Sicherheit in Dropbox Business

Ein Dropbox-Whitepaper

Dropbox

Inhalt

Überblick

Die digitale Transformation schreitet in verschiedenen Branchen weiter voran; daher ist es von entscheidender Bedeutung, dass Daten, Teams und Geräte geschützt werden, wo immer sie sich gerade befinden. Unternehmen, die sich auf Cloud-Lösungen wie Dropbox Business verlassen, um ortsunabhängige und dezentralisierte Arbeitsabläufe zu ermöglichen, müssen die Zusammenarbeit optimieren, Cloud-Risiken proaktiv begegnen und wirksame Kontrollmaßnahmen implementieren, um die Vertraulichkeit von geistigem Eigentum, die Integrität gespeicherter und gemeinsam genutzter Daten sowie die Verfügbarkeit von Daten durch verwaltete und robuste Cloud-Services zu gewährleisten.

Über 600.000 Unternehmen und Organisationen vertrauen auf Dropbox Business als Lösung für die sichere Zusammenarbeit von dezentralisierten und virtuellen Teams. Die Kernlösung von Dropbox Business umfasst den Smart Workspace für die Zusammenarbeit sowie Funktionen zur Dateisynchronisierung und -freigabe. Unsere Lösungen werden durch eine branchenführende Infrastruktur sowie durch Funktionen für erweiterte Unternehmenssicherheit, Team- und Inhaltssicherheit, elektronische Signaturen, sichere Übertragung und Data Governance unterstützt. Sofern nicht anders angegeben, gelten die Informationen in diesem Whitepaper für alle Dropbox Business-Produkte (Standard, Advanced und Enterprise) sowie Dropbox Education. Paper ist Teil von Dropbox Business und Dropbox Education.

Den Kern von Dropbox Business bildet unser umfassendes Sicherheitsprogramm, das Dropbox Trust Program, das auf einem vielschichtigen Sicherheitsansatz beruht, der im Zuge der Entwicklung globaler Ansätze für ortsunabhängiges Arbeiten unerlässlich ist.

In diesem Whitepaper werden die Sicherheitsfunktionen der Dropbox Business-Produkte, die betrieblichen Sicherheitsmaßnahmen von Dropbox, unsere Verpflichtung zu Datenschutz und Transparenz sowie Back-End-Richtlinien, unabhängige Zertifizierungen und Maßnahmen zur Einhaltung gesetzlicher Vorschriften erläutert, die Dropbox zu einer sicheren Lösung für Ihr Unternehmen machen.

Sofern nicht anders angegeben, gelten die Informationen in diesem Whitepaper für alle Dropbox Business-Produkte (Standard, Advanced und Enterprise) sowie Dropbox Education. Paper ist Teil von Dropbox Business und Dropbox Education.

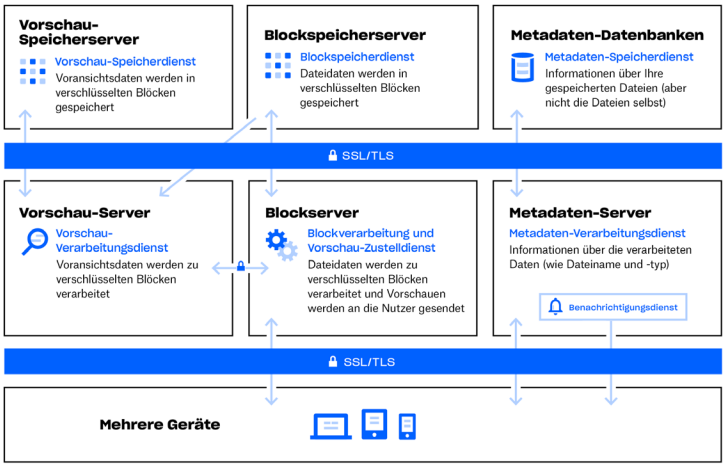
Technischer Hintergrund

Unsere nutzerfreundlichen Oberflächen sind auf einer Infrastruktur aufgebaut, die schnelle, zuverlässige Synchronisierung, Freigaben und Zusammenarbeit gewährleistet. Wir optimieren unser Produkt und unsere Architektur ständig, um unseren Nutzern schnellere Datenübertragungen zu bieten, die Zuverlässigkeit zu verbessern und unser Produkt an umgebungsbedingte Änderungen anzupassen. In diesem Abschnitt erläutern wir, wie Daten sicher übertragen, gespeichert und verarbeitet werden.

Dateiinfrastruktur

Dropbox-Nutzer können jederzeit auf ihre Dateien und Ordner zugreifen: von ihrem Desktop aus, über das Internet, über Mobilgeräte oder über mit Dropbox verbundene Anwendungen von Drittanbietern. All diese Clients stellen Verbindungen zu sicheren Servern her, damit Nutzer auf Dateien zugreifen, Dateien freigeben und verknüpfte Geräte aktualisieren können, wenn Dateien hinzugefügt, verändert oder gelöscht werden.

Die Datei-Infrastruktur von Dropbox setzt sich aus folgenden Komponenten zusammen:



- ***Metadatenserver***

  Grundinformationen über Nutzerdaten, sogenannte Metadaten, werden in einem speziell dafür vorgesehenen Speicherdienst aufbewahrt und dienen als Index für die Daten in den Nutzerkonten. Metadaten umfassen grundlegende Konto- und Nutzerinformationen wie die E-Mail-Adressen und Namen der einzelnen Nutzer sowie die Namen ihrer Geräte. Zu Metadaten gehören auch Grundinformationen über Dateien wie Dateiname und -format, durch die Funktionen wie Versionsverlauf, Wiederherstellung und Synchronisierung unterstützt werden.

- ***Metadaten-Datenbanken***

  Dateimetadaten werden in einem transaktionalen Key-Value-Store mit Multiversion Concurrency Control gespeichert und nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeitsanforderungen zu erfüllen.

- ***Blockserver***

  Dropbox bietet einen einzigartigen Sicherheitsmechanismus, der über die herkömmliche Verschlüsselung zum Schutz von Nutzerdaten hinausgeht. Blockserver verarbeiten die Dateien der Dropbox-Apps, indem sie jede Datei in Blöcke unterteilen, jeden Block mit einem starken Schlüssel schützen und nur die veränderten Blöcke synchronisieren. Wenn eine Dropbox-App eine neue Datei oder Änderungen an einer vorhandenen Datei erkennt, informiert die Anwendung die Blockserver über die Änderung. Dann werden die neuen oder veränderten Dateiblöcke verarbeitet und an die Blockspeicherserver übertragen. Außerdem werden Blockserver für die Bereitstellung von Dateien und Vorschauen für Nutzer verwendet. Ausführliche Informationen zur Verschlüsselung von Dateien während der Übertragung und im Ruhezustand durch diesen Dienst finden Sie unten im Abschnitt Verschlüsselung.

- ***Blockspeicherserver***

  Die Inhalte der Nutzerdateien werden in verschlüsselten Blöcken auf den Blockspeicherservern gespeichert.

  Vor der Übertragung unterteilt der Dropbox-Client die Dateien in Dateiblöcke, um sie auf die Speicherung vorzubereiten. Die Blockspeicherserver nutzen das Content-Addressable Storage(CAS)-Speicherverfahren. Dabei wird jeder verschlüsselte Dateiblock anhand seines Hash-Werts abgerufen.

- ***Vorschauserver***

  Die Vorschauserver erstellen Dateivorschauen. Vorschauen sind Abbildungen einer Nutzerdatei in einem für die schnelle Anzeige auf dem Endnutzergerät besser geeigneten Dateiformat. Vorschauserver rufen Dateiblöcke aus dem Blockspeicherserver ab, um Vorschauen zu erstellen. Wird eine Dateivorschau angefordert, rufen die Vorschauserver die zwischengespeicherte Vorschau aus den Vorschauspeicherservern ab und übermitteln sie an die Blockserver. Die Vorschauen werden Nutzern letztlich von Blockservern bereitgestellt.

- ***Vorschau-Speicherserver***

  Zwischengespeicherte Vorschauen werden verschlüsselt auf den Vorschau-Speicherservern gespeichert.

- ***Benachrichtigungsdienst***

  Dieser separate Dienst überprüft auf Änderungen an Dropbox-Konten. Hier werden keine Dateien oder Metadaten gespeichert bzw. übertragen. Jeder Client stellt eine Long-Poll-Verbindung zum Benachrichtigungsdienst her und befindet sich danach in Warteposition. Wenn eine Änderung an Dateien in Dropbox vorgenommen wird, teilt der Benachrichtigungsdienst diese dem/den relevanten Client(s) mit, indem die Long-Poll-Verbindung aufgehoben wird. Durch das Aufheben dieser Verbindung wird dem Client signalisiert, dass er eine sichere Verbindung zu Metadatenservern herstellen muss, um etwaige Änderungen synchronisieren zu können.

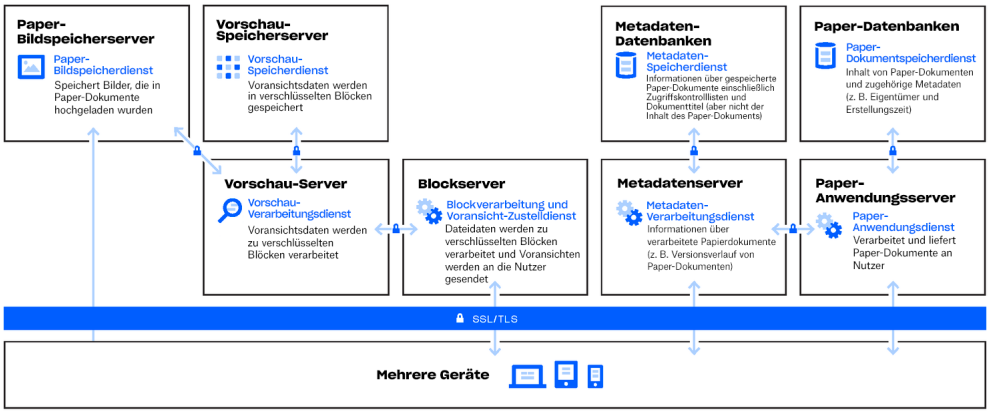
Dateidatenspeicherung

Dropbox speichert vor allem zwei Arten von Dateidaten: Dateimetadaten (z. B. Datum und Zeit der letzten Änderung einer Datei) sowie die eigentlichen Inhalte der Dateien (Dateiblöcke). Die Dateimetadaten befinden sich auf Dropbox-Servern, während die Dateiblöcke auf einem von zwei Systemen gespeichert sind: Amazon Web Services (AWS) oder Magic Pocket, dem Dropbox-internen Speichersystem. Magic Pocket besteht aus proprietärer Software sowie Hardware und wurde von Grund auf für Zuverlässigkeit und Sicherheit konzipiert. Sowohl in Magic Pocket als auch in AWS sind die gespeicherten Dateiblöcke verschlüsselt. Außerdem erfüllen beide Systeme hohe Anforderungen an die Zuverlässigkeit. Weitere Details finden Sie unten im Abschnitt Zuverlässigkeit.

Paper-Infrastruktur

Dropbox-Nutzer können jederzeit auf Paper-Dokumente zugreifen – über das Internet und Mobilgeräte oder über mit der Dropbox Paper-Anwendung verbundene Anwendungen von Drittanbietern. All diese Clients stellen Verbindungen mit sicheren Servern her, damit Sie auf Paper-Dokumente zugreifen und diese mit anderen Nutzern teilen sowie verknüpfte Geräte aktualisieren können, wenn Dokumente hinzugefügt, verändert oder gelöscht werden.

Die Infrastruktur von Dropbox Paper setzt sich aus folgenden Komponenten zusammen:



- ***Paper-Anwendungsserver***

  Die Anwendungsserver von Paper verarbeiten Nutzeranfragen, geben den Output bearbeiteter Paper-Dokumente an den Nutzer zurück und versenden Benachrichtigungen. Paper-Anwendungsserver schreiben von Nutzern eingehende Bearbeitungen in die Paper-Datenbanken, wo sie dauerhaft gespeichert werden. Die Kommunikationssitzungen zwischen den Paper-Anwendungsservern und den Paper-Datenbanken sind mit dem Secure Hypertext Transfer Protocol (HTTPS) gesichert.

- ***Paper-Datenbanken***

  Die Inhalte von Paper-Dokumenten sowie gewisse Metadaten darüber werden verschlüsselt und in den Paper-Datenbanken dauerhaft gespeichert. Zu den gespeicherten Daten gehören Informationen über das jeweilige Paper-Dokument (z. B. Titel, Eigentümer, Erstellungszeit usw.) und Inhalte des Paper-Dokuments wie Kommentare und Aufgaben. Die Paper-Datenbanken werden nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeitsanforderungen zu erfüllen.

- ***Metadatenserver***

  Paper nutzt die gleichen Metadatenserver, die im Dropbox-Infrastrukturdiagramm beschrieben sind, um Informationen über Paper-Dokumente zu verarbeiten, beispielsweise den Versionsverlauf von Paper-Dokumenten und die Mitgliedschaft in freigegebenen Ordnern. Dropbox verwaltet die Metadatenserver direkt, die sich in externen Rechenzentren Dritter befinden.

- ***Metadaten-Datenbanken***

  Paper nutzt die gleichen Metadaten-Datenbanken, die im Dropbox-Infrastrukturdiagramm beschrieben sind, um Informationen zu Papierdokumenten zu speichern, zum Beispiel Freigaben, Berechtigungen und Ordnerverknüpfungen. Paper-Dokumentenmetadaten werden in einem MySQL-Datenbankdienst gespeichert und nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeitsanforderungen zu erfüllen.

- ***Paper-Bildspeicherserver***

  In Paper-Dokumente eingefügte Bilder werden auf den Paper-Bildspeicherservern gespeichert und im Ruhezustand verschlüsselt. Bilddaten, die von der Paper-Anwendung an die Paper-Bildspeicherserver übermittelt werden und umgekehrt, werden in einer verschlüsselten Sitzung übertragen.

- ***Vorschauserver***

  Die Vorschauserver erstellen sowohl von Bildern, die in Paper-Dokumente eingefügt werden, als auch von Hyperlinks in Paper-Dokumenten Vorschauen. Wenn Bilder in Paper-Dokumente eingefügt werden, rufen die Vorschau-Server die auf den Paper-Bildspeicherservern gespeicherten Bilddaten über eine verschlüsselte Verbindung ab. Wenn Hyperlinks in Paper-Dokumente eingebettet werden, rufen die Vorschau-Server die Bilddaten ab und erstellen mit der vom Quelllink vorgegebenen Verschlüsselung eine Bildvorschau. Vorschauen werden Nutzern letztlich von Blockservern bereitgestellt.

- ***Vorschau-Speicherserver***

  Paper verwendet für die Speicherung der zwischengespeicherten Bildvorschau dieselben im Dropbox-Infrastrukturdiagramm beschriebenen Vorschau-Speicherserver. Zwischengespeicherte Vorschaublöcke werden verschlüsselt auf den Vorschau-Speicherservern gespeichert.

Paper-Dokumentspeicher

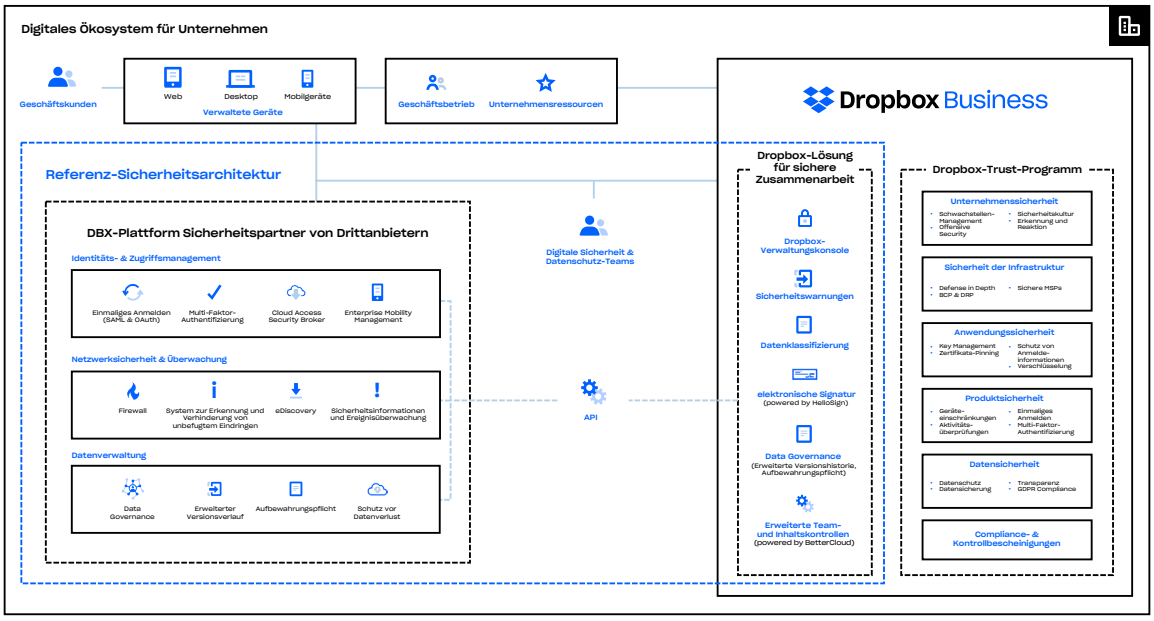
Dropbox speichert vor allem folgende Arten von Daten in Paper-Dokumenten: Metadaten über Paper-Dokumente (z. B. freigegebene Berechtigungen) und Inhalte, die der Nutzer hochgeladen hat. Wir verwenden für diese den Sammelbegriff Paper-Dokumentdaten und für Abbildungen, die in Paper hochgeladen werden, den Begriff Paper-Bilddaten. Diese Arten von Daten werden jeweils in Amazon Web Services (AWS) gespeichert. Paper-Dokumente werden im Ruhezustand in AWS verschlüsselt. AWS erfüllte hohe Standards in Bezug auf die Zuverlässigkeit. Weitere Details finden Sie unten im Abschnitt Zuverlässigkeit.

Dropbox Trust Program

Vertrauen ist das Fundament, auf dem wir unsere Geschäftsbeziehungen zu Millionen von Menschen und Unternehmen weltweit aufbauen. Wir schätzen dieses Vertrauen und nehmen den Schutz Ihrer Daten sehr ernst. Deshalb haben Sicherheit, Datenschutz, Transparenz und Compliance bei der Entwicklung von Dropbox nach wie vor oberste Priorität.

Das Dropbox-Programm zu Sicherheit, Compliance und Datenschutz (Dropbox Trust Program) bietet einen Risikobewertungsprozess für umgebungsbedingte und physische Risiken sowie Risiken für Nutzer und Dritte, Verletzungen geltender Gesetze, Vorschriften und vertraglicher Anforderungen und verschiedene andere Risiken, die die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder den Datenschutz von Systemen beeinträchtigen könnten. Leistungsüberprüfungen erfolgen mindestens einmal pro Jahr. Weitere Informationen zum Dropbox Trust Program finden Sie unter dropbox.com/business/trust.

Wir verfolgen einen vielschichtigen Ansatz zum Schutz des Unternehmens, der Infrastruktur, der Anwendungen und Produkte, die sich auf Ihre Organisation auswirken.



Sicherheit für höchste Ansprüche

Dropbox hat eine Strategie zum Informationssicherheitsmanagement entwickelt, die Zweck, Ausrichtung, Prinzipien und Grundregeln im Hinblick auf die Wahrung von Vertrauen erläutert. Dabei werden Risiken eingeschätzt und die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und der Datenschutz der Systeme von Dropbox für Unternehmen ständig verbessert. Darüber hinaus prüfen und aktualisieren wir regelmäßig die Sicherheitsrichtlinien, bieten Sicherheitsschulungen an, führen Anwendungs- und Netzwerksicherheitstests (einschließlich Penetrationstests) durch, überwachen die Einhaltung der Sicherheitsrichtlinien und führen interne und externe Risikobewertungen durch.

Unsere Richtlinien

Wir verfügen über umfangreiche Sicherheitsrichtlinien, die vom Dropbox-Team für Sicherheit und Missbrauchsschutz durchgesetzt werden. Alle Sicherheitsrichtlinien werden mindestens einmal im Jahr überprüft und bestätigt. Mitarbeiter, Praktikanten und Auftragnehmer nehmen bei Eintritt in das Unternehmen an obligatorischen Sicherheitsschulungen und später an weiterführenden Schulungen zur Förderung des Sicherheitsbewusstseins teil.

- ***Informationssicherheit***

  Sichere Aufbewahrung von Nutzer- und Dropbox-Informationen.

- ***Authentifizierung***

  Beschreibt, wie sich Dropbox-Mitarbeiter authentifizieren, um auf Informationssysteme und Daten zuzugreifen.

- ***Gerätesicherheit***

  Die Mindestsicherheitsanforderungen für Mobilgeräte, die für den Zugriff auf Unternehmensinformationen verwendet werden.

- ***Logische Zugriffskontrolle***

  Sicherer Zugriff auf Dropbox-Systeme, Nutzer und Informationen. Umfasst die Zugriffskontrolle auf Unternehmens- und Produktionsumgebungen.

- ***Datensicherheit***

  Beschreibt, wie Dropbox Daten durch spezifische Speicher-, Zugriffs- und Nutzungsanforderungen schützt.

- ***Sicherheit auf Reisen***

  Beschreibt, was Dropbox-Mitarbeiter tun sollten, bevor sie Auslandsreisen unternehmen.

