Smartsheet-Sicherheit

Ein detaillierter Überblick über die Sicherheitsfunktionen, -verfahren und -maßnahmen von Smartsheet

Zusammenfassung

Wir von Smartsheet sind uns darüber im Klaren, dass Software-as-a-Service-Plattformen (SaaS-Plattformen) der Enterprise-Klasse mehrere Schutzebenen und eine Vielzahl von IT-Schutzmaßnahmen und -Steuerelementen anbieten müssen, um sensible Unternehmensdaten zu schützen. Außerdem müssen diese Lösungen flexibel sein und sich in bestehende Datensicherheitssysteme und -prozesse integrieren lassen.

In diesem Whitepaper sollen die Sicherheits- und Governance-Funktionen, -Schutzmaßnahmen und -Praktiken von Smartsheet vorgestellt werden. In erster Linie konzentrieren wir uns auf vom Kunden gesteuerte Funktionen, deren Implementierung Smartsheet empfiehlt, um eine sichere, konforme und gut verwaltete Arbeitsumgebung aufrechtzuerhalten. Hinweis: Dieses Whitepaper umfasst keine Sicherheitsfunktionen, die noch nicht allgemein verfügbar sind.

Überblick

Um Ihre Organisation bestmöglich zu schützen, empfehlen wir die Implementierung von Steuerelementen in drei Fokusbereichen: Identitäts- und Zugriffsmanagement, Daten-Governance und globale Kontokonfiguration. Zusätzlich zu diesen Themen umfasst dieses Dokument allgemeine Informationen in Bezug auf die Sicherheits-, Datenschutz- und Compliance-Praktiken von Smartsheet.

- **Identitäts- und Zugriffsmanagement** konzentriert sich darauf, den Zugriff Ihrer Benutzer auf Smartsheet zu steuern und sicherzustellen, dass die Rolle und Identität der einzelnen Benutzer auf der Plattform Ihrer Organisationsstruktur und Ihren Richtlinien entsprechen. Außerdem geht es darum, wie Sie die Sicherheit bei der Zusammenarbeit mit externen Benutzern basierend auf Ihren Sicherheitseinstellungen gewährleisten.

- **Daten-Governance** muss sowohl auf Benutzerebene als auch über die Organisation hinweg umgesetzt werden. Für Benutzer gilt in Smartsheet standardmäßig das Prinzip der geringsten Privilegien. Zusätzliche Steuerelemente sind verfügbar, um die Sichtbarkeit weiter einzuschränken und zu kontrollieren, sodass Benutzer nur tatsächlich erforderliche Informationen zum tatsächlich erforderlichen Zeitpunkt zu sehen bekommen. Auf Organisationsebene decken wir sowohl einfache Mechanismen wie die sichere Freigabe und Benutzerberichte als auch optionale erweiterte Funktionen wie Datenegressrichtlinien ab.

- **Globale Kontokonfiguration** ermöglicht es Ihnen, die Ästhetik der Smartsheet-Umgebung an die Marke Ihrer Organisation anzupassen. Auch einfache Dinge wie etwa ein visueller Hinweis, dass sich Benutzer in der geschützten Umgebung der Organisation befinden, tragen bereits dazu bei, die Sicherheit zu gewährleisten. Stellen Sie die Konsistenz sicher, indem Sie Branding und Anpassungen festschreiben, sodass jedes einzelne Asset Ihrer Marke entspricht.

- **Sicherheits-, Datenschutz- und Compliance-Praktiken** beziehen sich auf die Aktionen und Schutzmaßnahmen, die Smartsheet außerhalb der Plattform ergreift, um das hohe Maß an Schutz für Kundendaten sicherzustellen. Smartsheet hat branchenführende, tiefgreifende Verteidigungsstrategien durch eine Kombination von Menschen, Prozessen und Technologien implementiert, um die Vertraulichkeit, Integrität und Verfügbarkeit von Smartsheet-Umgebungen und -Assets zu gewährleisten.

Inhaltsverzeichnis

Identitätsmanagement

Die Identität eines Benutzers in Smartsheet und damit dessen Zugriff auf das System zu verwalten, ist genauso wichtig wie das Management der Daten auf der Plattform.

Bereits zu Beginn der Smartsheet-Bereitstellung entscheiden Sie, welche Authentifizierungsmethode Sie verwenden. Smartsheet bietet verschiedene Optionen: Anmeldung per E-Mail und Kennwort oder per Einmalanwendung (SSO) über Google, Microsoft, SAML 2.0-Anbieter und Apple.

Sie können für Ihre Organisation eine oder mehrere Methoden auswählen, wobei wir die Durchsetzung einer einzigen SSO-Authentifizierungsmethode für alle Benutzer und die Deaktivierung der anderen Methoden empfehlen. Wir empfehlen außerdem das Hinzufügen einer weiteren Sicherheitsebene durch Implementierung der Multi-Faktor-Authentifizierung (MFA), wenn Sie Ihr SSO konfigurieren.

Smartsheet verfügt über eine robuste Reihe von REST-APIs. Bei der Smartsheet-API kommt zur Authentifizierung und Autorisierung OAuth 2.0 zum Einsatz. Ein HTTP-Header, der ein Zugriffstoken enthält, ist für die Authentifizierung jeder Anforderung erforderlich. Best Practice für zusätzliche Sicherheit ist die Verwendung von OAuth 2.0 für alle Integrationen, die Sie entwickeln.

Zugriffsmanagement

Benutzer und deren Zugriff zu verwalten, ist eine grundlegende administrative Funktion, die sich sowohl auf die Sicherheit als auch auf die Einführung von Smartsheet in Ihrer Organisation auswirkt. Organisationen müssen das richtige Gleichgewicht finden und sowohl die Zusammenarbeit fördern als auch die Risiken verwalten, die mit der immer stärkeren Verteilung von Daten und Teams einhergehen. Dafür bietet Smartsheet drei unterschiedliche Governance-Modelle, die sich an den primären Möglichkeiten unserer Kunden orientieren, die Anwendung zu verwalten.

