:

- Prüfung des Sicherheitsstatus der Konzeption und Implementierung der Cloud-Infrastruktur von Autodesk
- Ausarbeitung und Implementierung von Sicherheitsrichtlinien, einschließlich Identitäts- und Zugriffsmanagement, Kennwortmanagement und Schwachstellenmanagement
- Interne Prüfungen und Audits zur Sicherstellung der Einhaltung geltender Sicherheitsvorkehrungen
- Ermittlung und Implementierung von Technologien zum Schutz von Kundendaten
- Durchführung von Sicherheitsprüfungen gemeinsam mit externen Sicherheitsspezialisten
- Überwachung der Cloud-Services zur Ermittlung potenzieller Sicherheitsprobleme und Reaktion auf eventuelle Störfälle

Schwachstellenscans, Penetrationstests und externe Audits

Das Autodesk Security-Team führt regelmäßige Sicherheitsscans und Penetrationstests der Autodesk Construction Cloud-Services durch, die der SOC2-Zertifizierung unterliegen. Bei den Sicherheitsscans und Penetrationstests im Rahmen der SOC2-Zertifizierung werden alle Systeme nach den Vorgaben des Open Web Application Security Project (OWASP) und der SANS Top 25 nach zahlreichen Schwachstellen abgesucht.

Netzwerksicherheit

Die Sicherheit des Netzwerks wird durch eine Kombination aus physischen und logischen Kontrollmechanismen gewährleistet, darunter Verschlüsselung, Firewalls und Systemhärtungsmaßnahmen. Unabhängige Hardwarefirewalls sichern die Cloud-Umgebung von Autodesk nach außen ab. Alle außer die zur Bedienung von Kundenanfragen erforderlichen Ports sind gesperrt.

Sicherheitsstandards und Nachweise

- Der Sicherheitsstatus von Autodesk Construction Cloud wird anhand des Branchenstandards SSAE-16 AT 101 SOC2 nachgewiesen. Autodesk Construction Cloud wird planmäßig Teil des nächsten jährlichen SOC2-Audits bei Autodesk sein.
- Nach erfolgtem Auditing und erfolgter Zertifizierung wird Autodesk Construction Cloud ebenso wie alle Module und Services von BIM 360 nach ISO 27001, ISO 27017 und ISO 27018 zertifiziert sein.

Weitere Informationen zu den aktuellen Nachweisen für Autodesk Construction Cloud und zugehörige Services finden Sie im Autodesk Trust Center unter „Compliance“.

Datenschutz

Autodesk verfolgt bei der Erfassung und Verarbeitung personenbezogener Kundendaten einen transparenten Ansatz. Weitere Informationen finden Sie in der Datenschutzerklärung von Autodesk. Weitere Informationen finden Sie außerdem im Autodesk Trust Center unter „Privacy“.

Ressourcen

In den folgenden Ressourcen finden Sie allgemeine Informationen zu Autodesk sowie weitere Informationen zu den in diesem Dokument behandelten Themen.

- Weitere Informationen zu Autodesk finden Sie unter http://www.autodesk.de.
- Weitere Informationen zu unserem umfassenden Sicherheitskonzept finden Sie unter https://www.autodesk.de/trust/security.
- Die Autodesk Construction Cloud-Anwendungen werden in AWS gehostet. Daher zeichnen Autodesk und Amazon gemeinsam für die Sicherheit und die Infrastruktur verantwortlich. Weitere Informationen zur Sicherheit bei Amazon finden Sie in den folgenden Ressourcen:
    - AWS: Compliance
    - AWS: Kontrollen in Rechenzentren
    - AWS: Modell der gemeinsamen Verantwortung

USA
+1 866 475-3802
autodesk.com/construction

Australien und Asien-Pazifik
+61 1800 314435
acs.apac@autodesk.com
construction.autodesk.com/au

UK und EMEA
+44 808 1892253
acs.emea@autodesk.com
construction.autodesk.com/gb

ARTAKER CAD

ARTAKER Büroautomation GmbH

Wien | Linz | Graz | Salzburg | Telfs

Tel.: 01 585 11 55 - 0

info@artaker.com

www.artaker.com