- ***Sicherheitsrichtlinien für Vertrieb und Kundenerlebnis (CX)***

  Sichere Aufbewahrung von Nutzerinformationen, Schutz unserer Mitarbeiter und Support für unsere Nutzer.

- ***Physische Sicherheit***

  Gewährleistung einer sicheren und geschützten Umgebung für Menschen und Eigentum bei Dropbox.

- ***Richtlinien für physische Sicherheit in der Produktion***

  Verwaltung des physischen Zugangs zu Produktionsanlagen.

- ***Umgang mit Sicherheitsvorfällen***

  Beschreibt die Art und Weise, wie Dropbox mit gemeldeten Sicherheits-, Datenschutz- und Standortereignissen umgeht, und dokumentiert Pläne für den Umgang damit.

- ***Unberechtigte Verwendung urheberrechtlich geschützter Materialien***

  Verbot für Mitarbeiter, Dropbox oder Dropbox-Systeme zu verwenden, um nicht autorisierte Inhalte zu speichern oder weiterzugeben.

- ***Änderungsmanagement***

  Verwaltung von Änderungen an Produktionssystemen. Vorgesehen für alle Dropbox-Mitarbeiter, Auftragnehmer und Praktikanten mit Zugriff auf Systeme.

- ***Schutz von Nutzerdaten***

  Schutz und Handhabung von Nutzerinformationen und Nutzerdaten bei Dropbox in Übereinstimmung mit unserer Datenschutzrichtlinie.

- ***Richtlinie zu Business Continuity und Notfallmanagement***

  Beschreibt die Erhaltung, den Schutz und die Sicherheit von Personen (Dropbox-Mitarbeitern), Eigentum und (Geschäfts-)Prozessen.

- ***Dropbox-Datenschutzprogramm***

  Der Zweck, die Grundsätze und die Verantwortlichkeit für das Dropbox-Datenschutzprogramm.

- ***Dropbox-Programm zu Sicherheit, Compliance und Datenschutz***

  Beschreibt die Arbeitsweise von Dropbox und was es vertrauenswürdig macht.

- ***Sicherheit der Zahlungsumgebung***

  Sicherung und Wartung der speziellen Zahlungsumgebung, die bei Dropbox verwendet wird, um Kreditkartenzahlungen zu akzeptieren.

Mitarbeiterrichtlinien und -zugriff

Bei der Einstellung muss jeder Dropbox-Mitarbeiter eine Hintergrundüberprüfung durchlaufen. Außerdem müssen neue Mitarbeiter unsere Sicherheitsrichtlinien akzeptieren, eine Geheimhaltungsvereinbarung unterzeichnen und Sicherheitsschulungen absolvieren. Ausschließlich Mitarbeiter, die diese Verfahren erfolgreich abgeschlossen haben, erhalten entsprechend ihren Aufgaben innerhalb des Unternehmens physischen und logischen Zugriff auf die Unternehmens- und Produktionsumgebungen. Darüber hinaus müssen alle Mitarbeiter an einer jährlichen Sicherheitsschulung sowie regelmäßigen Schulungen für Sicherheitsbewusstsein anhand von informativen E-Mails, Vorträgen/Präsentationen und Ressourcen aus dem Intranet teilnehmen.

Der Zugriff von Mitarbeitern auf die Dropbox-Umgebung wird von einem zentralen Verzeichnis verwaltet und mit einer Kombination aus starken Passwörtern, mit Passphrase geschützten SSH-Schlüsseln und Zwei-Faktor-Authentifizierung authentifiziert. Für den Remotezugriff ist eine VPN-Verbindung mit Zwei-Faktor-Authentifizierung erforderlich. Darüber hinaus werden alle außerordentlichen Zugriffe vom Sicherheitsteam überprüft. Der Zugriff auf Unternehmens- und Produktionsnetzwerke ist durch definierte Richtlinien streng reguliert. So erfolgt der Zugriff auf das Produktionsnetzwerk ausschließlich mit einem SSH-Schlüssel, den nur Techniker erhalten, die aufgrund ihrer Arbeit Zugriff benötigen. Die Firewall-Konfiguration wird streng kontrolliert und ist auf eine kleine Anzahl von Administratoren beschränkt.

Darüber hinaus müssen Mitarbeiter, die Zugriff auf die Produktions- und Unternehmensumgebungen haben, den Best Practices für die Erstellung und Speicherung von privaten SSH-Schlüsseln folgen. Der Zugang zu anderen Ressourcen, einschließlich der Rechenzentren, Serverkonfigurationsprogrammen, Produktionsservern und Quellcode-Entwicklungsprogrammen wird nur mit ausdrücklicher Zustimmung des zuständigen Managements gewährt. Die Nachweise des Zugangsantrags, der Begründung und Genehmigung werden durch das Management aufbewahrt und der Zugang wird durch die zuständigen Mitarbeiter gewährt.

Dropbox nutzt technische Zugriffskontrollen und interne Richtlinien, um Mitarbeiter daran zu hindern, unbefugt auf Nutzerdateien zuzugreifen, und um den Zugriff auf Metadaten und sonstige Informationen zu den Nutzerkonten einzuschränken. Zum Schutz der Endnutzerdaten dürfen nur sehr wenige Entwickler, die für die Entwicklung der wichtigsten Dropbox-Dienste verantwortlich sind, auf die Umgebung zugreifen, in der die Nutzerdateien gespeichert sind. Der Zugriff eines Mitarbeiters wird sofort entzogen, sobald dieser das Unternehmen verlässt.

In dem Maße, in dem Dropbox zu einer Erweiterung der Infrastruktur unserer Kunden wird, stellen wir sicher, dass wir mit den Daten dieser Kunden verantwortungsvoll umgehen. Weitere Details finden Sie unten im Abschnitt Datenschutz.

Schwachstellenmanagement

Unser Sicherheitsteam führt regelmäßig automatisierte und manuelle Sicherheitstests und Maßnahmen zur Patchverwaltung durch und arbeitet mit externen Spezialisten zusammen, um potenzielle Sicherheitslücken und Bugs zu identifizieren und zu beheben.

Im Rahmen unseres Informationssicherheitsmanagement-Systems (ISMS) werden die in den Prüfungen ermittelten Ergebnisse und Empfehlungen an die Geschäftsleitung von Dropbox weitergegeben und ausgewertet. Bei Bedarf werden anschließend geeignete Maßnahmen ergriffen. Schwerwiegende Probleme werden dokumentiert, nachverfolgt und durch die Sicherheitsmitarbeiter behoben.

Änderungsmanagement

Alle Entwicklungs-, Problembehebungs- und Patchprozesse folgen unserer formellen Richtlinie für das Änderungsmanagement des Technikerteams von Dropbox, um zu gewährleisten, dass Systemänderungen vor der Implementierung in die Produktionsumgebung getestet und autorisiert werden. Quellcodeänderungen werden von Entwicklern initiiert, die eine Verbesserung an der Dropbox-App oder am Dropbox-Dienst vornehmen möchten. Änderungen werden in einem Versionskontrollsystem gespeichert und einer automatisierten Qualitätssicherung (QS) unterzogen, um die Einhaltung der Sicherheitsanforderungen zu prüfen. Bei erfolgreichem Abschluss des QS-Verfahrens werden die Änderungen implementiert. Änderungen, die durch das QS-Verfahren bestätigt wurden, werden automatisch in die Produktionsumgebung implementiert. Unser Software Development Lifecycle (SDLC) erfordert die Einhaltung sicherer Programmierrichtlinien sowie die Überprüfung von Codeänderungen auf potenzielle Sicherheitsrisiken durch unser QS-Verfahren und unsere manuellen Überprüfungsprozesse. Für die Produktionsumgebung freigegebene Änderungen werden protokolliert und archiviert. Die Teamleitung des Dropbox-Technikerteams wird über Änderungen automatisch informiert.

Nur befugte Mitarbeiter dürfen Änderungen an der Dropbox-Infrastruktur vornehmen. Das Dropbox-Sicherheitsteam ist für die Sicherheit der Infrastruktur verantwortlich. Darüber hinaus gewährleistet das Team, dass sich Server, Firewalls und sonstige sicherheitsrelevante Konfigurationen auf dem neuesten Stand befinden und dem Branchenstandard entsprechen. Firewall-Regeln und Personen mit Zugriff auf die Produktionsserver werden regelmäßig überprüft.

Scanning und Sicherheitspenetrationstests (intern und extern)

Unser Sicherheitsteam führt regelmäßig automatisierte und manuelle Sicherheitstests durch, um potenzielle Schwachstellen und Fehler in unseren Anwendungen für den Desktop, das Web (Dropbox und Paper) und Mobilgeräte (Dropbox und Paper) ausfindig zu machen und zu beheben.

Darüber hinaus hat Dropbox Drittanbieter beauftragt, regelmäßige Penetrations- und Schwachstellentests in den Produktionsumgebungen durchzuführen. Um die Sicherheit unserer Anwendungen zu gewährleisten, arbeiten wir mit externen Sicherheitsexperten, anderen Sicherheitsteams der Branche und der Forschungscommunity zusammen. Wir nutzen außerdem automatische Analysesysteme, um Schwachstellen zu identifizieren. Dazu zählen intern entwickelte Systeme, Open-Source-Systeme, die wir an unsere Bedürfnisse anpassen, und externe Anbieter, die wir mit der kontinuierlichen automatisierten Analyse beauftragen.

Abwehr schädlicher Inhalte von Dropbox

Wir verfügen über Scanfunktionen, die darauf abzielen, die Speicherung und Verbreitung schädlicher Inhalte in Dropbox zu verhindern. Unsere Scanner nutzen intern entwickelte Technologien sowie innovative Funktionen von Partnern wie Microsoft und Google, um Dropbox zu einem sicheren Ort für unsere Kunden zu machen.

Bug-Bounty-Programm

Neben den Penetrationstests, die wir in Zusammenarbeit mit professionellen Unternehmen durchführen, und unseren eigenen internen Prüfungen nutzen wir durch unser Bug-Bounty-Programm (ein Belohnungsprogramm für Finder von Schwachstellen) auch das Fachwissen der Sicherheitscommunity. Unser Bug-Bounty-Programm bietet Sicherheitsexperten Anreize für die verantwortungsvolle Meldung gefundener Softwarefehler. Diese Einbindung der externen Community sorgt für zusätzliche unabhängige Prüfungen unserer Anwendungen und unterstützt unser Sicherheitsteam dabei, den Schutz unserer Nutzer zu gewährleisten. Wir möchten im Hinblick auf Belohnungen für gefundene Schwachstellen sowie unsere Reaktions- und Behebungszeiten zu den führenden Unternehmen der Branche gehören.

Wir haben einen Rahmen für zulässige Meldungen und die infrage kommenden Dropbox-Apps sowie Richtlinien zur verantwortungsvollen Offenlegung entwickelt, die das Auffinden und Melden von Schwachstellen fördern und die Sicherheit unserer Nutzer erhöhen. Die Richtlinien im Einzelnen:

- Melden Sie Sicherheitsprobleme bitte unter Angabe aller Einzelheiten.
- Bitte seien Sie respektvoll gegenüber unseren bestehenden Anwendungen. Das Versenden von Spamming-Formularen durch automatische Schwachstellen-Scanner führt zu keiner Belohnung oder Prämie, da diese explizit nicht in den Geltungsbereich fallen.
- Geben Sie uns einen angemessenen Zeitraum zur Bearbeitung der Angelegenheit, bevor Sie Informationen über das Sicherheitsproblem veröffentlichen.
- Greifen Sie nicht ohne Zustimmung des Kontoinhabers auf Nutzerdaten zu.
- Sie dürfen die Daten nicht einsehen, ändern, speichern, aufbewahren, übertragen oder anderweitig auf sie zugreifen; löschen Sie sofort alle lokalen Informationen, wenn Sie die Schwachstelle an Dropbox gemeldet haben.
- Handeln Sie nach bestem Wissen und Gewissen, um Datenschutzverletzungen, die Zerstörung von Daten und die Unterbrechung oder Beeinträchtigung unserer Dienste (einschließlich DoS-Angriffen) zu vermeiden.

Probleme können in einem Bericht an Bugcrowd unter bugcrowd.com/dropbox gemeldet werden.

Physische Sicherheit

Infrastruktur

Nur bestimmte, durch Dropbox autorisierte Mitarbeiter haben Zutritt zu Subservice-Einrichtungen, in denen sich Produktionssysteme befinden, sofern dies für die Ausübung der Aufgaben dieser Mitarbeiter notwendig ist. Personen, die darüber hinaus Zutritt zu den Einrichtungen der Produktionsumgebung brauchen, erhalten ihn nur nach ausdrücklicher Genehmigung von der zuständigen leitenden Stelle.

Die leitende Stelle dokumentiert Anfrage, Begründung und Genehmigung, bevor befugte Personen die Genehmigung zum Zutritt erteilen. Wenn die Genehmigung erteilt wurde, wird ein autorisiertes Mitglied des Infrastrukturteams die entsprechende Subservice-Organisation kontaktieren, um den Zutritt für die Person zu beantragen, für die die Genehmigung erteilt wurde. Die Subservice-Organisation gibt die Informationen des Nutzers in sein eigenes System ein und gewährt Zutritt mit dem offiziellen Dropbox-Badge und, wo möglich, biometrischem Scanzugriff. Wenn diesen Personen der Zutritt gewährt wurde, liegt es im Verantwortungsbereich des Rechenzentrums, dass der Zutritt auf diese autorisierten Personen beschränkt bleibt.

Büroräume

- ***Physische Sicherheit***

  Das Dropbox-Team für die physische Sicherheit ist dafür zuständig, die Richtlinien für physische Sicherheit durchzusetzen und für die Einhaltung aller Sicherheitsbestimmungen in den Büroräumen zu sorgen.

- ***Bestimmungen für Besucher***

  Der physische Zugang zu Unternehmensgebäuden, bei denen es sich nicht um öffentliche Eingänge und Eingangshallen handelt, ist auf autorisierte Dropbox-Mitarbeiter und registrierte sowie von Dropbox-Mitarbeitern begleitete Besucher beschränkt. Ein Badge-Zugangssystem stellt sicher, dass nur autorisierte Personen Zugang zu eingeschränkten Bereichen in den Unternehmensgebäuden haben.

- ***Serverzugriff***

  Zutritt zu Bereichen mit Unternehmensservern und Netzwerkausrüstung ist autorisiertem Personal höherer Position mit dem entsprechenden Mitarbeiterausweis vorbehalten. Die Liste der autorisierten Personen, die Zutritt zu Unternehmens- und Produktionsumgebungen besitzen, wird mindestens vierteljährlich überprüft.

Umgang mit Sicherheitsvorfällen

Wir haben Richtlinien zum Umgang mit Sicherheitsvorfällen implementiert, um auf Probleme hinsichtlich Verfügbarkeit, Integrität, Sicherheit, Datenschutz und Vertraulichkeit reagieren zu können. Außerdem haben wir für derartige Vorfälle spezielle Teams, die in folgenden Bereichen geschult sind:

- umgehende Reaktion auf Hinweise zu potenziellen Sicherheitsvorfällen
- Bestimmung des Schweregrads eines Vorfalls
- falls nötig, Ergreifen von Maßnahmen zur Schadensbegrenzung und -minderung

- Kommunikation mit relevanten internen und externen Beteiligten, wozu die Benachrichtigung betroffener Kunden gehört, um unserer Meldepflicht bei Sicherheitsvorfällen nachzukommen und die jeweiligen gesetzlichen Vorschriften und Bestimmungen zu erfüllen
- Sicherung der Beweise zu Untersuchungszwecken
- Dokumentation einer nachträglichen Analyse und Entwicklung eines dauerhaften Triageplans

Unsere Richtlinien zum Umgang mit Sicherheitsvorfällen werden im Rahmen unserer SOC 2, ISO/IEC 27001 und anderer Sicherheitsbeurteilungen überprüft.

Infrastruktursicherheit

Netzwerksicherheit

Die Sicherheit des Back-End-Netzwerks hat für Dropbox oberste Priorität. Unsere Netzwerksicherheits- und Überwachungsmechanismen bieten eine mehrschichtige Sicherheitsstruktur zum Schutz von Daten und zur Abwehr von Angriffen. Wir nutzen branchenübliche Technologien, darunter Firewalls, Überprüfung auf Schwachstellen im Netzwerk, Überwachung der Netzwerksicherheit und Intrusion Detection Systeme, damit nur zulässiger Datenverkehr unsere Infrastruktur erreichen kann.

Unser eigenes internes Netzwerk ist nach Nutzung und Gefahrenstufe unterteilt. Die primären Netzwerke sind:

- mit dem Internet verbundene DMZ
- Prioritätsinfrastruktur-DMZ
- Produktionsnetzwerk
- Unternehmensnetzwerk

Der Zugriff auf die Produktionsumgebung ist auf autorisierte IP-Adressen beschränkt und erfordert an allen Endpunkten eine mehrstufige Authentifizierung. IP-Adressen mit Zugriffsrechten sind mit dem Unternehmensnetzwerk oder zugelassenen Dropbox-Mitarbeitern verknüpft. Autorisierte IP-Adressen werden vierteljährlich überprüft, damit eine sichere Produktionsumgebung gewährleistet werden kann. Änderungen an der IP-Adressenliste sind nur befugten Personen gestattet.

Datenverkehr aus dem Internet, der für unser Produktionsnetzwerk bestimmt ist, wird durch mehrere Ebenen aus Firewalls und Proxys gesichert.

Zwischen dem internen Netzwerk von Dropbox und dem öffentlichen Internet werden strenge Grenzen gezogen. Der Internetdatenverkehr zum und vom Produktionsnetzwerk wird von einem speziell dafür vorgesehenen Proxy-Dienst kontrolliert, der wiederum durch einschränkende Firewall-Regeln geschützt wird.

Dropbox setzt eine Reihe fortschrittlicher Tools ein, um Laptops und Desktops mit Mac- und Windows-Betriebssystemen sowie Produktionssysteme auf unerwünschte Aktivitäten zu überwachen. Sicherheitsprotokolle werden gemäß den branchenüblichen Aufbewahrungsrichtlinien zu gerichtlichen Zwecken und für die Vorfallreaktion zentral gesammelt.

Dropbox identifiziert und behebt Risiken durch regelmäßige Netzwerksicherheitstests sowie mithilfe von Audits, die sowohl von internen Sicherheitsteams als auch externen Sicherheitsexperten durchgeführt werden.

Points of Presence (PoPs)

Zur Optimierung der Website-Geschwindigkeit für die Nutzer setzt Dropbox auf die Content Delivery Networks (CDNs) von Drittanbietern sowie auf von Dropbox gehostete Points of Presence (PoPs), die sich an 31 Standorten rund um den Globus befinden. An diesen Standorten werden keine Nutzerdaten gespeichert, außerdem werden alle übertragenen Nutzerdaten mit SSL/TLS verschlüsselt. Physischer und logischer Zugriff auf von Dropbox gehostete PoPs ist ausschließlich auf autorisierte Dropbox-Mitarbeiter beschränkt. Dropbox führt Optimierungen sowohl auf der Transportebene (TCP) als auch auf der Anwendungsebene (HTTP) durch.

Peering

Dropbox hat eine offene Peering-Richtlinie, und alle Kunden sind herzlich eingeladen, mit uns Peering-Abkommen abzuschließen. Details finden Sie auf dropbox.com/peering.

Zuverlässigkeit

Ein Speichersystem ist nur dann von Nutzen, wenn es zuverlässig ist. Aus diesem Grund haben wir Dropbox mit mehreren Redundanzebenen versehen, um unsere Nutzer vor Datenverlusten zu schützen und Verfügbarkeit zu gewährleisten.

Dateimetadaten

Innerhalb eines Rechenzentrums werden redundante Kopien von Metadaten mindestens nach einem N+2-Verfügbarkeitsmodell auf mehrere unabhängige Geräte verteilt. Die Daten werden mindestens stündlich einer stufenweisen und alle 36 Stunden einer kompletten Datensicherung unterzogen. Metadaten werden auf von Dropbox gehosteten und verwalteten Servern in den USA gespeichert.

Dateiblöcke

Redundante Kopien von Dateiblöcken werden unabhängig voneinander in mindestens zwei geografischen Regionen gespeichert und zuverlässig innerhalb jeder Region repliziert. (**Hinweis:** Die Dateiblöcke von Kunden, die sich für eine Speicherung ihrer Daten in unserer deutschen, australischen, japanischen oder im Vereinigten Königreich befindlichen Infrastruktur entscheiden, werden nur innerhalb der entsprechenden Region repliziert. Mehr Informationen finden Sie unten im Abschnitt Rechenzentren und Managed Service-Anbieter). Sowohl Magic Pocket als auch AWS sind darauf ausgelegt, eine jährliche Datenlanglebigkeit von mindestens 99,999999999 % zu gewährleisten.

Die Architektur, Anwendungen und Synchronisierungsmechanismen von Dropbox arbeiten zusammen, um Nutzerdaten zu schützen und ihre Hochverfügbarkeit zu gewährleisten. Falls der Dienst einmal ausfällt, können Dropbox-Nutzer immer noch auf die Versionen ihrer Dateien zugreifen, die zuletzt mit den lokalen Dropbox-Ordnern auf ihren verknüpften Computern synchronisiert wurden. Mit der Desktop-App von Dropbox synchronisierte Dateien stehen jederzeit auf den Festplatten der Nutzer zur Verfügung, auch bei Systemauszeiten, bei Ausfällen oder bei der Arbeit offline. Änderungen an Dateien und Ordnern werden mit Dropbox synchronisiert, sobald der Dienst bzw. die Verbindung wiederhergestellt ist.