Smartsheet-Governance-Modelle

Der erste Ansatz ist unser dezentralisiertes (föderiertes) Modell, bei dem einzelne Geschäftsbereiche direkt ihren eigenen Einkauf und ihre Pläne kontrollieren. Bei diesem Modell ist die IT-Abteilung in der Regel nicht an der Verwaltung beteiligt und die Planabrechnung, Governance und Benutzerverwaltung erfolgen nach Ermessen der jeweiligen Abteilung. Dieses Modell richtet sich in der Regel an Unternehmen, die gerade erst mit der Verwendung von Smartsheet begonnen haben.

Der zweite Ansatz ist das zentralisierte (konsolidierte) Modell, bei dem alle Smartsheet-Pläne in ein einzelnes, von der IT geregeltes Abonnement konsolidiert wurden. Dies bietet direkte Kontrolle über Ausgaben, Benutzerverwaltung und Sicherheitssteuerung. Dieses Modell ist am besten für IT-Teams geeignet, die einen präzisen Überblick über sämtliche Aspekte der Smartsheet-Erfahrung wünschen.

Zu guter Letzt soll unser Hybrid-Modell einen Mittelweg bieten, bei dem die IT-Abteilung organisationsweite Einstellungen mit Enterprise Plan Manager kontrolliert, während die Lizenz- und Benutzerverwaltung direkt von Systemadministratoren der einzelnen Geschäftsbereiche geregelt wird. Die Abrechnung erfolgt ebenfalls nach Plan getrennt und unterstützt die Abrechnung auf Abteilungsebene oder ein Modell, bei dem Ausgaben von Smartsheet in das Budget der einzelnen Abteilungen aufgenommen werden, anstatt zentral von der IT-Abteilung abgerechnet zu werden.

Um hohe Sicherheitsstandards zu gewährleisten, empfiehlt Smartsheet unser Hybrid- oder zentralisiertes Modell, welches Ihnen mehr direkte IT-Kontrolle über Ihren Plan bzw. Ihre Pläne ermöglicht.

Benutzeradministration

Wenn verschiedene Teams in Ihrem Unternehmen Smartsheet unabhängig voneinander für eigene Anforderungen verwenden, können Sie mehrere separate Pläne erstellen. Auch Fusionen und Übernahmen führen möglicherweise zu einer Umgebung mit mehreren Smartsheet-Plänen.

Um Benutzer in diesen Plänen mit dem dezentralisierten Modell zu verwalten, empfehlen wir die Aktivierung der Kontoermittlung für jeden dieser Pläne. Wenn neue Benutzer mit Smartsheet in Berührung kommen, ist es ihnen oder jeder anderen Person der Domäne Ihrer Organisation möglich, eine Liste der Smartsheet-Pläne anzuzeigen, die Ihrem Unternehmen zugewiesen sind. Dies ist eine zentralisierte Möglichkeit, den Beitritt zu einem dieser bestehenden Pläne anzufordern, anstatt einen neuen zu erstellen. Diese Anforderungen werden automatisch zur Überprüfung und Genehmigung (über das Smartsheet Admin Center) an Ihre Systemadministratoren weitergeleitet.

Wenn Sie mehrere separate Pläne haben und Benutzer mit dem zentralisierten Modell verwalten möchten, müssen Sie möglicherweise eine Kontenzusammenführung durchführen. Hinweis: Kunden mit erweiterten Funktionen wie Dynamic View, Connectors und Control Center müssen mit dem Smartsheet-Support zusammenarbeiten, um bei einigen Aspekten der Zusammenführung weitere Unterstützung zu erhalten.

Wenn Sie das Hybrid-Modell und Enterprise Plan Manager verwenden, lautet eine Best Practice, Pläne anhand der Abteilungen/Teams/Kostenstellen zu organisieren. Das ermöglicht Ihnen das Definieren einer Richtlinie, um Benutzer automatisch entsprechend ihrer Zugehörigkeit zu einer dieser Einrichtungen den relevanten Plänen zuzuweisen.

Benutzerverwaltung

Smartsheet ist sich bewusst, dass das einzelne Hinzufügen von Benutzern nicht mehr praktikabel ist, wenn die Nutzung auf Dutzende, Hunderte oder sogar Tausende von Benutzern anwächst. Daher empfehlen wir zu Beginn die Nutzung der Funktion für den Massenimport von Benutzern im Admin Center, mit der sich einfach bis zu 1.000 Benutzer gleichzeitig Ihrer Smartsheet-Organisation hinzufügen lassen. Auf die gleiche Weise können Sie mit der Massenaktualisierung Rollen für bestehende Benutzer massenweise bearbeiten.

Fusionen und Übernahmen gehen oft mit einem Rebranding einher, bei dem Benutzer eine neue E-Mail-Adresse erhalten. Mithilfe der Benutzerzusammenführung können Sie die primäre E-Mail-Adresse von Benutzern massenweise aktualisieren und doppelte Konten löschen.

Ein konsolidierter Smartsheet-Plan bietet zwei zusätzliche Funktionen, um die Benutzerverwaltung weiter zu optimieren und automatisieren.

- Das automatisierte Benutzer-Provisioning (UAP) automatisiert den Prozess des Hinzufügens von Benutzern zu einem Enterprise-Konto. Wenn sich Benutzer mit ihrer Firmen-E-Mail-Adresse bei Smartsheet registrieren oder anmelden, werden Sie automatisch Ihrem Konto hinzugefügt. Zusätzlich haben Sie die Wahl, ob Benutzern Lizenzen gewährt werden sollen oder ob diese dem Konto automatisch als nicht lizenzierte Mitarbeiter (mit kostenlosem Zugriff) beitreten sollen.

    - Wenn Sie unser konsolidiertes Modell verwenden, empfehlen wir die Aktivierung des automatisierten Benutzer-Provisionings, damit Mitarbeiter automatisch dem zentralen, von der IT-Abteilung kontrollierten Konto beitreten.

    - Wenn Sie das Hybrid-Modell verwenden (und wenn Ihr Unternehmen über dokumentierte Abteilungs-/Kostenstelleninformationen für Ihre Benutzerliste verfügt), empfehlen wir die Aktivierung des automatischen Benutzer-Provisionings, da diese Informationen importiert werden können, um Benutzern automatisch den richtigen Plan zuzuweisen, wenn sie eine Lizenz anfordern. Sie können auch verwendet werden, um Bewegungen unlizenzierter Benutzer zwischen verschiedenen Plänen zu automatisieren.

