Tableau Online – Sicherheit in der Cloud

tableau

Inhalt

Betriebssicherheit 4

Systemwartung 4

Datensicherheit und Datenschutz 4

Privacy Shield 5

Datensicherung und -wiederherstellung 5

Disaster Recovery 5

Datenkontrolle 5

Benutzer- und Datenquellenfilter 6

Benutzersicherheit 7

Zugang und Authentifizierung 7

Rollen und Berechtigungen 8

Übertragungssicherheit (Netzwerksicherheit) 9

Verschlüsselung 9

Anwendungssicherheit 9

Mandantenfähige Architektur 10

Verwaltungsdashboard 10

Fazit 10

Einleitung

Die Sicherheit und der Schutz Ihrer Daten sind grundlegend für den Erfolg Ihrer Organisation. Darum genießt ihr Schutz bei Tableau oberste Priorität. Dieses Whitepaper enthält einen Überblick darüber, was Tableau unternimmt, um die Sicherheit und Verfügbarkeit von Kundendaten in Tableau Online zu gewährleisten.

Die auf Tableau Online veröffentlichten Daten sind durch Sicherheitsfunktionen der Enterprise-Ebene geschützt, wie zum Beispiel:

- Physische Sicherheit
- Betriebssicherheit
- Datensicherheit und Datenschutz
- Kontensicherheit
- Sicherheit von Daten während der Übermittlung
- Anwendungssicherheit

All dem liegt eine Infrastruktur zu Grunde, die fortlaufend auf Verfügbarkeit, Leistung, Kapazität und Sicherheit überwacht wird. Das Ergebnis dieser Überwachung wird verwendet, um regelmäßige Verbesserungen einzuführen, die zur Gewährleistung der Geheimhaltung, Integrität und Verfügbarkeit Ihrer Daten beitragen.

Tableau hat ein mehrschichtiges Sicherheitsmodell implementiert, das einen effektiven Schutz gegen ein breites Spektrum bekannter und neu auftretender Bedrohungen bietet. Als Teil von Tableaus Protokoll für den Umgang mit Störfällen wird jede Sicherheitsverletzung über die Trust-Website (https://trust.tableausoftware.com) oder direkt an die betroffenen Kunden gemeldet. Störfallberichte geben Auskunft über Umfang, Schweregrad und Lösung.

Tableau ist fortlaufend bestrebt, einen sicheren, erstklassigen gehosteten Service zu bieten, damit Sie sich auf die Sicherheit Ihrer Daten verlassen können.

Betriebssicherheit

SOC 2 und ISAE 3402

Jedes Jahr erarbeitet Tableau zusammen mit einer unabhängigen Wirtschaftsprüferfirma ein gründliches Audit der Kontrollziele und -aktivitäten für Tableau Online. Tableau ist stolz darauf, bekannt geben zu dürfen, dass die Kontrollverfahren für unseren Tableau Online-Dienst in einem SOC 2 Typ II-Bericht überprüft wurden, der gemäß den Bedingungen des Statement on Standards for Attestation Engagements Nr. 16 (SSAE 16) und dem International Standard on Assurance Engagements (ISAE) Nr. 3402 erstellt wurde. Der SOC 2 Typ II-Bericht für Tableau Online ist auf Anfrage erhältlich.

Rechenzentren

Tableau Online-Dienste werden in unabhängig geprüften Rechenzentren der Enterprise-Klasse mit integrierter Redundanz für alle kritischen Dienste gehostet. Die Rechenzentren sind mit Feuerunterdrückungs- und weiteren Überwachungsanlagen ausgestattet, die Probleme in der Umgebung erfassen und auf sie reagieren, bevor sie einen Ausfall verursachen. Überdies haben die Hostinganbieter Verträge mit externen Dienstleistern geschlossen, die die Fortsetzung des Betriebs im Falle eines längeren Stromausfalls gewährleisten.

Gegen Unterzeichnung einer Geheimhaltungsvereinbarung kann Tableau die Auditberichte für seine Rechenzentrumsanbieter auf Anfrage zur Verfügung stellen. Bitte wenden Sie sich für weitere Informationen an Ihren Tableau Kundenbetreuer.