Paper-Dokumente

Redundante Kopien von Paper-Dokumentdaten werden in einem Rechenzentrum auf unabhängigen Geräten nach einem N+1-Verfügbarkeitsmodell verteilt. Vollständige Sicherungskopien von Paper-Dokumentdaten werden außerdem täglich gespeichert. Für die Speicherung von Paper-Dokumenten nutzt Dropbox die AWS-Infrastruktur in den USA, die auf eine jahresbezogene Langlebigkeit der Daten von mindestens 99.999999999 % ausgelegt ist. Falls der Service einmal ausfällt, können Nutzer immer noch im „Offline"-Modus innerhalb der App für Mobilgeräte auf die zuletzt synchronisierten Versionen ihrer Paper-Dokumente zugreifen.

Dateisynchronisierung

Dropbox bietet branchenweit anerkannte erstklassige Dateisynchronisierung. Unsere Synchronisierungsmechanismen gewährleisten schnelle Dateiübertragungen und unterstützen den standortunabhängigen Datenzugriff über alle Geräte hinweg. Dropbox ist zudem resilient. Bei einer fehlgeschlagenen Verbindung nimmt ein Client den Vorgang nahtlos wieder auf, sobald eine neue Verbindung hergestellt werden kann. Dateien werden auf dem lokalen Client nur dann aktualisiert, wenn sie vorher in Dropbox vollständig synchronisiert und erfolgreich überprüft wurden. Ein Lastenausgleich auf mehreren Servern gewährleistet Redundanz und eine gleichbleibend zuverlässige Synchronisierung für den Endnutzer.

Delta-Synchronisierung

Dank dieser Synchronisierungsmethode werden nur modifizierte Dateiabschnitte herunter- und hochgeladen. Dropbox speichert jede hochgeladene Datei in separaten, verschlüsselten Blöcken und aktualisiert nur die geänderten Teile.

Streaming-Synchronisierung

Statt zu warten, bis der Datei-Upload abgeschlossen ist, beginnt die Streaming-Synchronisierung mit dem Download synchronisierter Blöcke auf ein zweites Gerät, bevor der Upload aller Blöcke vom ersten Gerät abgeschlossen ist. Diese Methode wird automatisch eingesetzt, wenn mindestens zwei Rechner mit demselben Dropbox-Konto verknüpft sind oder ein Ordner für mehrere Dropbox-Konten freigegeben ist.

Festplattenspeicher sparen

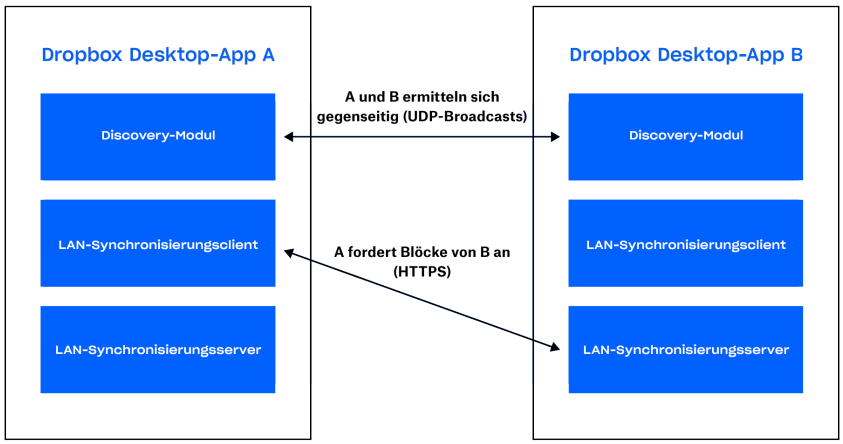
Nutzer können Speicherplatz auf ihren Computern freigeben, indem sie nur die Dateien offline verfügbar machen, die sie auf ihrer Festplatte haben möchten. Dadurch wird Speicherplatz auf dem Computer frei, da alles andere rein online auf dropbox.com gespeichert wird.

LAN-Synchronisierung

Bei der LAN-Synchronisierung werden neue und aktualisierte Dateien von anderen Computern im selben lokalen Netzwerk (LAN) herunter- bzw. in dieses hochgeladen. Dies spart Zeit und Bandbreite, da das Herunterladen der Datei von den Dropbox-Servern entfällt.

Architektur

Die LAN-Synchronisierung besteht aus drei Hauptkomponenten, die in der Desktop-App ausgeführt werden: Discovery Engine, Server und Client. Die Discovery Engine sucht nach Rechnern im Netzwerk, mit denen sie sich synchronisieren kann. Diese Suche beschränkt sich jedoch auf Rechner, die auf die jeweiligen privaten oder freigegebenen Dropbox-Ordner zugreifen dürfen. Der Server verarbeitet Anfragen von anderen Rechnern im Netzwerk und stellt die angefragten Dateiblöcke bereit. Der Client fragt die Dateiblöcke im Netzwerk an.



Discovery Engine

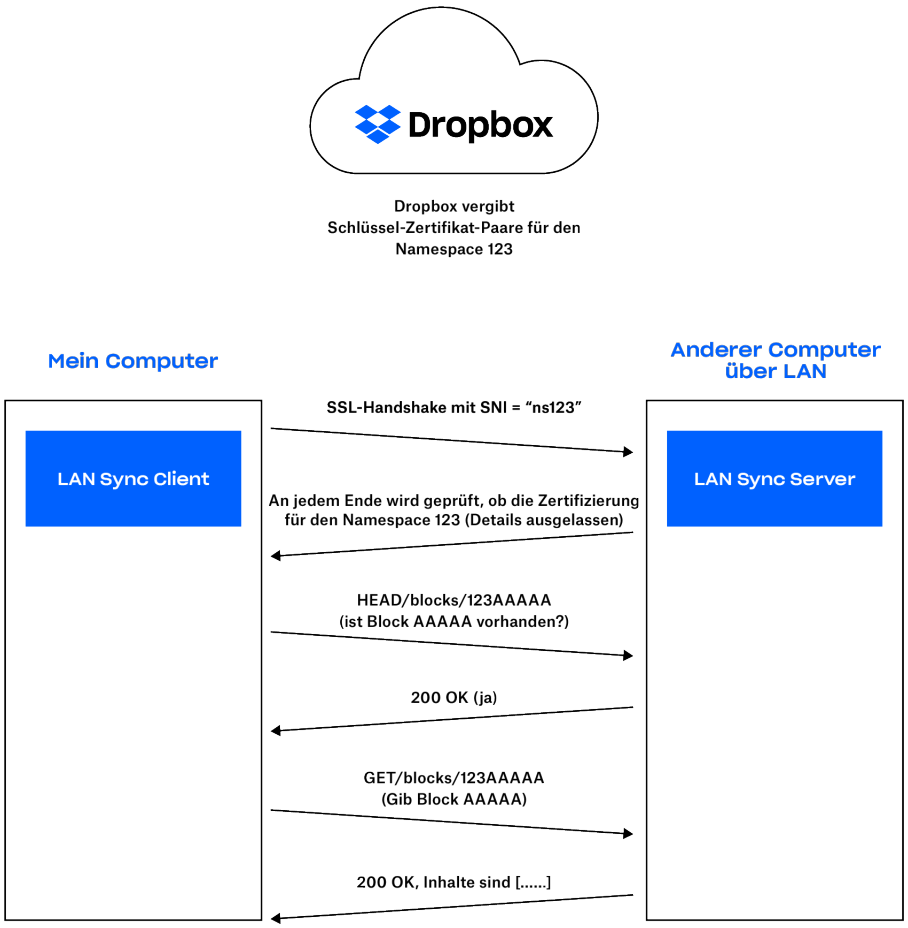
Alle Rechner im LAN nutzen Port 17500 (von IANA zur LAN-Synchronisierung reserviert), um UDP Broadcast-Pakete zu senden und zu empfangen. Diese Pakete enthalten die von diesem Computer verwendete Protokollversion, die unterstützten privaten und freigegebenen Dropbox-Ordner, den zum Ausführen des Servers verwendeten TCP-Port (kann bei Nichtverfügbarkeit von Port 17500 abweichen) sowie eine zufällige ID für den Rechner. Nachdem ein Paket erkannt wurde, wird die IP-Adresse des Rechners für jeden privaten oder freigegebenen Ordner zu einer Liste hinzugefügt, um als potenzielles Ziel vermerkt zu werden.

Protokoll

Die Dateiblöcke werden über HTTPS übertragen. Auf jedem Computer wird ein HTTPS-Server mit Endpunkten ausgeführt. Ein Client fragt bei mehreren Peers an, ob die Blöcke dort vorhanden sind. Die Blöcke werden jedoch nur von einem Server heruntergeladen.

Zum Schutz Ihrer Daten dürfen ausschließlich die Clients Dateiblöcke anfragen, die für den jeweiligen Ordner authentifiziert sind. Außerdem verhindern wir, dass sich Computer bei Ordnern als Server ausgeben, für die sie keine Berechtigung haben. Dazu generieren wir für jeden privaten oder freigegebenen Dropbox-Ordner SSL-Schlüssel-Zertifikat-Paare. Diese Paare werden von den Dropbox-Servern an die Computer verteilt, die für den Ordner authentifiziert wurden. Bei jeder Nutzeränderung (beispielsweise, wenn jemand aus einem freigegebenen Ordner entfernt wird) werden die Schlüssel-Zertifikat-Paare neu verteilt. Beide Enden der HTTP-Verbindung müssen sich mit demselben Zertifikat authentifizieren (das Zertifikat für den Dropbox- oder freigegebenen Ordner), um sicherzustellen, dass beide Enden der Verbindung authentifiziert sind.

Bei der Herstellung einer Verbindung teilen wir dem Server mit, mit welchem privaten Dropbox-Konto oder mit welchem Ordner wir eine Verbindung herstellen möchten. Hierfür nutzen wir eine Server Name Indication (SNI), damit der Server das korrekte Zertifikat verwendet.



Server/Client

Dank dem oben beschriebenen Protokoll muss der Server nur wissen, welche Blöcke vorhanden sind und wo er sie finden kann.

Der Client verfügt auf Grundlage der Ergebnisse der Discovery Engine über eine Liste von Peers für jeden privaten Dropbox-Ordner und freigegebenen Ordner. Wenn das LAN-Synchronisierungssystem eine Anfrage zum Download eines Dateiblocks erhält, sendet es eine Anfrage an eine zufällige Auswahl von Peers, die für den privaten Dropbox-Ordner oder den freigegebenen Ordner ermittelt wurden, und fordert dann den Block vom ersten Peer an, der die Anfrage bestätigt.

Zur Vermeidung von Latenzen verwenden wir Verbindungspools, sodass wir schon gestartete Verbindungen erneut verwenden können. Wir öffnen Verbindungen nur bei Bedarf und halten sie dann aktiv, falls wir sie erneut nutzen möchten. Außerdem beschränken wir die Anzahl der Verbindungen zu jedem einzelnen Peer.

Wenn ein Dateiblock nicht gefunden oder nicht erfolgreich heruntergeladen werden kann oder wenn die Verbindung zu langsam ist, holt sich das System den Block von den Dropbox-Servern.

Rechenzentren und Managed-Service-Anbieter

Die Unternehmens- und Produktionssysteme von Dropbox befinden sich extern in Subservice-Rechenzentren und bei Managed Service-Anbietern in unterschiedlichen Regionen der USA. Alle SOC-Berichte aus den Subservice-Rechenzentren und/oder Auftragnehmer-Sicherheitsprüfungen und Vertragspflichten werden mindestens einmal jährlich auf hinreichende Sicherheitsmaßnahmen überprüft. Diese Drittanbieter sind für die physischen, umgebungsbedingten und operativen Sicherheitskontrollen in der Peripherie der Dropbox-Infrastruktur verantwortlich. Dropbox sorgt für die logische, Netzwerk- und Anwendungssicherheit seiner Infrastruktur, die sich in den Rechenzentren der Drittanbieter befindet.

Amazon Web Services (AWS), der Managed Service-Anbieter (Managed Service Provider, MSP) für die Datenverarbeitung und Speicherung, ist für die logische und Netzwerksicherung der Dropbox-Dienste verantwortlich, die über seine Infrastruktur zur Verfügung gestellt werden. Die Verbindungen werden durch seine Firewall geschützt, die standardmäßig so konfiguriert ist, dass sie alle Anforderungen ablehnt. Dropbox beschränkt den Zugriff auf die Umgebung auf eine begrenzte Anzahl von IP-Adressen und Mitarbeitern.

Infrastruktur in Deutschland, Australien, Japan und dem Vereinigten Königreich

Dropbox bietet berechtigten Nutzern die Speicherung von Dateiblöcken in Regionen außerhalb der USA an. Unsere Infrastruktur wird von Amazon Web Services (AWS) in Deutschland, Australien, Japan und dem Vereinigten Königreich gehostet und innerhalb der entsprechenden Region repliziert, um Redundanz zu gewährleisten und Datenverlust zu verhindern. Dateimetadaten werden auf den eigenen Servern von Dropbox in den USA gespeichert. Paper-Dokumente und Vorschauen aller Kunden werden aktuell in den USA gespeichert.

Geschäftskontinuität

Dropbox hat in einem Managementsystem zur Sicherstellung der Geschäftskontinuität (Business Continuity Management System, BCMS) festgelegt, wie wir bei der Unterbrechung geschäftskritischer Prozesse und Aktivitäten unsere Dienste wieder aufnehmen oder weiterhin anbieten und wie wir als Unternehmen in solch einem Fall handeln. Wir führen regelmäßig einen Prozess mit folgenden Phasen durch:

- ***Geschäftliche Auswirkungen und Risikobewertungen***

  Wir führen mindestens einmal jährlich eine Geschäftsfolgenabschätzung (Business Impact Assessment, BIA) durch, um geschäftskritische Dropbox-Prozesse zu identifizieren, die potenziellen Auswirkungen von Unterbrechungen zu analysieren, priorisierte Zeitrahmen für die Wiederherstellung festzulegen und unsere wichtigsten Abhängigkeiten und Lieferanten zu ermitteln. Außerdem findet mindestens einmal jährlich eine unternehmensweite Risikobewertung statt, um die Risiken von schwerwiegenden Zwischenfällen systematisch zu identifizieren, zu analysieren und zu bewerten. Die Risikobewertung und die BIA fließen in die Geschäftskontinuitätspläne (Business Continuity Plans, BCPs) ein und legen die Prioritäten zur Gewährleistung der Geschäftskontinuität sowie die Strategien zur Schadensbegrenzung und Wiederherstellung fest.

- ***Geschäftskontinuitätspläne***

  Teams, die von der BIA als wichtig für die Dropbox-Geschäftskontinuität eingestuft werden, entwickeln anhand dieser Informationen BCPs für ihre wichtigsten Prozesse. Dank dieser Pläne wissen die Teams, wer bei einem Notfall für die Fortführung der Prozesse verantwortlich ist, wer in einem anderen Dropbox-Büro oder -Standort die Prozesse bei einem Ausfall übernehmen kann und welche Kommunikationsmethoden dabei zum Einsatz kommen sollen. Mithilfe dieser Pläne können wir uns auch auf einen schwerwiegenden Zwischenfall vorbereiten, indem wir unsere Notfallwiederherstellungspläne und weitere wichtige Informationen zentralisieren (z. B. wann und wie der Plan zum Einsatz kommen soll, Kontakt- und Meetinginformationen, wichtige Apps sowie Wiederherstellungsstrategien). Die Dropbox-Geschäftskontinuitätspläne sind in unseren unternehmensweiten Krisenmanagementplan (Crisis Management Plan, CMP) eingebunden, in dem die Dropbox-Teams für Krisenmanagement und den Umgang mit Sicherheitsvorfällen aufgeführt sind.

- ***Erprobung/Übung von Plänen***

  Dropbox testet mindestens einmal jährlich bestimmte Elemente der Geschäftskontinuitätspläne. Diese Tests berücksichtigen den Umfang und die Ziele des BCMS, basieren auf entsprechenden Szenarien und sind auf klar definierte Ergebnisse ausgerichtet. Der Umfang der Tests reicht von theoretischen Übungen bis zu großmaßstäblichen Simulationen realer Zwischenfälle. Anhand der Testergebnisse sowie der Erfahrungen aus echten Vorfällen aktualisieren und verbessern die Teams ihre Pläne, um Probleme zu beheben und ihre Reaktionsmöglichkeiten auszubauen.

- ***Analyse und Bestätigung des BCMS***

  Mindestens einmal jährlich wird das BCMS im Rahmen des Dropbox-Programms zu Sicherheit, Compliance und Datenschutz (Dropbox Trust Program) von unseren Führungskräften analysiert.

Notfallwiederherstellung

Damit die Informationssicherheit in Krisen oder Katastrophenfällen mit Auswirkungen auf den Betrieb von Dropbox Business gewährleistet bleibt, gibt es einen Notfallwiederherstellungsplan. Das Dropbox-Technikteam überprüft diesen Plan jährlich. Darüber hinaus werden ausgewählte Elemente des Plans mindestens einmal im Jahr getestet. Die entsprechenden Ergebnisse werden dokumentiert und eventuell aufgetretene Probleme werden nachverfolgt und behoben.

Unser Notfallwiederherstellungsplan (Disaster Recovery Plan, DRP) ist auf Probleme mit der Beständigkeit und Verfügbarkeit ausgerichtet, die wie folgt definiert sind:

- Ein Katastrophenfall mit Auswirkungen auf die Beständigkeit umfasst mindestens eines der folgenden Ereignisse:
  - vollständiger oder unwiederbringlicher Verlust eines primären Rechenzentrums mit Metadaten oder mehrerer Rechenzentren, die Dateiblöcke speichern
  - Verlust der Möglichkeit, Daten aus einem Rechenzentrum mit Metadaten zu erreichen oder zu übertragen bzw. die Dateiinhalte von mehreren Rechenzentren zu speichern
- Ein Katastrophenfall mit Auswirkungen auf die Verfügbarkeit besteht aus mindestens einem der folgenden Ereignisse:
  - Ausfall, der länger als 10 Tage andauert
  - Verlust der Möglichkeit, Daten aus einem Speicherdienst/Rechenzentrum mit Metadaten bzw. aus mehreren Speicherdiensten/Rechenzentren, die Dateiblöcke speichern, zu erreichen oder zu übertragen

Wir bestimmen ein Recovery Time Objective (RTO) und ein Recovery Point Objective (RPO). Das RTO ist die Zeitspanne nach einem Katastrophenfall, in der ein Unternehmensprozess oder -dienst wieder ein bestimmtes Serviceniveau erreicht haben muss, und das RPO der maximale Zeitraum, in dem Daten aufgrund einer Unterbrechung des Dienstes verloren gehen dürfen. Außerdem messen wir bei unserem mindestens jährlich durchgeführten Disaster-Recovery-Test die Recovery Time Actual (RTA), d. h. die bis zur vollständigen Wiederherstellung des Dienstes tatsächlich verstrichene Zeit.

Die Dropbox-Pläne zum Umgang mit Sicherheitsvorfällen, zur Geschäftskontinuität und zur Notfallwiederherstellung werden regelmäßig und bei größeren betrieblichen oder umgebungsbedingten Änderungen getestet.

Anwendungssicherheit

Dropbox-Nutzeroberflächen

Der Dropbox-Dienst kann über verschiedene Nutzeroberflächen genutzt werden. Jede Nutzeroberfläche verfügt über Sicherheitseinstellungen und -funktionen, die die Nutzerdaten verarbeiten und schützen und gleichzeitig einen nutzerfreundlichen Zugriff gewährleisten.

- ***Web***

  Auf diese Oberfläche kann über jeden aktuellen Webbrowser zugegriffen werden. Sie gestattet Nutzern das Hochladen, Herunterladen, Ansehen und Freigeben ihrer Dateien. Die Weboberfläche erlaubt Nutzern außerdem das Öffnen lokaler Versionen ihrer Dateien über die entsprechende Standardanwendung ihres Rechners.

- ***Desktop***

  Die Dropbox-Desktop-App ist ein leistungsstarker Synchronisierungsclient, bei dem Dateien lokal für den Offlinezugriff gespeichert werden. Nutzer haben darüber vollen Zugriff auf ihre Dropbox-Konten und die Anwendung läuft auf Windows- und Mac-Betriebssystemen. Die Dateien können direkt im Dateibrowser des Betriebssystems angesehen und freigegeben werden.

- ***Mobil***

  Die Dropbox-App steht für iOS- und Android-Geräte zur Verfügung, sodass Nutzer auch unterwegs Zugriff auf all ihre Dateien haben. Über die App für Mobilgeräte können Nutzer ebenfalls Dateien für den Offlinezugriff bereitstellen.

- ***API***

  Die Dropbox-APIs bieten flexible Möglichkeiten zum Lesen und Schreiben in Dropbox-Nutzerkonten sowie zum Zugriff auf erweiterte Funktionen wie Suche, Dateiversionen und Wiederherstellen von Dateien. Mithilfe der APIs können der Nutzungszyklus eines Kontos von Dropbox Business verwaltet, Aktivitäten für alle Mitglieder eines Teams durchgeführt und der Zugriff auf Administratorfunktionen von Dropbox Business gewährt werden.

Paper-Nutzeroberflächen

Der Paper-Dienst kann über eine Reihe von Benutzeroberflächen genutzt werden. Jede verfügt über Sicherheitseinstellungen und Features, die Nutzerdaten verarbeiten und schützen und gleichzeitig einen einfachen Zugang gewährleisten.

- ***Web***

  Auf diese Oberfläche können Nutzer über jeden modernen Webbrowser zugreifen. Sie können darüber Paper-Dokumente erstellen, ansehen, herunterladen und freigeben.