- Verzeichnisintegrationen ermöglichen Ihnen die direkte Synchronisierung Ihrer Benutzer von Microsoft Azure Active Directory (AD) in Smartsheet. Binden Sie Smartsheet in Ihre bestehende Automatisierung in Azure AD ein, um das On- und Offboarding von Benutzern vollständig zu automatisieren und so das Risiko zu minimieren, dass Benutzer in ihren Smartsheet-Konten verweilen oder diese erneut besuchen. Ein weiterer Vorteil sind die in einem Chargeback-Bericht von Smartsheet enthaltenen AD-Attribute auf Benutzerebene wie etwa Abteilung/Kostenstelle/Geschäftseinheit. Der Bericht ist im Admin Center verfügbar und kann zur Optimierung des internen Chargebacks verwendet werden. Empfohlene Best Practice ist die Synchronisierung aller Benutzer im Verzeichnis mit dem Smartsheet-Konto Ihrer Organisation. Dadurch wird verhindert, dass diese Benutzer bei der ersten Anmeldung zusätzliche „Schatten-IT"-Smartsheet-Konten erstellen. Als zweite Sicherheitsebene können Sie auch das automatisierte Benutzer-Provisioning aktiviert lassen, um alle Benutzer abzufangen, die noch nicht über das Verzeichnis synchronisiert werden.

Wenn eine Person Ihre Organisation verlässt, muss ihr Zugriff auf Smartsheet entfernt werden. Dafür bieten wir zwei Möglichkeiten. Wenn Sie einen Benutzer löschen, werden er und seine Assets aus Ihrem Smartsheet-Konto entfernt. Allerdings werden möglicherweise auch Elemente entfernt, die noch in Verwendung sind, wodurch davon abhängige Lösungen möglicherweise nicht mehr funktionieren. Smartsheet empfiehlt stattdessen die Deaktivierung von Benutzern. Dadurch haben diese ebenfalls keinen Zugriff auf Smartsheet mehr, doch die Zugänglichkeit ihrer Inhalte bleibt erhalten, weshalb keine Überlegungen zur Stabilität der Lösung oder zur Übertragung der Inhaberschaft erforderlich sind.

Rollen und Benutzertypen in Smartsheet

Unabhängig von Ihrer Benutzer-Provisioning-Methode müssen Sie Smartsheet-Rollen für die Personen in Ihrer Organisation festlegen.

Hinweis: Eine Rollenzuweisung sorgt nicht dafür, dass die Person Zugriff auf die Smartsheet-Assets in Ihrer Organisation erhält. Die Assets müssen zusätzlich direkt für diese Personen freigegeben werden. Somit bestimmen sowohl die Rolle als auch die Berechtigungen für den Zugriff auf Assets darüber, was Stakeholder in Smartsheet sehen und tun können. Smartsheet unterstützt die folgenden primären Rollen:

- Lizenzierter Benutzer: Verwendung lizenzierter Funktionen, zum Beispiel Erstellen von Sheets.

- Gruppenadministrator: Erstellen und Verwalten von Smartsheet-Gruppen.*

  * Bei einem Gruppenadministrator muss es sich außerdem um einen lizenzierten Benutzer handeln.

- Systemadministrator: Verwalten von Benutzern, Kontoeinstellungen und der Sicherheitssteuerung.

Wir empfehlen ausdrücklich, mindestens zwei aktive Systemadministratoren für das Smartsheet-Konto Ihrer Organisation zuzuweisen, damit es nicht zu Unterbrechungen kommt, falls ein Systemadministrator nicht verfügbar ist.

Gruppenadministratoren können Smartsheet-Gruppen erstellen, die es Benutzern ermöglichen, Inhalte für die gesamte Gruppe anstatt für einzelne Mitglieder freizugeben. Gruppenadministratoren können nur Gruppen verwalten, die sie besitzen. Falls zur Einschränkung der Zusammenarbeit mit externen Mitarbeitern erforderlich, lässt sich die Gruppenmitgliedschaft auf Stakeholder in Ihrer Organisation beschränken.

Wenn Sie einem Benutzer keine der oben aufgeführten Rollen zuweisen, wird sein Zugriff auf die Smartsheet-Assets (Sheets, Berichte, Dashboards oder WorkApps) eingeschränkt, die für ihn freigegeben wurden. Stakeholder müssen lizenzierte Benutzer sein, um Smartsheet-Assets zu erstellen, und können dann direkt über die Smartsheet-App eine Lizenz anfordern. Systemadministratoren können Anforderungen einzeln oder massenweise im Abschnitt Lizenzanforderungsmanagement im Admin Center nachverfolgen und bearbeiten. Wenn Sie bereits einen Vorgang für die Verwaltung von Lizenzanforderungen etabliert haben, profitieren Sie möglicherweise von einem benutzerdefinierten Upgrade-Bildschirm, der Benutzer zum Einreichen ihrer Lizenzanforderung auf diese internen Prozesse verweist.

Externe Mitarbeiter

Alle Stakeholder, die sich außerhalb Ihrer Domäne befinden und für die Ihre Smartsheet-Assets freigegeben wurden, gelten als externe Mitarbeiter. Smartsheet ermöglicht Ihrer Organisation die uneingeschränkte Zusammenarbeit mit beliebigen vertrauenswürdigen externen Parteien, ohne dass für diese externen Mitarbeiter Kosten anfallen. Um die Sicherheit bei der Zusammenarbeit mit externen Mitarbeitern sicherzustellen, empfehlen wir den Einsatz drei zentraler Admin-Steuerelemente:

Sichere Freigabe ermöglicht Ihnen die Angabe bestimmter Domänen oder E-Mail-Adressen, die vertrauenswürdig und für die Zusammenarbeit mit externen Mitarbeitern autorisiert sind.

Berichte zum Sheetzugriff bieten eine Liste der externen Mitarbeiter, die Zugriff auf die Smartsheet-Inhalte Ihrer Organisation haben.

Zugriff auf Elemente widerrufen – zentral über das Admin Center, sodass externe Mitarbeiter von Inhalten entfernt werden, auf die sie nicht mehr zugreifen müssen.