Systemwartung

Das für die Instandhaltung der Tableau Online-Infrastruktur zuständige Team führt regelmäßige Wartungsarbeiten durch, um die Stabilität, Sicherheit und Leistung der Systeme sicherzustellen. Planmäßige Wartungszeiträume werden mindestens zwei Tage im Voraus auf der Tableau Trust-Website bekannt gegeben. Zusätzlich erhalten Site-Administratoren E-Mail-Benachrichtigungen über anstehende Arbeiten, und für alle Benutzer wird eine Mitteilung angezeigt, wenn sie sich bei der Tableau Online-Website anmelden.

Datensicherheit und Datenschutz

Privacy Shield

In Bezug auf personenbezogene Daten, die sich auf Personen mit Wohnsitz im Europäischen Wirtschaftsraum (EWR) beziehen, ist Tableau zertifizierter aktiver Teilnehmer beim Privacy Shield-Abkommen und unterliegt den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission.

Datensicherung und -wiederherstellung

Von allen kritischen Komponenten werden Backups erstellt. Die Backup-Medien werden verschlüsselt und immer an einem sicheren Ort aufbewahrt. Backups auf Festplatten werden in gesicherten Rechenzentrumsräumen aufbewahrt. Backups bei externen Backup-Anbietern werden sowohl bei der Datenübermittlung als auch im Datenspeicher verschlüsselt. Nur genehmigte Systemadministratoren haben Zugang zu Backups.

Gemäß der Backup-Richtlinie für Tableau Online werden tägliche Backups 31 Tage lang gespeichert.

Mit diesen Backups kann Tableau das gesamte Tableau Online-System wiederherstellen.
Mit den Backups lassen sich derzeit keine einzelnen Kunden-Sites wiederherstellen. Das bedeutet, dass Tableau Arbeitsmappen oder Daten von einzelnen Kunden, die bei anderen Ereignissen außer einem Systemausfall verloren gehen, nicht wiederherstellen kann.

Disaster Recovery

Für jede Instanz des Tableau Online-Dienstes betreibt Tableau primäre und Backup-Rechenzentren an verschiedenen geografischen Standorten. Ist ein primäres Rechenzentrum vorübergehend nicht verfügbar, werden die Systeme an der Backup-Site weiterbetrieben. Dieser wird in diesem Fall für die Bedienung des Produktionsdatenverkehrs umkonfiguriert. Die Daten werden anschließend mit dem letzten Backup wiederhergestellt.

Tableau Online ist eine schreibgeschützte Anwendung. Die Daten werden generell aus Datenquellen geliefert, die von den Kunden verwaltet werden. Daher können Visualisierungen erneut veröffentlicht werden, indem die Informationen direkt von der Quelle bezogen werden, anstatt sie von einem Backup wiederherstellen zu müssen. Das Wiederherstellungspunktziel (Recovery Point Objective, RPO) kann hierdurch drastisch verkürzt werden.

Datenkontrolle

Ihre Daten sind Ihr Eigentum, selbst wenn Sie sie in Tableau Online gespeichert haben. Nur die von Ihnen ermächtigten Personen haben Zugriff auf die an Ihrer Site gespeicherten Daten oder Arbeitsmappen. Mitarbeiter und andere Kunden von Tableau haben keinen Zugriff auf Ihre Daten. Einzige Ausnahme ist eine kleine, kontrollierte Zahl von vertrauenswürdigen Tableau-Administratoren, die für die Verwaltung der Systeme zuständig sind, auf denen der Dienst läuft. Es besteht ein dokumentierter Prozess für die Ermächtigung von Benutzern mit diesem Zugriffsniveau, und alle Zugriffe auf administrativer Ebene werden vierteljährlich überprüft und genehmigt.

Sie sollten allerdings darauf achten, dass Ihre Daten in Ihren eigenen Datenquellen sicher gespeichert werden. Nur Arbeitsmappen, Datenextrakte und zwischengespeicherte Daten werden in Tableau Online gespeichert.