- ***Mobilität***

  Die Paper-App für Mobilgeräte von Dropbox steht für iOS- und Android-Geräte sowie Tablets zur Verfügung; somit erhalten Nutzer die Möglichkeit, unterwegs auf alle ihre Paper-Dokumente zuzugreifen. Es handelt sich um eine Hybridanwendung aus nativem Code (iOS oder Android) in Verbindung mit einem internen Webansichtsbrowser.

- ***API***

  Die oberhalb beschriebene Dropbox-API enthält Endpunkte und Datentypen für die Verwaltung von Dokumenten und Ordner in Dropbox Paper, einschließlich der Unterstützung von Funktionen wie Berechtigungsverwaltung, Archivieren und endgültiges Löschen.

Verschlüsselung

Datensicherheit bei der Übertragung

Um Daten bei der Übertragung zwischen Dropbox-Apps und unseren Servern zu schützen, verwendet Dropbox Secure Sockets Layer (SSL)/Transport Layer Security (TLS) und richtet einen sicheren Tunnel ein, der durch eine AES-Verschlüsselung (Advanced Encryption Standard) mit mindestens 128 Bit geschützt ist. Die zwischen einem Dropbox-Client (derzeit Desktop, Mobilgerät, API oder Web) und dem gehosteten Dienst übertragenen Dateidaten werden per SSL/TLS verschlüsselt. Paper-Dokumente, die zwischen einem Paper-Client (zurzeit Mobilgerät, API oder Web) und dem gehosteten Dienst übertragen werden, sind ebenfalls per SSL/TLS verschlüsselt. Für Endpunkte, die von uns kontrolliert werden (Desktop und Mobilgeräte), und aktuelle Browser verwenden wir eine sichere Verschlüsselung und Perfect Forward Secrecy (PFS) sowie Certificate Pinning. Darüber hinaus kennzeichnen wir alle Authentifizierungscookies als sicher und aktivieren HTTP Strict Transport Security (HSTS) sowie den Parameter „includeSubDomains“.

Hinweis: Dropbox setzt ausschließlich auf TLS und verzichtet aufgrund bekannter Schwachstellen auf die Nutzung von SSLv3. TLS wird allerdings häufig als „SSL/TLS“ bezeichnet, weshalb wir diese Bezeichnung hier verwenden.

Um Attacker-in-the-Middle-Angriffen vorzubeugen, werden die Frontend-Server von Dropbox mithilfe öffentlicher Zertifikate authentifiziert, die dem Client vorliegen. Eine verschlüsselte Verbindung wird hergestellt, bevor Dateien oder Paper-Dokumente übertragen werden. So wird die sichere Übertragung zu den Frontend-Servern von Dropbox gewährleistet.

Datensicherheit im Ruhezustand

Von Nutzern hochgeladene Dropbox-Dateien werden im Ruhezustand nach AES (Advanced Encryption Standard) mit 256 Bit verschlüsselt. Dateien werden in separaten Dateiblöcken in verschiedenen Rechenzentren gespeichert. Jeder Block wird fragmentiert und sicher verschlüsselt. Nur Dateiblöcke, die seit der letzten Dateiversion geändert wurden, werden synchronisiert. Auch Paper-Dokumente werden im Ruhezustand nach AES (Advanced Encryption Standard) mit 256 Bit verschlüsselt. Paper-Dokumente werden mithilfe von Drittanbietersystemen in mehreren Verfügbarkeitszonen gespeichert.

Schlüsselverwaltung

Die Schlüsselverwaltung von Dropbox verfügt über operative, technische und verfahrenstechnische Sicherheitsmaßnahmen mit sehr begrenztem Direktzugriff auf Schlüssel. Die Generierung, der Austausch und die Speicherung des Schlüssels werden für die dezentralisierte Verarbeitung verteilt.

- ***Schlüssel für die Dateiverschlüsselung***

  Um die Komplexität zu verringern, fortschrittliche Funktionen zu ermöglichen und eine sichere Kryptografie zu gewährleisten, übernehmen wir für unsere Nutzer die Verwaltung der Schlüssel für die Dateiverschlüsselung. Kontrollmechanismen in der Infrastruktur des Produktionssystems sowie Sicherheitsrichtlinien bieten einen zuverlässigen Schutz bei der Generierung und Speicherung der Schlüssel.

- ***Interne SSH-Schlüssel***

  Der Zugriff auf Produktionssysteme wird durch eindeutige SSH-Schlüsselpaare eingeschränkt. Sicherheitsrichtlinien und -verfahren gewährleisten die Sicherheit der SSH-Schlüssel. Dank einem internen System wird der sichere Austausch von öffentlichen Schlüsseln verwaltet und private Schlüssel werden sicher gespeichert. Interne SSH-Schlüssel können ohne einen getrennten zweiten Faktor für die Authentifizierung nicht für den Zugriff auf Produktionssysteme genutzt werden.

- ***Schlüsselverteilung***

  Dropbox stellt vertrauliche Schlüssel automatisch für Systeme bereit, die für den Betrieb erforderlich sind, und verwaltet sie entsprechend.

Certificate Pinning

Dropbox nutzt Certificate Pinning in aktuellen Browsern, die die HTTP Public Key Pinning-Spezifizierung unterstützen, sowie in unseren Clients für Desktop- und Mobilgeräte. Certificate Pinning ist eine zusätzliche Überprüfung, mit der sichergestellt wird, dass der Dienst, zu dem eine Verbindung hergestellt wird, nicht gefälscht ist. Wir setzen diesen Mechanismus zum Schutz vor erfahrenen Hackern ein, die Ihre Aktivitäten ausspionieren wollen.

Schutz von Authentifizierungsdaten

Zum Schutz der Anmeldedaten von Nutzern geht Dropbox über gewöhnliches Hashing hinaus. Im Einklang mit den Best Practices der Branche wird jedes Passwort mit einem zufällig generierten nutzerspezifischen Salt kombiniert. Außerdem nutzen wir iteratives Hashing, um den zum Hacken erforderlichen Rechenaufwand zu erhöhen. Mit diesen beiden Verfahren werden Brute-Force-, Wörterbuch- und Rainbow-Table-Angriffe wirkungslos. Für zusätzlichen Schutz verschlüsseln wir die Hash-Werte mit einem Schlüssel, der getrennt von der Datenbank gespeichert ist, sodass die Passwörter selbst bei einer Kompromittierung der Datenbank sicher sind.

Malware-Scans

Wir haben ein automatisiertes System entwickelt, das nach Malware sucht, sobald Inhalte außerhalb des Kontos des ursprünglichen Nutzers geteilt werden. Das System nutzt sowohl proprietäre Technologien als auch branchenübliche Erkennungsmodule und verhindert die Verbreitung von Malware.

Produktsicherheit

Dropbox bietet Features zur administrativen Kontrolle und Transparenz, mit denen IT- und Endnutzer effektiv ihre Daten verwalten und sichern können. Mit Dropbox haben Sie alles, was Sie für Ihre Arbeit brauchen, an einem Ort – Ihre Tools, Inhalte und andere Nutzer. Dropbox ist mehr als nur ein sicherer Speicherplatz – es ist eine intelligente, nahtlose Möglichkeit, Ihren bereits bestehenden Workflow zu optimieren.

Nachstehend finden Sie eine Übersicht über die verschiedenen Features für Admins und Endnutzer sowie Integrationen in Drittanbieter-Apps zur Verwaltung kritischer IT-Prozesse.

Hinweis: Die Verfügbarkeit der Features hängt vom gewählten Abo ab. Mehr Informationen erhalten Sie unter dropbox.com/business/plans .

Inhaltliche Kontrollen

Der Schutz sensibler Unternehmensressourcen – beispielsweise geistiges Eigentum (IP) und persönlich identifizierbare Informationen (PII) – ist für IT- und Datensicherheitsteams von entscheidender Bedeutung. Von differenzierten Inhaltsberechtigungen bis hin zu Datenaufbewahrungspflichten und gesetzlichen Bestimmungen bietet Dropbox branchenführende Lösungen zur Verwaltung, zur Überwachung und zum Schutz Ihrer Inhalte. Nachfolgend sind die wichtigsten Dropbox-Produkte und -Features zur Inhaltskontrolle aufgeführt.

Granulare Inhaltsberechtigungen und Zugriffsberechtigungen auf freigegebene Dateien und Ordner

- ***Berechtigungen für freigegebene Dateien***

  Ein Teammitglied, das Eigentümer einer freigegebenen Datei ist, kann den Zugriff für bestimmte Nutzer sperren und die Kommentierung der Datei deaktivieren.

- ***Berechtigungen für freigegebene Dateien***

  Ein Teammitglied, das Eigentümer eines freigegebenen Ordners ist, kann den Zugriff darauf für bestimmte Nutzer sperren, Lese-/Bearbeitungsrechte für bestimmte Nutzer ändern und das Eigentumsrecht eines Ordners übertragen. Abhängig von den globalen Freigabeberechtigungen des Teams kann außerdem jeder Eigentümer eines freigegebenen Ordners hier festlegen, ob Nicht-Teammitglieder beitreten, andere Personen mit Bearbeitungsrechten die Mitgliedschaft verwalten und Links an Personen außerhalb des Ordners freigegeben werden dürfen.

- ***Passwörter für freigegebene Links***

  Jeder geteilte Link kann vom Eigentümer mit einem Passwort geschützt werden. Vor der Übertragung von Datei- oder Ordnerdaten prüft eine Zugriffskontrolle das Passwort und alle anderen Anforderungen (z. B. Zugriffskontrolllisten für Team, Gruppe oder Ordner). Nach erfolgreicher Überprüfung wird ein sicheres Cookie im Browser des Nutzers gespeichert, sodass sich der Browser an das bestätigte Passwort „erinnert“. Mithilfe von Freigabefunktionen können Administratoren auch Standardpasswörter festlegen, anstatt sie als optional zu betrachten, um die Inhalte ihres Teams besser zu schützen.

- ***Begrenzte Gültigkeit freigegebener Links***

  Nutzer können für jeden geteilten Link eine Gültigkeitsdauer festlegen, um anderen Nutzern vorübergehend Zugriff auf Dateien oder Ordner zu geben. Mithilfe von Freigabefunktionen können Administratoren auch Standardpasswörter festlegen, anstatt sie als optional zu betrachten, um die Inhalte ihres Teams besser zu schützen.

Freigabeberechtigungen für Paper-Dokumente und Paper-Ordner

- ***Berechtigungen für Paper-Dokumente und freigegebene Paper-Ordner***

  Ein Teammitglied, das Eigentümer eines Paper-Dokuments oder eines freigegebenen Paper-Ordners ist, kann den Zugriff für bestimmte Nutzer sperren und die Bearbeitung des Paper-Dokuments deaktivieren.

- ***Berechtigungen für Paper-Dokumente***

  Ein Teammitglied, das Eigentümer eines Paper-Dokuments ist, kann den Zugriff für bestimmte Nutzer sperren, die unter „Freigabe“ aufgeführt sind. Der Eigentümer und die Bearbeiter eines Paper-Dokuments

können die Berechtigungen für bestimmte Nutzer ansehen/bearbeiten und die Richtlinie für Links zu dem Dokument ändern. Die Link-Richtlinie legt fest, welche Nutzer das Dokument öffnen können und welche Berechtigungen sie haben. Der Team-Admin kann die Richtlinien für Links und die Dokumentenfreigabe für das ganze Team festlegen.

- ***Berechtigungen für Paper-Ordner***

  Ein Teammitglied, das Nutzer eines Ordners ist, kann die Freigaberichtlinie des Ordners ändern und den Zugriff bestimmter Nutzer sperren, die dem Ordner hinzugefügt wurden.

Datei- und Ordneraktionen

- ***Team-Ordner für Dateien***

  Administratoren können Team-Ordner erstellen, wodurch Gruppen und andere Nutzer für die Inhalte, die sie brauchen, automatisch der erforderlichen Zugriffsebene (ansehen oder bearbeiten) zugeordnet werden.

- ***Differenzierte Zugriffs- und Freigabefunktionen***

  Mit Freigabefunktionen können Admins die Mitgliedschaft sowie die Berechtigungen auf der höchsten Ordnerebene oder für Unterordner verwalten, damit Nutzer und Gruppen innerhalb und außerhalb des Unternehmens nur auf bestimmte Ordner zugreifen können.

- ***Team-Ordner-Manager***

  Admins können alle ihre Team-Ordner ansehen und die Freigaberichtlinien von einem zentralen Ort aus anpassen, um Fehler bei der Freigabe vertraulicher Informationen zu verhindern.

- ***Freigegebene Ordner für Paper-Dokumente***

  Admins können freigegebene Paper-Ordner erstellen, wodurch andere Nutzer für die Inhalte, die sie brauchen, automatisch der erforderlichen Zugriffsebene – kommentieren oder bearbeiten – zugeordnet werden.

- ***Remote-Löschen***

  Wenn Mitarbeiter aus dem Team ausscheiden oder ein Gerät abhandenkommt, können Administratoren Dropbox-Daten und lokale Dateikopien gerätefern löschen. Die Dateien werden sowohl von Rechnern als auch Mobilgeräten entfernt, sobald eine Internetverbindung zustande kommt und die Dropbox-App ausgeführt wird.

- ***Konten übertragen***

  Nachdem einem Nutzer der Zugriff entzogen wurde (entweder manuell oder über den Verzeichnisdienst), können Administratoren Dateien und das Eigentum an Paper-Dokumenten, die er erstellt hat, vom Konto dieses Nutzers auf das eines anderen Teammitglieds übertragen. Die Kontoübertragungsfunktion kann bei der Entfernung eines Nutzers oder zu jedem beliebigen Zeitpunkt nach der Löschung eines Nutzerkontos verwendet werden.

Die folgenden Funktionen sind als Add-on-Features verfügbar (kontaktieren Sie für weitere Informationen den Vertrieb):

- ***Scaninhalt***

  Mit dem Add-on für erweiterte Steuerfunktionen für Teams und Inhalte können Advanced- und Enterprise-Kunden von Dropbox Business auf neue und vorhandene Inhalte in Dropbox prüfen, um Datenschwachstellen zu ermitteln und zu vermeiden.

- ***Einrichten und Auslösen benutzerdefinierter Arbeitsabläufe***

  Mit dem Add-on für erweiterte Steuerfunktionen für Teams und Inhalte können Administratoren individuelle Maßnahmen zu Dateien festlegen, die gegen die Unternehmensrichtlinien verstoßen.

- ***Einrichten von Warnungen***

  Admins können Sicherheitsfragen in Echtzeit überwachen und Datenschwachstellen vermeiden. Sie erhalten Warnmeldungen über extern freigegebene Dateien und gescannte vertrauliche Daten.

Transparenz von Inhalten

Sicherheitswarnmeldungen und -benachrichtigungen

Administratoren von Dropbox Enterprise erhalten Benachrichtigungen in Echtzeit, wenn missbräuchliche Aktivitäten, riskante Aktivitäten oder potenzielle Datenlecks in ihren Konten erkannt werden. Die folgenden Ereignisse können überwacht werden:

- Massenlöschungen
- Datenverschiebung in Massenvorgängen
- extern freigegebener sensibler Inhalt
- Malware, die von außerhalb Ihres Teams geteilt wurde
- Malware, die innerhalb Ihres Teams geteilt wurde
- zu viele fehlgeschlagene Anmeldeversuche
- Anmeldung aus einem Land mit hohem Risiko
- Erkennung von Ransomware

Dropbox bietet außerdem die Möglichkeit, Warnschwellenwerte zu konfigurieren, Benachrichtigungsempfänger anzupassen und Warnmeldungen auszulösen, wenn Ordner mit vertraulichen Dateien extern freigegeben werden. Administratoren können Warnmeldungen auch als überprüft, geklärt oder geschlossen markieren. Darüber hinaus zeigt ein Dashboard-Widget allgemeine Einblicke über Teamwarnmeldungen und Trends der vergangenen Woche an.

Bericht und Seite für externe Freigaben

Dropbox bietet mit dem Bericht und der Seite zur externen Freigabe zusätzliche Transparenz. Administratoren können einen Bericht entweder über die Dashboard-Seite oder die Seite für die externe Freigabe erstellen. Der Bericht listet alle Dateien und Ordner des Teams auf, die außerhalb des Teams freigegeben sind, sowie alle geteilten Links. Die Seite für die externe Freigabe ist eine zusätzliche Seite in der Verwaltungskonsole, die es Administratoren ermöglicht, die Dateien und Ordner, die direkt aus dem Team und den geteilten Links heraus geteilt werden, zu sehen und zu filtern (Dateityp, wer geteilt hat, Linkeinstellungen und vieles mehr).

Freigabefunktionen

Mit den Freigabeeinstellungen haben Teamadministratoren mehr Kontrolle über die Freigabe und den Zugriff auf die Inhalte ihres Teams. Administratoren können auf Teamebene standardmäßige Ablaufzeiten, Passworteinschränkungen oder beides festlegen. Diese Einschränkungen verringern das Risiko von Datenverlusten, da die Nutzer nicht mehr selbst die Einschränkungen festlegen müssen.

Datenklassifizierung

Teams auf Dropbox Enterprise können persönliche und sensible Daten automatisch kennzeichnen lassen, um sie besser vor der Veröffentlichung zu schützen. Administratoren erhalten Warnungen vor Datenverlust (DLP) per E-Mail und in der Verwaltungskonsole, wenn Dateien oder Ordner, die in Teamordnern mit vertraulichen Informationen gespeichert sind, außerhalb ihres Teams geteilt werden. Administratoren haben die Möglichkeit, sensible Daten, die in gemeinsamen und persönlichen Ordnern von Teammitgliedern gespeichert sind, automatisch zu identifizieren und zu klassifizieren. Dropbox Enterprise-Administratoren können die automatische Datenklassifizierung über die Admin-Konsole aktivieren.

Add-on für Data Governance

Data Governance ist die Gesamtheit der Prozesse, Technologien und Teams, die zusammenwirken, um die Datenbestände eines Unternehmens zu verwalten und zu schützen. Dazu gehört die Fähigkeit, Unternehmensdaten zu speichern, zu identifizieren, zu finden und nach Bedarf abzurufen.

Das Dropbox Data Governance Add-on bündelt eine Reihe von Features, die es Unternehmen ermöglichen, ihre Daten besser zu kontrollieren und zu sichern und gleichzeitig die Risiken und Kosten zu reduzieren, die mit der Einhaltung von Vorschriften und Compliance-Anforderungen verbunden sind. Derzeit umfasst dieses Add-on vier wichtige Features für Team- und Compliance-Administratoren.

- ***Erweiterter Versionsverlauf***

  Ihr Standard-Dateiversionsverlauf hängt von der Art Ihres Dropbox-Kontos ab. Mit Dropbox Business können Sie jedoch ein Add-on für den erweiterten Versionsverlauf (EVH) separat oder als Teil des Data Governance Add-on-Pakets erwerben, mit dem Sie alle Dateien wiederherstellen können, die in den letzten 10 Jahren gelöscht oder geändert wurden.

- ***Aufbewahrungspflicht***

  Durch das Festlegen einer Aufbewahrungspflicht für ein Teammitglied können Team- und Compliance-Administratoren Inhalte anzeigen und exportieren, die von diesem Mitglied erstellt oder geändert wurden. Mitglieder, die von einer Aufbewahrungspflicht betroffen sind, werden nicht über die Aufbewahrung benachrichtigt und behalten weiterhin ihre Berechtigungen zum Erstellen, Bearbeiten und Löschen von Dateien.

- ***Datenaufbewahrung***

  Die Datenaufbewahrung ermöglicht es Teams und Compliance-Administratoren, das versehentliche Löschen von Inhalten, deren Aufbewahrung innerhalb einer bestimmten Zeitspanne vorgeschrieben ist, zu verhindern. Dieses Feature ermöglicht es den Kunden, Daten über 10 Jahre ab dem Datum der letzten „Dateiversion“ aufzubewahren.

- ***Datenlöschung***

  Die Datenlöschung ermöglicht es Team- und Compliance-Administratoren, Daten zu einem bestimmten Datum dauerhaft zu löschen, um die Anforderungen an die Datenaufbewahrung und -löschung zu erfüllen. Administratoren können die Aktivitäten überwachen, indem sie Berichte erhalten, die sie über bevorstehende Dateilöschungen in Kenntnis setzen.

Wiederherstellung und Versionskontrolle

Dropbox Business-Kunden haben die Möglichkeit, gelöschte Dateien und Paper-Dokumente sowie frühere Versionen von Dateien und Paper-Dokumenten wiederherzustellen, sodass Änderungen an wichtigen Daten nachverfolgt und abgerufen werden können.

Datensicherheit auf Mobilgeräten

- ***Daten löschen***

  Einen zusätzlichen Schutz bietet die Option, nach zehn fehlgeschlagenen Anmeldeversuchen mit dem PIN-Code alle Dropbox-Daten von dem Gerät löschen zu lassen.

- ***Interner Speicher und Offlinedateien***

  Dateien werden normalerweise nicht im internen Speicher von Mobilgeräten gespeichert. Mit den Dropbox-Clients für Mobilgeräte können Nutzer einzelne Dateien und Ordner zur späteren Offline-Ansicht auf dem Gerät speichern. Diese Dateien und Ordner werden automatisch aus dem internen Speicher des Geräts gelöscht, wenn die Verknüpfung zwischen einem Gerät und einem Dropbox-Konto in der App für Mobilgeräte oder in der Weboberfläche aufgehoben wird.

- ***Offline-Paper-Dokumente***

  Offline-Paper-Dokumente werden automatisch aus dem internen Speicher des Geräts gelöscht und der Nutzer wird abgemeldet, wenn die Verknüpfung zwischen einem Gerät und Paper über die Sicherheitsseite des Dropbox-Kontos aufgehoben wird.