Daten-Governance

Effektive Daten-Governance ist für moderne Unternehmen unerlässlich, um sicherzustellen, dass Informationen im Besitz der Organisation in Übereinstimmung mit geltenden Vorschriften, Unternehmensrichtlinien und branchenbasierten Best Practices erstellt, verwendet, freigegeben und geschützt werden.

Diese Steuerelemente sind nicht nur aus regulatorischen Gründen erforderlich, sondern gewährleisten außerdem die Effizienz, Vertraulichkeit des Geschäfts und Geschäftskontinuität:

Auf Benutzerebene muss die Organisation effektive Tools bereitstellen, um die Sichtbarkeit einzuschränken, damit nur relevante Stakeholder relevante Informationen zu sehen bekommen.

Auf Organisationsebene muss das Unternehmen mit anwendbaren Tools für eine effektive Erstellung und Durchsetzung von Richtlinien ausgestattet sein.

Daten-Governance auf Benutzerebene

Die meisten Benutzer sind mit den Berechtigungsstufen in Smartsheet (Betrachter, Bearbeiter, Administrator und Inhaber) vertraut. Dynamic View und WorkApps bieten zusätzliche, detailliertere Steuerelemente und eine höhere Flexibilität, um effektive Daten-Governance-Funktionen auf Benutzerebene zur Verfügung zu stellen. Die Einschränkung des Zugriffs auf die relevantesten Inhalte fördert die Prozesseffizienz (da sich Benutzer auf die Elemente konzentrieren müssen, die ihre Aufmerksamkeit erfordern), gewährleistet aber außerdem die Sicherheit, indem das von Smartsheet verfolgte Prinzip der geringsten Privilegien standardmäßig auf einer detaillierteren Ebene angewendet wird.

Dynamic View

Nicht alle Geschäftsprozesse erfordern vollständige Transparenz. Bei vielen Prozessen – Auftragsmanagement, Zusammenarbeit mit Anbietern, Projekte, an denen sowohl interne als auch externe Teams beteiligt sind – muss engmaschig kontrolliert werden, welche Inhalte für wen freigegeben werden.

Dynamic View ermöglicht die Zusammenarbeit ohne Kompromisse bei der Vertraulichkeit. Mit Dynamic View können Sheetinhaber relevante Zeilen und Felder selektiv für bestimmte Mitarbeiter freigeben, ohne die zugrunde liegenden Sheets freizugeben. Dies ermöglicht verschiedene Anwendungsfälle, bei denen bestimmte Unternehmensbenutzer Elemente selektiv für Anbieter, gemischte interne und externe Teams oder organisationsübergreifend freigeben und zur Zusammenarbeit nur in bestimmten Bereichen einladen können. Alle haben Zugriff auf die erforderlichen Informationen – und zwar ausschließlich darauf.

WorkApps

WorkApps ermöglichen es Ihnen, Ihre Arbeit zu optimieren und die Zusammenarbeit unter Verwendung benutzerfreundlicher Apps zu vereinfachen, die direkt aus Sheets, Formularen, Dashboards, Berichten und mehr erstellt werden. Sie können das jeweilige App-Erlebnis auf Ihre Teammitglieder basierend auf der Rolle der einzelnen Personen zuschneiden und ausgehend von denselben zugrunde liegenden Datensätzen zusammenarbeiten. Apps werden mit derselben mehrstufigen Sicherheit der Enterprise-Klasse wie die Smartsheet-Plattform skaliert.

WorkApps beseitigen die Notwendigkeit, die in der WorkApp enthaltenen Assets freizugeben. Sie können eine WorkApp mit einer gefilterten Ansicht ausgewählter Sheets und Berichte erstellen, ohne dass diese Sheets oder Berichte für die Endbenutzer freigegeben werden müssen. Den Benutzern wird nur die „WorkApp“-Ansicht dieser Assets angezeigt.

Steuerelemente für Daten-Governance-Richtlinien auf Organisationsebene

Smartsheet ermöglicht es Administratoren, sicherzustellen, dass die Funktionen der Plattform in Übereinstimmung mit den Governance-Richtlinien der Organisation verwendet werden. Mithilfe dieser Steuerelemente implementieren Administratoren gute Leitlinien für die Daten-Governance, um sicherzustellen, dass Daten korrekt und nur von Personen verarbeitet werden, die mit diesen Daten umgehen müssen.

Administratoren legen selbst fest, wie Benutzer mit bestimmten Funktionen interagieren sollen. Sollen Sheetinhaber in der Lage sein, ihre Sheets zu veröffentlichen und neue Automatisierungen zu erstellen? Haben Sie ein bestimmtes Speichersystem, von dem aus Dateien angehängt werden müssen? Sollen externe Mitarbeiter in der Lage sein, für sie freigegebene Inhalte herunterladen? Dies sind einige Beispiele für Fragen, die sich Administratoren stellen sollten, um effektiv die geeigneten organisationsweiten Steuerelemente für die Implementierung zu evaluieren.

Diese Richtlinien erstrecken sich auch auf die sichere Freigabe. Wenn Sie die Freigabe von Daten und Assets auf bestimmte Domänen oder E-Mail-Adressen einschränken möchten, handelt es sich um das passende Tool. Wie bereits erwähnt wird anhand der sicheren Freigabe auch festgelegt, ob Ihre Organisation Smartsheet-Elemente für andere Organisationen wie Anbieter und Partner freigeben kann.

Steuerung des Widgets für Webinhalte

Dashboards unterstützen die Möglichkeit, interaktive Inhalte (Videos, Diagramme, Dokumente und mehr) einzubetten. Administratoren haben die Möglichkeit, diese Funktion zu aktivieren oder deaktivieren und eine genehmigte Liste unterstützter Domänen für das Widget für Webinhalte zu definieren. Als Best Practice empfehlen wir, dies auf interne Unternehmensdomänen zu beschränken.

Automatisierungsberechtigungen

Steuern Sie, wer Automatisierungen von Sheets erhalten kann. Die Optionen sind organisiert von „Eingeschränkt“ (aktiviert Aktionen nur für Benutzer, für die das Sheet freigegeben ist) bis hin zu „Uneingeschränkt“ (Automatisierung gilt für sämtliche E-Mail-Adressen und Drittanbieterintegrationen, wie z. B. Slack). Wir empfehlen die Überprüfung dieser Steuerung, um sicherzustellen, dass die Konfiguration mit dem von Ihrer Organisation gewünschten Maß an interner und externer Zusammenarbeit übereinstimmt.

