DATENSICHERHEIT BEI AUTODESK BIM 360

Februar 2019

AUTODESK.

INHALT

- Geltung und Verweise
- Sicherheitszertifikate
- Datenverschlüsselung
- Zugangskontrolle
- Sicherheit des physischen Rechen-zentrums
- Notfallwiederherstellung
- Tests und Prüfungen
- Authentifizierung

GELTUNG UND VERWEISE

Autodesk beschreibt die Maßnahmen zur Datensicherheit für ihre Produkte auf folgender Webseite: https://www.autodesk.com/trust/security

Zusätzlich wird die Datensicherheit in Bezug auf die **BIM 360** Dienste auf folgender Webseite erläutert: https://www.autodesk.com/bim-360/construction-management-software/security. Deren deutsche Übersetzung finden Sie auf den folgenden Seiten in diesem Dokument. Nur der englische originale Wortlaut auf der Webseite ist rechtlich relevant.

Eine umfassende Beschreibung befindet sich im Sicherheits-Whitepaper.

SICHERHEITSZERTIFIKATE

- Vertraulichkeit, Integrität und Verfügbarkeit unserer Kundendaten sind für den Geschäftsbetrieb von entscheidender Bedeutung, und wir nehmen diese Verantwortung ernst.
- Autodesk® BIM 360 basiert auf erstklassigen Cloud-Software-Praktiken und wird von Amazon Web Services (AWS) bereitgestellt, dem weltweit führenden Anbieter von Cloud-Infrastrukturen.
- Autodesk hat den SSAE-16 AT 101 **SOC 2-Attest** sowie die Zertifizierungen **ISO 27001**, **ISO 27017** und **ISO 27018**, um unsere Sicherheitslage zu überprüfen.
- Es werden regelmäßig Audits mit zertifizierten Produkten durchgeführt, um Sicherheit und Verfügbarkeit zu gewährleisten.

DATENVERSCHLÜSSELUNG

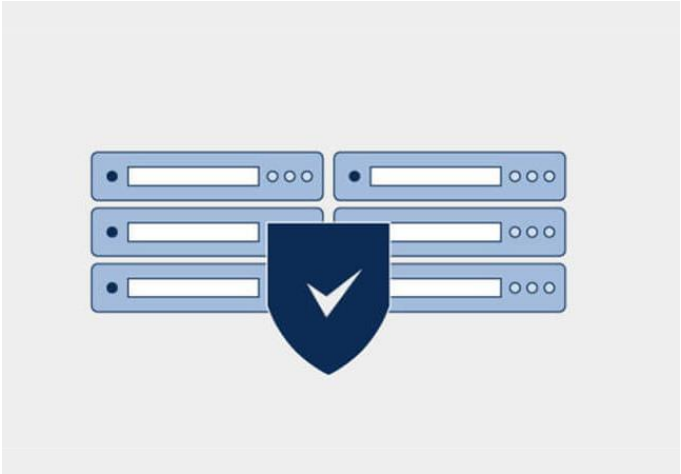
- BIM 360 wurde für die Berücksichtigung der **Privatsphäre ausgelegt**.
- Alle auf BIM 360 hochgeladenen Dateien werden in der Cloud **verschlüsselt gespeichert**. Die Speicherlösung verwendet die erweiterte 256-Bit-Verschlüsselung (AES-256).
- Der **Netzwerkverkehr** mit vertraulichen Informationen wie Anmeldeinformationen und Sitzungstoken wird mithilfe der **TLS-Verschlüsselungstechnologie** sicher übertragen.

ZUGANGSKONTROLLE

- Unsere Cloud-Infrastruktur wird in erstklassigen Datenzentren gehostet, die von unserem **zuverlässigen Partner Amazon Web Services** verwaltet werden.
- Wir verwenden rollenbasierte Zugriffs-steuerungsmethoden, die den privilegierten Zugriff auf die Informationsressourcen basierend auf dem Konzept der **geringsten Privilegien einschränken**.
- Die Zugangsberechtigung erfordert eine Genehmigung durch das Management, das für die Vertraulichkeit, Integrität und Verfügbarkeit verantwortlich ist.

SICHERHEIT DES PHYSISCHEN RECHENZENTRUMS

- Alle Daten werden in sicheren, von Amazon Web Services betriebenen Rechenzentren gespeichert.
- Die Rechenzentren sind durch eine Reihe von Sicherheitskontrollen vor unberechtigtem physischem Zugriff und Umweltgefahren geschützt.
- Das europäische Rechenzentrum von Amazon liegt in Irland.
- Weitere Informationen zur physischen Sicherheit der AWS Rechenzentren befinden sich hier: https://aws.amazon.com/de/compliance/data-center/controls/?nc1=h_ls#Physical_Access



NOTFALLWIEDERHERSTELLUNG

- BIM 360 bietet erstklassigen Service, um sicherzustellen, dass Sie nicht von ungeplanten Ausfällen betroffen sind.
- Falls es trotzdem zu ungeplanten Ausfällen kommt steht Ihnen unser Cloud Operational Team rund um die Uhr (24/7) zur Verfügung, um den vollen Zugriff auf den Dienst so schnell wie möglich wiederherzustellen.
- Die Rechenzentren sind so konzipiert, dass sie System- und Hardwareausfälle verkraften und die Auswirkungen minimal halten.

TESTS UND PRÜFUNGEN

- Unser dediziertes Cloud Security-Team führt regelmäßig Sicherheitsüberprüfungen und Penetrationstests durch und begleitet die externen Prüfungen der BIM 360 Dienste.

- Sicherheits-Scans und Penetrationstests decken ein breites Spektrum an Sicherheitslücken ab, die durch das Open Web Application Security-Projekt (OWASP) und SANS Top 25 (häufigste Softwarefehler) definiert werden.

AUTHENTIFIZIERUNG

- BIM 360 unterstützt SAML (Secure Assertion Markup Language), um die Einmalanmeldung (Single Sign-On) mit Authentifizierungsdiensten zu vereinfachen.

- Wir unterstützen auch die Zwei-Faktor-Authentifizierung, um einem Benutzerkonto während der Anmeldung eine zweite Authentifizierungsebene hinzuzufügen.

AUTODESK®

Make anything™