Steuerfunktionen für Teams

Unternehmen haben individuelle Bedürfnisse. Deshalb haben wir einige Tools entwickelt, mit denen Admins Dropbox für Unternehmen an die Anforderungen ihrer Teams anpassen können. Zum weiteren Schutz von Konten und Daten bietet Dropbox für Unternehmen Tools für Endnutzer. Folgende Authentifizierungs-, Wiederherstellungs-, Protokollierungs- und andere Sicherheitsfunktionen stehen in den verschiedenen Dropbox-Benutzeroberflächen zur Verfügung.

Im Folgenden stellen wir mehrere Funktionen zur Kontrolle und Transparenz vor, die über die Verwaltungskonsole von Dropbox Business zur Verfügung stehen.

Differenzierte Inhaltsberechtigungen

- ***Verschiedene Admin-Rollen***

  Dropbox enthält unterschiedliche Admin-Rollen für effektivere Teamverwaltung. Konto-Administratoren können über eine von drei Zugriffsebenen verfügen. Ein Team kann unbegrenzt viele Administratoren haben und jedes Teammitglied kann eine Administratorrolle bekommen.

- ***Team-Admin***

  Kann Sicherheits- und Freigabeberechtigungen innerhalb des Teams festlegen, Administratoren erstellen und Nutzer verwalten. Der Team-Admin hat alle verfügbaren Admin-Rechte. Team-Admins sind die Einzigen, die Administratorrollen zuweisen oder ändern können. Jedes Konto von Dropbox für Unternehmen muss über mindestens einen Team-Admin verfügen.

- ***Nutzer-Admin***

  Kann die wichtigsten Verwaltungsaufgaben im Team wahrnehmen. Dazu gehören das Hinzufügen und Entfernen von Teammitgliedern, das Verwalten von Gruppen und das Einsehen des Aktivitätsfeeds des Teams.

- ***Support-Admin***

  Kann allgemeine Serviceanfragen von Teammitgliedern bearbeiten, z. B. die Wiederherstellung gelöschter Dateien oder Hilfe für Teammitglieder, die für die zweistufige Überprüfung gesperrt sind. Support-Admins können auch Passwörter von allen Nicht-Administrator-Nutzern zurücksetzen und Aktivitätsprotokolle spezifischer Teammitglieder exportieren.

- ***Verwaltung der Abrechnung***

  Kann auf die Abrechnungsseiten in der Verwaltungskonsole zugreifen.

- ***Verwaltung von Inhalten***

  Kann Teamordner innerhalb des Content Managers erstellen und verwalten.

- ***Verwaltung von Berichten***

  Kann innerhalb der Verwaltungskonsole Berichte erstellen und hat Zugriff auf die Aktivitätsseite.

- ***Sicherheitsverwaltung***

  Kann Sicherheitswarnungen, externe Freigaben und Sicherheitsrisiken verwalten.

- ***Compliance-Admin (nur für Teams mit dem Add-on Data Governance verfügbar)***

  Kann Data-Governance-Seiten verwalten (Aufbewahrungspflichten, Datenspeicherung und -löschung) und auch auf Content Manager zugreifen.

- ***Gruppen***

  Teams können Listen von Nutzern innerhalb von Dropbox erstellen und verwalten und ihnen so ganz einfach Zugriff auf bestimmte Ordner geben. In Dropbox können außerdem Active Directory-Gruppen mit dem Active Directory-Connector synchronisiert werden.

- ***Unternehmensverwaltete Gruppen***

  Nur Administratoren können Mitgliedschaften zu diesem Gruppentyp erstellen, löschen und verwalten. Es ist Nutzern nicht möglich, eine Anfrage zum Beitreten oder Verlassen einer unternehmensverwalteten Gruppe zu stellen.

- ***Nutzerverwaltete Gruppen***

  Administratoren können wählen, ob Nutzer ihre eigenen Gruppen erstellen und verwalten können. Administratoren können nutzerverwaltete Gruppen außerdem jederzeit in unternehmensverwaltete Gruppen umwandeln, um die Kontrolle über sie zu übernehmen.

- ***Einschränkung mehrerer Konten auf Computern***

  Administratoren können verhindern, dass Teammitglieder ein zweites Dropbox-Konto mit Computern verknüpfen, die mit ihrem arbeitsbezogenen Dropbox-Konto verknüpft sind.

- ***Nutzerstatus „Gesperrt"***

  Admins können den Zugriff von Nutzern auf ihr Konto sperren, dabei jedoch deren Daten und Freigabebeziehungen sichern, um Unternehmensinformationen zu schützen. Die Admins können das Konto später reaktivieren oder löschen.

- ***Als Nutzer anmelden***

  Team-Admins können sich als Mitglieder ihres Teams anmelden. Dadurch erhalten die Administratoren direkten Zugriff auf die Dateien, Ordner und Paper-Dokumente in den Konten der Teammitglieder, sodass sie Änderungen oder Freigaben im Namen der Teammitglieder vornehmen oder Audits von Ereignissen auf Dateiebene durchführen können. Anmeldungen als Nutzer werden im Aktivitätsprotokoll des Teams aufgezeichnet, und die Administratoren können festlegen, dass Nutzer über diese Ereignisse benachrichtigt werden.

- ***Freigabeberechtigungen***

  Team-Admins haben umfassende Kontrolle über die Freigabemöglichkeiten ihres Teams in Dropbox, einschließlich ob:

  - Teammitglieder Dateien und Ordner an Personen außerhalb des Teams freigeben können
  - Teammitglieder Ordner bearbeiten können, deren Eigentümer Personen außerhalb des Teams sind
  - von Teammitgliedern erstellte geteilte Links bei Personen außerhalb des Teams funktionieren
  - Teammitglieder Dateianfragen erstellen und Dateien von Teammitgliedern und/oder Personen außerhalb des Teams sammeln können
  - Personen außerhalb des Teams Kommentare zu Dateien des Teams anzeigen und verfassen können
  - Teammitglieder Paper-Dokumente und Paper-Ordner für Personen außerhalb des Teams freigeben können
  - Berechtigungen zum endgültigen Löschen erteilt werden

Der Team-Admin eines Kontos von Dropbox Business kann die Möglichkeit zum endgültigen Löschen von Dateien und Paper-Dokumenten ausschließlich auf Team-Admins beschränken.

Onboarding und Bereitstellung für Nutzer

Methoden der Bereitstellung für Nutzer und des Identitätsmanagements

- ***E-Mail-Einladung***

  Mithilfe eines Tools in der Verwaltungskonsole von Dropbox für Unternehmen können Admins manuell eine E-Mail-Einladung generieren.

- ***Active Directory***

  Administratoren von Dropbox für Unternehmen können das Erstellen und Entfernen von Konten aus einem vorhandenen Active Directory-System über unseren Active Directory-Connector oder einen externen Identitätsanbieter automatisieren. Nach der Integration kann die Mitgliedschaft mit Active Directory verwaltet werden.

- ***Einmaliges Anmelden (kurz SSO)***

Mit Dropbox Business können Teammitglieder auch über einen zentralen Identitätsanbieter Zugriff erhalten. Unsere SSO-Implementierung, die die branchenübliche Security Assertion Markup Language 2.0 (SAML 2.0) verwendet, macht die Bereitstellung leichter und sicherer, indem ein vertrauenswürdiger Identitätsanbieter die Kontrolle über die Authentifizierung erhält und Teammitgliedern ohne zusätzliches Passwort Zugriff auf Dropbox gibt. Dropbox arbeitet auch mit führenden Identitätsverwaltungsanbietern zusammen, damit die Bereitstellung von Nutzern bzw. deren Aufhebung automatisch erfolgen kann. Mehr Informationen finden Sie unten im Abschnitt API-Integrationen in Dropbox Business.

- ***API***

  Kunden können mithilfe der API von Dropbox Business nutzerdefinierte Lösungen für Nutzerbereitstellung und Identitätsverwaltung entwickeln. Mehr Informationen finden Sie unten im Abschnitt API-Integrationen in Dropbox Business.

Zweistufige Überprüfung

Diese sehr empfehlenswerte Sicherheitsfunktion fügt dem Dropbox-Konto eine zusätzliche Sicherheitsebene hinzu. Wenn diese Option ausgewählt wurde, erfordert Dropbox zusätzlich zur Eingabe des Passworts jedes Mal die Eingabe eines 6-stelligen Sicherheitscodes, wenn ein Nutzer sich bei Dropbox anmeldet oder eine Verknüpfung mit einem neuen Computer, Smartphone oder Tablet herstellt.

- Administratoren können die zweistufige Überprüfung für alle oder nur spezifische Teammitglieder einrichten.
- Darüber hinaus können Team-Admins verfolgen, welche Teammitglieder eine zweistufige Überprüfung aktiviert haben.
- Die Codes für die zweistufige Überprüfung können per SMS oder über Apps gesendet werden und entsprechen dem TOTP-Algorithmus (Time-Based One-Time Password).
- Falls der Nutzer den Code auf diese Weise nicht abrufen kann, hat er die Möglichkeit, einen einmaligen 16-stelligen Zugangscode anzufordern. Der Nutzer kann alternativ auch eine zweite Telefonnummer angeben, um einen Zugangscode per SMS zu erhalten.
- Dropbox unterstützt außerdem den offenen Standard FIDO Universal 2nd Factor (U2F), bei dem Nutzer sich statt des sechsstelligen Codes mit einem USB-Sicherheitsschlüssel authentifizieren können, den sie eingerichtet haben.

Installationsprogramm für Unternehmen

Wird eine skalierte Bereitstellung gewünscht, können Administratoren den Dropbox-Desktop-Client mit unserem Enterprise-Installationsprogramm für Windows über verwaltete Softwarelösungen und Bereitstellungsmechanismen im Hintergrund und gerätefern installieren.

Verwaltete Geräte und Anmeldung

- ***Enterprise Mobility Management (EMM)***

  Dropbox kann in EMM-Drittanbieterfunktionen integriert werden, damit Administratoren von Dropbox Business mit Enterprise-Abo mehr Kontrolle darüber erhalten, wie Teammitglieder Dropbox auf Mobilgeräten verwenden. Administratoren können die Nutzung mobiler Apps für Dropbox Enterprise-Konten ausschließlich auf verwaltete (vom Unternehmen bereitgestellte oder private) Geräte beschränken, Einblick in die App-Nutzung erhalten (einschließlich verfügbarem Speicherplatz und Zugriffsorten) sowie verloren gegangene oder gestohlene Geräte per Remotezugriff löschen. Beachten Sie bitte, dass die Paper-App für Mobilgeräte nicht durch EMM verwaltet werden kann.

- ***Gerätezulassungen***

  Dropbox ermöglicht es Administratoren von Dropbox Education und Dropbox Business mit Advanced- oder Enterprise-Abo, die Anzahl der Geräte, die ein Nutzer mit Dropbox synchronisieren kann, zu begrenzen und zu entscheiden, ob Genehmigungen von Nutzern oder Administratoren verwaltet werden. Administratoren können auch eine Ausnahmenliste von Nutzern erstellen, die nicht auf eine bestimmte Anzahl von Geräten beschränkt sind. Beachten Sie bitte, dass die Paper-App für Mobilgeräte nicht von den Gerätegenehmigungen betroffen ist.

- ***Obligatorische zweistufige Überprüfung***

  Administratoren können die zweistufige Überprüfung für alle Teammitglieder oder ausgewählte Nutzer einrichten. Andere mehrstufige Authentifizierungsmöglichkeiten können über die SSO-Implementierung des Teams erfolgen.

- ***Passwortverwaltung***

  Die Administratoren von Education-, Advanced- und Enterprise-Teams können bestimmen, dass Nutzer sichere, komplexe Passwörter für ihre Konten verwenden müssen. Wenn diese Funktion aktiviert wird, müssen Teammitglieder sich von ihren Websitzungen abmelden und bei der erneuten Anmeldung neue Passwörter erstellen. Ein integriertes Tool analysiert die Stärke der Passwörter, indem es sie mit einer Datenbank häufig genutzter Wörter, Namen, Muster und Nummern vergleicht. Wenn ein Nutzer ein Passwort angibt, das zu gebräuchlich ist, wird er aufgefordert, ein individuelleres Passwort festzulegen, das schwieriger zu erraten ist. Administratoren können auch Passwörter für das ganze Team oder einzelne Nutzer zurücksetzen.

- ***Domainverwaltung***

  Dropbox bietet eine Reihe von Tools für Unternehmen an, mit denen sich das Onboarding von Nutzern und die Kontrolle der Dropbox-Nutzung vereinfachen und beschleunigen lassen.

  - **Domainüberprüfung**
    Unternehmen können das Eigentumsrecht an ihren Domains beanspruchen und die übrigen Domainverwaltungstools freischalten.

  - **Obligatorische Einladungen**
    Administratoren können durchsetzen, dass einzelne Dropbox-Nutzer, die zum Dropbox-Team des Unternehmens eingeladen wurden, zum Team migrieren oder die E-Mail-Adresse ihres privaten Kontos ändern.

  - **Domain-Analyse**
    Administratoren werden wichtige Informationen angezeigt, wie die Anzahl der individuellen Dropbox-Konten, die geschäftliche E-Mail-Adressen nutzen.

  - **Kontoerfassung**
    Administratoren können erzwingen, dass alle Dropbox-Nutzer, die eine geschäftliche E-Mail-Adresse verwenden, dem Unternehmensteam beitreten oder die E-Mail-Adresse ihres privaten Kontos ändern.

- ***Verwaltung von Websitzungen***

  Admins können festlegen, wie lange Teammitglieder auf dropbox.com angemeldet sein dürfen. Administratoren können die Dauer aller Websitzungen und/oder Sitzungen im Leerlauf begrenzen. Sitzungen, die diese Dauer überschreiten, werden automatisch abgemeldet/beendet. Außerdem können Administratoren die Websitzungen einzelner Nutzer verfolgen und beenden.

- ***App-Zugriff***

  Administratoren haben die Möglichkeit, den Zugriff von Drittanbieter-Apps auf Nutzerkonten zu prüfen und zu widerrufen.

- ***Verknüpfung von Geräten aufheben***

  Die Verknüpfung von Computern oder Mobilgeräten mit Nutzerkonten kann vom Administrator in der Verwaltungskonsole oder durch den Nutzer in den Sicherheitseinstellungen seines Einzelkontos aufgehoben werden. Damit werden auf den Computern die Authentifizierungsdaten gelöscht. Darüber hinaus können lokale Kopien der Dateien entfernt werden, wenn der Computer das nächste Mal mit dem Internet verbunden

ist (siehe nachstehend unter **Remote-Löschen**). Auf Mobilgeräten werden Dateien, die als Favoriten gekennzeichnet sind, sowie zwischengespeicherte Daten und Anmeldedaten gelöscht. Offlineversionen von Paper-Dokumenten werden ebenfalls aus der Paper-App für Mobilgeräte gelöscht. Ist die zweistufige Überprüfung aktiviert, müssen Nutzer alle Geräte beim erneuten Verknüpfen neu authentifizieren. In den Kontoeinstellungen der Nutzer kann außerdem eine automatische E-Mail-Benachrichtigung bei der Verknüpfung mit Geräten eingerichtet werden.

- ***Netzwerksteuerung***

  Administratoren von Dropbox Business mit Enterprise-Abo können die Dropbox-Nutzung im Unternehmensnetzwerk auf das Enterprise-Teamkonto beschränken. Diese Funktion lässt sich in die Lösungen des Netzwerksicherheitsanbieters für das Unternehmensnetzwerk integrieren und sperrt jegliche Nutzung bis auf die des genehmigten Kontos. Beachten Sie bitte, dass Paper zurzeit nicht durch die Netzwerksteuerung verwaltet wird.

Mobile Sicherheit

- ***Scans von Fingerabdrücken***

  Nutzer können Touch ID oder Face ID für iOS-Geräte sowie die Fingerabdruckerkennung (sofern unterstützt) auf Android-Geräten nutzen, um die Dropbox-App für Mobilgeräte zu entsperren.

Zugriffstransparenz

- ***Identitätsüberprüfung durch den technischen Support***

  Bevor der Dropbox-Support Fehler behebt oder Kontoinformationen bereitstellt, muss der Team-Admin einen einmaligen, zufällig generierten Sicherheitscode angeben, um seine Identität nachzuweisen. Diese PIN ist nur über die Verwaltungskonsole erhältlich.

Kontoaktivität der Nutzer

Jeder Nutzer kann die folgenden Seiten von seinen Kontoeinstellungen aus einsehen, um aktuelle Informationen über seine Kontoaktivitäten zu erhalten.

- ***Die Seite „Freigabe“***

  Auf dieser Seite werden die freigegebenen Ordner angezeigt, die sich derzeit in der Nutzer-Dropbox befinden, sowie die freigegebenen Ordner, die der Nutzer hinzufügen kann. Nutzer können die Freigabe von Ordnern sowie Dateien aufheben und Freigabeberechtigungen festlegen.

- ***Die Seite „Dateien“***

  Auf dieser Seite werden die Dateien angezeigt, die für den Nutzer freigegeben wurden, sowie die jeweiligen Freigabedaten. Ein Nutzer kann seinen Zugriff auf diese Dateien aufheben. In der Navigationsoberfläche für Paper-Dokumente kann der Nutzer die Ansicht „Für mich freigegeben“ auswählen, um zu sehen, welche Paper-Dokumente von anderen Nutzern für ihn freigegeben wurden.

- ***Die Seite „Links“***

  Auf dieser Seite werden alle vom Nutzer erstellten aktiven freigegebenen Links sowie das jeweilige Erstellungsdatum angezeigt. Außerdem sind hier alle Links zu sehen, die von anderen Personen für den Nutzer freigegeben wurden. Der Nutzer kann Links deaktivieren oder Berechtigungen ändern.

- ***E-Mail-Benachrichtigungen***

  Nutzer können E-Mail-Benachrichtigungen für den Fall aktivieren, dass ein neues Gerät oder eine neue App mit ihrem Dropbox-Konto verknüpft wird.

Kontoberechtigungen für Nutzer

- ***Verknüpfte Geräte***

  Der Bereich **Geräte** in den Sicherheitseinstellungen eines Nutzerkontos zeigt alle Computer und Mobilgeräte an, die mit dem Konto verknüpft sind. Für jeden Computer werden die IP-Adresse, das Land und der ungefähre Zeitpunkt der letzten Aktivität angezeigt. Nutzer können die Verknüpfung zu jedem Gerät aufheben und dabei eine Option aktivieren, mit der die Dateien auf einem verknüpften Computer gelöscht werden, sobald dieser das nächste Mal mit dem Internet verbunden wird.

- ***Aktive Websitzungen***

  Im Bereich **Sitzungen** finden sich alle Webbrowser, die zurzeit in einem Nutzerkonto angemeldet sind. Für jeden Webbrowser werden die IP-Adresse, das Land und der Anmeldezeitpunkt der neuesten Sitzung sowie der ungefähre Zeitpunkt der letzten Aktivität angezeigt. Nutzer können jede Sitzung standortunabhängig über ihre Sicherheitseinstellungen beenden.

- ***Verknüpfte Apps***

  Der Abschnitt über **verknüpfte Apps** enthält eine Liste aller Drittanbieter-Apps mit Zugriff auf Nutzerkonten. Außerdem erfahren Sie, inwieweit jede dieser Apps auf die Konten zugreifen kann. Nutzer können die Zugriffsberechtigung einer App auf ihr Dropbox-Konto jederzeit widerrufen.

Aktivitätsfeed

Dropbox für Unternehmen zeichnet Dateiaktionen im Aktivitätsfeed des Teams auf, der über die Verwaltungskonsole eingesehen werden kann. Für den Aktivitätsfeed stehen flexible Filteroptionen zur Verfügung, wodurch Admins gezielt Konto-, Datei- oder Paper-Dokumentereignisse untersuchen können. Sie können beispielsweise den vollständigen Verlauf einer Datei oder eines Paper-Dokuments und die Interaktionen der Nutzer einsehen oder alle Aktivitäten des Teams in einem bestimmten Zeitraum überprüfen. Der Aktivitätsfeed kann als Bericht im CSV-Format heruntergeladen und auch über Partnerlösungen von Drittanbietern direkt in SIEM (Security Information and Event Management) oder ein anderes Analysetool integriert werden. Die folgenden Inhaltsereignisse werden im Aktivitätsfeed aufgezeichnet:

- ***Freigabe von Dateien, Ordnern und Links***

  Sofern zutreffend, enthalten Berichte Angaben dazu, ob Personen außerhalb des Teams involviert sind.

  Freigegebene Dateien

  - Teammitglied oder teamfremder Nutzer wurde hinzugefügt oder entfernt.
  - Berechtigungen für ein Teammitglied oder einen teamfremden Nutzer wurden geändert.
  - Gruppe wurde hinzugefügt oder entfernt.
  - Freigegebene Datei wurde zum Dropbox-Ordner des Nutzers hinzugefügt.
  - Inhalt einer Datei, die über eine Datei- oder Ordner-Einladung freigegeben wurde, wurde angezeigt.
  - Geteilte Inhalte wurden in den Dropbox-Ordner des Nutzers kopiert.
  - Freigegebene Inhalte wurden heruntergeladen.
  - Datei wurde kommentiert.
  - Kommentar wurde geklärt oder nicht geklärt.
  - Kommentar wurde gelöscht.

- Abo für Kommentarbenachrichtigungen wurde hinzugefügt oder gekündigt.
- Einladung zu einer Datei des Teams wurde angenommen.
- Zugriff auf eine Datei des Teams wurde angefragt.
- Freigabe einer Datei wurde aufgehoben.