Anlagensteuerung

Legen Sie fest, ob Planmitglieder Dateien von ihrem eigenen Computer oder von Cloud-Speicherservices von Drittanbietern wie Google Drive, OneDrive, Box, Dropbox, Evernote oder Egnyte durch das Anhängen eines Links (URL) hochladen können. Um die Aufnahme von Daten aus nicht genehmigten Quellen zu verhindern, aktivieren Sie nur die Anbieter von Anlagen, die gemäß den internen Richtlinien Ihres Unternehmens genehmigt wurden.

Veröffentlichungssteuerung

Durch das Veröffentlichen eines Sheets, Berichts oder Dashboards werden eine eindeutige URL, auf die jeder zugreifen kann, ohne sich bei Smartsheet anzumelden, sowie ein iframe-Code erzeugt, den Sie in den Quellcode einer Website einbetten können, um das Sheet oder den Bericht dort anzuzeigen.

Sie können die Veröffentlichung von Sheets, Berichten, Dashboards und iCal untersagen – in diesem Fall wird die Schaltfläche „Veröffentlichen“ nicht mehr auf dem Smartsheet-Asset angezeigt. Sie können außerdem den Zugriff auf veröffentlichte Elemente auf Personen in Ihrer Smartsheet-Organisation beschränken. Uns ist aufgefallen, dass sicherheitsbewusste Kunden in der Regel die Veröffentlichung zulassen, aber den Zugriff auf veröffentlichte Elemente auf Personen in ihrem Konto beschränken.

Sichere Freigabe

Mit dieser Funktion können Sie die Freigabe nach Domäne oder nach spezifischer E-Mail-Adresse einschränken (z. B. um sicherzustellen, dass Sheets nur für Personen freigegeben werden, die eine E-Mail-Adresse des Unternehmens haben). Smartsheet empfiehlt ausdrücklich die Implementierung der sicheren Freigabe, um die Zusammenarbeit mit externen Mitarbeitern zu kontrollieren. Um Aktualisierungen und die Pflege Ihrer sicheren Freigabeliste zu vereinfachen, empfehlen wir außerdem, angeforderte Aktualisierungen in einem Smartsheet-Webformular zu erfassen.

Steuerung von Offline-Formulareinreichungen

Bei Verwendung der Mobil-App aktiviert Smartsheet automatisch die Offline-Einreichung von Formularen, um Anwendungsfälle zu unterstützen, in denen Benutzer möglicherweise keine konsistente Verbindung haben (z. B. auf einer Baustelle). Dieses Steuerelement ermöglicht es Administratoren, die Offline-Einreichung von Formularen zu deaktivieren (oder wieder zu aktivieren), um zu kontrollieren, ob ein Benutzer die Mobil-App ohne Verbindung starten kann, um Formulare zu übermitteln.

Steuerung der Kommunikationsintegration

Von Smartsheet unterstützte Kommunikationsservices sind Google Chat, Microsoft Teams, Slack und Cisco Webex. Kontoadministratoren können nach eigenem Ermessen einen Service oder mehrere Services aktivieren.

Protokollierung und Berichterstattung

Sie können Berichte herunterladen, die verschiedene Aspekte der Smartsheet-Nutzung über Ihre Organisation hinweg abdecken, um kontinuierliche Einblicke in die Nutzung, Benutzer, Inhalte, Abrechnung und den Zugriff im Zusammenhang mit Smartsheet zu erhalten:

Bericht zum Sheetzugriff

Generiert eine Excel-Datei mit den Namen aller Sheets, Berichte und Dashboards im Eigentum der lizenzierten Benutzer im Konto, den Namen des Arbeitsbereichs, in dem diese Elemente gespeichert sind (falls zutreffend), sowie den Mitarbeitern, für die das jeweilige Sheet freigegeben ist, und dem Zeitstempel der letzten Änderung. Wir empfehlen die regelmäßige Überprüfung dieses Berichts, um die Liste der externen Mitarbeiter zu prüfen, die Zugriff auf Assets im Eigentum der Personen in Ihrer Organisation haben.

Bericht über veröffentlichte Elemente

Generiert eine Excel-Datei mit allen veröffentlichten Elementen. Gut geeignet für die Datensicherheit oder um nachzuverfolgen, wer bestimmte Elemente veröffentlicht hat. Anhand dieses Berichts können Sie die Konfiguration der Veröffentlichungssteuerung nach Bedarf festlegen.

Benutzerlistenbericht

Generiert eine Excel-Datei mit allen Mitgliedern (sowohl eingeladen als auch aktiv) des Kontos, einem Zeitstempel für den Zeitpunkt der Hinzufügung zum Konto, ihren Zugriffsstufen (Systemadministrator, Gruppenadministrator usw.), der Anzahl der Sheets im Eigentum sowie dem Zeitstempel für ihre letzte Anmeldung bei Smartsheet.

Bericht über Anmeldeverlauf

Systemadministratoren in Mehrbenutzerkonten können über das Admin Center eine Excel-Datei mit einer Liste der aktuellen Anmeldehistorie erhalten, um zu sehen, welche Benutzer in Ihrem Konto sich kürzlich angemeldet haben.

Chargeback-Bericht

Der Chargeback-Bericht ist im Admin Center verfügbar und kann von Kunden, die die Directory-Integration verwenden, zur Optimierung des internen Chargebacks genutzt werden. Hierdurch werden dem vorhandenen Bericht Spalten für Geschäftseinheit, Abteilung und Kostenstelle hinzugefügt, wenn Kunden ihre Benutzerliste herunterladen, und die für die interne Chargeback-Berichterstattung erforderlichen Daten bereitgestellt.

Für die weitere detaillierte Nachverfolgung von Benutzeraktionen auf Sheet-, Dashboard- und Zellenebene stehen Ihnen das Aktivitätsprotokoll, der Zellenverlauf und Systemspalten zur Verfügung.

