AUTODESK

Whitepaper: Sicherheit in Autodesk® Fusion 360

Oktober 2022

Inhalt

1. Einführung

Autodesk® Fusion 360™ ist das erste Tool für 3D-CAD, -CAM und -CAE seiner Art. Es führt Ihren gesamten Produktentwicklungsprozess in einer einzigen cloudbasierten Plattform für Mac und PC zusammen. Die Werkzeuge von Fusion 360 ermöglichen die schnelle und einfache Erkundung von Entwurfsideen mit einem sicheren und integrierten Werkzeugsatz, der vom Konzept bis zur Fertigung reicht und auch Webbrowser und mobile Geräte umfasst.

1.1 Zweck und Umfang dieses Dokuments

Dieses Dokument erläutert Autodesk-Vorgänge, den Softwareentwicklungsprozess und die in der Umgebung implementierten Sicherheitsmaßnahmen. In diesem Dokument bezieht sich Autodesk Fusion 360 sowohl auf die Fusion 360-Client-Software als auch auf die Fusion 360-Browserzugriffs-Software.

Das Sicherheits-Framework von Autodesk basiert auf Branchenstandards zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten.

Fusion 360 wurde für hohe Verfügbarkeit und Skalierbarkeit entwickelt und bietet unseren Kunden einen schnellen und flexiblen Cloud-Service. Autodesk nutzt Amazon Web Services (AWS), einen führender Anbieter von Cloud-Infrastruktur, als Cloud-Hosting-Provider. Autodesk vertraut auf das Shared-Responsibility-Modell von AWS als Hosting-Provider. Dieses Modell umfasst die Infrastruktur aus Hardware, Software, Netzwerk und Einrichtungen, die AWS-Cloud-Services ausführen. (Weitere Informationen finden Sie unter: https://aws.amazon.com/de/compliance/shared-responsibility-model/).

2. Autodesk-Sicherheit

Das Autodesk-Sicherheits-Framework basiert auf Branchenstandards, um konsistente Sicherheitsverfahren zu gewährleisten, die uns die sichere Erstellung, Ausführung und Aufbewahrung von Daten ermöglichen.

- **Sichere Entwicklung:** Die Einbettung von Sicherheitsfunktionen in unsere Produkte von Grund auf ist ein wichtiger Schritt, um die Investition unserer Kunden in Autodesk-

Produkte und -Dienste zu schützen. Wir integrieren Sicherheit in alle Phasen der Softwareentwicklung.

- **Sichere Ausführung:** Wir integrieren Sicherheit direkt in unsere Infrastruktur. Unser ganzheitlicher Ansatz umfasst die Bereitstellung von Tools für den Endpunktschutz, standardisierte Patching- und Härtungsanforderungen, Identitäts- und Zugriffsmanagement-Kontrollen sowie offensive Sicherheitsmaßnahmen.

- **Sichere Arbeit:** Die Sicherheit bei Autodesk konzentriert sich auf drei Hauptziele, die die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen schützen:

    - Vertraulichkeit: Nur befugte Personen haben Zugriff auf Informationen.
    - Integrität: Informationen sind vollständig und richtig.
    - Verfügbarkeit: Daten sind für Kunden zugänglich und verfügbar.

Der Chief Security Officer (CSO) ist verantwortlich für die Entwicklung, Implementierung und Steuerung der Sicherheitsstrategie und des Sicherheitsprogramms und stellt sicher, dass die Sicherheitsrichtlinien und -standards auf alle Produkte und Umgebungen von Autodesk angewendet werden. Das CSO- und Security-Team wird von Autodesk-Führungskräften und dem Board of Directors unterstützt.

3. Fusion 360 Engineering

Das Fusion 360 Engineering-Team ist für das Entwerfen, Implementieren und Testen der Fusion 360-Clientsoftware und der Cloud-Dienstanwendung verantwortlich.

Entwicklung, Programmierung, Test und Wartung von Fusion 360 basieren auf einem agilen Softwareentwicklungsprozess. Während der Entwurfsphase werden detaillierte Entwurfsdokumente von Architekten erstellt und geprüft, um die Funktionalität und Skalierbarkeit des Entwurfs zu bewerten. Während der Implementierungsphase führen Softwareingenieure und Architekten Peer-Code-Überprüfungen durch, um Abweichungen von den Verfahren zur Anwendungsentwicklung von Fusion 360 zu ermitteln. Der gesamte während des Prozesses erstellte Code umfasst Funktionseinheitstests, und User Storys sind erst vollständig, wenn die Qualitätssicherungsabteilung die Kriterien für die Definition of Done und

die Abnahme überprüft hat. Auch Leistungstests für Fusion 360 sind in den Entwicklungszyklus integriert. Das Fusion 360-Team führt Lasttests während der gesamten Entwicklungsphasen durch, um die Änderungen, die sich negativ auf die Leistung auswirken, so früh wie möglich im Prozess zu erkennen.

3.1 Mitarbeiterschulung

Alle Mitarbeiter von Autodesk müssen die Wichtigkeit der Informationssicherheit als Teil ihrer Einweisung nach der Neueinstellung bestätigen. Mitarbeiter müssen den Verhaltenskodex des Unternehmens lesen, verstehen und an einer Schulung dazu teilnehmen. Der Kodex verpflichtet jeden Mitarbeiter, seine Geschäftstätigkeit gesetzeskonform, ethisch einwandfrei, mit Integrität und mit Respekt für Kollegen und die Nutzer, Partner und Konkurrenten des Unternehmens zu betreiben.

Mitarbeiter von Autodesk müssen die Richtlinien des Unternehmens in Bezug auf Vertraulichkeit, Geschäftsethik, angemessene Nutzung und professionelle Standards einhalten. Neue Mitarbeiter müssen eine Vertraulichkeitsvereinbarung unterzeichnen. Die Einweisung für neue Mitarbeiter legt den Schwerpunkt auf die Vertraulichkeit und den Schutz der Kundendaten.

Zur Implementierung von optimalen Verfahren für die Sicherheit hat Autodesk ein jährliches Programm für die Softwarezertifizierung (Software Security Certification Program (SSCP)) für alle Mitarbeiter in den Bereichen Engineering und Cloud Infrastructure eingeführt.

4. Produktsicherheit bei Fusion 360

Autodesk Fusion 360 verfügt über integrierte Sicherheitsfunktionen, von der gesicherten Kommunikation mit den Cloud-Diensten bis hin zu Sicherheits- und Zusammenarbeitsfunktionen im Produkt selbst, die von Benutzern gesteuert werden können.

4.1 Kommunikationssicherheit

Die gesamte Kommunikation zwischen Autodesk Fusion 360 und Cloud-Diensten erfordert sichere HTTPS-Verbindungen.

4.2 Verschlüsselung

Die Kommunikation zwischen Fusion 360 und den Back-End-Diensten sowie innerhalb der Back-End-Dienste erfolgt über einen verschlüsselten Kanal.

4.3 Authentifizierung

Für den Zugriff auf Autodesk Fusion 360 sind Anmeldedaten bestehend aus einer Autodesk-ID, einer Benutzer-ID und einem Kennwort erforderlich. Die Anmeldedaten werden während der Netzwerkübertragung gesichert und nur als Salted-Hash gespeichert.

Fusion 360 bietet Endbenutzern die Möglichkeit, bei der Anmeldung eine mehrstufige Authentifizierung zu verwenden. Benutzer, die diese Funktion verwenden möchten, können über ihr autorisiertes sicheres persönliches Gerät (z. B. Mobiltelefon) einen Code erhalten, den sie zusammen mit ihrem Kennwort nutzen können.

4.4 Datensicherheit

Alle Fusion 360-Konstruktionen werden in der Cloud verschlüsselt gespeichert. Die Speicherlösung verwendet zum Verschlüsseln von Daten den Advanced Encryption Standard (AES-256) mit 256 Bit.

Lokal unterliegen im Cache gespeicherte Konstruktionen den Anwenderberechtigungen des Betriebssystems für die Zugriffssteuerung.

4.5 Erstellung von Konstruktionsversionen

Autodesk Fusion 360 legt für jede Konstruktion einen Versionsverlauf an. Die Versionierung schützt die Integrität der Daten, indem sie es Benutzern ermöglicht, zu früheren Versionen zurückzukehren, und eine überprüfbare Liste mit Informationen zu jeder Dateiänderung bereitstellt.

4.6 Sicherheit bei der Zusammenarbeit über Hubs und Gruppen

Projekte bieten eine einfache Grundlage für die Gewährung oder Beschränkung des Zugriffs auf Autodesk Fusion 360-Konstruktionen für eine Gruppe von Teamkollegen. Einladungen zu Projekten werden vom Eigentümer oder Moderator des Projekts genehmigt. So wird sichergestellt, dass Mitglieder die strengen Regeln einhalten, die beim Gewähren von Zugriff für neue Benutzer gelten.

Unternehmen können Team-Hubs auswählen, mit denen sie die Kontrolle über die Eigentümerschaft und den Zugriff auf alle von Mitgliedern erstellten Projekte ausüben können. Datenschutzeinstellungen für Projekte, wie z. B. offene, geschlossene und geheime Projekte, ermöglichen eine kontrollierte Zusammenarbeit. Mit Team-Hubs können Mitglieder den Zugriff von Benutzern beschränken, die zu dem Projekt eingeladen wurden. Team-Hubs ermöglichen es außerdem Kundenadministratoren, Konten von ehemaligen Mitarbeitern zu deaktivieren und die Projekteigentümerschaft auf andere Mitglieder des Teams zu übertragen.

4.7 Öffentliche Freigabe

Mit der öffentlichen Freigabe können Benutzer mit externen Projektbeteiligten zusammenarbeiten, die nicht über eine Autodesk-ID oder Fusion 360-Berechtigung verfügen. Fusion 360-Benutzer erstellen einen Link, der schreibgeschützten Zugriff auf die Konstruktion bietet. Benutzer haben auch die Möglichkeit, Download- und Exportfunktionen zu aktivieren. Der Benutzer kann die öffentliche Freigabe, die durch diesen Link angeboten wird, jederzeit aufheben.

5. Cloud-Infrastruktur

Das Cloud Infrastructure-Team ist verantwortlich für die Definition und Durchführung von Prozeduren für die folgenden Aktionen: Management der Anwendungsfreigabe, Upgrades für Hardware und Betriebssystem, Überwachung des Systemzustands und weitere Aktivitäten, die für die Funktion von Autodesk Fusion 360 erforderlich sind.

5.1 Hochverfügbarkeit

Autodesk Fusion 360 wurde für ein hohes Maß an Verfügbarkeit entwickelt. Dies wird durch redundante Systeme in der unterstützenden Infrastruktur und die Lastverteilung über eine skalierbare Anzahl von Instanzen hinweg erreicht.

5.2 Datenreplikation und Redundanz

Die Kundendaten werden zwischen Amazon Web Services (AWS) Availability Zones (AZs) repliziert. Die Replikation begrenzt das Risiko von Datenverlusten oder einer Verzögerung bei der Dienstwiederaufnahme, wenn ein Failover auf ein Backup-Rechenzentrum erforderlich ist.

5.3 Redundante Stromversorgungssysteme

AWS-Rechenzentren enthalten redundante Stromversorgungssysteme, um den Betrieb rund um die Uhr gewährleisten zu können. Unterbrechungsfreie Stromversorgungen (USV) stellen im Falle eines Ausfalls automatisch ein Backup der primären Stromsysteme bereit. Generatoren in jedem Rechenzentrum bieten bei einem Ausfall eine langfristige Backup-Stromversorgung.

5.4 Redundante Internetverbindungen

Ein redundantes System mit mehreren Anbietern wird verwendet, um die Internetverbindung zu jedem Rechenzentrum aufrechtzuerhalten.

Die Autodesk Fusion 360-Clientsoftware verfügt auch über einen Offline-Modus. Damit können Benutzer weiterhin auf lokale Kopien ihrer Konstruktion zugreifen und diese bearbeiten, wenn sie nicht mit dem Internet verbunden sind.

5.5 Sicherheit der physischen Infrastruktur

Die Autodesk Fusion 360-Anwendung läuft in sicheren AWS-Rechenzentren, die durch eine Reihe von Sicherheitsmaßnahmen vor unberechtigtem physischen Zugang und Umweltgefahren geschützt sind. Einige physische und umwelttechnische Kontrollen sind unten zusammengefasst. Eine vollständige Übersicht über AWS-Sicherheitsprozesse finden Sie hier.

5.6 Zugangskontrolle

AWS-Rechenzentren werden rund um die Uhr von professionellen Sicherheitsmitarbeitern bewacht. Die Umgebung jedes Rechenzentrums sowie Räume, die Rechnerausrüstung und unterstützende Systeme enthalten, sind durch Videoüberwachung geschützt. Die Videoüberwachung wird auf digitalen Medien gespeichert, sodass die jüngsten Aktivitäten bei Bedarf angesehen werden können. Die Eingänge in den Rechenzentren werden durch Zugangskontrollmechanismen geschützt, die immer nur von einer Person passiert werden können. Alle Besucher und Auftragnehmer müssen sich ausweisen, um eingelassen zu werden. Zudem werden sie jederzeit von autorisiertem Personal begleitet. Nur Mitarbeiter mit legitimen geschäftlichen Gründen erhalten Zugang zum Rechenzentrum, und alle Besuche werden elektronisch protokolliert.

5.7 Brandschutz

Brandmelde- und -bekämpfungssysteme, wie z. B. Rauchmelder und durch Hitze ausgelöste Sprinkleranlagen, sind in jedem Rechenzentrum installiert, um Räume mit Rechnerausrüstung und unterstützenden Systemen zu schützen. Brandmeldesensoren sind in der Decke und unter einem Doppelboden installiert.

5.8 Klimaanlagen

Die Klimasteuerung für Rechenzentren schützt Server, Router und andere Geräte, die ggf. ausfallen, wenn die strengen Vorgaben zu Umweltbedingungen verletzt werden. Die Überwachung erfolgt durch Systeme und Personal, um gefährliche Bedingungen wie Überhitzung zu vermeiden. Anpassungen, die Temperatur- und andere Umgebungsbedingungen innerhalb akzeptabler Bereiche halten, werden automatisch von Steuerungssystemen vorgenommen.

6. Störfallmanagement

Autodesk verfügt über eine Richtlinie für das Störfallmanagement, die optimale Verfahren für die Behebung von Störfällen definiert. Die Autodesk-Richtlinie für das Störfallmanagement legt den Schwerpunkt auf die Protokollierung von Behebungsschritten sowie die Verwendung von Fehlerursachenanalysen, um eine Wissensdatenbank mit umsetzbaren Verfahren aufzubauen. Das Ziel der Autodesk-Richtlinie für das Störfallmanagement besteht nicht nur darin, Vorfälle schnell und effektiv zu beheben, sondern auch darin, Informationen zu Störfällen zu sammeln und zu verteilen, sodass Prozesse kontinuierlich verbessert werden und zukünftige Reaktionen auf gesammeltes Wissen aufbauen können.

7. Patch-Management

Das Cloud Infrastructure-Team verfügt über eine Richtlinie für das Patch-Management, die eine effektive Patchbereitstellung sicherstellt. Wo immer möglich erfolgt die Suche nach neuen Patches und die Erstellung von Bereitstellungslisten, die von autorisierten Cloud Infrastructure-Mitarbeitern genehmigt werden können, automatisch. Die Patching-Richtlinie legt auch Kriterien fest, anhand derer die Auswirkungen eines Patches auf die Systemstabilität ermittelt werden. Wenn ein Patch möglicherweise eine große Auswirkung hat, wird der Regressionstest

abgeschlossen, bevor der Patch bereitgestellt wird. Das Änderungsmanagement verfolgt die Bereitstellung von Patches auf Produktionssystemen.

8. Änderungsmanagement

Das Cloud Infrastructure-Team verfügt über eine Änderungsmanagementrichtlinie, die die folgenden Aktivitäten umfasst:

- **Formular für Änderungsanforderung.** Für alle Änderungen muss ein Formular für die Änderungsanforderung eingereicht werden. Das Formular enthält den Namen des Änderungsinitiators, die Änderungspriorität, die geschäftliche Begründung für die Änderung und das Implementierungsdatum für die angeforderte Änderung.

- **Wiederherstellungspläne.** Das Cloud Infrastructure-Team erstellt vor der Bereitstellung detaillierte Wiederherstellungspläne, sodass der Systemstatus wiederhergestellt werden kann, wenn eine Änderung zu einer Unterbrechung des Dienstes führt. Wiederherstellungspläne enthalten in Skripten definierte ausführbare Anweisungen, die den Systemzustand mit minimalen manuellen Schritten wiederherstellen.

- **Definierte Wartungsfenster.** Das Cloud Infrastructure-Team legt geplante, notfallbedingte und erweiterte Wartungsfenster fest. Geplante Wartungsarbeiten werden außerhalb der Hauptlastzeiten durchgeführt.

- **Testplan.** Das Cloud Infrastructure-Team definiert eine Reihe von Tests, um zu überprüfen, ob die Funktionen nach der Bereitstellung einer Änderung verfügbar sind.

- **Testausführung.** Nach Abschluss der Bereitstellung führen das Cloud Infrastructure- und das Autodesk Fusion 360 QA-Team die Tests durch, um zu überprüfen, ob die als gefährdet erkannten Funktionen weiterhin verfügbar sind.

9. Kapazitätsmanagement

Da der Kundenzugriff auf Cloud-Dienste über ein Self-Service-Modell nach Bedarf erfolgt, sind die Datenverkehrsströme sehr variabel und können hohe Auslastungsspitzen aufweisen. Wenn eine Spitze auftritt, kann die Verfügbarkeit eines Dienstes beeinträchtigt werden. Dies ist dann

der Fall, wenn der Pool der Rechenressourcen, die den Dienst steuern, erschöpft ist. Um ein hohes Verfügbarkeitsniveau zu gewährleisten, implementiert das Cloud Infrastructure-Team eine Richtlinie für das Kapazitätsmanagement. Diese umfasst Folgendes:

- **Regelmäßige Erfassung der Ressourcennutzung.** Die Ressourcennutzung für Autodesk Fusion 360 wird in regelmäßigen Abständen über eine Reihe von Infrastrukturkomponenten erfasst, darunter virtuelle Instanzen, virtuelle Speichervolumen und virtuelle Netzwerkgeräte. Nutzungsstatistiken werden in einem Repository für das Kapazitätsmanagement gespeichert.

- **Kapazitätsplanung.** Das Cloud Infrastructure-Team erstellt mithilfe des Kapazitätsmanagements einen detaillierten Kapazitätsplan, in dem die aktuellen Nutzungsniveaus dokumentiert und zukünftige Niveaus basierend auf statistischen Analysen und den Auswirkungen bevorstehender Verbesserungen der Geschäftsfunktionen modelliert werden. Der Kapazitätsplan wird bei Bedarf oder bei erheblichen Änderungen der Nutzungsmuster aktualisiert.

- **Ressourcenzuweisung.** Rechenressourcen werden zugewiesen, wenn Kunden sie anfordern. Vorgewärmte Rechenressourcen sind immer verfügbar. Wenn eine Aktivitätsspitze auftritt, werden neue Ressourcen instanziiert. So wird zum Beispiel die Verfügbarkeit für Autodesk Fusion-Browserressourcen in der Regel in weniger als 10 Minuten erreicht.

- **Aktivitätsüberwachung.** Aktivitäts-Dashboards und -warnungen werden für alle Backend-Dienste definiert, sodass Ingenieure die Systemaktivitäten überwachen und nach dem Auftreten eines Problems Analysen durchführen können.

10. Warnungen und Überwachung

Um eine möglichst kurze Reaktionszeit (Mean Time to Remediation) zu gewährleisten, verwendet Autodesk automatisierte Systeme zur Überwachung von Fusion 360. Diese validieren den Integritätsstatus eines Dienstes. Jede einzelne Komponente, von der Datenbank bis zu den Diensten, wird einzeln überwacht.

Wirken sich Ereignisse auf Dienste aus, werden Warnungen generiert, und das Cloud Infrastructure-Team wird durch einen Eskalationsprozess benachrichtigt.

Die Dienstintegrität beschreibt auch die Beziehung zwischen Autodesk-Diensten. Ein Dienst wie Autodesk Fusion 360 reagiert sehr empfindlich auf den ACM-Dienst (Zugriffssteuerung). Jeder Dienst muss stabil laufen, wenn ein abhängiger Dienst ausfällt, und sollte ordnungsgemäß beendet werden, wenn er nicht mehr ohne Datenverlust für den Kunden ausgeführt werden kann.

Der Status des Fusion 360-Dienstes wird vom Health Dashboard-Dienst von Autodesk öffentlich angezeigt: https://health.autodesk.com.

11. Keine Ausfallzeiten während der Bereitstellung

Wenn Patches auf die Produktionsumgebung angewendet werden, wird ein Blau/Grün-Bereitstellungsansatz für den Autodesk Fusion-Browser und andere Fusion 360-Dienste angewendet. Dadurch wird sichergestellt, dass der Dienst nicht für Kunden ausfällt.

12. Autodesk Fusion 360 – Operative Kontrollen

Autodesk Fusion 360 schützt vertrauliche Kundendaten vor nicht autorisiertem Zugriff.

- **Physische Einschränkungen für Rechenzentren.** Physische Einschränkungen für Rechenzentren verhindern, dass nicht autorisierte Personen Zugang zu der von Autodesk Fusion 360 verwendeten Hardware und unterstützenden Systemen erhalten.
- **Hintergrundprüfungen.** Mitarbeiter mit physischem Zugang zu den von Autodesk Fusion 360 verwendeten Rechenressourcen und unterstützenden Systemen müssen eine Hintergrundprüfung durchlaufen.
- **Datenreplikation.** Bei der Datenreplikation werden Kundendaten in redundante Rechenzentren kopiert, sodass die Geschäftskontinuität gewahrt bleibt, wenn ein Failover zwischen den Standorten auftritt.
- **Redundante Technologien**. Redundante Technologien wie Load Balancer und geclusterte Datenbanken begrenzen die Ausfälle einzelner Komponenten.

13. Autodesk-Sicherheit

Das Autodesk Security-Team besteht aus Experten für Informationssicherheit, die sich mit der Identifizierung und Durchsetzung von Sicherheitsverfahren in der Autodesk Cloud-Umgebung befassen. Das Autodesk Security-Team ist u. a. für folgende Aufgaben zuständig:

- Überprüfen des Sicherheitszustands bei der Planung und Implementierung der Cloud-Infrastruktur von Autodesk
- Definieren und Sicherstellen der Implementierung von Sicherheitsrichtlinien, einschließlich Identitäts- und Zugriffsmanagement, Kennwortmanagement und Sicherheitsrisikomanagement
- Verbessern der Einhaltung etablierter Sicherheitsverfahren durch interne Überprüfungen und Audits
- Identifizieren und Implementieren von Technologien zum Schutz von Kundendaten
- Einbinden von Sicherheitsexperten anderer Anbieter zur Durchführung von IT-Sicherheitsbewertungen
- Überwachen der Cloud-Dienste auf mögliche Sicherheitsprobleme und Reagieren auf Vorfälle nach Bedarf
- Jährliche Überprüfung der Sicherheitsrichtlinien von Autodesk

13.1 Sicherheitslückenscans und Penetrationstests

Fusion 360-Dienste werden jährlich einem Penetrationstest unterzogen und regelmäßig auf Sicherheitsbedrohungen und Schwachstellen überprüft. Die Anwendung durchläuft auch statische Analysen und durch Drittanbieter durchgeführte Bibliotheksscans. Sicherheitsscans und Penetrationstests decken eine Vielzahl von Schwachstellen ab, die vom Open Web Application Security Project (OWASP) und den SANS-Top-25 definiert sind.

13.2 Netzwerksicherheit

Die Netzwerksicherheit wird durch eine Kombination aus physischen und logischen Kontrollen erzwungen, einschließlich Verschlüsselung, Firewalls und Systemhärtungsverfahren. AWS bietet

außerdem Netzwerksicherheitsfunktionen, die die physischen Rechenzentren schützen. Weitere Informationen finden Sie unter Bewährte Methoden für Sicherheit, Identität und Compliance.

13.3 Verschlüsselung

Der gesamte Netzwerkdatenverkehr wird verschlüsselt, wenn er über das Internet an die Grenzen der Autodesk Cloud-Umgebung übertragen wird. Ruhen vertrauliche Informationen, wie z. B. Anmeldedaten, Anwendungssitzungsinformationen, Zugriffs-Token und Benutzerprofile, werden diese verschlüsselt.

13.4 Datenschutz

Autodesk ist bei der Erfassung und Nutzung personenbezogener Daten von Kunden transparent. Weitere Informationen finden Sie in der Datenschutzerklärung von Autodesk.

14. Ressourcen

Die folgenden Ressourcen enthalten allgemeine Informationen zu Autodesk und anderen Themen, auf die im Hauptabschnitt dieses Dokuments Bezug genommen wird.

- **Autodesk:** Informationen zu Autodesk finden Sie unter http://www.autodesk.de.
- **Autodesk Trust Center:** Informationen zum Autodesk Trust Center finden Sie unter https://www.autodesk.de/trust/overview.
- **Autodesk Fusion 360:** Informationen zu Fusion 360 finden Sie unter https://www.autodesk.de/products/fusion-360.