Freigegebene Ordner

- Neuer freigegebener Ordner wurde erstellt.
- Teammitglied, teamfremder Nutzer oder Gruppe wurde hinzugefügt oder entfernt.
- Freigegebener Ordner wurde zum Dropbox-Konto des Nutzers hinzugefügt oder Nutzer hat eigenen Zugriff auf einen freigegebenen Ordner entfernt.
- Freigegebener Ordner aus einem Link wurde hinzugefügt.
- Berechtigungen für ein Teammitglied oder einen teamfremden Nutzer wurden geändert.
- Eigentum eines Ordners wurde an einen anderen Nutzer übertragen.
- Ordnerfreigabe wurde aufgehoben.
- Mitgliedschaft für einen freigegebenen Ordner wurde beansprucht.
- Zugriff auf freigegebenen Ordner wurde angefragt.
- Anfragender Nutzer wurde zu einem freigegebenen Ordner hinzugefügt.
- Hinzufügen zu einem Ordner wurde für teamfremde Nutzer erlaubt oder verweigert.
- Allen Teammitgliedern bzw. nur dem Eigentümer wurde erlaubt, Personen zu einem Ordner hinzuzufügen.
- Gruppenzugriff auf einen freigegebenen Ordner wurde geändert.

Geteilte Links

- Link wurde erstellt oder entfernt.
- Inhalte eines Links wurden für alle mit dem Link oder nur für Teammitglieder sichtbar gemacht.
- Inhalte eines Links wurden mit einem Passwort geschützt.
- Gültigkeitsdauer eines Links wurde festgelegt oder entfernt.
- Link wurde angezeigt.
- Inhalte eines Links wurden heruntergeladen.
- Inhalte eines Links wurden in den Dropbox-Ordner eines Nutzers kopiert.
- Link zu einer Datei wurde über eine API-App erstellt.
- Link wurde für ein Teammitglied, einen teamfremden Nutzer oder eine Gruppe freigegeben.
- Teamfremden Nutzern wurde die Anzeige von Links zu Dateien in einem freigegebenen Ordner erlaubt oder verweigert.
- Album wurde geteilt.

Dateianfragen

- Dateianfrage wurde erstellt, geändert, geschlossen oder gelöscht.
- Nutzer wurden zu Dateianfrage hinzugefügt.
- Frist für Dateianfrage wurde hinzugefügt oder entfernt.
- Ordner für Dateianfrage wurde geändert.
- Dateien wurden über Dateianfrage empfangen.
- Dateien wurden via Email to Dropbox empfangen.

Ereignisse zu einzelnen Dateien und Ordnern

- Datei wurde zu Dropbox hinzugefügt.
- Ordner wurde erstellt.
- Datei wurde angesehen.
- Datei wurde bearbeitet.
- Datei wurde heruntergeladen.
- Eine Datei oder ein Ordner wurde kopiert.
- Eine Datei oder ein Ordner wurde verschoben.
- Eine Datei oder ein Ordner wurde umbenannt.
- Eine Datei wurde auf eine frühere Version zurückgesetzt.
- Änderungen an Dateien wurden rückgängig gemacht.
- Eine gelöschte Datei wurde wiederhergestellt.
- Eine Datei oder ein Ordner wurde gelöscht.
- Eine Datei oder ein Ordner wurde endgültig gelöscht.

Erfolgreiche und fehlgeschlagene Anmeldeversuche

- Erfolgreicher oder fehlgeschlagener Anmeldeversuch.
- Fehlgeschlagener Anmeldeversuch oder Fehler über einmaliges Anmelden (kurz SSO).
- Fehlgeschlagener Anmeldeversuch oder Fehler über EMM.
- Abgemeldet.
- Änderung der IP-Adresse für Websitzung.

Passwörter

Die Einstellungen für Passwörter oder die zweistufige Überprüfung können angepasst werden. Admins können die Passwörter der Nutzer nicht einsehen.

- Passwort wurde geändert oder zurückgesetzt.
- Zweistufige Überprüfung wurde aktiviert, zurückgesetzt oder deaktiviert.

- Zweistufige Überprüfung wurde eingerichtet oder geändert, um SMS oder eine App für Mobilgeräte zu nutzen.
- Backup-Telefonnummer für die zweistufige Überprüfung wurde hinzugefügt, geändert oder entfernt.
- Sicherheitsschlüssel für die zweistufige Überprüfung wurde hinzugefügt oder entfernt.

Mitgliedschaft

Hinzufügen und Entfernen von Teammitgliedern.

- Ein Teammitglied wurde eingeladen.
- Ist dem Team beigetreten.
- Ein Teammitglied wurde entfernt.
- Ein Teammitglied wurde zeitweilig gesperrt bzw. die Sperre wurde aufgehoben.
- Ein Teammitglied wurde wiederhergestellt oder entfernt.
- Der Beitritt zum Team basierend auf der Kontodomain wurde angefragt.
- Eine Teambeitrittsanfrage basierend auf der Kontodomain wurde genehmigt oder abgelehnt.
- Domaineinladungen zu vorhandenen Domainkonten wurden versendet.
- Nutzer ist dem Team aufgrund der Kontoerfassung beigetreten.
- Nutzer hat die Domain aufgrund der Kontoerfassung verlassen.
- Teammitgliedern wurde die Möglichkeit zum Vorschlagen neuer Teammitglieder erlaubt oder verweigert.
- Ein Neues Teammitglied wurde vorgeschlagen.

Apps

Verknüpfung von Drittanbieter-Apps mit Dropbox-Konten

- Eine Anwendung wurde autorisiert oder entfernt.
- Eine Teamanwendung wurde autorisiert oder entfernt.

Geräte

Verknüpfung von Computern oder Mobilgeräten mit Dropbox-Konten.

- Ein Gerät wurde verknüpft oder die Verknüpfung wurde aufgehoben.
- Remote-Löschen wurde eingesetzt und alle Dateien wurden erfolgreich gelöscht oder das Löschen einiger Dateien ist fehlgeschlagen.
- Änderung der IP-Adresse für Desktop-Computer oder Mobilgerät.

Admin-Aktionen

Änderungen der Einstellungen in der Verwaltungskonsole, wie etwa die Berechtigungen für freigegebene Ordner.

- ***Authentifizierung und einmaliges Anmelden (kurz SSO)***
  - Das Passwort eines Teammitglieds wurde zurückgesetzt.
  - Die Passwörter aller Teammitglieder wurden zurückgesetzt.

- Teammitgliedern wurde die Deaktivierung der zweistufigen Überprüfung erlaubt oder verweigert.
- SSO wurde aktiviert oder deaktiviert.
- Die Anmeldung über SSO wurde als erforderlich festgelegt.
- Die SSO-URL wurde geändert oder entfernt.
- Das SSO-Zertifikat wurde aktualisiert.
- Der SSO-Identitätsmodus wurde geändert.

- ***Mitgliedschaft***
  - Anfragen zum Beitritt eines Nutzers zum Team basierend auf der Kontodomain wurden erlaubt oder verweigert.
  - Festlegung, dass Teambeitrittsanfragen automatisch genehmigt werden oder manuelle Administratorgenehmigung brauchen.

- ***Verwaltung von Mitgliederkonten***
  - Der Name eines Teammitglieds wurde geändert.
  - Die E-Mail-Adresse eines Teammitglieds wurde geändert.
  - Admin-Status wurde gewährt bzw. entfernt oder die Admin-Rolle wurde geändert.
  - Ein Teammitglied hat sich an- oder abgemeldet.
  - Die Inhalte des Kontos eines entfernten Teammitglieds wurden übertragen oder gelöscht.
  - Die Inhalte des Kontos eines entfernten Teammitglieds wurden endgültig gelöscht.

- ***Allgemeine Freigabeeinstellungen***
  - Das Hinzufügen von freigegebenen Ordnern von teamfremden Nutzern durch Teammitglieder wurde erlaubt oder verweigert.
  - Teammitgliedern wurde die Freigabe von Ordnern an teamfremde Nutzer erlaubt oder verweigert.
  - Warnmeldungen für Nutzer, bevor diese Ordner für teamfremde Nutzer freigeben, wurden aktiviert.
  - Teamfremden Nutzern wurde die Anzeige von geteilten Links erlaubt oder verweigert.
  - Geteilte Links sind standardmäßig nur für Teammitglieder verfügbar.
  - Personen wurde das Verfassen von Kommentaren zu Dateien erlaubt oder verweigert.
  - Teammitgliedern wurde das Erstellen von Dateianfragen erlaubt oder verweigert.
  - Ein Logo für Seiten mit geteilten Links wurde hinzugefügt, geändert oder entfernt.
  - Teammitgliedern wurde die Freigabe von Paper-Dokumenten und Paper-Ordnern an teamfremde Nutzer erlaubt oder verweigert.

- ***Teamordner-Verwaltung für Dateien***
  - Ein Teamordner wurde erstellt.
  - Ein Teamordner wurde umbenannt.
  - Ein Teamordner wurde archiviert oder aus dem Archiv verschoben.
  - Ein Teamordner wurde dauerhaft gelöscht.
  - Ein Teamordner wurde zu einem freigegebenen Ordner herabgestuft.

- ***Domainverwaltung***
  - Es wurde versucht, eine Domain zu überprüfen, oder eine Domain wurde erfolgreich überprüft oder eine Domain wurde entfernt.
  - Eine Domain wurde vom Dropbox-Support überprüft oder entfernt.
  - Der Versand von Domaineinladungen wurde aktiviert oder deaktiviert.
  - „Neue Nutzer automatisch einladen“ wurde aktiviert oder deaktiviert.
  - Der Kontoerfassungsmodus wurde geändert.
  - Die Kontoerfassung wurde vom Dropbox-Support bewilligt oder aufgehoben.
- ***Enterprise Mobility Management (EMM)***
  - EMM wurde im Testmodus (optional) oder Bereitstellungsmodus (erforderlich) aktiviert.
  - Der EMM-Token wurde aktualisiert.
  - Teammitglieder wurden zur EMM-Liste ausgeschlossener Nutzer hinzugefügt oder daraus entfernt.
  - EMM wurde deaktiviert.
  - Ein Bericht mit EMM-Ausnahmenliste wurde erstellt.
  - Ein EMM-Bericht zur Nutzung der App für Mobilgeräte wurde erstellt.
- ***Änderungen an anderen Teameinstellungen***
  - Teams wurden zusammengeführt.
  - Das Team wurde zu Dropbox Business hochgestuft oder zu einem kostenlosen Team herabgestuft.
  - Der Teamname wurde geändert.
  - Ein Team-Aktivitätsbericht wurde erstellt.
  - Teammitgliedern wurden mehrere mit einem Computer verknüpfte Konten erlaubt oder verweigert.
  - Das Erstellen von Gruppen wurde allen Teammitgliedern oder nur Admins erlaubt.
  - Teammitgliedern wurde das endgültige Löschen von Dateien erlaubt oder verweigert.
  - Eine Dropbox-Support-Sitzung für einen Reseller wurde gestartet oder beendet.

Gruppen

Erstellen, Löschen und Informationen zur Mitgliedschaft für Gruppen.

- Eine Gruppe wurde erstellt, umbenannt, verschoben oder gelöscht.
- Ein Mitglied wurde hinzugefügt oder entfernt.
- Die Zugriffsart eines Gruppenmitglieds wurde geändert.
- Gruppe wurde zu „von Team verwaltet“ oder „von Administrator verwaltet“ geändert.
- Externe ID einer Gruppe wurde geändert.

Paper-Aktivitätsprotokoll

Admins können eine bestimmte Paper-Aktivität im Aktivitätsfeed auswählen oder einen vollständigen Aktivitätsbericht herunterladen. Die folgenden Paper-Ereignisse werden aufgezeichnet:

- Paper wurde aktiviert oder deaktiviert.
- Paper-Dokument wurde erstellt, bearbeitet, exportiert, archiviert, endgültig gelöscht oder wiederhergestellt.
- Paper-Dokument wurde kommentiert oder Kommentare wurden geklärt.
- Paper-Dokument wurde für Teammitglieder und teamfremde Nutzer freigegeben oder Freigabe wurde aufgehoben.
- Teammitglieder oder teamfremde Nutzer haben Zugriff auf Paper-Dokument angefragt.
- Teammitglieder oder teamfremde Nutzer wurden in Paper-Dokument erwähnt.
- Paper-Dokument wurde von Teammitgliedern oder teamfremden Nutzern angesehen.
- Paper-Dokument wurde abonniert.
- Berechtigungen für Paper-Dokument haben sich geändert (Bearbeiten, Kommentieren, nur Betrachten).
- Externe Freigaberichtlinien für Paper-Dokument wurden geändert.
- Paper-Ordner wurde erstellt, archiviert oder endgültig gelöscht.
- Paper-Dokument wurde einem Ordner hinzugefügt oder daraus entfernt.
- Paper-Ordner wurde umbenannt.
- Paper-Dokument- und -Ordnerübertragungen.

Dropbox Passwords

Dropbox Passwords ist eine sichere und einfache Möglichkeit, Nutzernamen, Passwörter und Kredit- sowie Debitkarten geräteübergreifend zu speichern, zu synchronisieren und automatisch auszufüllen, damit Sie Ihre Online-Anmeldedaten schützen können. Dropbox Passwords schützt die sensiblen Nutzernamen und Passwörter Ihrer Online-Konten sowie Kredit- und Debitkarteninformationen mit Zero-Knowledge-Verschlüsselung in der Cloud und auf Ihren Geräten. Unsere Produkte sind für die tägliche Anwendung konzipiert und wurden mit einem Fokus auf Sicherheit entwickelt.

Zero-Knowledge-Verschlüsselung

Dropbox Passwords speichert Ihre verschlüsselten Daten in der Cloud – aber die Schlüssel zum Entschlüsseln dieser Daten werden nur auf Ihren Geräten gespeichert. **Dropbox hat niemals Zugriff darauf.** Diese Schlüssel sind lang, zufällig und werden auf Ihrem Gerät generiert. Sie verlassen Ihr Gerät nie, außer wenn Sie ein neues Gerät verbinden oder registrieren. Diese Übertragung verwendet Public-Key-Kryptografie, um die Schlüssel während der Übertragung sowohl kryptografisch zu signieren als auch zu schützen. So sind sie entschlüsselungssicher und werden gleichzeitig auf Authentizität geprüft. Dies wird oft als Zero-Knowledge-Verschlüsselung bezeichnet, da die verschlüsselten Daten für alle nutzlos sind, die nicht über die Schlüssel verfügen – einschließlich Dropbox. Das bedeutet, dass **nur Sie Ihre Informationen einsehen können** und Ihre Daten im unwahrscheinlichen Fall, dass Dropbox gehackt wird, immer noch sicher sind. Die verschlüsselten Daten werden von sichtbaren Dropbox-Ordnern getrennt und können nicht mit Dropbox-Clients oder -APIs durchsucht werden.

Einzelheiten zur Verschlüsselung

Dropbox verschlüsselt Ihre Daten mit XChaCha20-Poly1305 im kombinierten Modus für die implizite Authentifizierung. Unsere Browsererweiterungen und Apps für Mobilgeräte verwenden alle Verschlüsselungsimplementierungen, die von libsodium unterstützt werden, einem geprüften und weit verbreiteten Fork von NaCl.

Jede Verschlüsselungsoperation generiert eine zufällige 192-Bit-Nonce, die für eine spätere Entschlüsselung mit den verschlüsselten Daten gespeichert wird. Im Gegensatz zu AES-GCM unterstützt XChaCha20-Poly1305 zufällige Nonces. Beim Entschlüsseln wird die 192-Bit-Nonce aus den Daten gelesen und zum Entschlüsseln der verschlüsselten Daten verwendet. Jede nachfolgende Verschlüsselung erzeugt eine zufällige 192-Bit-Nonce, die von der vorherigen Nonce unabhängig ist. Dropbox Passwords generiert Zufallszahlen mithilfe von libsodium, das auf allen von uns unterstützten Plattformen standardmäßig einen kryptografisch sicheren Zufallszahlengenerator verwendet.

Schlüssel und Wiederherstellungswörter

Wir generieren einen symmetrischen 256-Bit-Schlüssel (den Verschlüsselungsschlüssel) aus 128-Bit-Entropie (dem Nutzerschlüssel) via Blake2-Hashing. Dieser Verschlüsselungsschlüssel bleibt ausschließlich auf den Geräten seines Besitzers und nach Möglichkeit im sichersten Speicher, auf den wir auf diesen Geräten Zugriff haben. Auf iPhones speichern wir den Verschlüsselungsschlüssel beispielsweise im iOS-Schlüsselbund.

Wir verwenden 128-Bit-Entropie als Quelle, weil sie ausreichende Sicherheit bietet und mit dem BIP-39-Standard für die Sicherung dabei nur 12 Wiederherstellungswörter erfordert. BIP-39 bietet eine nutzerfreundliche Möglichkeit, große Zufallsschlüssel darzustellen, indem diese Schlüssel in eine Liste mit 12 Wörtern umgewandelt werden. Jeder 128-Bit-Schlüssel hat eine entsprechende Liste von Wörtern und jede Liste mit 12 Wörtern steht eindeutig für 128 Bits. Der einzige Punkt besteht darin, dass die 12 Wörter tatsächlich 132 Bits entsprechen, sodass die zusätzlichen vier Bits als Prüfsumme zum Identifizieren von Fehlern verwendet werden. Die Wiederherstellungswörter bieten Ihnen eine Möglichkeit, Ihren Verschlüsselungsschlüssel wiederherzustellen, falls Ihr Gerät verloren geht oder gestohlen wird. Wir empfehlen, die Wörter auszudrucken und an einem sicheren Ort aufzubewahren. Sie können sie auch einem zuverlässigen Freund oder Familienmitglied geben oder auf einem USB-Stick speichern.

Geräteregistrierung

Wenn sich ein Nutzer auf einem neuen Gerät bei Dropbox Passwords anmeldet, muss dieses Gerät ein sicheres Registrierungsverfahren durchlaufen, um auf die Passwords-Daten des Nutzers zugreifen zu können. Dieses Verfahren hilft sicherzustellen, dass der Zugriff auf den geheimen Schlüssel und die Passwords-Daten eines Nutzers nur auf registrierten Geräten des Nutzers möglich ist. Es stellt auch sicher, dass ein Nutzer nur dann zusätzliche Geräte registrieren kann, wenn er Zugriff auf ein vorhandenes registriertes Gerät oder seine Wiederherstellungswörter hat. Das Geräteregistrierungsverfahren läuft wie folgt ab.

Ein neu zu registrierendes Gerät generiert zufällig ein 256-Bit-Geräteschlüsselpaar aus öffentlichem/privatem Schlüssel und lädt den öffentlichen Schlüssel auf den Dropbox-Server hoch. Dann tritt entweder Szenario **A**, **B** oder **C** ein.

A: Wenn der Nutzer zuvor noch kein Gerät registriert hat, generiert das zu registrierende Gerät nach dem Zufallsprinzip einen geheimen 128-Bit-Nutzerschlüssel. Sowohl der Nutzerschlüssel als auch das Geräteschlüsselpaar werden an einem sicheren, betriebssystemspezifischen Ort gespeichert, wie im folgenden Abschnitt zur Schlüsselspeicherung beschrieben. Das Gerät initialisiert die Passwords-Daten des Nutzers, verschlüsselt sie und lädt die verschlüsselten Daten auf den Dropbox-Server hoch.

B: Wenn der Nutzer zuvor ein oder mehrere Geräte registriert hat, wird eine Anfrage zur Genehmigung der Registrierung an jedes dieser Geräte gesendet. Der öffentliche Schlüssel des zu registrierenden Geräts wird an die Anfrage angehängt. Der Nutzer muss die Anfrage dann auf einem seiner registrierten Geräte genehmigen. Bei Genehmigung verschlüsselt das registrierte Gerät den Nutzerschlüssel mit seinem privaten Schlüssel und dem öffentlichen Schlüssel des zu registrierenden Geräts über X25519 ECDH mit XSalsa20-Poly1305. Das registrierte Gerät lädt den verschlüsselten Nutzerschlüssel auf den Dropbox-Server hoch, um ihn an das zu registrierende Gerät zu senden. Das zu registrierende Gerät lädt den Nutzerschlüssel herunter und entschlüsselt ihn unter Verwendung seines privaten Schlüssels und des öffentlichen Schlüssels des registrierten Geräts. Das zu registrierende Gerät lädt dann die verschlüsselten Passwords-Daten herunter und entschlüsselt sie mit dem Nutzerschlüssel.

C: Wenn der Nutzer zuvor ein Gerät registriert hat, aber nicht mehr darauf zugreifen kann, kann er seine 12 Wiederherstellungswörter eingeben, um den Nutzerschlüssel lokal zu rekonstruieren. Das zu registrierende Gerät lädt dann die verschlüsselten Passwords-Daten herunter und entschlüsselt sie mit dem Nutzerschlüssel.

Schlüsselspeicherung

Browsererweiterungen

Bei Webbrowsern wird der Nutzerschlüssel im lokalen Speicher der Browsererweiterung gespeichert. Werte im lokalen Speicher der Browsererweiterung können nur über die Erweiterung abgerufen werden. Code auf Websites, die der Nutzer besucht, kann den lokalen Speicher der Browsererweiterung nicht auslesen. Darüber hinaus verbieten Browsererweiterungen die Ausführung von Code, der nicht im signierten Erweiterungspaket enthalten ist, was das Risiko einer XSS-Schwachstelle beseitigt, die auf Werte im lokalen Speicher zugreifen würde.

Ein Angreifer mit uneingeschränktem Zugriff auf das Gerät des Nutzers kann auf den Nutzerschlüssel zugreifen, indem er die Datei im lokalen Speicher auf der Festplatte ausliest. Beispiele für solche Bedrohungen sind Angreifer mit physischem Zugriff auf das Gerät oder Angreifer, die Malware auf dem Gerät ausführen. Zum Schutz vor diesen Szenarien kann der Nutzer eine Passphrase für das lokale Gerät konfigurieren.

Wenn eine Passphrase konfiguriert ist, wird der Nutzerschlüssel im Ruhezustand im lokalen Speicher der Browsererweiterung verschlüsselt. Der Verschlüsselungsschlüssel wird von der Passphrase durch Argon2-Passwort-Hashing abgeleitet; die verwendete Verschlüsselungsmethode ist XChaCha20-Poly1305. Bei jedem Neustart der Browsererweiterung muss der Nutzer seine Passphrase eingeben, um den Nutzerschlüssel zu entschlüsseln und seine Daten zu entsperren. Folglich kann ein Angreifer ohne die Passphrase den in der Datei im lokalen Speicher auf der Festplatte gespeicherten Nutzerschlüssel nicht entschlüsseln.

iOS

Unter iOS wird der Nutzerschlüssel im iOS-Schlüsselbund gespeichert, eine verschlüsselte Datenbankdatei auf der Festplatte. Diese Datei wird mit einem geheimen Schlüssel verschlüsselt, der im Secure Enclave-Hardwaremodul gespeichert ist; AES256-GCM wird als Verschlüsselungsmethode verwendet. Nur die signierte Dropbox Passwords iOS-App kann auf die Elemente zugreifen, die sie im Schlüsselbund gespeichert hat. Dadurch wird verhindert, dass anderer Code, der auf dem Gerät des Nutzers ausgeführt wird, auf den Nutzerschlüssel zugreift.

Android

Unter Android wird der Nutzerschlüssel in einem EncryptedSharedPreferences-Objekt gespeichert; das ist eine verschlüsselte Einstellungsdatei auf der Festplatte. Diese Datei wird mit einem Hauptschlüssel verschlüsselt, der in der sicheren Android Keystore-Hardware gespeichert ist; AES256-GCM wird als Verschlüsselungsmethode verwendet. Nur die signierte Dropbox Passwords-Android-App kann auf den Hauptschlüssel zugreifen, der zum Entschlüsseln der Einstellungsdatei verwendet wird.

Lokale Authentifizierung

Dropbox Passwords bietet optionale Maßnahmen zur lokalen Authentifizierung, um den Zugriff auf die Passwords-Daten eines Nutzers auf seinem physischen Gerät weiter einzuschränken. Für Apps für Mobilgeräte kann die lokale OS-Authentifizierungsgeste wiederverwendet werden (d. h.: ein PIN-Code mit zusätzlicher biometrischer Authentifizierung). Für Browsererweiterungen kann eine optionale Passphrase konfiguriert werden. Diese Mechanismen bieten eine zusätzliche Sicherheitsebene für die Anwendung, wenn das Betriebssystem des Nutzergeräts entsperrt ist. Dadurch kann der Nutzer seine Passwords-Daten sichern, wenn ein anderer Nutzer auf sein Gerät zugreift, z. B. ein Familienmitglied oder ein Kollege.

Vorschlag zur Passwortstärke

Dropbox hat das Open-Source-Tool zxcvbn entwickelt, das von mehreren Passwortmanagern verwendet wird, um die Passwortstärke zu schätzen. Das Tool vergleicht Passwörter mit einer Datenbank von 30.000 gängigen Passwörtern, gebräuchlichen Vor- und Nachnamen laut US-Volkszählungsdaten, beliebten englischen Wörtern aus Wikipedia sowie Film und Fernsehen aus den USA und anderen gängigen Mustern wie Daten, Wiederholungen (aaa), Sequenzen (abcd), Tastaturmustern (qwertyuiop) und Leet (1337) Speak. Wenn das Passwort, das ein Nutzer eingibt, gängig ist, fordert das Tool ihn auf, ein eindeutigeres und schwieriger zu erratendes Passwort einzugeben. Die Verwendung der Einstellung **„Sehr stark“** trägt dazu bei, die höchste Kontosicherheit für Nutzer zu gewährleisten.

Datensicherheit, Datenschutz und Transparenz

Tagtäglich vertrauen Menschen zu Hause und in Organisationen Dropbox ihre wichtigste Arbeit an. Wir betrachten es deshalb als unsere Aufgabe, diese Informationen zu schützen und sie vertraulich zu behandeln.

Datenschutzrichtlinie

Unsere Datenschutzrichtlinie kann unter dropbox.com/privacy eingesehen werden. Die Datenschutzrichtlinie, die Dienstleistungsvereinbarung, die Allgemeinen Geschäftsbedingungen sowie die Richtlinie über die zulässige Nutzung von Dropbox enthalten folgende Informationen:

- Welche Art von Daten erheben wir und warum?
- An wen geben wir Informationen weiter?

- Wie schützen wir diese Daten und wie lange bewahren wir sie auf?
- Wo bewahren wir Ihre Daten auf und wohin übertragen wir sie?
- Wie gehen wir vor, wenn Richtlinien geändert werden müssen oder wenn Sie Fragen haben?

Transparenz

Dropbox verpflichtet sich, die Anzahl und Art der Auskunftsanträge zu Nutzerdaten offenzulegen, die wir von Strafverfolgungsbehörden erhalten. Wir prüfen die Rechtmäßigkeit aller Anträge sorgfältig und benachrichtigen Nutzer, soweit gesetzlich zulässig, wenn ihr Konto von den Auskunftsanträgen einer Strafverfolgungsbehörde betroffen ist.

Diese Bemühungen unterstreichen unsere Verpflichtung, die Privatsphäre unserer Nutzer und deren Daten zu schützen. Zu diesem Zweck veröffentlichen wir einen Transparenzbericht und haben eine Reihe von Richtlinien zu behördlichen Anfragen erstellt. Die folgenden Richtlinien regeln unsere Vorgehensweise beim Erhalt sowie bei der Überprüfung und Beantwortung von behördlichen Anfragen hinsichtlich der Daten unserer Nutzer:

- ***Transparenz***

  Wir sind der Ansicht, dass es Onlinediensten gestattet sein sollte, die Anzahl und die Art der erhaltenen behördlichen Anfragen zu veröffentlichen und Personen darüber zu informieren, wenn Angaben zu ihnen angefragt wurden. Diese Art der Transparenz stärkt die Position von Nutzern, indem sie dabei unterstützt werden, Fälle und Muster von Eingriffen durch Regierungen besser zu verstehen. Wir werden weiterhin detaillierte Informationen zu diesen Anfragen veröffentlichen und uns für das Recht auf die Weitergabe weiterer derart wichtiger Informationen einsetzen.

- ***Widerstand gegen zu breit gefasste Anfragen***

  Datenanfragen von Regierungen sollten sich auf spezifische Personen und rechtmäßige Untersuchungen beschränken. Wir werden uns gegen pauschale und zu breit gefasste Anfragen wehren.

- ***Schutz für alle Nutzer***

  Gesetze, durch die Menschen unterschiedlichen Schutz genießen, abhängig davon, wo sie leben oder welche Staatsbürgerschaft sie haben, sind veraltet und spiegeln nicht den globalen Charakter von Onlinediensten wider. Wir werden uns weiterhin für eine Änderung dieser Gesetze einsetzen.

- ***Bereitstellung vertrauenswürdiger Dienste***

  Regierungen sollten niemals Hintertüren in Onlinedienste implementieren oder in die Infrastruktur eindringen, um an Nutzerdaten zu gelangen. Wir arbeiten auch weiterhin daran, unsere Systeme zu schützen und die Gesetzgebung zu ändern, um klar darauf hinzuweisen, dass solche Aktivitäten illegal sind.

Unsere Transparenzberichte sind einsehbar unter dropbox.com/transparency.

Datenschutzzertifizierungen, Bescheinigungen und Einhaltung von Vorschriften

Jeden Tag vertrauen Menschen und Organisationen Dropbox ihre wichtigsten Arbeitsdateien an. Deshalb betrachten wir es als unsere Aufgabe, diese Dateien zu schützen und vertraulich zu behandeln. Unser Einsatz für Ihre Privatsphäre steht im Mittelpunkt jeder Entscheidung, die wir treffen.

ISO/IEC 27018 (Verhaltenskodex für den Schutz personenbezogener Daten in der Cloud) sowie ISO/IEC-27701 (Erweiterung für ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutz-Informationsmanagement)

Dropbox Business war einer der ersten namhaften Clouddienst-Anbieter mit ISO/IEC 27018- und ISO/IEC 27701-Zertifizierung.

ISO/IEC 27018 ist der globale Standard für Datenschutz und Datensicherheit in der Cloud. Er wurde im August 2014 veröffentlicht und beschäftigt sich speziell mit Datenschutz und Datensicherheit bei Nutzern.

ISO/IEC 27701 ist die erste zertifizierbare globale Norm für das Datenschutz-Informationsmanagement. Sie wurde 2019 veröffentlicht, um einen Rahmen für die Erweiterung von Information Security Management Systems (ISMS) unter ISO/IEC 27001 auf ein Privacy Information Management System (PIMS) zu bieten, indem auch Überlegungen zum Datenschutz berücksichtigt werden.

Die Normen erläutern zahlreiche Anforderungen an Dropbox hinsichtlich der Verwendung Ihrer Unternehmensdaten:

- ***Ihr Unternehmen hat die Kontrolle über Ihre Daten***

  Wir verwenden die personenbezogenen Daten, die Sie uns mitteilen, ausschließlich zur Erbringung der Dienstleistungen, für die Sie sich registriert haben. Sie können Dateien und Paper-Dokumente in Dropbox nach Bedarf hinzufügen, ändern oder löschen.

- ***Wir unterstützen den transparenten Umgang mit Ihren Daten***

  Wir geben Ihnen Auskunft darüber, wo Ihre Daten auf unseren Servern gespeichert sind und mit welchen Drittunternehmen wir zusammenarbeiten. Wir teilen Ihnen mit, was passiert, wenn Sie ein Konto schließen oder eine Datei oder ein Paper-Dokument löschen – und wir benachrichtigen Sie auch, wenn sich einer dieser Aspekte ändert.

- ***Ihre Daten sind sicher und geschützt***

  ISO/IEC 27018 und ISO/IEC 27701 wurden als Erweiterungen für ISO/IEC 27001 entwickelt, eine der weltweit anerkanntesten Normen für Informationssicherheit. Wir haben unsere ISO/IEC-27001-Zertifizierung im Oktober 2021 verlängert.

- ***Unsere Praktiken werden regelmäßig geprüft***

  Im Rahmen unserer ISO/IEC-27018-, ISO/IEC-27701- und ISO/IEC-27001-Zertifizierungen und ihrer Beibehaltung unterziehen wir uns einer jährlichen Prüfung durch ein unabhängiges Unternehmen. All unsere ISO/IEC-Zertifikate können hier abgerufen werden.

Datenübertragungen

Bei der Übertragung von Daten aus der EU, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz stützt sich Dropbox auf eine Reihe von rechtlichen Mechanismen, unter anderem auf Verträge mit unseren Kunden und deren verbundenen Unternehmen, Standardvertragsklauseln und Angemessenheitsbeschlüsse der Europäischen Kommission zu bestimmten Ländern, wie zutreffend.

In Bezug auf die Erhebung, Verwendung und Speicherung personenbezogener Daten, die aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz in die USA übertragen

werden, befolgt Dropbox die Bestimmungen des EU-US Privacy Shield sowie des Swiss-US Privacy Shield des US-Handelsministeriums, obwohl Dropbox sich nicht auf das EU-US Privacy Shield oder Swiss-US Privacy Shield als Rechtsgrundlage für die Übermittlung personenbezogener Daten beruft. Dropbox hat gegenüber dem US-Handelsministerium bestätigt, dass Dropbox die Privacy-Shield-Prinzipien in Bezug auf solche Daten einhält. Weitere Informationen zum Privacy Shield finden Sie unter https://www.privacyshield.gov.

Beschwerden und Streitfälle hinsichtlich unserer Privacy Shield-Compliance werden durch JAMS, eine unabhängige Drittorganisation, untersucht und gelöst. Weitere Informationen hierzu finden Sie in unserer Datenschutzrichtlinie (dropbox.com/privacy).

Datenschutz-Grundverordnung (DSGVO) der Europäischen Union

Die DSGVO (Datenschutz-Grundverordnung) ist eine Verordnung der Europäischen Union aus dem Jahr 2018, die umfassende Regeln für die Handhabung und den Schutz personenbezogener Daten aufstellt.

Dropbox setzt sich stets für die Sicherheit und den Schutz der Nutzerdaten gemäß den rechtlichen Vorschriften und Best Practices ein. Deshalb haben wir Dropbox an die DSGVO angepasst. Dabei haben wir einen Datenschutzbeauftragten ernannt, unser Datenschutzprogramm für die Sicherstellung der Nutzerrechte neu gestaltet, unsere Datenverarbeitungsvorgänge dokumentiert und unsere internen Prozesse für den Fall einer Sicherheitslücke verbessert. Wir passen uns weiterhin an, um sicherzustellen, dass unser Prozess und unsere Praktiken bei zukünftigen Anweisungen von Datenschutzbehörden bestimmte Elemente der neuen Regeln einhalten oder übertreffen.

EU Cloud Code of Conduct

Der EU Cloud Code of Conduct ist ein freiwilliges Instrument, mit dem ein Clouddienst-Anbieter wie Dropbox seine Verpflichtung für die Einhaltung der DSGVO unter Beweis stellen kann. Dropbox Business, das sich aus den Abonnements Standard, Advanced, Enterprise und Education für Teams zusammensetzt, wurde für konform mit dem EU Cloud Code of Conduct erklärt und erhielt die Konformitätskennzeichnung „Level 2“. Dies bedeutet, dass diese Dienste technische, organisatorische und vertragliche Maßnahmen implementiert haben, die die Anforderungen dieses Kodex erfüllen. Weitere Informationen zum EU Cloud Code of Conduct und zur Konformität von Dropbox mit diesem Kodex finden Sie auf der offiziellen Website des Kodex.

Weitere Informationen zu unserer Datenschutzrichtlinie und unseren Datenschutzpraktiken finden Sie im Dropbox-Whitepaper über Informationssicherheit und Datenschutz.

Kompatibilität

Es gibt verschiedene behördliche und branchenspezifische Anforderungen an Sicherheit und Datenschutz, die Ihr Unternehmen möglicherweise einhalten muss. Wir haben uns entschieden, die etabliertesten Normen mit Compliance-Maßnahmen zu kombinieren, die den spezifischen Anforderungen an die Unternehmen oder Branchen entsprechen, in denen unsere Kunden tätig sind.

ISO

Die Internationale Organisation für Normung (ISO) hat eine Reihe von weltweit anerkannten Standards für die Sicherheit von Informationen und der Gesellschaft ausgearbeitet, die Organisationen dabei helfen sollen, zuverlässige und innovative Produkte und Dienstleistungen zu entwickeln. Dropbox hat seine Rechenzentren, Systeme, Anwendungen, Mitarbeiter und Prozesse im Rahmen einer Reihe von Audits durch eine unabhängige Drittpartei, das in den Niederlanden ansässige Unternehmen EY CertifyPoint, zertifizieren lassen. EY CertifyPoint hat eine ISO-Zertifizierung des Raad voor Accreditatie (des niederländischen Zertifizierungsrats).

ISO/IEC 27001 (Informationssicherheit)

ISO/IEC 27001 ist weltweit als wichtigste Norm für Informationssicherheitsmanagement (ISMS) anerkannt. Diese Norm umfasst auch die Best Practices für Sicherheit, die bereits in der Norm ISO/IEC 27002 ausgeführt sind. Wir halten unsere umfassenden physischen, technischen und rechtlichen Bestimmungen und Maßnahmen bei Dropbox immer auf dem neuesten Stand und verbessern sie immer weiter, damit wir uns des von Ihnen entgegengebrachten Vertrauens auch wirklich würdig erweisen.

ISO/IEC 27001-Zertifikat für Dropbox Business und Dropbox Education ansehen.

ISO/IEC 27017 (Cloud-Sicherheit)

ISO/IEC 27017 ist ein internationaler Standard für Cloud-Sicherheit, der einen Leitfaden für Sicherheitsaspekte bietet, die bei der Bereitstellung und Nutzung von Cloud-Diensten zu berücksichtigen sind. Unser Leitfaden zur gemeinsamen Verantwortung erklärt verschiedene Einzelheiten der Sicherheits-, Datenschutz- und Compliance-Anforderungen, denen Dropbox gemeinsam mit seinen Kunden Folge leisten kann.

ISO/IEC 27017-Zertifikat für Dropbox Business und Dropbox Education ansehen.

ISO/IEC 27018 (Datenschutz und Datensicherheit in der Cloud)

ISO/IEC 27018 ist ein internationaler Standard für Datenschutz und Datensicherheit, der sich speziell an Serviceanbieter wie Dropbox richtet, die in der Cloud arbeiten und im Auftrag ihrer Kunden vertrauliche Daten verarbeiten. Diese Zertifizierung dient als Grundlage bei der Beantwortung grundsätzlicher Richtlinien- und Vertragsanforderungen oder Fragen unserer Kunden zu diesem Thema.

ISO/IEC 27018-Zertifikat für Dropbox Business und Dropbox Education ansehen.

ISO/IEC 22301 (Geschäftskontinuität)

ISO/IEC 22301 ist ein internationaler Standard für Business Continuity. Er dient Organisationen als Leitfaden zur Frage, wie sie die Auswirkungen von Störfällen verringern und angemessen darauf reagieren können, um den potenziellen Schaden auf ein Minimum zu begrenzen. Das Business Continuity Management System von Dropbox (BCMS) ist Teil unserer allgemeinen Risikomanagementstrategie zum Schutz von Personen und Betriebsabläufen in Krisenfällen.

ISO/IEC 22301-Zertifikat für Dropbox Business und Dropbox Education ansehen.

ISO/IEC 27701 (Datenschutz-Informationsmanagement)

ISO 27701 ist eine internationale Norm für Datenschutz-Informationsmanagement. Sie bietet einen Rahmen zur Erweiterung von Information Security Management Systems unter ISO 27001 auf ein Privacy Information Management System (PIMS). Dropbox Business und Dropbox Education haben beide diese Zertifizierung als Verarbeiter personenbezogener Daten erhalten.

ISO-27701-Zertifikat für Dropbox Business und Dropbox Education ansehen.

SOC

Die vom amerikanischen Wirtschaftsprüferverband AICPA (American Institute of Certified Public Accountants) entwickelten Service Organization Controls (SOC)-Berichte SOC 1, SOC 2 und SOC 3 liefern Vorgaben für die Dokumentation von internen Kontrollmechanismen einer Organisation. Dropbox hat seine Systeme, Anwendungen, Mitarbeiter und Prozesse im Rahmen einer Reihe von Audits durch eine unabhängige Drittpartei, Ernst & Young LLP, validiert.

SOC 3 für Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Datenschutz

Der SOC 3-Prüfbericht umfasst alle fünf Trust Services-Kriterien: Sicherheit, Vertraulichkeit, Prozessintegrität, Verfügbarkeit und Datenschutz (TSP-Abschnitt 100). Der Dropbox-Bericht zur allgemeinen Verwendung ist eine Kurzfassung unseres SOC 2-Berichts und enthält eine Bewertung durch unseren externen Auditor hinsichtlich der effektiven Entwicklung und Umsetzung unserer Kontrollmechanismen.

SOC 3-Bericht für Dropbox Business und Dropbox Education ansehen.

SOC 2 für Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Datenschutz

Der SOC 2-Bericht bietet unseren Kunden einen detaillierten Sicherheitsnachweis unserer Kontrollmechanismen und umfasst alle fünf Trust Services-Kriterien: Sicherheit, Verfügbarkeit, Prozessintegrität, Vertraulichkeit und Datenschutz (TSP Abschnitt 100). Der SOC 2-Bericht enthält eine detaillierte Beschreibung der Prozesse von Dropbox und der mehr als 100 Kontrollmechanismen, die wir zum Schutz Ihrer Daten einsetzen. Neben der Bewertung durch unseren externen Auditor hinsichtlich der effektiven Entwicklung und Umsetzung unserer Kontrollmechanismen befasst sich dieser Bericht auch mit den Prüfvorgängen und Ergebnissen des Auditors hinsichtlich der einzelnen Kontrollmechanismen. Darüber hinaus enthält unser SOC 2-Bericht (manchmal auch SOC 2+ genannt) ein geprüftes Mapping unserer Kontrollen hinsichtlich der zuvor genannten ISO-Standards und bietet unseren Kunden zusätzliche Transparenz. Den SOC 2-Bericht für Dropbox Business und Dropbox Education erhalten Sie auf Anfrage.

SOC 1 / SSAE 18 / ISAE 3402 (früher SSAE 16 oder SAS 70)

Der SOC 1-Bericht bietet spezifische Sicherheitsnachweise für Kunden, die Dropbox für Unternehmen oder Dropbox Education als wesentlichen Bestandteil ihres Programms zur internen Kontrolle der Finanzberichterstattung (ICFR) festlegen. Diese spezifischen Sicherheitsnachweise dienen vornehmlich der Konformität unserer Kunden mit dem Sarbanes-Oxley Act (SOX). Die unabhängige Prüfung durch Dritte erfolgt gemäß den Vorgaben der Standards for Attestation Engagements No. 18 (SSAE 18) und des International Standard on Assurance Engagements No. 3402 (ISAE 3402). Diese Standards ersetzen das veraltete Statement on Standards for Attestation Engagement No. 16 (SSAE 16) und das Statement on Auditing Standards No. 70 (SAS 70). Den SOC 1-Bericht für Dropbox für Unternehmen und Dropbox Education erhalten Sie auf Anfrage.

CSA

Cloud Security Alliance: Security, Trust and Assurance Registry (CSA STAR)

CSA Security, Trust & Assurance Registry (STAR) ist ein kostenfreies und öffentlich zugängliches Verzeichnis, das ein Sicherheitsnachweis-Programm für Cloud-Dienste anbietet. Dies soll Nutzern dabei helfen, die Sicherheitsstandards der Anbieter, die sie aktuell verwenden oder deren Dienste sie in Betracht ziehen, besser einzuschätzen.

Dropbox Business und Dropbox Education wurden nach CSA STAR Level 2 bzw. Level 2 Attestation geprüft und zertifiziert. CSA STAR Level 2 setzt eine unabhängige Prüfung unserer Sicherheitsmechanismen durch EY CertifyPoint (für die Zertifizierung) und Ernst & Young LLP (für die Attestierung) nach den Vorgaben von ISO/IEC 27001, den SOC 2 Trust Services-Kriterien und der CSA Cloud Controls Matrix (CCM), Version 4.0.2 voraus.

Unsere Zertifizierung und Bescheinigungen nach CSA STAR Level 2 finden Sie auf der CSA-Website.

HIPAA/HITECH

Dropbox schließt auf Wunsch mit Kunden von Dropbox Business und Dropbox Education Geschäftspartnerverträge (Business Associate Agreements, BAA) ab, die dem Health Insurance Portability and Accountability Act (HIPAA) sowie dem Health Information Technology for Economic and Clinical Health Act (HITECH) entsprechen müssen. Siehe Dropbox und HIPAA/HITECH für weitere Informationen.

Dropbox stellt einen Assurance-Bericht von Dritten zur Verfügung, in dem unsere Kontrollen für die Sicherheits-, Datenschutz- und Meldungsregeln für den Verletzungsfall bezüglich HIPAA und HITECH bewertet sowie unsere internen Praktiken und Empfehlungen für Kunden aufgeführt werden, die mit Dropbox Business oder Dropbox Education den Sicherheits- und Datenschutzanforderungen gemäß HIPAA/HITECH entsprechen möchten.

Kunden, die diese Dokumente anfordern oder mehr über den Kauf von Dropbox für Unternehmen oder Dropbox Education erfahren möchten, wenden sich bitte an unser Vertriebsteam. Wenn Sie derzeit ein Team-Admin für Dropbox für Unternehmen oder Dropbox Education sind, können Sie in der Verwaltungskonsole auf der Seite „Konto“ ein BAA elektronisch unterzeichnen.

Bitte nehmen Sie zur Kenntnis, dass die Möglichkeit, über die Verwaltungskonsole einen elektronischen BAA zu unterzeichnen, ausschließlich in den USA basierten Kunden zur Verfügung steht.

NIST 800-171

Das National Institute of Standards and Technology (NIST) in den USA entwickelt und pflegt Normen und Richtlinien zum Schutz von Informationssystemen. NIST Special Publication (SP) 800171 Revision 2 (R2) bietet Richtlinien zum Schutz kontrollierter unklassifizierter Informationen (Controlled Unclassified Information, CUI) in nicht staatlichen Informationssystemen und Organisationen. Jede Organisation, die CUI der US-Regierung verarbeitet oder speichert, darunter Forschungseinrichtungen und der Bildungssektor, muss NIST SP 800-171 R2 einhalten. Die CUI-Systeme, -Prozesse und -Kontrollen von Dropbox wurden durch das unabhängige externe Audit-Unternehmen Ernst & Young LLP validiert.

Der Bericht zu NIST SP 800-171 R2 für Dropbox Business und Dropbox Education ist über unser Vertriebsteam oder (für Bestandskunden von Dropbox Business) beim Support verfügbar.

Bitte nehmen Sie zur Kenntnis, dass Dropbox Paper nicht durch den Bericht zu NIST SP 800-171 R2 abgedeckt ist.

FERPA und COPPA (Studierende und Kinder)

Dropbox Business und Dropbox Education stellen ihre Dienstleistungen in Übereinstimmung mit den im US-amerikanischen Family Education Rights and Privacy Act (FERPA) vorgegebenen Pflichten für Anbieter bereit. Bildungseinrichtungen mit Schülern im Alter von unter 13 Jahren können gemäß dem US-amerikanischen Children's Online Privacy Protection Act (COPPA) Dropbox Business oder Dropbox Education ebenfalls verwenden. Einzige Voraussetzung dafür ist, dass sie sich mit bestimmten Vertragsbedingungen einverstanden erklären, die die Einrichtung dazu verpflichten, für die Verwendung unserer Dienstleistungen die Zustimmung der Eltern einzuholen.

FDA 21 CFR Part 11

Title 21 des Code of Federal Regulations (CFR) regelt Lebensmittel und Arzneimittel innerhalb der USA für die Food and Drug Administration (FDA), die Drug Enforcement Administration und die Office of National Drug Control Policy. Part 11 von Title 21 legt die Kriterien fest, nach denen die FDA elektronische Datensätze und Unterschriften als vertrauenswürdig, zuverlässig und allgemein gleichwertig mit physischen Datensätzen und handschriftlichen Signaturen einstuft.

Weitere Informationen dazu, wie Dropbox Sie bei der Compliance mit FDA 21 CFR Part 11 unterstützen kann, finden Sie im Whitepaper zu Dropbox und FDA 21 CFR Part 11 sowie im entsprechenden Hilfecenter-Artikel.

PCI DSS

Dropbox hält als Händler den Payment Card Industry Data Security Standard (PCI DSS) ein. Jedoch sind Dropbox für Unternehmen, Dropbox Education und Dropbox Paper nicht dafür vorgesehen, Transaktionen mit Kreditkarten zu verarbeiten oder zu speichern. Die PCI Attestation of Compliance (AoC) als Nachweis unseres Händlerstatus erhalten Sie auf Anfrage.

Weitere Informationen zu den Compliance-Richtlinien von Dropbox Business und Dropbox Education erhalten Sie unter dropbox.com/business/trust/compliance.

Apps für Dropbox

DBX Platform umfasst eine starke Gruppe hochqualifizierter Entwickler, die Anwendungen auf Basis unserer flexiblen Schnittstellen zur Anwendungsprogrammierung (APIs, Application Programming Interfaces) erstellen. Dabei haben bisher mehr als 750.000 Entwickler Apps und Dienstleistungen für Produktivität, Zusammenarbeit, Sicherheit, Verwaltung und vieles mehr auf der Plattform entwickelt.

Vorgefertigte Komponenten

Chooser, Saver und Embedder sind vorgefertigte Web- und Mobilkomponenten, die einen einfachen Zugriff auf Dropbox in Apps/Sites von Drittanbietern in nur wenigen Codezeilen ermöglichen.

- Der Chooser ermöglicht die Auswahl von Dateien aus Dropbox.
- Der Saver ermöglicht es Nutzern, Dateien direkt in Dropbox zu speichern.
- Der Embedder ermöglicht es Nutzern, Dateien und Ordner aus Dropbox anzuzeigen.

Die Autorisierung für diese Komponenten erfolgt vollständig über Dropbox. Apps erhalten Zugriff auf die von ihnen ausgewählten Dateien über freigegebene Dropbox-Links oder kurzlebige Download-Links. Diese vorgefertigten Komponenten können unabhängig oder in Verbindung mit der unten beschriebenen API verwendet werden.

API-Integrationen in Dropbox Business

Die öffentliche Dropbox-API ermöglicht Drittanbieterentwicklern den Zugriff auf und die Interaktion mit Dropbox innerhalb ihrer Anwendungen. Dazu gehören die Interaktion mit Dateien und Metadaten, die Freigabe und die Teamfunktionalität.

Autorisierung

Dropbox verwendet für die Autorisierung das branchenübliche OAuth-Protokoll, mit dem Nutzer den Apps Zugriff auf ihr Konto gewähren können, ohne ihre Anmeldedaten weitergeben zu müssen. Wir unterstützen OAuth 2.0 für die Authentifizierung von API-Anfragen; Anfragen werden über die Dropbox-Website oder die App für Mobilgeräte authentifiziert. Dropbox unterstützt OAuth-Best Practices, einschließlich kurzlebiger Zugriffstoken und PKCE für verteilte Anwendungen.

Nutzerberechtigungen

Apps, die die Dropbox-API verwenden, können mit der nachfolgenden Berechtigungsebene für die Dropbox eines Endnutzers entwickelt werden:

- ***App-Ordner***

  In der Dropbox eines Nutzers wird für jede App ein eigener Ordner erstellt, der den Namen der App erhält. Die App erhält ausschließlich für diesen Ordner eine Lese- und Schreibberechtigung und der Nutzer kann der App Inhalte zuweisen, indem er Dateien in diesen Ordner verschiebt. Darüber hinaus kann die App auch Datei-/Ordnerzugriff über Chooser bzw. Saver anfordern.

- ***Vollständige Dropbox***

  Die App erhält vollständigen Zugriff auf alle Dateien und Ordner in der Dropbox eines Nutzers und kann mithilfe von Chooser bzw. Saver Zugriff auf bestimmte Dateien/Ordner anfordern.

Anwendungen können auch bestimmte Berechtigungsebenen anfordern und ihr Verhalten durch Zugriff auf Teilmengen von API-Endpunkten einschränken. Beispielsweise können Anwendungen auf den schreibgeschützten Zugriff auf Dateien beschränkt sein – oder auf die Möglichkeit, Inhalte hochzuladen, aber keine Freigaben zu erstellen.

Teamberechtigungen

Admins von Dropbox Business können Anwendungen für Verwaltungsfunktionen autorisieren, die sich in der Verwaltungskonsole des Teams befinden. Die Aktionen, die teamverknüpfte Apps ausführen können, sind durch Berechtigungsebenen begrenzt, die angeben, welche Teameinstellungen die App lesen oder verwalten darf.

Gängige Kombinationen von Berechtigungsebenen umfassen:

- ***Teaminformationen***

  schreibgeschützte Informationen über das Team und die Nutzung auf hoher Ebene

- ***Team-Auditing***

  Schreibgeschützter Zugriff auf Teaminformationen und das detaillierte Ereignisprotokoll.

- ***Zugriff auf Teammitgliederdateien***

  Die Möglichkeit, Aktionen im Namen der Nutzer im Team durchzuführen, beispielsweise die Verwaltung ihrer Dateien und Ordner.

- ***Teamverwaltung***

  Hinzufügen und Entfernen von Teammitgliedern.

WebHooks

Mithilfe von WebHooks können Webanwendungen in Echtzeit Benachrichtigungen über Änderungen in der Dropbox eines Nutzers erhalten. Wenn ein Uniform Resource Identifier (URI) für den Empfang von WebHooks registriert ist, wird ihm bei jeder Änderung an den registrierten Nutzern der App eine HTTP-Anfrage gesendet. Mithilfe der API von Dropbox für Unternehmen können WebHooks außerdem verwendet werden, um Benachrichtigungen über Änderungen der Teammitgliedschaft zu generieren. Viele Sicherheits-Apps verwenden WebHooks, um Admins zu helfen, Teamaktivitäten nachzuverfolgen und zu verwalten.

Extensions

Apps können Erweiterungs-URIs registrieren, wodurch Aktionen in den Menüs „Teilen“ und „Öffnen“ in der Dropbox-Nutzeroberfläche angezeigt werden können. Erweiterungen ermöglichen es Nutzern, nutzerdefinierte Arbeitsabläufe von Drittanbietern direkt über eine Datei in einer Dropbox-Oberfläche zu starten. Wenn eine Aktion ausgelöst wird, leitet Dropbox die Nutzer an den angegebenen URI um, wobei eine Dateikennung übermittelt wird, die mit der API verwendet werden kann, um beliebige Dateivorgänge durchzuführen. Eine App muss autorisiert werden, bevor eine registrierte Erweiterung für den Nutzer sichtbar ist. In den Menüs „Freigeben“ und „Öffnen“ können wir einen ausgewählten Satz von Erweiterungsintegrationen anbieten. Diese Apps können jedoch erst dann auf den Inhalt zugreifen, wenn der Nutzer sie autorisiert hat.

Dropbox-Richtlinien für Entwickler

Wir bieten eine Reihe von Richtlinien und praktischen Tipps, um Entwickler bei der Erstellung von API-Apps zu unterstützen, die den Datenschutz der Nutzer respektieren und gleichzeitig die Dropbox-Erfahrung für alle Nutzer verbessern.

- ***App-Schlüssel***

  Für jede eigene App, die ein Entwickler erstellt, muss ein einmaliger Dropbox-App-Schlüssel verwendet werden. Wenn eine App Dienste oder Software anbietet, in der DBX Platform für andere Entwickler zur Verfügung gestellt wird, muss jeder dieser Entwickler seinen eigenen Dropbox-App-Schlüssel registrieren.

- ***App-Berechtigungen***

  Entwickler werden darauf hingewiesen, dass eine App mit den geringstmöglichen Berechtigungen auskommen sollte. Wenn ein Entwickler eine App für die Genehmigung zum Produktionsstatus einreicht, überprüfen wir anhand des Funktionsumfangs dieser App, ob sie nicht unnötig viele Berechtigungen anfordert.

- ***Überprüfung der App***

  - **Entwicklungsstatus:** Wenn eine Dropbox-API-App zum ersten Mal erstellt wird, erhält sie anfangs den Entwicklungsstatus. Die App funktioniert genauso wie eine App im Produktionsstatus, allerdings kann sie mit höchstens 500 Dropbox-Nutzern verknüpft werden. Sobald eine App mit 50 Dropbox-Nutzern verknüpft ist, hat der Entwickler zwei Wochen Zeit, um den Produktionsstatus zu beantragen und gewährt zu bekommen, bevor die Verknüpfung mit weiteren Dropbox-Nutzern blockiert wird.

  - **Produktionsstatus und Genehmigung:** Um die Genehmigung für den Produktionsstatus zu erhalten, müssen alle API-Apps unsere Branding-Richtlinien und Allgemeinen Geschäftsbedingungen für Entwickler erfüllen, in denen auch erläutert wird, wofür die DBX Platform nicht genutzt werden darf. Dazu gehören die Förderung von IP- oder Urheberrechtsverletzungen, das Erstellen von Filesharing-Netzwerken und das illegale Herunterladen von Inhalten. Entwickler werden vor der Überprüfung aufgefordert zu erläutern, wie ihre App funktioniert und wie sie die Dropbox-API nutzt. Sobald der Produktionsstatus für die App genehmigt wurde, wird die Beschränkung hinsichtlich der maximal zulässigen Dropbox-Nutzer aufgehoben.

Team-App-Verwaltung

Innerhalb der Team-Verwaltungskonsole können die Administratoren von Dropbox Business verknüpfte Apps und Integrationen für ihr Team verwalten.

API-Partnerschaften

Dropbox arbeitet eng mit seinen Technologiepartnern zusammen, um es ihnen zu ermöglichen, Integrationen für ihre beliebten Softwarepakete zu entwickeln. Diese Partner erstellen Anwendungen mit den APIs von Dropbox und kooperieren intensiv mit den Architekten von Dropbox, um die Best Practices für Sicherheit und UX zu befolgen. Dazu gehören eine Vielzahl von Anwendungen für die Endnutzerproduktivität sowie Sicherheits- und Verwaltungstools wie folgende:

- ***Sicherheitsinformations- und Ereignis-Management (SIEM) und Analysen***

  Verknüpfen Sie Ihr Konto von Dropbox für Unternehmen mit SIEM- und Analysetools, um die Nutzerfreigabe, Anmeldeversuche, Verwaltungsaufgaben und vieles mehr nachzuverfolgen und zu beurteilen. Betrachten und verwalten Sie die Protokolle zur Mitarbeiteraktivität und sicherheitsrelevante Daten über Ihr zentrales Protokollverwaltungstool.

- ***Data Loss Prevention (DLP)***

  Scannen Sie automatisch Metadaten und Datei-Inhalte, um Benachrichtigungen, Berichte und Aktivitäten auszulösen, wenn wichtige Änderungen in Ihrem Konto von Dropbox für Unternehmen vorgenommen werden. Wenden Sie Unternehmensrichtlinien auf Ihre Bereitstellung von Dropbox für Unternehmen an und erfüllen Sie vorgeschriebene Compliance-Anforderungen.

- ***eDiscovery und gesetzliche Aufbewahrungspflicht***

  Nutzen Sie die Daten im Konto von Dropbox für Unternehmen bei Rechtsstreitigkeiten, Schlichtungen und behördlichen Untersuchungen. Suchen Sie nach relevanten elektronisch gespeicherten Informationen, tragen Sie sie zusammen und bewahren Sie Ihre Daten durch den gesamten eDiscovery-Prozess hindurch auf, um Ihrem Unternehmen Zeit und Geld zu sparen.

- ***Digitales Rechtemanagement (DRM)***

  Schützen Sie vertrauliche oder urheberrechtlich geschützte Daten in Mitarbeiterkonten durch Drittanbieterlösungen. Verschaffen Sie sich Zugriff auf leistungsstarke DRM-Funktionen wie clientseitige Verschlüsselung, Wasserzeichen, Audit-Trails, Widerrufen der Zugriffsrechte und Nutzer- bzw. Gerätesperrung.

- ***Datenmigration und On-Premises-Backup***

  Migrieren Sie Daten von vorhandenen Servern oder aus anderen cloudbasierten Lösungen in Dropbox und sparen Sie auf diese Weise Zeit, Geld und Arbeit. Automatisieren Sie Backups von Ihrem Konto von Dropbox für Unternehmen auf die On-Premise-Server.

- ***Identitätsmanagement und einmaliges Anmelden (kurz SSO)***

  Automatisieren Sie die Bereitstellung sowie Aufhebung der Bereitstellung und beschleunigen Sie das Onboarding für neue Mitarbeiter. Optimieren Sie die Verwaltung und erhöhen Sie die Sicherheit durch die Integration von Dropbox für Unternehmen in ein bestehendes Identitätssystem.

- ***Unternehmensspezifische Prozesse***

  Entwickeln Sie eigene Anwendungen zur Integration von Dropbox in bestehende Unternehmensprozesse, um interne Arbeitsabläufe zu optimieren.

Auf der Seite Dropbox-App-Integrationen finden Sie eine Liste dieser Technologiepartner. Endnutzer können im App Center ausgewählte Apps und Integrationen von Dropbox und Drittanbietern entdecken.

Dropbox-Integrationen

Wir arbeiten außerdem mit einigen unserer führenden Technologiepartner zusammen, um Integrationen zu erstellen, die in Dropbox-Oberflächen enthalten sind. Diese tiefgreifenden Integrationen werden von Dropbox und dem Partner gemeinsam entwickelt. Dazu zählen:

Dropbox Extensions

Mit diesen Integrationen können Sie verschiedene Arten von App-Erweiterungen verwenden, um Aktionen wie das Veröffentlichen eines Videos, das Hinzufügen von Dateien zu E-Mails und Chats, das Versenden einer Datei zur elektronischen Signatur und vieles mehr direkt über Dropbox nahtlos durchzuführen. Diese Anwendungen werden vom Partner erstellt, während Dropbox das Auffinden ausgewählter Erweiterungspartner über die Menüs „Öffnen mit“ und „Freigeben für“ erleichtert.

Slack, Zoom und Trello

Diese Integrationen werden direkt von Dropbox erstellt, sodass Nutzer in Dropbox Slack-Gespräche führen, Besprechungen starten und Aufgaben erstellen können. Endnutzer authentifizieren sich bei diesen Tools über OAuth.

Microsoft Office für Mobilgeräte und Web

Unsere Microsoft Office-Integration gestattet Nutzern das Öffnen von in ihrer Dropbox gespeicherten Word-, Excel- und PowerPoint-Dateien, das Ändern dieser Dateien in den Office-Apps für Mobilgeräte oder für das Web und das Speichern der Änderungen direkt in Dropbox. Beim ersten Öffnen einer Dropbox-Datei in der jeweiligen Office-App für Mobilgeräte oder der Web-Anwendung des Office-Produkts wird der Nutzer aufgefordert, den Zugriff zu gewähren. Bei zukünftigen Anwendungsstarts bleiben diese Verknüpfungen erhalten.

Adobe Acrobat und Acrobat Reader

Dank unserer Integrationen mit den Desktop- und Mobilgeräte-Versionen (Android und iOS) dieser Apps haben Nutzer die Möglichkeit, in ihren Dropbox-Ordnern gespeicherte PDF-Dateien anzuzeigen, zu bearbeiten und freizugeben. Beim ersten Öffnen einer Dropbox-Datei in der jeweiligen App wird der Nutzer aufgefordert, den Zugriff zu gewähren. Änderungen an PDF-Dateien werden automatisch in Dropbox gespeichert.

Zusammenfassung

Dropbox Business bietet Teams nicht nur intuitive Tools zur effektiven Zusammenarbeit, sondern auch die erforderlichen Sicherheitsmaßnahmen und Compliance-Zertifizierungen, die Unternehmen brauchen. Mit einem vielschichtigen Ansatz, der eine zuverlässige Backend-Infrastruktur mit anpassbaren Richtlinien kombiniert, bieten wir Unternehmen eine leistungsstarke Lösung, die auf die jeweiligen Anforderungen und Bedürfnisse zugeschnitten werden kann. Wenn Sie an weiteren Informationen zu Dropbox Business interessiert sind, setzen Sie sich bitte mit unserem Vertriebsteam unter sales@dropbox.com in Verbindung.