- **Aktivitätsprotokoll:** Bietet ein Audit-Protokoll der Änderungen, die an einem Asset vorgenommen wurden, sowie der Person, die sie vorgenommen hat, und den Zeitpunkt der Änderungen. Dies beinhaltet Bearbeitungen wie das Löschen von Zeilen (einschließlich der gelöschten Daten), die Person, die das Element angezeigt hat, und die Angabe, ob Änderungen an Freigabeberechtigungen vorgenommen wurden.

- **Zellenverlauf:** Zeigt ein Protokoll der Änderungen auf Zellebene sowie die Person, die sie vorgenommen hat, deren Rolle und den Zeitpunkt der Änderungen an. Benutzer können einfach Daten aus dem Zellenverlauf kopieren und einfügen, um frühere Informationen wiederherzustellen, die unter Umständen fälschlicherweise gelöscht oder geändert wurden.

- **Systemspalten:** Zeigt den Zeitpunkt der letzten Bearbeitung jeder Zeile sowie den Mitarbeiter an, der die Änderung vorgenommen hat.

Erweiterte Steuerung der Daten-Governance

Smartsheet bietet einige erweiterte Funktionen, die Kunden mit besonders strengen Datenschutzanforderungen die Daten-Governance-Steuerung ermöglichen. Diese Funktionen sind in Smartsheet Advance Platinum und Smartsheet Safeguard enthalten.

Vom Kunden verwaltete Verschlüsselungsschlüssel

Smartsheet verwendet Verschlüsselung, um die Daten von Kunden zu schützen und ihnen zu helfen, die Kontrolle über sie zu behalten. Vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) sind für Organisationen gedacht, die über sensible oder regulierte Daten verfügen, für die sie ihren eigenen Verschlüsselungsschlüssel verwalten müssen. CMEK ermöglichen es Enterprise-Organisationen, Cloud-SaaS-Anwendungen zu verwenden und zugleich eine Datensteuerung aufrechtzuerhalten, die mit der einer lokalen

Installation vergleichbar ist. So wird dem Datenspeicher in Smartsheet eine vom Kunden verwaltete Verschlüsselungsebene hinzugefügt, um erweiterte Datensicherheits- und Governance-Richtlinien zu fördern.

Hinweis: Um CMEK zu verwenden, brauchen Kunden Zugriff auf Amazon Web Services Key Management Service (AWS KMS), da Kundenschlüssel direkt in AWS eingerichtet und verwaltet werden.

Smartsheet verwendet CMEK, um die Daten Ihrer Organisation so zu verschlüsseln, dass sie jederzeit unter Ihrer Kontrolle bleiben. Genauer gesagt speichert oder kontrolliert Smartsheet diese Verschlüsselungsschlüssel nicht und muss diese Schlüssel vom AWS Key Management Service (KMS) des Kunden anfordern und abrufen, wenn auf Ihre Sheetdaten zugegriffen werden muss.

Da Ihre Organisation die im AWS Key Management System gespeicherten CMEK kontrolliert, können Sie Smartsheet den Zugriff auf die CMEK und damit den Zugriff auf Ihre Daten jederzeit verweigern. Durch die Zerstörung der Hauptschlüssel im AWS Key Management System kann Ihre Organisation Ihre Daten effektiv aus den Smartsheet-Systemen löschen. Eine böswillige Partei könnte mit CMEK verschlüsselte Daten auch mit einer Kopie der Datenbank, des Quellcodes und der Cloud-Verschlüsselungsschlüssel von Smartsheet nicht lesen.

Datenegressrichtlinien

Die Datenfreigabe birgt immer ein gewisses Maß an Risiko in sich, doch beim Umgang mit besonders vertraulichen Daten muss unbedingt sichergestellt werden, dass Unternehmensdaten in Ihrem Konto und unter Ihrer Kontrolle bleiben.

Systemadministratoren können Datenegressrichtlinien zum Schutz vertraulicher Daten verwenden, indem sie detailliert steuern, wie Daten sowohl innerhalb als auch außerhalb Ihrer Organisation exportiert werden können.

Datenegressrichtlinien können implementiert werden, um zu verhindern, dass interne und externe Mitarbeiter die folgenden Aktionen in Sheets, Berichten und Dashboards durchführen:

- Als neu speichern
- Als Vorlage speichern
- Als Anlage senden
- Veröffentlichen
- Drucken
- Exportieren

Benutzer, die versuchen, eine eingeschränkte Aktion auszuführen, erhalten eine Benachrichtigung, dass dieses Verhalten aufgrund der von Ihrer Organisation implementierten Datenegressrichtlinie untersagt ist.

Diese Einschränkungen sollen Mitarbeiter daran hindern, vertrauliche Informationen zu böswilligen Zwecken zu speichern oder freizugeben.

Ereignisberichte

Um die Informationssicherheit zu gewährleisten, benötigen viele Unternehmen kontinuierliche Einblicke in die Art und Weise, auf die ihre Geschäftsanwendungen wie Smartsheet verwendet werden. Die Transparenz folgender Aspekte sollte sichergestellt werden:

- Wer Sheets erstellt
- Wer Arbeitsbereiche erstellt
- Wer Objekte löscht
- Wer für wen ein Sheet freigegeben hat

Ereignisberichte bieten detaillierte Einblicke in das Benutzerverhalten und Aktivitäten innerhalb des Smartsheet-Kontos Ihrer Organisation. Mit dieser Funktion können Sie Datenverluste überwachen und ungewöhnliche Nutzungsmuster identifizieren, um die Sicherheits- und Compliance-Richtlinien Ihrer Organisation besser durchzusetzen.

Ereignisberichte bieten einen JSON-Datenfeed von Smartsheet-Nutzungsereignissen („Ereignissen“) in einem Plan (Organisation) und werden über die Ereignisberichte-API abgerufen. Bei dem Service werden zu mehr als 120 Ereignissen in Smartsheet Berichte erstellt und ab dem Datum, an dem der Feed aktiviert wird, bis zu sechs Monate lang Daten gespeichert.

