Sicherheit in Dropbox Business

Ein Dropbox-Whitepaper

Dropbox

Inhaltsverzeichnis

Einleitung

Mehr als 500.000 Unternehmen und Organisationen verwenden Dropbox Business als einheitlichen Arbeitsplatz für alle Inhalte ihrer Teams und ermöglichen ihnen damit problemlose Zusammenarbeit und nahtlose Freigaben. Dropbox Business ist jedoch nicht nur ein benutzerfreundliches Kollaborationstool, sondern schützt gleichzeitig die Daten. Wir haben eine moderne Infrastruktur entwickelt, mit der Team-Administratoren eigene Richtlinien auf verschiedenen Ebenen festlegen können. In diesem Whitepaper erläutern wir die Back-End-Richtlinien und Optionen für Administratoren, die Dropbox Business zu einem sicheren Tool machen, mit dem Teams ihre kreative Energie entfalten können.

Dieses Whitepaper befasst sich auch mit der Sicherheit von Dropbox Paper („Paper“), einer Arbeitsfläche für die Zusammenarbeit, wo Teams Ideen gemeinsam entwickeln und freigeben können. Paper ist online und für mobile Geräte erhältlich. Mit diesem Tool können Teammitglieder Projekte verwalten, Dokumente erstellen und freigeben und in Echtzeit Feedback austauschen.

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 von Dropbox Business und Dropbox Education.

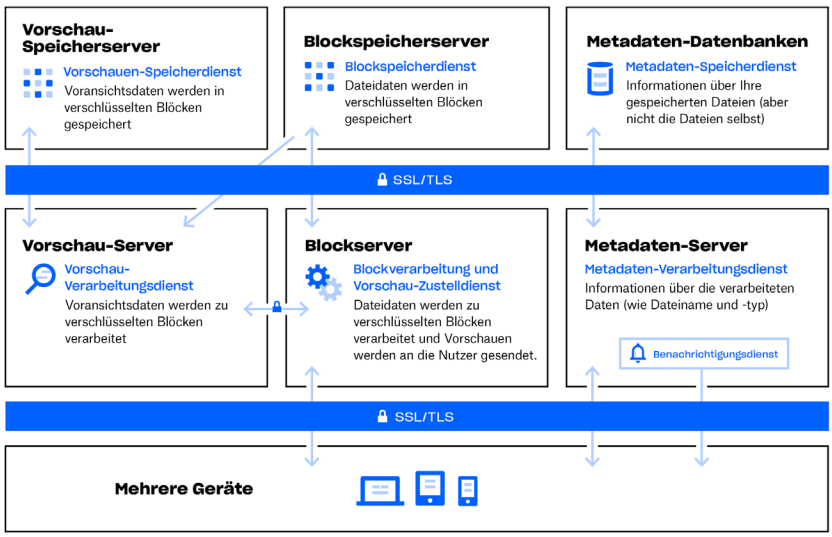
Technischer Hintergrund

Unsere benutzerfreundlichen Oberflächen sind auf einer Infrastruktur aufgebaut, die schnelle, zuverlässige Synchronisierung, Freigaben und Zusammenarbeit gewährleistet. Wir entwickeln unser Produkt und unsere Architektur ständig weiter, 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.

Datei-Infrastruktur

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 eigens 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. Dazu gehören auch Grundinformationen über Dateien wie Dateiname und -format, durch die Funktionen wie Versionsverlauf, Wiederherstellung und Synchronisierung unterstützt werden.

- ***Datenbanken für Metadaten***

  Dateimetadaten werden in einem MySQL-Datenbankdienst 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-Anwendungen, indem sie jede Datei in Blöcke unterteilen, jeden Block mit einem starken Schlüssel schützen und nur die veränderten Blöcke synchronisieren. Wenn eine Dropbox-Anwendung eine neue Datei oder Änderungen an einer vorhandenen Datei erkennt, informiert die Anwendung die Blockserver über die Änderung. Daraufhin 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-Wertes abgerufen.

- ***Vorschau-Server***

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

- ***Vorschau-Speicherserver***

  Zwischengespeicherte Vorschauen werden verschlüsselt auf den Vorschau-Speicherservern gespeichert.

- ***Benachrichtigungsservice***

  Für die Überprüfung auf Änderungen an Dropbox-Konten wird ein separater Dienst eingesetzt. 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 Änderungen an Dateien in Dropbox vorgenommen werden, teilt der Benachrichtigungsdienst diese Änderung 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 alle Änderungen synchronisieren zu können.

Durch das Verteilen von Informationen unterschiedlicher Ebenen auf diese Dienste wird die Synchronisierung nicht nur schneller und zuverlässiger, sondern auch sicherer. Dank dieser Dropbox-Architektur kann der Zugriff auf einen dieser Dienste nicht zur Replizierung von Dateien verwendet werden. Weitere Informationen zur Verschlüsselung in den verschiedenen Diensten finden Sie unten im Abschnitt Verschlüsselung.

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. Zudem erfüllen beide Systeme hohe Anforderungen an die Zuverlässigkeit. Weitere Details finden Sie unten im Abschnitt Zuverlässigkeit.

Dateisynchronisierung

Dropbox bietet branchenweit anerkannte erstklassige Dateisynchronisierung. Unsere Synchronisierungsmechanismen gewährleisten schnelle Dateiübertragungen und unterstützen den standortunabhängigen Datenzugriff über alle Geräte hinweg. Dropbox ist auch fehlertolerant. 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 mit 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 Sychronisierungsmethode werden nur modifizierte Dateiabschnitte herunter- und hochgeladen. Dropbox speichert jede hochgeladene Datei in separaten, verschlüsselten Blöcken und aktualisiert nur die geänderten Teile.

- ***Streaming-Synchronisierung***

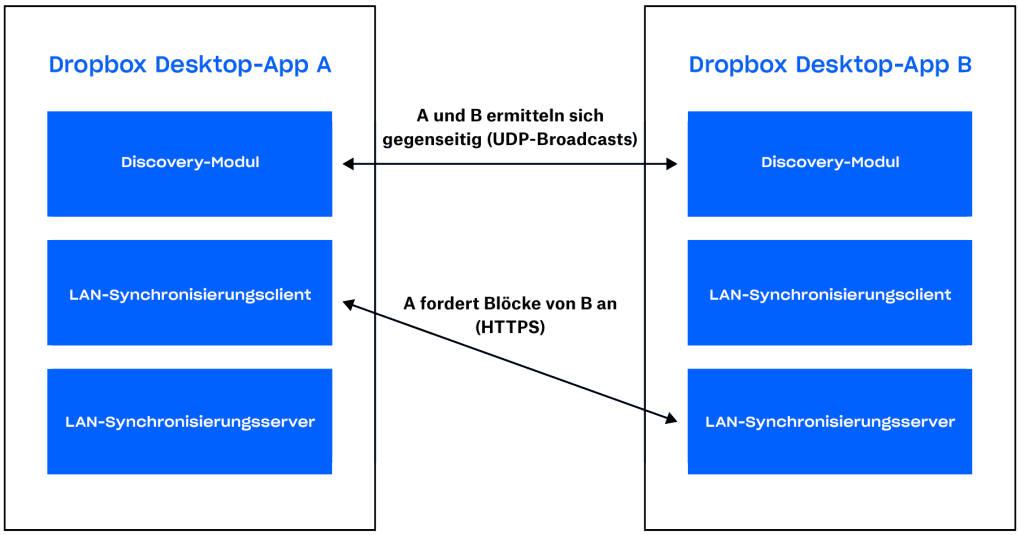
  Anstatt zu warten, bis der Datei-Upload abgeschlossen ist, beginnt die Streaming-Synchronisierung mit dem Download synchronisierter Blöcke auf ein zweites Gerät, bevor der Upload aller Blöcke vom ersten Gerät abgeschlossen ist. Diese Methode wird automatisch eingesetzt, wenn mindestens zwei Rechner mit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

- ***LAN-Synchronisierung***

  Bei der LAN-Synchronisierung werden neue und aktualisierte Dateien von anderen Computern im selben lokalen Netzwerk (LAN) herunter- bzw. auf diese 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 im Netzwerk nach Rechnern, 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 ist dafür verantwortlich, die Dateiblöcke im Netzwerk anzufragen.