Tableau hat Zugriff auf Kennzahlen, die sich auf die Systemauslastung, den Kontostatus und die Leistung beziehen, und darf diese überwachen. Zu diesen Kennzahlen gehören:

- Belegter Gesamtspeicher nach Konto und nach Benutzer
- Genutzte Gesamtbandbreite nach Konto und nach Benutzer
- Summe der Arbeitsmappen und Ansichten nach Konto und nach Benutzer
- Zugriffsdaten und -uhrzeiten nach Benutzer (Anmeldungen)
- Anzahl und Typ der Datenquellen (z. B. SQL Server, Salesforce.com) nach Konto und nach Benutzer
- Daten und Uhrzeiten der Datenaktualisierungen nach Konto und nach Benutzer
- Leistungsmetriken für die Site

Es gibt vier Möglichkeiten, wie Daten zu Tableau Online gelangen:

1. Durch Veröffentlichung einer Arbeitsmappe, in die die Daten eingebettet sind
2. Durch „Pushen“ der Daten von einer lokalen Quelle an eine Tableau-Datenextraktion Diese Methode führt immer zu einem Datenextrakt, nicht zu einer Echtzeitverbindung. Daher besteht keine Notwendigkeit, ein Virtual Private Network (VPN) oder einen Secure Tunnel in Ihrer Unternehmensumgebung zu erstellen. Für Datenquellen, die Tableau Online nicht direkt erreichen kann, können Sie Datenextrakte veröffentlichen und mithilfe des Tableau Online-Synchronisierungsclients automatische Aktualisierungen planen.
3. Verbindung mit einem Webdienst über eine Anwendungsprogrammierschnittstelle (API). Für die meisten Cloud-Datenquellen, wie Salesforce.com und Google Analytics, wird die API-Verbindung verwendet, um Datenextrakte zu generieren, für die regelmäßige Aktualisierungen geplant werden können.
4. Direktverbindung mit auf einer Cloud-Plattform gehosteten Daten. Für diese Datenquellen kann Tableau Online eine Direktverbindung in Echtzeit oder eine extraktbasierte Verbindung herstellen.

Benutzer- und Datenquellenfilter

Durch Hinzufügen von Benutzer- und Datenquellenfiltern können Sie zusätzliche Sicherheit in Ihren Arbeitsmappen und Datenquellen definieren. Benutzerfilter sind eine Sonderform von Filtern, mit denen Sie einschränken können, welche Daten eine bestimmte Person in einer veröffentlichten Ansicht sehen kann. Bei einem Umsatzbericht, der mit Regionalleitern geteilt wird, können Sie zum Beispiel festlegen, dass nur der Regionalleiter West die Umsätze der Region West sehen darf, der Regionalleiter Ost die Umsätze der Region Ost usw. Anstatt für jeden Regionalleiter eine eigene Ansicht zu erstellen, können Sie einen Benutzerfilter definieren, mit dem jeder Regionalleiter die Daten für eine bestimmte Region sehen kann.

Ein Benutzerfilter wird für ein einzelnes Feld definiert. Benutzer oder Gruppen erhalten die Berechtigung, eine Teilmenge der Elemente in dem betreffenden Feld zu sehen. Im dem Umsatzberichtbeispiel oben wird der Benutzerfilter für das Feld „Region“ definiert, und jedem Regionalleiter wird die Berechtigung zur Ansicht einer entsprechenden Region erteilt.

Datenquellenfilter funktionieren ähnlich wie Benutzerfilter. Mit ihnen können Sie einen Filter mit allgemeiner Gültigkeit für eine veröffentlichte Datenquelle festlegen. Datenquellenfilter können nützlich sein, um die Daten zu beschränken, die Benutzer sehen können, wenn Sie eine Arbeitsmappe oder Datenquelle veröffentlichen. Wenn Sie eine Datenquelle in Tableau Online veröffentlichen, werden die Datenquelle und alle zugehörigen Dateien oder Extrakte in ihrer Gesamtheit an den Server transportiert. Beim Veröffentlichen einer Datenquelle können Sie Zugriffsberechtigungen zum Herunterladen oder Ändern der Datenquelle definieren. Sie können auch auswählen, welche Benutzer und Gruppen externe Abfragen über Tableau Online an der Datenquelle durchführen können. Wenn Benutzer die Abfrageberechtigung, aber keine Berechtigung zum Herunterladen haben, können Sie ein reiches Datenmodell mit berechneten Feldern, Aliasen, Gruppen, Mengen usw. teilen – aber nur für Abfragen.

Benutzer, die diese Datenquelle abfragen, können außerdem nie Datenquellenfilter sehen oder ändern, die bei der ursprünglich veröffentlichten Datenquelle vorhanden sind, obwohl diese Datenquellenfilter auf alle Benutzerabfragen angewandt werden. Dies ist eine fantastische Möglichkeit, um den Zugriff auf eine beschränkte Teilmenge Ihrer Daten zu gewähren.

Benutzersicherheit

Zugang und Authentifizierung

Nur die Benutzer, die Sie ausdrücklich zu Ihrer Site hinzufügen, haben Zugriff auf Ihre Inhalte und Arbeitsmappen. Administratoren, die Sie hierzu ermächtigen, sind für alle Kontoverwaltungsfunktionen zuständig, einschließlich für das Hinzufügen und Entfernen von Benutzern und für das Zuweisen von Berechtigungen. Die Kontoverwaltung liegt vollständig in Ihrer Kontrolle. Wenn ein Benutzer in Ihrer Site nicht mehr ermächtigt ist, müssen Sie ihn einfach nur entfernen, damit er keinen Zugriff mehr auf die in Tableau Online gespeicherten Inhalte hat.

In Tableau Online stehen zwei Authentifizierungsmethoden zur Verfügung. Sie haben die Flexibilität, Ihre Site für die Verwendung einer der beiden Methoden zu konfigurieren.

1. Tableau-Konto

Tableau-Konten werden standardmäßig verwendet und in einem von Tableau gepflegten Identity Store geschützt. Diese Authentifizierungsmethode gibt Site-Administratoren die Möglichkeit, Benutzer schnell und ohne Notwendigkeit der Integration mit einem separaten Identitätsanbieter zu konfigurieren. Die Konten werden von Kunden verwaltet und ermöglichen eine sichere Authentifizierung bei Tableau Online. Das Konto dient auch für den Zugriff auf andere Tableau-Dienste und -Ressourcen wie die Tableau-Website, das Kunden-/Partnerportal von Tableau und die Tableau-Foren.

Die Benutzer werden mit ihrer E-Mail-Adresse als Benutzernamen und einem vom Benutzer ausgewählten Kennwort authentifiziert. Wenn Administratoren einen Benutzer zu ihrer Site hinzufügen, wird dem Benutzer eine E-Mail mit einer Anleitung für die Einrichtung des Kennworts zugesendet. Administratoren legen weder Benutzerkennwörter fest, noch haben sie die Möglichkeit, gespeicherte Kennwörter abzurufen. Kennwörter werden mit einem starken Hash-Algorithmus mit Salt und Hash versehen.

Konten werden nach 10 fehlgeschlagenen Versuchen 10 Minuten lang gesperrt. Mit jeder nachfolgenden Sperre verdoppelt sich die Sperrdauer. Ein Benutzer darf höchstens fünf parallele Sitzungen haben. Die Sitzungen werden nach acht Stunden wegen Zeitüberschreitung geschlossen.

Kennwörter müssen mindestens acht Zeichen lang sein und Buchstaben sowie Ziffern enthalten.

2. SAML

Mit SAML können Administratoren ihre Site unter Verwendung ihres eigenen SAML 2.0-fähigen Identitätsanbieters (IP) für Single Sign-On konfigurieren. Weitere Informationen finden Sie im Abschnitt über Site-Authentifizierung in der Online-Produktanleitung.

Hinweis: Die Funktionen in Bezug auf SAML und Single Sign-On sind derzeit nur auf Anfrage erhältlich. Wenden Sie sich an den Tableau-Support, wenn Sie diese Funktionen anfordern möchten.

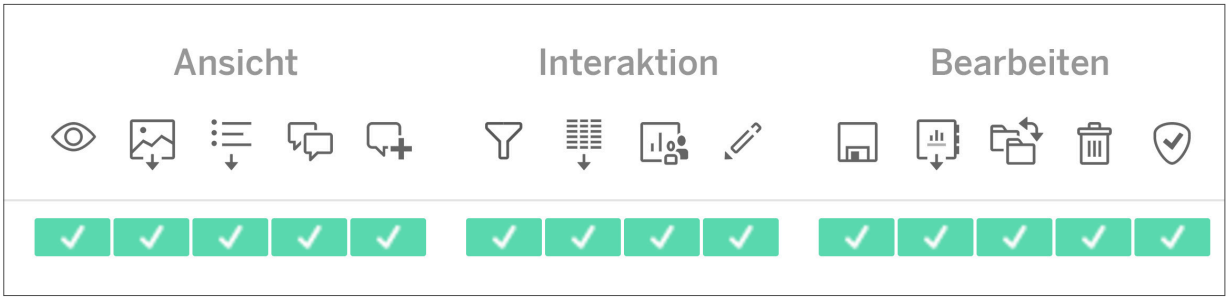
Tableau Online erzwingt nach zwei Stunden Inaktivität eine Zeitüberschreitung einer Sitzung.

Rollen und Berechtigungen

Der Zugriff in Tableau Online wird durch eine Kombination aus Rollen und Berechtigungen für die Site gesteuert. Jeder zu Tableau Online hinzugefügte Benutzer muss eine zugehörige Rolle für die Site haben. Die Rolle für die Site wird vom Administrator zugewiesen und bestimmt über die Zugriffsrechte des Benutzers, zum Beispiel ob der Benutzer in Tableau Online veröffentlichte Inhalte veröffentlichen, mit diesen interagieren oder sie nur anzeigen darf. Weitere Details über Site-Rollen finden sich hier. Berechtigungen werden in Bezug auf Inhalte (Projekte, Arbeitsmappen, Ansichten und Datenquellen) zugewiesen. Die Zuweisung kann für einzelne Benutzer oder Gruppen erfolgen. Wenn Sie Berechtigungen angeben, geben Sie anhand von Regeln an, wer zum Arbeiten mit dem betreffenden Inhalt berechtigt ist.

Berechtigungen können für Aktionen wie Erstellen, Anzeigen, Ändern und Löschen vergeben werden. Einem Projekt zugewiesene Berechtigungen steuern die

Standardzugriffsrechte für alle Arbeitsmappen und Ansichten, die in dem Projekt veröffentlicht werden. Administratoren können Benutzergruppen wie „Finanzbenutzer“ erstellen, um das Verwalten der Berechtigungen zu vereinfachen.



Das Fenster „Berechtigungen“
Es stehen über 20 parametrisierte Anpassungen zur Verfügung, um die Verwaltung der Objektsicherheit zu vereinfachen. Weitere Informationen finden Sie im Kapitel Verwalten von Berechtigungen in der Online-Dokumentation.

Übertragungssicherheit (Netzwerksicherheit)

Verschlüsselung

Die gesamte Kommunikation zwischen dem Client (Tableau Desktop oder unterstützter Browser) und Tableau Online wird mit TLS verschlüsselt, das für den Schutz von Daten während der Übertragung sorgt.

Verbindungen zu Datenquellen können je nach den Verschlüsselungsfähigkeiten der Datenquelle verschlüsselt sein oder auch nicht. Kunden sollten wissen, welche Verschlüsselungsoptionen für die Datenquellen, die sie zu verwenden beabsichtigen, zur Verfügung stehen.

Außerdem enthalten die Tableau-Produkte zahlreiche integrierte Sicherheitsmechanismen zur Vorbeugung gegen Spoofing, Hijacking und SQL-Injection-Angriffe. Tableau testet seine Produkte darüber hinaus aktiv auf Sicherheitslücken und reagiert auf neue Bedrohungen durch regelmäßige Updates.

Sie sollten sich darüber im Klaren sein, dass Funktionen, die E-Mail verwenden (z. B. Abonnement-E-Mails) mit SMTP gesendet werden, das standardmäßig nicht verschlüsselt ist.

Anwendungssicherheit

Anwendungssicherheit ist eine Kombination aus sicheren Designpraktiken. Hierzu gehört unter anderem das Definieren von Sicherheitsanforderungen, die Bedrohungsmodellierung, Codeüberprüfungen und Sicherheitstests. Automatische und manuelle Sicherheitslückentests werden im Zuge des Entwicklungsprozesses durchgeführt. Für die Durchführung von Penetrationstests von Anwendungen vor größeren Releases werden externe Sicherheitsfirmen

hinzugezogen. Tableau hat sich zur Zusammenarbeit mit externen Sicherheitsexperten beim Testen, Aufdecken, Überprüfen und Beheben von Sicherheitsschwachstellen verpflichtet.

Darüber hinaus hat Tableau einen externen Sicherheitslücken-Scanningdienst implementiert, der die dem Internet ausgesetzten Ressourcen und Dienste des Unternehmens (einschließlich Tableau Online) fortlaufend auf Sicherheitslücken untersucht. Jeder Befund generiert eine Warnung, die nach Schweregrad und Auswirkung bewertet ist. Die Priorität etwaiger notwendiger Abhilfemaßnahmen basiert auf dieser Bewertung.

Mandantenfähige Architektur

Tableau Online ist eine mandantenfähige Lösung und bietet keine dedizierte Umgebung für die einzelnen Kunden. Die Anwendung erzwingt die Trennung zwischen Kunden durch logische Partitionierung von Benutzern, Daten und Metadaten nach Site. Alle hochgeladenen oder mit dem Dienst verknüpften Daten werden programmatisch mit dem Kunden verknüpft, der Inhaber der Daten ist. Diese Kontrollen gewährleisten, dass ein Kunde nicht auf die Daten eines anderen Kunden zugreifen kann.

Verwaltungsdashboards

Tableau Online veröffentlicht eine Reihe von Standard-Dashboards, die Nutzungsstatistiken für Ihre Site enthalten. Einige der zur Verfügung gestellten Details umfassen die Benutzeraktivität, die Zahl der Ansichten und die Nutzung der Datenquelle. Administratoren können mithilfe dieser Standard-Dashboards einen Eindruck davon gewinnen, wie ihre Site genutzt wird.

Detaillierte Hinweise über diese Dashboards finden Sie im Abschnitt Verwaltungsansichten im Online-Produkhandbuch.

Fazit

Der Tableau Online-Dienst wird auf der Basis eines robusten Sicherheitsmodells gebaut und betrieben, das Best Practices der Branche einbezieht und von externen Sicherheitsexperten überprüft wird. Tableau ist sich dessen bewusst, wie wichtig Ihre Daten sind, und nimmt die Verantwortung für ihren Schutz sehr ernst.

Über Tableau

Tableau unterstützt Benutzer bei der Umwandlung von Daten in praktisch umsetzbare Erkenntnisse, die den Unternehmenserfolg fördern. Sie können einfach eine Verbindung zu beliebigen Daten herstellen, ganz gleich, wo und in welchem Format sie gespeichert sind. Führen Sie auf schnelle Weise Ad-hoc-Analysen durch, um potenzielle Geschäftschancen zu ermitteln. Erstellen Sie per Drag & Drop interaktive Dashboards mit fortgeschrittenen visuellen Analysen. Anschließend können Sie diese in Ihrem Unternehmen gemeinsam nutzen und so Kollegen die Möglichkeit geben, die Daten aus ihrer Perspektive auszuwerten. Von globalen Unternehmen über neu gegründete Startups bis hin zu kleinen Firmen können Benutzer mit der Analyseplattform von Tableau überall ihre Daten sichtbar und verständlich machen.

Weitere Informationen

Kostenlose Testversion herunterladen

Warum Geschäftsanalysen in der Cloud?

Fünf bewährte Methoden für die Erstellung nützlicher Kampagnen-Dashboards

Alle Whitepapers anzeigen