Um von diesem Feed zu profitieren, werden Ereignisberichte in der Regel in andere Sicherheitssysteme integriert, die Überwachung, Benachrichtigungen, Richtlinienerstellung und -durchsetzung und Schutz vor Datenverlusten (DLP) bieten. Diese App werden von Drittanbietern verkauft – in der Regel Cloud Access Security Broker Systems (CASB-Systeme), Security Information and Event Management Systems (SIEM-Systeme) oder eine Kombination aus CASB- und SIEM-Systemen. Ab und zu entwickeln Unternehmen ihre eigenen Überwachungs- und Reaktionssysteme, anstatt auf die Systeme von Drittanbietern zurückzugreifen.

Wichtige Anwendungsfälle für Ereignisberichte:

- Schutz vor Datenverlusten
- Umgang mit personenbezogenen Daten
- Daten-Governance
- Einblicke in die Zusammenarbeit gewinnen

Datenspeicherungssteuerung

Je mehr Inhalte Ihre Organisation in einer SaaS-Anwendung aufbewahrt, desto größer ist das Risiko, dem Ihr Unternehmen ausgesetzt ist.

Die Datenspeicherungssteuerung von Smartsheet gibt Organisationen die Möglichkeit, eine Richtlinie zu erstellen, die basierend auf durchzusetzenden Kriterien vorschreibt, wann Inhalte gelöscht werden sollen.

Diese Richtlinien können auf dem Datum basieren, an dem ein Sheet erstellt oder das letzte Mal geändert wurde, um sicherzustellen, dass nur aktive oder aktuelle Inhalte in Ihrer Smartsheet-Instanz verbleiben und Ihr Risikoprofil eingeschränkt wird.

Globale Kontokonfiguration

Die Kontosicherheit ist nicht auf technische Funktionen wie die Datenverschlüsselung, die Klassifizierung oder Authentifizierungsoptionen beschränkt. Sicherheit kann auch einen so einfachen Vorgang wie die Anbringung des Logos Ihrer Organisation auf sämtlichen zugehörigen Elementen beinhalten.

Steuerelemente für die globale Kontokonfiguration ermöglichen Ihnen die Implementierung eines visuellen Brandings (und weiterer Einschränkungen), damit Ihre Benutzer wissen, dass Sie auf die richtigen Informationen zugreifen.

Systemadministratoren können Logos global hinzufügen, um Ihre Smartsheet-Bereitstellung an organisationsweiten Branding-Anforderungen auszurichten. Mit der Branding-Sperre stellen Sie sicher, dass jedes neue Asset mit dem gleichen Branding versehen wird.

Steuerelemente für die Anpassung und Kontokonfigurationen von Smartsheet ermöglichen es Ihnen außerdem, benutzerdefinierte Willkommensbildschirme festzulegen. Sie können benutzerdefinierte Hilfe-Bildschirme mit Beschreibungen der ersten Schritte, Lizenzanforderungsbildschirme, über die Benutzer Sie kontaktieren können, oder benutzerdefinierte Willkommensbildschirme mit Branding, die bei der Benutzeranmeldung angezeigt werden, festlegen. Diese Bildschirme können die Anforderung enthalten, dass ein Benutzer den Vertragsbedingungen zustimmen muss, bevor er auf weitere Informationen zugreift.

Wenn Sie eine konsistente visuelle Identität mit benutzerdefinierten Informationen kombinieren, wissen Benutzer, dass sie auf die richtigen Tools und Informationen zugreifen, was die Sicherheit optimiert.

Sicherheits-, Datenschutz- und Compliance-Praktiken von Smartsheet

Die Cybersicherheits-, Datenschutz- und Datensicherheitsprogramme bei Smartsheet basieren auf einem ganzheitlichen Ansatz und beginnen mit strategischen Informationssicherheitsrichtlinien, die vom Smartsheet Information Security Steering Committee (ISSC) und der Unternehmensführung definiert und unterstützt werden. Diese Richtlinien wurden so konzipiert, dass sie mit den strategischen Risikomanagementpraktiken des Unternehmens übereinstimmen, Sicherheitsrisiken proaktiv verwalten und überwachen, die Sicherheit durch Prozessreife und eine effektive Systemarchitektur fördern und die Benutzer mittels Schulungen und Sensibilisierung in die Lage versetzen, umsichtige Entscheidungen über Sicherheitsrisiken zu treffen.

Datensicherheit

Wir haben die Sicherheit direkt in unsere Plattform integriert, um sicherzustellen, dass Ihr wichtigster Vermögenswert – Ihre Daten – geschützt wird. Smartsheet beauftragt Drittanbieter mit der Durchführung von Audits unserer Sicherheitspraktiken, einschließlich einer Beurteilung und Bescheinigung nach SOC 2 Typ II, und technischer Sicherheitsbeurteilungen durch externe Penetrationstestfirmen. Darüber hinaus automatisiert das Schwachstellenmanagement-Programm von Smartsheet die Identifizierung und Behebung von Netzwerk- und Systemschwachstellen in Smartsheet-Unternehmens- und Produktionsumgebungen. Smartsheet verwendet eine Verschlüsselung, um Ihre Daten zu schützen und Ihnen zu helfen, die Kontrolle über sie zu behalten. Darauf können Sie sich bei Smartsheet verlassen: Alle Daten werden mit vom National Institute of Standards and Technology (NIST) genehmigten Verschlüsselungen, Technologie für Transportschichtsicherheit (TLS), AES-256-Bit-Verschlüsselung von Daten im Ruhezustand und dem Amazon-S3-Service für die Speicherung und Bereitstellung hochgeladener Dateien dauerhaft gespeichert.

Datenschutz

Wir bei Smartsheet wissen, wie wichtig der Schutz Ihrer Daten ist, und respektieren Ihr Recht, zu wissen, wie Informationen über Sie erfasst und verwendet werden. In unserem Datenschutzhinweis wird beschrieben, wie Smartsheet über unsere Websites, Mobilanwendungen und die Smartsheet-Arbeitsausführungsplattform gesammelte personenbezogene und andere Informationen erfasst, verwendet und weitergibt.

- Wir erkennen die Datenschutzrechte unserer potenziellen Neukunden, Kunden und Partner an und halten uns an weltweite Datenschutzbestimmungen, einschließlich der Datenschutz-Grundverordnung der Europäischen Union (DSGVO).

- Wir bieten eine Datenverarbeitungsvereinbarung für Kunden, die spezifische Bedingungen für die Verarbeitung von Inhalten mit personenbezogenen Daten benötigen. Wenn Sie ein DPA mit Smartsheet durchsetzen möchten, können Sie unter smartsheet.com/legal/DPA ein Formular einreichen, in dem Sie den Bedingungen des DPA zustimmen.