Discovery Engine

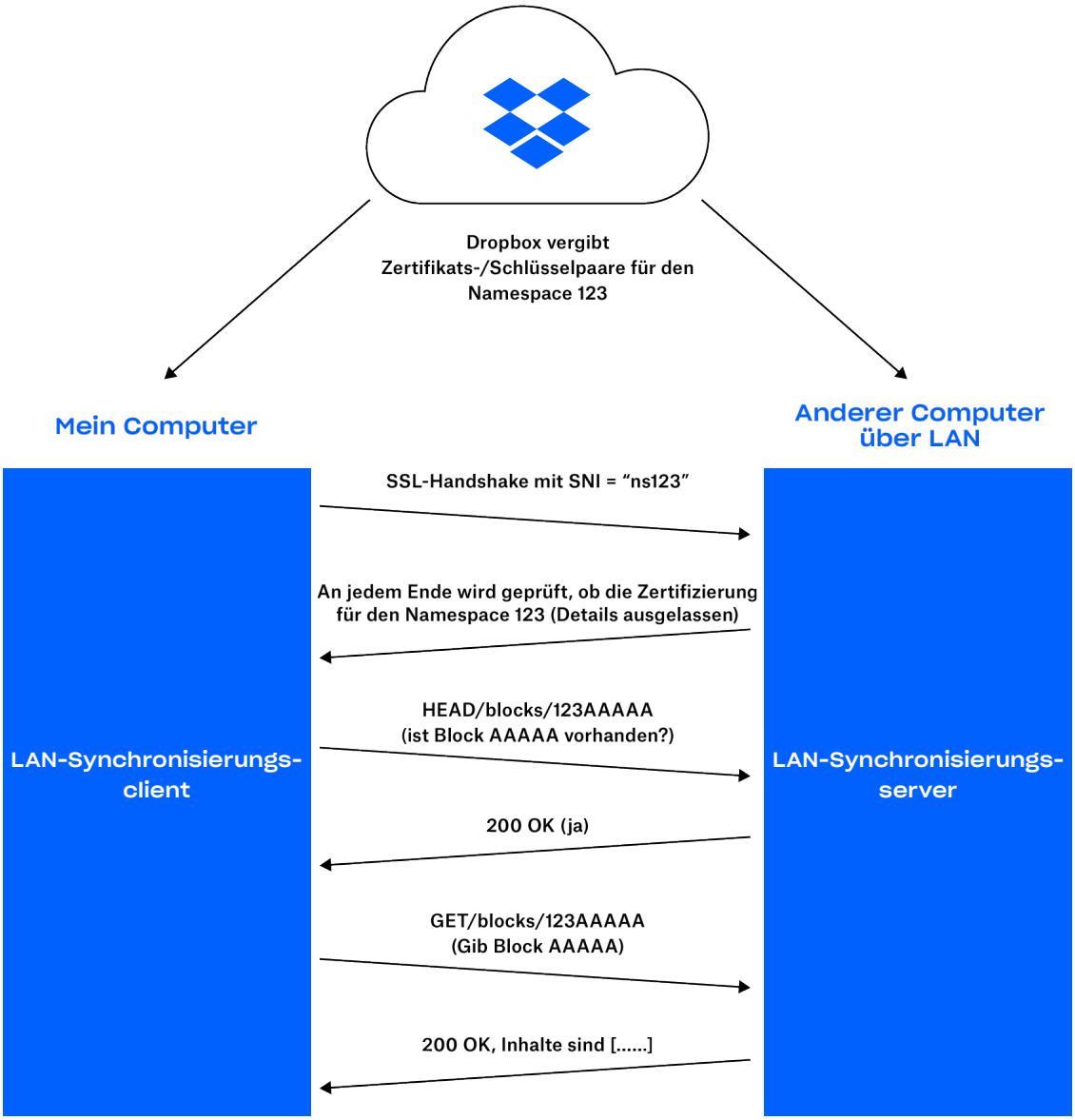
Alle Rechner im LAN nutzen den Port 17500 (von IANA zur LAN-Synchronisierung reserviert), um UDP Broadcast-Pakete zu senden und zu empfangen. Diese Pakete enthalten die von diesem Computer verwendete Protokollversion, die unterstützten privaten und freigegebenen Dropbox-Ordner, den zum Ausführen des 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 auf ein potenzielles Ziel zu verweisen.

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-/Zertifikatspaare. 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-/Zertifikatspaare 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 weiß, welches Zertifikat er verwenden muss.



Server/Client

Dank des oben beschriebenen Protokolls 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- oder den freigegebenen Ordner ermittelt wurden, und fordert dann den Block vom ersten Peer an, der die Anfrage bestätigt.

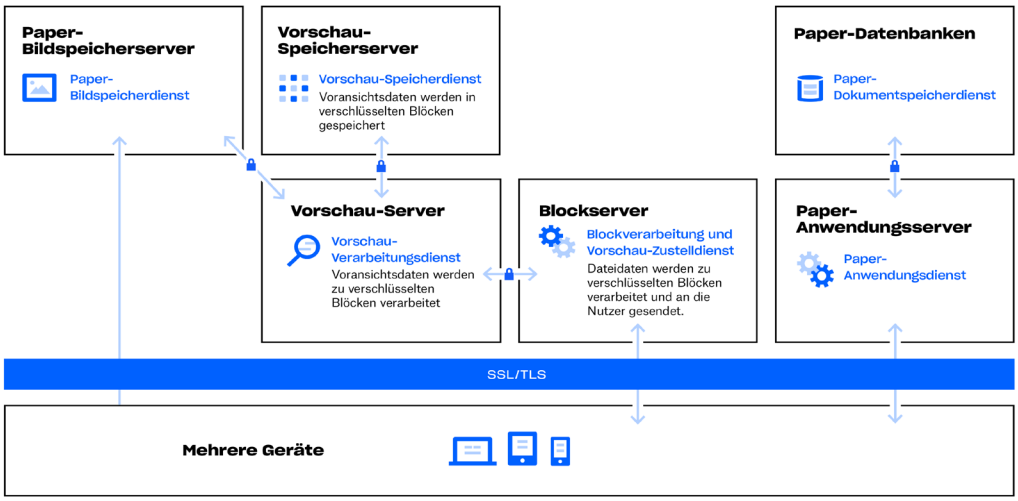
Zur Vermeidung von Latenzen verwenden wir Verbindungspools, sodass wir bereits gestartete Verbindungen erneut verwenden können. Wir öffnen Verbindungen nur bei Bedarf und halten sie dann offen, falls wir sie erneut nutzen möchten. Außerdem beschränken wir die Anzahl der Verbindungen zu jedem einzelnen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

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 sie für andere Nutzer freigeben 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 Kommunikation der Paper-Anwendungsserver mit den Paper-Datenbanken wird stark verschlüsselt.

- ***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. der Titel, Freigaben und Berechtigungen, Dateizuordnungen 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.

- ***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.

- ***Vorschau-Server***

  Die Vorschau-Server 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 Bildvoransicht. Vorschauen werden Nutzern letztlich von Blockservern bereitgestellt.

- ***Vorschau-Speicherserver***

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

Paper-Dokumentenspeicher

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.

Zuverlässigkeit

Ein Speichersystem ist nur dann von Nutzen, wenn es auch 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 Dateimetadaten mindestens nach einem N+2-Verfügbarkeitsmodell auf mehrere unabhängige Geräte verteilt. Die Daten werden stündlich einer stufenweisen und alle drei Tage 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 oder japanischen Infrastruktur entscheiden, werden nur innerhalb der entsprechenden Region repliziert. Weitere 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 Service 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 dem Desktop-Client/lokalen Ordner 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 Service bzw. die Verbindung wiederhergestellt ist.

Paper-Dokumente

Redundante Kopien von Paper-Dokumentdaten werden in einem Rechenzentrum auf unabhängigen Geräten nach einem N+2-Verfügbarkeitsmodell verteilt. Vollständige Sicherungskopien von Paper-Dokumentdaten werden zudem 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.

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
- Gegebenenfalls Ergreifen von Maßnahmen zur Schadensbegrenzung und -minderung
- Kommunikation mit relevanten internen und externen Beteiligten. Dazu gehört die Benachrichtigung betroffener Kunden, um unserer Meldepflicht bei Zwischenfällen nachzukommen und die jeweiligen gesetzlichen Vorschriften und Bestimmungen zu erfüllen.
- Sicherung der Beweise zu Untersuchungszwecken
- Dokumentation einer nachträglichen Analyse und Entwicklung eines nachhaltigen Triage-Plans

Unsere Richtlinien zum Umgang mit Sicherheitsvorfällen werden im Rahmen unserer SOC 2+, ISO 27001 und anderer Sicherheitsabschätzungen überprüft.

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 Meeting-Informationen, 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.

Notfallplan

Damit die Informationssicherheit in Krisen oder Katastrophenfällen mit Auswirkungen auf den Betrieb von Dropbox Business gewährleistet bleibt, gibt es einen Notfallwiederherstellungsplan. Das Dropbox-Infrastrukturteam 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) geht auf Probleme mit der Beständigkeit und Verfügbarkeit ein, die wie folgt definiert sind:

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

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.

Rechenzentren und Managed Service-Anbieter

Die Unternehmens- und Produktionssysteme von Dropbox befinden sich in Subservice-Rechenzentren und bei Managed Service-Anbietern in unterschiedlichen Regionen der USA. Alle SOC-Berichte aus den Subservice-Rechenzentren und/oder Auftragnehmer-Sicherheitseinschätzungen 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 Umgebungszugriff auf eine begrenzte Anzahl von IP-Adressen und Mitarbeitern.

Infrastruktur in Deutschland, Australien und Japan

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 und Japan gehostet und innerhalb der entsprechenden Region repliziert, um Redundanz zu gewährleisten und Datenverlust zu verhindern. Dateimetadaten werden in den eigenen Servern von Dropbox in den USA gespeichert. Paper-Dokumente und Vorschauen aller Kunden werden aktuell in den USA gespeichert.

Produktmerkmale (Sicherheit, Kontrolle und Transparenz)

Dropbox bietet Funktionen zur administrativen Kontrolle und Transparenz, mit denen IT- und Endnutzer effektiv ihre Unternehmen und Daten verwalten können. Nachstehend finden Sie eine Erläuterung verschiedener Features für Administratoren und Endnutzer sowie Integrationen in Drittanbieter-Apps zur Verwaltung kritischer IT-Prozesse.

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

Verwaltungsfunktionen für Administratoren

Organisationen haben individuelle Bedürfnisse. Daher haben wir einige Tools entwickelt, mit denen Administratoren Dropbox Business an die Anforderungen ihrer Teams anpassen können. Im Folgenden stellen wir mehrere Funktionen zur Kontrolle und Transparenz vor, die über die Verwaltungskonsole von Dropbox Business zur Verfügung stehen.

Kontrolle

- ***Verschiedene Administratorebenen***

  Dropbox beinhaltet unterschiedliche Administratorebenen 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-Administrator**
  Kann Sicherheits- und Freigabeberechtigungen innerhalb des Teams festlegen, Administratoren erstellen und Nutzer verwalten. Der Team-Administrator hat alle verfügbaren Administratorrechte. Team-Administratoren sind die einzigen, die Administratorrollen zuweisen oder ändern können. Jedes Dropbox Business-Konto muss über mindestens einen Team-Administrator verfügen.

- **Nutzer-Administrator**
  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-Administrator**
  Kann allgemeine Service-Anfragen von Teammitgliedern bearbeiten, z. B. die Wiederherstellung gelöschter Dateien oder Hilfe für Teammitglieder, die für die zweistufige Überprüfung gesperrt sind. Support-Administratoren können auch Kennwörter von allen Nicht-Administrator-Nutzern zurücksetzen und Aktivitätsprotokolle bestimmter Teammitglieder exportieren.

- ***Methoden der Bereitstellung für Nutzer und des Identitätsmanagements***

  - **E-Mail-Einladung**
    Mithilfe eines Tools in der Dropbox Business-Verwaltungskonsole können Administratoren manuell eine E-Mail-Einladung generieren.

  - **Active Directory**
    Dropbox Business-Administratoren 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 (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 das Leben leichter und sicherer, indem ein vertrauenswürdiger Identitätsanbieter die Kontrolle über die Authentifizierung erhält und Teammitgliedern ohne zusätzliches Kennwort Zugriff auf Dropbox gibt. Dropbox arbeitet auch mit führenden Identitätsverwaltungsanbietern zusammen, sodass die Bereitstellung von Nutzern bzw. deren Aufhebung automatisch erfolgen kann. Weitere Informationen finden Sie unten im Abschnitt API-Integrationen in Dropbox Business.

  - **API**
    Kunden können mithilfe der Dropbox Business-API benutzerdefinierte Lösungen für Nutzerbereitstellung und Identitätsverwaltung entwickeln. Weitere Informationen finden Sie unten im Abschnitt API-Integrationen in Dropbox Business.

- ***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 lässt.

  - **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 Privatkontos ändern.

- ***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.

- ***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.

- ***Kennwortverwaltung***

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

- ***Gruppen***

  Teams können Listen von Nutzern innerhalb von Dropbox erstellen und verwalten und ihnen so ganz einfach Zugriff auf bestimmte Ordner gewähren. 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 zur Mitgliedschaft in oder zum 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.

- ***Freigabeberechtigungen***

  Team-Administratoren haben umfassende Kontrollen über die Freigabemöglichkeiten ihres Teams in Dropbox, einschließlich:

  - ob Teammitglieder Dateien und Ordner an Personen außerhalb des Teams freigeben können

- ob Teammitglieder Ordner bearbeiten können, deren Eigentümer Personen außerhalb des Teams sind
- ob von Teammitgliedern erstellte freigegebene Links bei Personen außerhalb des Teams funktionieren
- ob Teammitglieder Dateianfragen erstellen und Dateien von Teammitgliedern und/oder Personen außerhalb des Teams sammeln können
- ob Personen außerhalb des Teams Kommentare zu Dateien des Teams anzeigen und verfassen können
- ob Teammitglieder Paper-Dokumente und Paper-Ordner für Personen außerhalb des Teams freigeben können

- ***Team-Ordner für Dateien***

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

  - **Differenzierte Zugriffs- und Freigabefunktionen**
    Mittels Freigabefunktionen können Administratoren 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**
    Administratoren 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***

  Administratoren können freigegebene Paper-Ordner erstellen, wodurch andere Nutzer für die Inhalte, die sie benötigen, automatisch der erforderlichen Zugriffsebene (kommentieren oder bearbeiten) zugeordnet werden.

- ***Endgültiges Löschen von Berechtigungen***

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

- ***Verwaltung von Websitzungen***

  Administratoren 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 Remote-Löschen). Auf Mobilgeräten werden Dateien, die als Favoriten gekennzeichnet sind, sowie zwischengespeicherte Daten und Anmeldedaten gelöscht. Offline-Versionen 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.

- ***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-Anwendung 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.

- ***Nutzerstatus „Gesperrt"***

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

- ***Als Nutzer anmelden***

  Team-Administratoren 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 Benutzer über diese Ereignisse benachrichtigt werden.

- ***Netzwerksteuerung***

  Administratoren eines Dropbox Business-Teams 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 mit einem bestimmten Registrierungsschlüssel. Beachten Sie bitte, dass Paper zurzeit nicht durch die Netzwerksteuerung verwaltet wird.

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

  Dropbox kann in EMM-Drittanbieterfunktionen integriert werden, damit Administratoren von Dropbox Business-Teams 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 Remote-Zugriff 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-Teams mit Advanced- oder Enterprise-Abo, die Anzahl der Geräte, die ein Nutzer mit Dropbox synchronisieren kann, zu begrenzen und zu entscheiden, ob Zulassungen von Nutzern oder Administratoren verwaltet werden. Administratoren können auch eine Ausnahmeliste 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 Gerätezulassungen betroffen ist.

Transparenz

- ***Aktivitätsfeed***

  Dropbox Business zeichnet die Aktivitäten von Nutzern und Administratoren im Aktivitätsfeed des Teams auf, der über die Verwaltungskonsole eingesehen werden kann. Für den Aktivitätsfeed stehen flexible Filteroptionen zur Verfügung, wodurch Administratoren 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 Ereignisse werden im Aktivitätsfeed aufgezeichnet:

  - **Anmeldungen**
    Erfolgreiche oder fehlgeschlagene Anmeldeversuche bei Dropbox
    - Erfolgreicher oder fehlgeschlagener Anmeldeversuch
    - Fehlgeschlagener Anmeldeversuch oder Fehler über einmaliges Anmelden (SSO)
    - Fehlgeschlagener Anmeldeversuch oder Fehler über EMM
    - Abmeldung
    - Änderung der IP-Adresse von Websitzungen
  - **Kennwörter**
    Änderungen der Einstellungen für Kennwörter oder zweistufige Überprüfung. Administratoren können die Kennwörter der Nutzer nicht einsehen.
    - Kennwort 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
    - Teammitglied wurde eingeladen
    - Teammitglied ist dem Team beigetreten
    - Teammitglied wurde entfernt
    - Teammitglied wurde zeitweilig gesperrt bzw. Sperre wurde aufgehoben
    - Entferntes Teammitglied wurde wiederhergestellt
    - Beitritt zum Team basierend auf der Kontodomain wurde angefordert

- Anforderung zum Beitritt zum Team basierend auf der Kontodomain wurde bestätigt oder abgelehnt
- Domaineinladungen zu vorhandenen Domainkonten wurden versendet
- Nutzer ist dem Team aufgrund der Kontoerfassung beigetreten
- Nutzer hat das Team aufgrund der Kontoerfassung verlassen
- Teammitgliedern wurde die Möglichkeit zum Vorschlagen neuer Teammitglieder erlaubt oder verweigert
- Neues Teammitglied wurde vorgeschlagen

- **Apps**
  Verknüpfung von Drittanbieter-Apps mit Dropbox-Konten
  - Anwendung wurde autorisiert oder entfernt
  - Teamanwendung wurde autorisiert oder entfernt

- **Geräte**
  Verknüpfung von Computern oder Mobilgeräten mit Dropbox-Konten
  - Ein Gerät wurde verknüpft oder 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

- **Aktivitäten des Administrators**
  Änderungen an den Einstellungen in der Verwaltungskonsole, z. B. Berechtigungen für freigegebene Ordner

  Authentifizierung und einmaliges Anmelden (SSO)
  - Das Kennwort eines Teammitglieds wurde zurückgesetzt
  - Die Kennwörter aller Teammitglieder wurden zurückgesetzt
  - Teammitgliedern wurde die Deaktivierung der zweistufigen Überprüfung erlaubt oder verweigert
  - SSO wurde aktiviert oder deaktiviert
  - Anmeldung per SSO wurde obligatorisch
  - SSO-URL wurde geändert oder entfernt
  - SSO-Zertifikat wurde aktualisiert
  - SSO-Identitätsmodus wurde geändert

  Mitgliedschaft
  - Anforderung zum Beitritt eines Nutzers zum Team basierend auf der Kontodomain wurde erlaubt oder verweigert
  - Festlegung, dass Team-Beitrittsänträge automatisch zugelassen werden oder manuelle Administratorbestätigung benötigen

  Verwaltung von Mitgliederkonten
  - Der Name eines Teammitglieds wurde geändert
  - Die E-Mail-Adresse eines Teammitglieds wurde geändert
  - Administratorstatus wurde gewährt bzw. entfernt oder die Administratorrolle geändert

- Teammitglied hat sich an- oder abgemeldet
- Inhalte eines entfernten Nutzerkontos wurden übertragen oder gelöscht
- Inhalte eines entfernten Nutzerkontos wurden endgültig gelöscht

Allgemeine Freigabeeinstellungen

- Hinzufügen von Teammitgliedern zu freigegebenen Ordnern von Nicht-Teammitgliedern wurde erlaubt oder verweigert
- Teammitgliedern wurde die Freigabe von Ordnern an Nicht-Teammitglieder erlaubt oder verweigert
- Warnungen für Nutzer, bevor diese Ordner für Nicht-Teammitglieder freigeben, wurden aktiviert
- Nicht-Teammitgliedern wurde die Anzeige von freigegebenen Links erlaubt oder verweigert
- Freigegebene 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
- Logo für Seiten mit freigegebenen Links wurde hinzugefügt, geändert oder entfernt
- Teammitgliedern wurde die Freigabe von Paper-Dokumenten und Paper-Ordnern an Nicht-Teammitglieder erlaubt oder verweigert

Team-Ordner-Verwaltung für Dateien

- Team-Ordner wurde erstellt
- Team-Ordner wurde umbenannt
- Team-Ordner wurde aufgeräumt oder aus dem Archiv verschoben
- Team-Ordner wurde endgültig gelöscht
- Team-Ordner wurde zu einem freigegebenen Ordner heruntergestuft

Domainverwaltung

- Es wurde versucht, eine Domain zu überprüfen oder eine Domain wurde erfolgreich überprüft oder eine Domain wurde entfernt
- Domain wurde vom Dropbox-Support überprüft oder entfernt
- Versand von Domaineinladungen wurde aktiviert oder deaktiviert
- „Neue Nutzer automatisch einladen“ wurde aktiviert oder deaktiviert
- Kontoerfassungmodus wurde geändert
- Kontoerfassung wurde vom Dropbox-Support bewilligt oder aufgehoben

Enterprise Mobility Management (EMM)

- EMM wurde im Testmodus (optional) oder Bereitstellungsmodus (erforderlich) aktiviert
- EMM-Token wurde aktualisiert
- Teammitglieder wurden zur EMM-Liste ausgeschlossener Nutzer hinzugefügt oder daraus entfernt
- EMM wurde deaktiviert
- Bericht zur EMM-Ausnahmenliste wurde erstellt
- EMM-Bericht zur Nutzung der App für Mobilgeräte wurde erstellt

Änderungen an anderen Teameinstellungen

- Teams wurden zusammengeführt
- Team wurde zu Dropbox Business hochgestuft oder zu einem kostenlosen Team heruntergestuft
- Name des Teams wurde geändert
- Aktivitätsbericht für das Team wurde erstellt
- Teammitgliedern wurden mehrere mit einem Computer verknüpfte Konten erlaubt oder verweigert
- Das Erstellen von Gruppen wurde allen Teammitgliedern oder nur Administratoren erlaubt
- Teammitgliedern wurde das endgültige Löschen von Dateien erlaubt oder verweigert
- Dropbox-Support-Sitzung für einen Reseller wurde gestartet oder beendet

- **Freigabe von Dateien, Ordnern und Links**
  Sofern zutreffend, enthalten Berichte Angaben dazu, ob Personen außerhalb des Teams involviert sind.

  Freigegebene Dateien

  - Teammitglied oder Nicht-Teammitglied wurde hinzugefügt oder entfernt
  - Berechtigungen für ein Teammitglied oder Nicht-Teammitglied wurden geändert
  - Gruppe wurde hinzugefügt oder entfernt
  - Freigegebene Datei wurde zum Dropbox-Ordner eines Nutzers hinzugefügt
  - Inhalt einer Datei, die über eine Datei- oder Ordner-Einladung freigegeben wurde, wurde angezeigt
  - Freigegebene Inhalte wurden in den Dropbox-Ordner eines Nutzers kopiert
  - Freigegebene Inhalte wurden heruntergeladen
  - Kommentar zu einer Datei wurde erstellt
  - Kommentar wurde gelöst oder als ungelöst gekennzeichnet
  - Kommentar wurde gelöscht
  - Abonnement für Kommentierungsbenachrichtigungen 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, Nicht-Teammitglied 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 Nicht-Teammitglied wurden geändert
  - Eigentum eines Ordners wurde an einen anderen Nutzer übertragen
  - Freigabe eines Ordners 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 Nicht-Teammitglieder erlaubt oder verweigert
- Allen Teammitgliedern bzw. nur dem Eigentümer wurde erlaubt, Personen zu einem Ordner hinzuzufügen
- Gruppenzugriff auf einen freigegebenen Ordner wurde geändert

Freigegebene Links

- Links wurden erstellt oder entfernt
- Inhalte eines Links wurden für alle mit dem Link oder nur für Teammitglieder sichtbar gemacht
- Inhalte eines Links wurden mit einem Kennwort geschützt
- Gültigkeitsdauer eines Links wurde festgelegt oder entfernt
- Link wurde angesehen
- 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, ein Nicht-Teammitglied oder eine Gruppe freigegeben
- Nicht-Teammitgliedern wurde die Anzeige von Links zu Dateien in einem freigegebenen Ordner erlaubt oder verweigert
- Album wurde freigegeben

Dateianfragen

- Dateianfrage wurde erstellt, geändert oder geschlossen
- Benutzer wurden zu Dateianfrage hinzugefügt
- Frist für Dateianfrage wurde hinzugefügt oder entfernt
- Ordner für Dateianfrage wurde geändert
- Dateien wurden über Dateianfrage empfangen

- **Gruppen**
  Informationen zum Erstellen und Löschen von Gruppen sowie zur Gruppenmitgliedschaft einzelner Nutzer
  - Gruppe wurde erstellt, umbenannt, verschoben oder gelöscht
  - Nutzer wurde hinzugefügt oder entfernt
  - Zugriffsart eines Gruppenmitglieds wurde geändert
  - Gruppe wurde in „von Team verwaltet“ oder „von Administrator verwaltet“ geändert
  - Externe ID einer Gruppe wurde geändert
- **Dateiereignisse**
  Individuelle Datei- und Ordnerereignisse
  - Datei wurde zum Dropbox-Ordner hinzugefügt

- Ordner wurde erstellt
- Datei wurde angezeigt
- Datei wurde bearbeitet
- Datei wurde heruntergeladen
- Datei oder Ordner wurde kopiert
- Datei oder Ordner wurde verschoben
- Datei oder Ordner wurde umbenannt
- Frühere Version einer Datei wurde wiederhergestellt
- Änderungen in Dateien wurden zurückgenommen
- Gelöschte Datei wurde wiederhergestellt
- Datei oder Ordner wurde gelöscht
- Datei oder Ordner wurde endgültig gelöscht

- **Paper-Aktivitätsprotokoll**
  Administratoren 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, aufgeräumt, endgültig gelöscht oder wiederhergestellt
  - Paper-Dokument wurde kommentiert oder Kommentare wurden geklärt
  - Paper-Dokument wurde für Teammitglieder und Nicht-Teammitglieder freigegeben oder Freigabe wurde aufgehoben
  - Teammitglieder oder Nicht-Teammitglieder haben Zugriff auf Paper-Dokument angefragt
  - Teammitglieder oder Nicht-Teammitglieder wurden in Paper-Dokument erwähnt
  - Paper-Dokument wurde von Teammitgliedern oder Nicht-Teammitgliedern angesehen
  - Paper-Dokument wird gefolgt
  - Berechtigungen für Paper-Dokument haben sich geändert (bearbeiten, kommentieren, nur ansehen)
  - Externe Freigaberichtlinien für Paper-Dokument wurden geändert
  - Paper-Ordner wurde erstellt, aufgeräumt oder endgültig gelöscht
  - Paper-Dokument wurde einem Ordner hinzugefügt oder daraus entfernt
  - Paper-Ordner wurde umbenannt
  - Paper-Dokument- und -Ordnerübertragung

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

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

Verwaltungsfunktionen für Nutzer

Zum weiteren Schutz von Konten und Daten bietet Dropbox Business Tools für Endnutzer. Folgende Authentifizierungs-, Wiederherstellungs-, Protokollierungs- und andere Sicherheitsfunktionen stehen in den verschiedenen Dropbox-Benutzeroberflächen zur Verfügung.

Wiederherstellung und Versionskontrolle

Alle 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.

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 Kennworts jedes Mal die Eingabe eines sechsstelligen 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 Teammitglieder oder ausgewählte Nutzer einrichten.
- Darüber hinaus können Team-Administratoren 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 (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 zudem den offenen Standard FIDO Universal 2nd Factor (U2F), bei dem Nutzer sich mit einem USM-Sicherheitsschlüssel authentifizieren können, den sie anstelle des sechsstelligen Codes festgelegt haben.

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. Ein Nutzer kann die Freigabe von Ordnern sowie Dateien aufheben und Freigabeberechtigungen festlegen (siehe unten).

- ***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 (siehe unten).

- ***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 und beschreibt, inwieweit jede dieser Apps auf die Konten zugreifen kann. Nutzer können die Zugriffsberechtigung einer App auf ihr Dropbox-Konto jederzeit widerrufen.

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.

- ***Daten löschen***

  Einen zusätzlichen Schutz bietet die Option, nach zehn fehlgeschlagenen Anmeldeversuchen mit dem Pincode 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.

Berechtigungen für 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 Ordner***

  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 zudem 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.

- ***Kennwörter für freigegebene Links***

  Jeder freigegebene Link kann vom Eigentümer mit einem Kennwort geschützt werden. Vor der Übertragung von Datei- oder Ordnerdaten prüft eine Zugriffskontrolle das Kennwort 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 Kennwort „erinnert“.

- ***Begrenzte Gültigkeit freigegebener Links***

  Nutzer können für jeden freigegebenen Link eine Gültigkeitsdauer festlegen, um anderen Nutzern vorübergehend Zugriff auf Dateien oder Ordner zu gewähren.

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-Administrator kann die Link- und Freigaberichtlinie für Dokumente 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.

API-Integrationen in Dropbox Business

Über die Dropbox Business-API und unsere Partner können weitere Sicherheitstools zur Verwaltung von Daten und Konten hinzugefügt werden:

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

  Verknüpfen Sie Ihr Dropbox Business-Konto 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 Dateiinhalte, um Benachrichtigungen, Berichte und Aktivitäten auszulösen, wenn wichtige Änderungen in Ihrem Dropbox Business-Konto vorgenommen werden. Wenden Sie Unternehmensrichtlinien auf Ihre Dropbox Business-Bereitstellung an und erfüllen Sie vorgeschriebene Compliance-Anforderungen.

- ***eDiscovery und gesetzliche Aufbewahrungspflicht***

  Nutzen Sie die Daten im Dropbox Business-Konto 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 Dropbox Business-Konto auf die On-Premise-Server.

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

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

- ***Unternehmensspezifische Prozesse***

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

Wenn Entwickler Zugriff auf die Teamfunktionen von Dropbox Business erhalten, können Administratoren geschäftskritische Anwendungen für ihr Team bereitstellen und verwalten. Davon profitieren insbesondere Geschäftskunden, da Dropbox Business jetzt noch problemloser in ihre vorhandenen Drittanbieterlösungen integriert werden kann. Weitere Informationen zur Dropbox Business-API finden Sie unten im Abschnitt Apps für Dropbox.

Anwendungssicherheit

Dropbox-Benutzeroberflächen

Der Dropbox-Dienst kann über verschiedene Benutzeroberflächen genutzt werden. Jede Benutzeroberfläche verfügt über Sicherheitseinstellungen und -funktionen, die die Nutzerdaten verarbeiten und schützen und gleichzeitig einen benutzerfreundlicher 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-Desktopanwendung ist ein leistungsstarker Synchronisierungsclient, bei dem Dateien lokal für den Offlinezugriff gespeichert werden. Nutzer haben vollen Zugriff auf ihre Dropbox-Konten und die Anwendung läuft auf Windows-, Mac- oder Linux-Betriebssystemen. Die Dateien können direkt im Dateibrowser des jeweiligen Betriebssystems angesehen und freigegeben werden.

- ***Mobil***

  Die Dropbox-App steht für iOS-, Android-, Windows- und Kindle Fire-Smartphones und -Tablets zur Verfügung, sodass Nutzer auch unterwegs Zugriff auf all ihre Dateien haben. Über die App für Mobilgeräte können Nutzer Dateien auch 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, Versionen und Wiederherstellen von Dateien. Mithilfe der APIs kann der Nutzungszyklus eines Dropbox Business-Kontos verwaltet, können Aktivitäten für alle Mitglieder eines Teams durchgeführt und kann der Zugriff auf Dropbox Business-Administratorfunktionen gewährt werden.

Paper-Benutzeroberflächen

Der Paper-Dienst kann über eine Reihe von Benutzeroberflächen genutzt werden. Jede verfügt über Sicherheitseinstellungen und Elemente, 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.

- ***Mobil***

  Die Paper-App für Mobilgeräte von Dropbox steht für iOS- und Android-Mobilgeräte und 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 beinhaltet Endpunkte und Datentypen für die Verwaltung von Dokumenten und Ordner in Dropbox Paper, einschließlich der Unterstützung von Funktionen wie Berechtigungsverwaltung, Aufräumen 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 jedoch häufig als „SSL/TLS“ bezeichnet, weshalb wir diese Bezeichnung hier verwenden.

Um Man-in-the-Middle-Angriffen vorzubeugen, werden die Front-End-Server von Dropbox mithilfe öffentlicher Zertifikate authentifiziert, die dem Client vorliegen. Eine verschlüsselte Verbindung wird ausgehandelt, bevor Dateien oder Paper-Dokumente übertragen werden. So wird die sichere Übertragung zu den Front-End-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 von Dropbox 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 eines internen Systems 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 bei den meisten Systemen und Implementierungen auch in unserem Desktop-Client und dem Client für 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 Anmeldeinformationen von Nutzern geht Dropbox über gewöhnliches Hashing hinaus. Im Einklang mit branchenüblichen Best Practices wird jedes Kennwort mit einem zufällig generierten benutzerspezifischen Salt kombiniert. Zudem 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 Kennwörter selbst bei einer Kompromittierung der Datenbank sicher sind.

Malware-Scans

Wir haben ein automatisiertes Scansystem entwickelt, das die Verbreitung von Malware über freigegebene Dropbox-Links verhindern soll. Das System nutzt sowohl proprietäre Technologien als auch branchenübliche Erkennungsmodule.

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 500.000 Entwickler Apps und Dienstleistungen für Produktivität, Zusammenarbeit, Sicherheit, Verwaltung und vieles mehr auf der Plattform entwickelt.

Dropbox-API

Die Dropbox-API bietet Zugriff auf Nutzerebene für Entwickler und ist eine flexible Möglichkeit, Dateien in Dropbox zu lesen und zu schreiben. Interaktionen im Rahmen der Authentifizierung, mit Dateien oder Metadaten, mit freigegebenen Dateien, Ordnern und Links, mit Paper-Dokumenten und Paper-Ordnern sowie Dateivorgänge werden über die Dropbox-API verarbeitet.

Apps, die die Dropbox-API verwenden, können mit einer der nachfolgenden Berechtigungsebenen 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 (siehe unten).

- ***Komplette 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 (siehe unten).

Chooser und Saver

Mithilfe von Chooser und Saver erhalten Nutzer mit nur wenigen Codezeilen einfachen Zugriff auf Dropbox. Mit dem Chooser können Nutzer Dateien aus Dropbox auswählen, mit dem Saver werden Dateien direkt in Dropbox gespeichert. Im Grunde übernehmen die Drop-Ins die Aufgaben der bekannten Dialogfelder „Öffnen“ und „Speichern“ und beschränken den Zugriff der App auf die Dateien und/oder Ordner, die der Nutzer für diese Aktionen einmalig festlegt.

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.

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 Dropbox Business-API (siehe unten) können WebHooks außerdem verwendet werden, um Benachrichtigungen über Änderungen der Teammitgliedschaft zu generieren. Viele Sicherheits-Apps verwenden WebHooks, um Administratoren zu helfen, Teamaktivitäten nachzuverfolgen und zu verwalten.

Dropbox Business-API

Mit der Dropbox Business API können Apps ganze Dropbox Business-Konten verwalten und Dropbox-API-Aktivitäten für alle Mitglieder eines Teams durchführen. Sie bietet Apps einen programmgesteuerten Zugriff auf die Verwaltungsfunktionen von Dropbox Business.

Neben Dropbox-API-Abfragen bietet die Dropbox Business-API zusätzliche Endpunkte, die speziell für Unternehmen entwickelt wurden. Dazu zählen Endpunkte für Auditing sowie Nutzer- und Gruppenverwaltung.

App-Berechtigungstypen

Es gibt vier verschiedene Berechtigungstypen für die Dropbox Business-API mit jeweils unterschiedlichen Zugriffsmöglichkeiten auf Team- und Nutzerdaten. Bei der Anforderung der Zugriffsberechtigung sollten sich Entwickler auf die Zugriffsebene beschränken, die ihre App auch wirklich benötigt:

- ***Teaminformationen***

  Informationen zum Team sowie aggregierte Nutzungsdaten

- ***Team-Auditing***

  Teaminformationen sowie ein detailliertes Aktivitätsprotokoll

- ***Zugriff auf Teammitgliederdateien***

  Teaminformationen und -Auditing sowie die Fähigkeit, in der Rolle eines Teammitglieds beliebige Aktionen durchzuführen

- ***Teamverwaltung***

  Teaminformationen sowie die Fähigkeit, Teammitglieder hinzuzufügen, zu bearbeiten und zu löschen

Ebenso wie die Dropbox-API setzt auch die Dropbox Business-API auf OAuth 2.0 zur Authentifizierung aller API-Anfragen. Mit den OAuth-Token der Dropbox Business-API wird ein umfangreicher Zugriff auf Kontodaten möglich. Die OAuth-Antwort beinhaltet ein zusätzliches team_id-Feld. Der Entwickler ist für die Sicherheit der OAuth-Token auf der Serverseite verantwortlich und muss sicherstellen, dass die Daten nicht in einer unsicheren Umgebung zwischengespeichert oder auf Clientgeräte heruntergeladen werden. Die Entwickler müssen einen Dropbox Business-Team-Administrator durch den OAuth-2.0-Standardprozess führen, damit ihre Anwendung auf einem Dropbox Business-Konto installiert wird.

Weitere Informationen zu Dropbox-APIs finden Sie unter dropbox.com/developers.

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 Apps unsere Branding-Richtlinien und Allgemeinen Geschäftsbedingungen für Entwickler erfüllen, in denen auch erläutert wird, wofür die Dropbox-Plattform 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.

API-Partnerschaften

Dropbox arbeitet eng mit unseren Partnern zusammen, um Integrationen in beliebte Softwarepakete zu entwickeln. Dank dieser Integrationen ist es möglich, über die Benutzeroberfläche auf Daten in Dropbox zuzugreifen, sodass die Bedienung für die Endnutzer beider Dienste nahtlos und sicher erfolgt.

- ***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.

- ***AutoCAD***

  Dropbox ist eine Partnerschaft mit Autodesk eingegangen, um das Öffnen von AutoCAD-Projektdateien zu ermöglichen, die in Dropbox gespeichert sind. Diese können nahtlos wieder in Dropbox gespeichert werden, ohne die AutoCAD-Desktopanwendung zu verlassen. Beim ersten Öffnen einer Dropbox-Datei in der mobilen AutoCAD-App wird der Nutzer aufgefordert, den Zugriff zu gewähren.

Netzwerksicherheit

Die Sicherheit unseres Backend-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 freien 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 20 Standorten rund um den Globus befinden. An diesen Standorten werden keine Nutzerdaten gespeichert, zudem 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.

Schwachstellenmanagement

Unser Sicherheitsteam führt in Zusammenarbeit mit externen Sicherheitsexperten regelmäßig automatisierte und manuelle Sicherheitstests durch, um potenzielle Schwachstellen und Fehler zu beheben.

Sicherheitsexperten werten diese Aktivitäten aus und das Sicherheitsteam weist den Elementen verschiedene Prioritätsstufen zu. 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

Das Technikerteam von Dropbox hat formelle Richtlinien für das Änderungsmanagement aufgestellt, um zu gewährleisten, dass Anwendungsänderungen vor der Implementierung in die Produktionsumgebung autorisiert werden. Quellcodeänderungen werden von Entwicklern initiiert, die eine Verbesserung an der Dropbox-Anwendung oder am Dropbox-Dienst vornehmen möchten. Änderungen werden in einem System mit Versionskontrolle 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 automatisch über Änderungen 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, Firewall 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 Unternehmens- und Produktionsumgebungen durchzuführen. Um die Sicherheit unserer Anwendungen zu gewährleisten, arbeiten wir mit externen Sicherheitsexperten, anderen Sicherheitsteams der Branche und der Forschungscommunity zusammen.

Darüber hinaus suchen wir auch mit unseren automatischen Analysesystemen nach Schwachstellen. 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.

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 allgemeinen Sicherheitscommunity. Unser Bug-Bounty-Programm bietet Sicherheitsexperten Anreize und eine zentrale Anlaufstelle 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 Branchenführern gehören.

Wir haben einen Rahmen für zulässige Meldungen und die infrage kommenden Dropbox-Anwendungen 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.
- Gewähren 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 und bearbeiten Sie diese nicht.
- Beeinträchtigen Sie die Leistung unseres Dienstes nicht mutwillig. Dies schließt auch DoS-Angriffe ein.

Probleme können in einem Bericht an HackerOne unter hackerone.com/dropbox gemeldet werden.

Informationssicherheit bei Dropbox

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 Dropbox Business-Systeme 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 die Bereiche Informationssicherheit, Schutz von Nutzerdaten, physische Sicherheit, Umgang mit Sicherheitsvorfällen, Geschäftskontinuität, logischer Zugriff, Zutritt zur Produktionsumgebung, Änderungsmanagement und Vertrieb und Kundenerlebnis umfassen. Diese Richtlinien werden mindestens einmal im Jahr überprüft und genehmigt und vom Dropbox-Sicherheitsteam umgesetzt. Mitarbeiter, Praktikanten und Auftragnehmer nehmen bei Eintritt in das Unternehmen an obligatorischen Sicherheitsschulungen und später am weiterführenden Schulungsprogramm zur Förderung des Sicherheitsbewusstseins teil.

- ***Informationssicherheit***

  Richtlinien bezüglich Nutzer- und Dropbox-Daten mit den Schwerpunkten Gerätesicherheit, Authentifizierungsanforderungen, Daten- und Systemsicherheit, Schutz von Nutzerdaten, Beschränkungen und Richtlinien für die Nutzung von Ressourcen durch Mitarbeiter sowie Handhabung von potenziellen Problemen

- ***Schutz von Nutzerdaten***

  Unsere Anforderungen an den Schutz und die Verarbeitung von Nutzerinformationen sowie -daten bei Dropbox, um die Datenschutzrichtlinie einzuhalten

- ***Physische Sicherheit***

  So sorgen wir bei Dropbox für eine sichere und geschützte Umgebung für Menschen und Eigentum (siehe Abschnitt Physische Sicherheit weiter unten)

- ***Umgang mit Sicherheitsvorfällen***

  Unsere Anforderungen, wie auf potenzielle Sicherheitsstörfälle reagiert werden muss, einschließlich Beurteilung, Kommunikation und Untersuchungsverfahren

- ***Logischer Zugriff***

  Richtlinien für den Schutz von Dropbox-Systemen sowie Nutzer- und Dropbox-Daten, einschließlich Zugriffskontrollen in Unternehmens- und Produktionsumgebungen

- ***Zutritt zur Produktionsumgebung***

  Unsere Verfahren für den beschränkten Zutritt zum physischen Produktionsnetzwerk, einschließlich Management-Überprüfung der Mitarbeiter und Entzug von Berechtigungen für Mitarbeiter, die das Unternehmen verlassen haben

- ***Änderungsmanagement***

  Richtlinien für Codeprüfungen und Verwaltung von sicherheitsrelevanten Änderungen durch autorisierte Entwickler an Anwendungsquellcode, Systemkonfiguration und Produktionsversionen

- ***Vertrieb und Kundenerlebnis***

  Zugangsrichtlinien hinsichtlich Nutzer-Metadaten für unser Supportteam einschließlich Ansicht, Supportangebot und Durchführung von Maßnahmen in Dropbox-Nutzerkonten

- ***Geschäftskontinuität***

  Richtlinien und Verfahren zur Aufrechterhaltung oder Wiederherstellung wichtiger Geschäftsfunktionen im Falle einer Unterbrechung, von der Planung und Dokumentation bis zur Ausführung

- ***Krisenverwaltung***

  Richtlinien und Verfahren, mit denen Dropbox auf ein außerordentlich weit verbreitetes Ereignis reagiert, das unsere wichtigsten Prozesse unterbrechen oder unsere strategischen Ziele bedrohen kann

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 ihrer 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 komplexen Kennwörtern, passphrase-geschützten SSH-Schlüsseln, zweistufiger Überprüfung und OTP-Token authentifiziert. Für den Remote-Zugriff ist ein VPN-Zugang mit zweistufiger Überprüfung 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, Serverkonfigurationsprogramme, Produktionsserver und Quellcode-Entwicklungsprogramme wird nur mit ausdrücklicher Zustimmung des zuständigen Managements gewährt. Die Nachweise des Zugangsantrags, der Begründung und Genehmigung werden durch das Management verwahrt 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 der Nutzerkonten einzuschränken. Zum Schutz der Endnutzerdaten dürfen nur sehr wenige Techniker, die für die Entwicklung der wichtigsten Dropbox-Dienste verantwortlich sind, auf die Umgebung zugreifen, in der die Nutzerdateien gespeichert sind. Der Zugang 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.

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. Einzelpersonen, die außerdem Zutritt zu den Einrichtungen der Produktionsumgebung benötigen, ist dies nur nach ausdrücklicher Genehmigung von der zuständigen leitenden Stelle gestattet.

Das Management dokumentiert Anfrage, Begründung und Genehmigung, bevor die entsprechenden Personen Zugriff erhalten. Wenn die Genehmigung erteilt wurde, wird ein autorisiertes Mitglied des Infrastrukurteams 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 Zugriff mit dem offiziellen Dropbox-Badge und, wo möglich, biometrischen Scan-Zugriff. Wenn diesen Personen der Zugang gewährt wurde, liegt es im Verantwortungsbereich des Rechenzentrums, dass der Zugang nur auf diese autorisierten Einzelpersonen 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.

Compliance

Es gibt viele verschiedene Normen und Vorschriften, an die sich Organisationen halten müssen. 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 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 den Niederlanden ansässige Unternehmen EY CertifyPoint, zertifizieren lassen. EY CertifyPoint hat eine ISO-Zertifizierung vom Raad voor Accreditatie (dem niederländischen Zertifizierungsrat).

ISO 27001 (Informationssicherheit)

ISO 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 27002 ausgeführt sind. Wir halten unsere umfassenden physischen, technischen und rechtlichen Bestimmungen und Maßnahmen bei Dropbox stets auf dem neuesten Stand und verbessern sie immer weiter, damit wir uns des von Ihnen entgegengebrachten Vertrauens auch wirklich würdig erweisen.

ISO 27001-Zertifikat für Dropbox Business und Dropbox Education ansehen

ISO 27017 (Cloud-Sicherheit)

ISO 27017 ist ein internationaler Standard für Cloud-Sicherheit, der einen Leitfaden für Sicherheitsaspekte bietet, die bei der Bereitstellung und Nutzung von Clouddiensten 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 27017-Zertifikat für Dropbox Business und Dropbox Education ansehen

ISO 27018 (Datenschutz und Datensicherheit in der Cloud)

ISO 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 27018-Zertifikat für Dropbox Business und Dropbox Education ansehen

ISO 22301 (Geschäftskontinuität)

ISO 22301 ist ein internationaler Standard für Geschäftskontinuität. 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 Dropbox Business Continuity Management System (BCMS) ist Teil unserer allgemeinen Risikomanagementstrategie zum Schutz von Personen und Betriebsabläufen in Krisenfällen.

ISO 22301-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 Servicegrundsätze (Trust Service Principles, TSP) 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 für Sicherheit, Vertraulichkeit, Prozessintegrität, Verfügbarkeit 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 beinhaltet unser SOC 2-Bericht (manchmal auch SOC 2+ genannt) ein geprüftes Mapping unserer Kontrollen hinsichtlich der zuvor genannten ISO-Standards und liefert unseren Kunden zusätzliche Transparenz. Die Trust Service-Kriterien ersetzen die seit Kurzem veralteten Trust Service-Prinzipien. 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 Business 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 Business und Dropbox Education erhalten Sie auf Anfrage.

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 Clouddienste 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 zertifiziert und attestiert. 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 27001, den SOC 2 Trust Services-Kriterien und der CSA Cloud Controls Matrix (CCM) Version 3.0.1 voraus. Dropbox hat außerdem die Selbsteinschätzung nach CSA STAR Level 1 für Dropbox Business und Dropbox Education durchgeführt. Dabei handelt es sich um einen umfassenden Fragenkatalog auf Basis des Consensus Assessments Initiative Questionnaire (CAIQ) in Übereinstimmung mit der Cloud Controls Matrix (CCM) von CSA. Darin haben wir knapp 300 Fragen beantwortet, die ein Kunde oder Auditor einem Cloud-Anbieter stellen könnte.

Unsere Zertifikate und Attestierung nach CSA STAR Level 1 und Level 2 auf der CSA-Website ansehen

HIPAA/HITECH

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

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.

Bei Interesse an diesen Dokumenten oder der Anschaffung von Dropbox Business oder Dropbox Education wenden Sie sich an unser Vertriebsteam. Wenn Sie Team-Administrator eines Dropbox Business- oder Dropbox Education-Teams sind, können Sie in der Verwaltungskonsole auf der Kontoseite einen Geschäftspartnervertrag (BAA) elektronisch unterzeichnen. Weitere Details finden Sie in unserem Leitfaden Erste Schritte mit HIPAA.

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.

Deutschland: Bericht zur C5-Zertifizierung des BSI

Der Anforderungskatalog Cloud Computing (C5) ist ein Regelwerk des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Sicherheit bei der Bereitstellung von Clouddiensten. Die Verfahren zur Gewährleistung der Informationssicherheit C5-zertifizierter Organisationen entsprechen nachweislich den „Sicherheitsempfehlungen für Cloud Computing Anbieter“ des BSI. Der Anforderungskatalog beruht auf bestehenden internationalen Sicherheitsstandards wie ISO 27001 und CSA STAR. Um die C5-Zertifizierung zu erhalten, wurden die Systeme, Prozesse und Kontrollmaßnahmen von Dropbox durch den unabhängigen, in Deutschland ansässigen externen Auditor Ernst & Young GmbH geprüft und verifiziert. Die unabhängige Prüfung wird gemäß dem International Standard on Assurance Engagements No. 3000 (ISAE 3000) durchgeführt.

Der Bericht beinhaltet eine ausführliche Beschreibung der Systeme, Anwendungen, Prozesse und Kontrollen von Dropbox sowie der Testverfahren unseres unabhängigen Auditors und der jeweiligen Prüfungsergebnisse. Den C5-Bericht für Dropbox Business und Dropbox Education erhalten Sie auf Anfrage.

Bitte nehmen Sie zur Kenntnis, dass Dropbox Paper nicht durch den C5-Bericht abgedeckt ist.

Schüler und Kinder (FERPA und COPPA)

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.

Vereinigtes Königreich: Digital Marketplace G-Cloud

Im Vereinigten Königreich wird Dropbox Business im Digital Marketplace für Clouddienst-Beschaffung der Regierung geführt. Sehen Sie sich hierzu die Einträge zum Dropbox Business Standard-Abo, Dropbox Business Advanced-Abo und Dropbox Enterprise-Abo auf der Digital Marketplace-Website an.

Bitte nehmen Sie zur Kenntnis, dass Dropbox Paper nicht im Digital Marketplace G-Cloud-Angebot im Vereinigten Königreich enthalten ist.

PCI DSS

Dropbox hält als Händler den Payment Card Industry Data Security Standard (PCI DSS) ein. Jedoch sind Dropbox Business, 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

Besuchen Sie www.dropbox.com/business/trust/compliance

Datenschutz

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

Datenschutzrichtlinien

Unsere Datenschutzrichtlinien können unter dropbox.com/privacy eingesehen werden. Die Datenschutzrichtlinien, die Geschäftsvereinbarung, die Allgemeinen Geschäftsbedingungen sowie die Nutzungsbedingungen von Dropbox enthalten folgende Informationen:

- Welche Art von Daten sammeln 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?

ISO 27018

Dropbox Business war einer der ersten namhaften Clouddienstanbieter mit ISO 27018-Zertifizierung. Das ist eine weltweite Norm für den Datenschutz und die Informationssicherheit in der Cloud. ISO 27018 wurde im August 2014 veröffentlicht und behandelt insbesondere den Schutz personenbezogener Daten und die Informationssicherheit in der Cloud. Die Norm erläutert zahlreiche Anforderungen an Dropbox hinsichtlich der Verwendung Ihrer Unternehmensdaten:

- ***Ihre Organisation 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 27018 ist eine Erweiterung von ISO 27001, einer international anerkannten Zertifizierungsnorm für Informationssicherheit. Im Oktober 2014 haben wir unsere Zertifizierung nach ISO 27001 erhalten. Die Anforderungen an die Datensicherheit und den Datenschutz nach ISO 27018 – besonders hinsichtlich der Verschlüsselung und des streng kontrollierten Mitarbeiterzugriffs – greifen ineinander.

- ***Unsere Geschäftspraktiken unterliegen der unabhängigen Kontrolle.***

  Im Rahmen unserer ISO 27017- und ISO 27001-Zertifizierungen und der Beibehaltung derselben unterziehen wir uns einer jährlichen Prüfung durch ein unabhängiges Unternehmen. Unser ISO 27018-Zertifikat kann hier abgerufen werden.

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 Nutzerdaten zu erlangen. 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.

EU-USA- und Schweiz-USA-Datenschutzschild

Bei der Datenübermittlung aus der Europäischen Union, dem Europäischen Wirtschaftsraum und der Schweiz stützt sich Dropbox auf eine Vielzahl von Rechtsinstrumenten, einschließlich der Verträge mit unseren Nutzern. Dropbox hält die Bestimmungen der zwischen der EU und den USA und der Schweiz und den USA geltenden Datenschutzschild-Rahmenbedingungen („Privacy Shield“) ein, die vom U.S. Department of Commerce in Bezug auf die Erfassung, Verwendung und Speicherung personenbezogener Informationen, die aus der Europäischen Union, dem Europäischen Wirtschaftsraum und der Schweiz in die USA übermittelt werden, erlassen wurden. Die Datenschutzschild-Zertifizierung von Dropbox finden Sie unter www.privacyshield.gov/list. Weitere Informationen zum Datenschutzschild finden Sie unter www.privacyshield.gov.

Durch das Einhalten der Datenschutzschild-Bestimmungen wird dafür gesorgt, dass eine Organisation angemessenen Datenschutz gemäß der EU-Datenschutzrichtlinie bietet. Beschwerden und Streitfragen hinsichtlich unserer Datenschutzschild-Compliance werden von JAMS, einem unabhängigen Drittunternehmen, untersucht und geklärt. Weitere Informationen finden Sie in unseren Datenschutzrichtlinien (dropbox.com/privacy).

Datenschutz-Grundverordnung (DSGVO) der Europäischen Union

Die Datenschutz-Grundverordnung 2016/679 (DSGVO) ist eine Verordnung der Europäischen Union, die eine wesentliche Änderung des bislang geltenden Rahmens für die Verarbeitung von personenbezogenen Daten innerhalb der EU darstellt. Die DSGVO führte eine Reihe neuer oder strengerer Anforderungen ein, die für Unternehmen wie Dropbox, das personenbezogene Daten verwaltet, gelten. Die DSGVO trat am 25. Mai 2018 in Kraft und ersetzte die bis dahin geltende EU-Richtlinie 95/46 EG, besser bekannt als die Datenschutzrichtlinie.

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.

Weitere Informationen zu unseren Datenschutzrichtlinien und -praktiken finden Sie im Dropbox-Whitepaper über Informationssicherheit und Datenschutz.

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. Daher haben Sicherheit, Compliance und Datenschutz 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.

Zusammenfassung

Dropbox Business bietet nicht nur benutzerfreundliche Tools zur effektiven Zusammenarbeit, sondern auch die erforderlichen Sicherheitsmaßnahmen und Compliance-Zertifizierungen, die die Organisationen benötigen. 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.