Betriebsmanagement

Wir haben Richtlinien und Methoden implementiert, um sicherzustellen, dass Ihre Daten geschützt und an mehreren physischen Standorten gesichert sind. Unsere Teams untersuchen kontinuierlich neue Sicherheitsbedrohungen und implementieren aktualisierte Gegenmaßnahmen, um nicht autorisierten Zugriff auf den Abonnementdienst zu verhindern oder nicht geplante Ausfälle zu vermeiden. Der Zugriff auf alle Smartsheet-Produktionssysteme und -Daten ist auf der Grundlage des Prinzips der geringsten Privilegien und des tatsächlichen Informationsbedarfs auf autorisierte Mitglieder des Smartsheet-Teams für den technischen Betrieb beschränkt. Smartsheet veröffentlicht Systemstatusinformationen auf der Smartsheet-Statusseite. Smartsheet informiert Kunden in der Regel per E-Mail und/oder Textnachricht über bedeutende Systemvorfälle, wenn sie sich auf der Smartsheet-Statusseite für automatische Aktualisierungen registriert haben.

Datencenter-Sicherheit, -Kontinuität und -Redundanz

Wir arbeiten mit branchenweit anerkannten Hostingpartnern zusammen, um sicherzustellen, dass Sie Dienste für Ihre Organisation zuversichtlich mit einer zuverlässigen Plattform bereitstellen können. Wir verfügen über standortübergreifende Datenredundanz, hosten an AWS-Standorten und unsere Standorte sind gemäß SOC 1, SOC 2, ISO 27001 und FISMA geprüft und zertifiziert. Unsere Überwachung beinhaltet biometrische Scanprotokolle, kontinuierliche Aufsicht und die Verwaltung der Produktionsumgebung rund um die Uhr. Smartsheet erhält interne Prozesse und Pläne aufrecht, um mit Ereignissen in Bezug auf die Geschäftskontinuität und Szenarien im Zusammenhang mit der Notfallwiederherstellung umzugehen. Diese Pläne werden jährlich überprüft und getestet und in der gesamten Organisation an entsprechendes Personal weitergegeben. Unsere Rechenzentren sind geografisch (ungefähr 970 km) voneinander isoliert, um zu verhindern, dass bei einer großflächigen Naturkatastrophe mehrere Rechenzentren gleichzeitig beeinträchtigt werden.

Audits und Zertifizierungen

Die folgenden sicherheits- und datenschutzbezogenen Audits und Zertifizierungen gelten für grundlegende Anwendungsservices in Smartsheet.

- **SOC 2/SOC 3:** Smartsheet wird jährlich im Rahmen des SOC-Auditprozesses geprüft und getestet. Die sich daraus ergebenden externen Auditberichte bescheinigen die Konzeption und operative Wirksamkeit interner Steuerelemente in unserem gesamten Unternehmen, einschließlich Sicherheit, Verfügbarkeit und Vertraulichkeit.

- **Zertifizierung nach EU-U.S. Privacy Shield und Swiss-U.S. Privacy Shield:** Kundendaten, die an die abgedeckten Services übermittelt werden, fallen unter eine jährliche Zertifizierung nach dem EU-U.S. Privacy Shield Framework und dem Swiss-U.S. Privacy Shield Framework, wie sie vom Handelsministerium der Vereinigten Staaten verwaltet werden. Die aktuelle Zertifizierung ist unter privacyshield.gov/list zu finden, wenn nach „Smartsheet“ gesucht wird.

- **FedRAMP (Moderate):** Smartsheet wurde für das FedRAMP Connect-Programm durch das Joint Authorization Board (JAB) ausgewählt, welches Smartsheet Gov basierend auf der Nachfrage von Regierungsbehörden priorisierte. Smartsheet Gov ist eine separate Smartsheet-Umgebung, die von FedRAMP autorisiert wurde, sodass es für die US-Regierung einfacher wird, Smartsheet zur Verwaltung ihrer Arbeit zu nutzen und gleichzeitig leichter ihre Sicherheits- und Compliance-Anforderungen zu erfüllen.

- **Sarbanes-Oxley Act von 2002:** Smartsheet ist ein öffentliches Unternehmen und unterliegt den Bestimmungen des Sarbanes-Oxley (SOX). Die SOX-Compliance unterstützt beim Aufbau eines kohärenten internen Teams und verbessert die Kommunikation zwischen an Audits beteiligten Teams.

Wie auf unserer Webseite mit rechtlichen Informationen aufgeführt, verwendet Smartsheet von Amazon Web Services, Inc. („AWS“) bereitgestellte Infrastruktur, um Kundendaten zu hosten. Informationen zu sicherheits- und datenschutzbezogenen Audits und Zertifizierungen, die AWS erhalten hat, darunter die Zertifizierung nach ISO 27001 und SOC-Berichte, sind auf der Sicherheits-Website und der Compliance-Website von AWS verfügbar. Eine vollständige Liste unserer Zertifizierungen und zusätzliche Whitepapers und Datensheets finden Sie auf der Compliance-Seite im Smartsheet Trust Center.

Fazit und zusätzliche Ressourcen

Für die Arbeit von heute (und morgen) braucht es eine moderne Plattform für das Arbeitsmanagement, die benutzerfreundlich und sicher ist. Durch kontinuierlichen Fokus und laufende Investitionen haben wir Smartsheet von Grund auf mit strengen Anforderungen und Funktionen zur Vertraulichkeit von Daten aufgebaut. Neben den bereits verfügbaren Funktionen befinden sich einige zusätzliche Sicherheitsfunktionen derzeit in Entwicklung. Weitere Informationen zu den Sicherheitsfunktionen, -programmen und -schutzmaßnahmen von Smartsheet finden Sie unter smartsheet.com/trust und in den nachfolgenden zusätzlichen Ressourcen:

Smartsheet-Systemadministrator – Onlinehilfe
Smartsheet-Funktionen nach Plan
Smartsheet-Integrationen
Smartsheet-API-Dokumentation

sales@smartsheet.com
+44 (20) 39001410
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet