Dropbox Business

Gemeinsame Verantwortung: Zusammenarbeit für die Datensicherheit

Dropbox arbeitet mit seinen Business- und Education-Kunden eng zusammen, um die Sicherheit ihrer Daten zu gewährleisten. Wir schützen unsere Infrastruktur, unser Netzwerk und unsere Anwendungen mit umfassenden Sicherheitsmaßnahmen. Die Dropbox-Mitarbeiter erhalten Schulungen zu Sicherheits- und Datenschutzverfahren. Unsere Unternehmenskultur räumt der Vertrauenswürdigkeit höchste Priorität ein und unsere Systeme und Verfahren werden von Dritten nach strengen Gesichtspunkten getestet und geprüft.

Dropbox sorgt somit für die Sicherheit aller Aspekte des Diensts, die unter unserer Kontrolle stehen. Die Kunden dagegen sind maßgeblich für die Sicherheit ihrer Teams und Daten verantwortlich. Als Administrator eines Teams, das mit Dropbox Business oder Dropbox Education arbeitet, können Sie Ihr Konto so konfigurieren, nutzen und überwachen, dass es die Anforderungen Ihres Unternehmens an Sicherheit, Datenschutz und Compliance erfüllt.

In diesem Leitfaden möchten wir Ihnen erläutern, wie Dropbox Ihr Konto schützt und wie Sie die Transparenz und Kontrolle im Hinblick auf die Daten Ihres Teams wahren können.

Verantwortungsbereiche von Dropbox

Integration von Sicherheitsmaßnahmen in unsere Architektur

Mehrere Tausend Unternehmen weltweit vertrauen uns ihre wichtigste Arbeit an. Um dieses Vertrauen nicht zu enttäuschen, arbeiten wir kontinuierlich an sicheren Produkten, auf die sich Administratoren wie Sie verlassen können. Nachfolgend stellen wir einige unserer Maßnahmen zur Absicherung unserer Architektur und unserer Netzwerke vor.

Verteilte Architektur

In der Dropbox-Architektur werden Informationen unterschiedlicher Ebenen auf mehrere Dienste verteilt. Dies sorgt nicht nur für eine schnellere und zuverlässigere Synchronisierung, sondern auch für mehr Sicherheit. Diese Beschaffenheit der Dropbox-Architektur verhindert, dass der Zugriff auf einen dieser Dienste dazu verwendet werden kann, Dateien oder Paper-Dokumente zu replizieren.

Sichere Netzwerke

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. Der Zugriff auf die Produktionsumgebung ist auf autorisierte IP-Adressen beschränkt und erfordert an allen Endpunkten eine mehrstufige Authentifizierung.

Verschlüsselung von Nutzerdaten

Dropbox Business- und Dropbox Education-Kunden nutzen zur Interaktion mit unserem System die Dropbox-Anwendungen für Mobilgeräte, Desktops und das Web. Alternativ werden APIs eingesetzt. Unabhängig von der verwendeten App schützen wir Ihre Dateien und Paper-Dokumentdaten bei der Übertragung und im Ruhezustand.

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“.

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

Gespeicherte Dateien werden bei Dropbox nach AES mit 256 Bit verschlüsselt. Die Speicherung der Dateien erfolgt in Form separater Dateiblöcke in verschiedenen Rechenzentren. 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.

Stets zuverlässiger Service

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. Innerhalb eines Rechenzentrums werden redundante Kopien von Metadaten mindestens nach einem N+2-Verfügbarkeitsmodell auf mehrere unabhängige Geräte verteilt. Stufenweise Backups von Metadaten werden stündlich durchgeführt, vollständige Backups alle drei Tage. Die Speicherung der Metadaten erfolgt auf Servern, die von Dropbox gehostet und verwaltet werden. Für die Speicherung von Dateiblöcken nutzt Dropbox sowohl eigene Systeme als auch Systeme von Dritten, die auf eine jahresbezogene Langlebigkeit der Daten von mindestens 99,999999999 % ausgelegt sind.

Bei einem seltenen Serviceausfall können Dropbox-Nutzer immer noch auf ihren verknüpften Computern über den lokalen Dropbox-Ordner auf die neuesten synchronisierten Versionen ihrer Dateien zugreifen. 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.

Redundante Kopien von Paper-Dokumentdaten werden auf ähnliche Weise in einem Rechenzentrum auf unabhängigen Geräten nach einem N+1-Verfügbarkeitsmodell verteilt und wir haben eine tägliche Datensicherung der Paper-Dokumentdaten konfiguriert. Für die Speicherung von Paper-Dokumenten nutzt Dropbox Systeme von Dritten, 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.

Beschränkter Mitarbeiterzugriff auf Back-End-Systeme

Als Dropbox Business- oder Dropbox Education-Kunde erwarten Sie von uns selbstverständlich einen verantwortungsvollen Umgang mit Ihren Daten, wenn Sie uns Ihre Dateien oder Paper-Dokumente bei der Speicherung in Dropbox anvertrauen. Um dieser Verantwortung Rechnung zu tragen, wird der Zugriff der Dropbox-Mitarbeiter auf unsere internen Systeme streng kontrolliert. Dies gilt für unsere Unternehmens- und Produktionsnetzwerke gleichermaßen. So erfolgt der Zugriff auf das Produktionsnetzwerk ausschließlich mit einem SSH-Schlüssel, den nur Techniker erhalten, die aufgrund ihrer Arbeit Zugriff benötigen. Auch die Konfiguration der Firewall steht unter strenger Kontrolle und kann nur von wenigen Administratoren verändert werden. 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.

Schulung des Sicherheits- und Datenschutzbewusstseins der Mitarbeiter

Zur Wahrung der Sicherheit unserer Services gehört auch sicherzustellen, dass die Mitarbeiter bei Dropbox Sicherheitsbewusstsein entwickeln und verdächtige Aktivitäten erkennen können. Deshalb müssen alle Dropbox-Mitarbeiter der Einhaltung von Sicherheitsrichtlinien zustimmen, bevor sie Systemzugriff erhalten. Zudem nehmen sie an verpflichtenden Sicherheits- und Datenschutzschulungen für neue Mitarbeiter sowie Folgeschulungen teil und erhalten regelmäßige Schulungen zu Sicherheitsbewusstsein per E-Mail, in Gesprächen, Präsentationen und verfügbaren Ressourcen in unserem Intranet.

Validierung unserer Verfahren

Die Wirksamkeit unserer Sicherheitsverfahren wird von Dritten überprüft. Spezialisten führen regelmäßig Penetrations- und Schwachstellentests in den Unternehmens- und Produktionsumgebungen von Dropbox durch. Dabei erkannte Probleme werden von unserem Sicherheitsteam mit hoher Priorität behandelt und behoben. Zusätzlich bewerten externe Prüfer unsere Sicherheitsverfahren im Hinblick auf internationale und branchenspezifische Standards. Weitere Informationen über die von Dropbox verwendeten Verfahren finden Sie online in unserem SOC 3-Bericht und unseren ISO 27001-, 27017-, 27018- und 22301- Zertifikaten. Darüber hinaus können Sie unseren SOC 2-Bericht, eine Zuordnung der HIPAA-Anforderungen, unser BSI C5-Prüfprotokoll (verfügbar auf Englisch und Deutsch) und die zusammengefassten Ergebnisse der Penetrationstests im Rahmen einer Vertraulichkeitsvereinbarung anfordern.

Mitteilung von Problemen

Dienststatus

Dropbox Business- und Dropbox Education-Kunden können auf einer externen Website Angaben zum Status des Dropbox-Diensts abrufen. Als aktueller Kunde können Sie unter status.dropbox.com jederzeit den aktuellen Status der Website überprüfen und sich über vorangegangene Unterbrechungen und Wartungsarbeiten informieren.

Benachrichtigung über Sicherheitsverletzungen

Dropbox benachrichtigt Sie gemäß den geltenden Vorschriften im Falle von Datenschutzverletzungen. Wir verfügen über Richtlinien und Verfahren zum Umgang mit Sicherheitsverletzungen, einschließlich eines Benachrichtigungsverfahrens bei Sicherheitsverletzungen, die es uns ermöglichen, betroffene Kunden ggf. zu informieren. Wenn Sie ein HIPAA Business Associate Agreement oder eine europäische Datenverarbeitungsvereinbarung abgeschlossen haben, werden Sie entsprechend den Vorgaben in diesen Vereinbarungen benachrichtigt.

Tools für Ihre Sicherheit

Wir möchten Ihnen und anderen Administratoren von Dropbox Business und Dropbox Education Tools an die Hand geben, mit deren Hilfe Sie verantwortungsvolle, fundierte Entscheidungen zur Sicherheit Ihres Teams treffen können. Die Verwaltungskonsole ist mit Sicherheitselementen ausgestattet, die Sie im Namen Ihres Teams aktivieren können, um Ihr Konto gemäß Ihren Anforderungen zu konfigurieren, zu nutzen und zu überwachen. In Leitfäden wie dem hier vorliegenden, im Sicherheits-Whitepaper zu Dropbox Business, im Hilfecenter und über unser Supportteam erfahren Sie, wie Sie diese Einstellungen verwenden, um Ihr Konto verantwortungsvoll zu konfigurieren.

Verantwortungsbereiche des Kunden

Auseinandersetzung mit unseren Verfahren

Die Auswahl der zu Ihren Unternehmensanforderungen passenden Variante von Dropbox Business oder Dropbox Education ist ein sehr wichtiger Prozess. Nehmen Sie sich Zeit, unsere Praktiken zu überprüfen, wie Sie es auch bei jeder anderen Anwendung tun würden. Um Ihnen die nötigen Instrumente, die Sie für die Überprüfung unserer Sicherheitspraktiken benötigen, bereitzustellen, stehen unsere ISO 27001-, 27017-, 27018-, 22301- Zertifikate, unser Bericht zur Einhaltung von SOC 3 und unsere CSA STAR Level 1-Selbstbeurteilung und Level 2-Zertifizierung online zur Verfügung. Um Sie bei der richtigen Entscheidung zu unterstützen, bieten wir Ihnen im Rahmen einer Geheimhaltungsvereinbarung den Zugriff auf weitere Dokumente. Dazu zählen unsere SOC 1- und SOC 2-Prüfprotokolle, unser C5-Prüfprotokoll (verfügbar auf Englisch und Deutsch), eine Zuordnung unserer internen Praktiken und Empfehlungen für Kunden, die die HIPAA/HITECH-Anforderungen an Sicherheit, Datenschutz und Benachrichtigungen über Sicherheitsverletzungen erfüllen möchten, sowie die zusammengefassten Ergebnisse der aktuellen Anwendungspenetrationstests. Unsere Allgemeinen Geschäftsbedingungen, die Nutzungsbedingungen und ein standardmäßiger Unternehmensvertrag stehen Ihnen online zur Verfügung, um sicherzustellen, dass Dropbox Business oder Dropbox Education eine gute Lösung für Ihr Team ist.

Konfiguration von Freigaberechten Ansichtsberechtigungen

Bei Dropbox Business und Dropbox Education können Sie Ihr Konto je nach Ihren Anforderungen an Sicherheit, Zusammenarbeit und Datenschutz flexibel konfigurieren. Administratoren können die entsprechenden Einstellungen über die Verwaltungskonsole überprüfen und ändern, um sie an die jeweilige Freigabe- oder Regulierungsumgebung anzupassen. Die Konten können beispielsweise so konfiguriert werden, dass keine Freigabe von Ordnern, Links und Paper-Dokumenten für Personen außerhalb des Teams möglich ist. Wenn Teammitglieder freigegebene Ordner für Dropbox-Dateien erstellen, können sie die Ordnereinstellungen weiter anpassen und die Zugriffsberechtigungen verwalten (Bearbeitungs- oder reiner Lesezugriff).

Starke Authentifizierung

Verfahren für eine starke Authentifizierung sorgen für die Sicherheit Ihrer Teamdaten. Administratoren sollten die verfügbaren Authentifizierungseinstellungen überprüfen und gemäß ihren jeweiligen Sicherheitsanforderungen aktivieren. Bei Dropbox Business- und Dropbox Education-Konten stehen folgende Optionen zur Verfügung:

Zweistufige Überprüfung

Team-Administratoren können die Teammitglieder bei der Kontoanmeldung zur zweistufigen Überprüfung verpflichten. Dieses sehr empfehlenswerte Sicherheitselement 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 oder eines Sicherheitsschlüssels, wenn ein Nutzer sich bei Dropbox anmeldet oder eine Verknüpfung mit einem neuen Computer, Smartphone oder Tablet herstellt.

Einmaliges Anmelden (SSO)

Wenn Ihr Unternehmen seine Kennwortrichtlinien und die Authentifizierung bereits über einen zentralen Identitätsanbieter verwaltet, empfiehlt sich die Einrichtung einer Option zum einmaligen Anmelden (Single Sign-on, SSO) für Ihr Dropbox Business- oder Dropbox Education-Team. Wenn Sie dazu Ihren bestehenden SSO-Anbieter nutzen, müssen sich die Teammitglieder kein zusätzliches Kennwort merken. Außerdem gelten in diesem Fall für den Zugriff auf Dropbox dieselben Kennwortrichtlinien wie für andere Services in Ihrem Unternehmen.

Regelmäßige Zugriffsüberprüfungen

Der Zugriff auf Ihr Teamkonto muss immer wieder angepasst werden, wenn sich die Teamzugehörigkeit, interne Rollen oder Geräte der Nutzer ändern. Überprüfen Sie den Zugriff daher häufig, damit nur berechtigte Nutzer, Geräte und Apps Zugang zu Ihrem Konto haben und Ihre Informationen nicht in falsche Hände gelangen. Über die Verwaltungskonsole können Sie die Zugriffsberechtigungen ganz einfach bearbeiten oder entfernen.

Teammitglieder

Über die Verwaltungskonsole können Teammitglieder unkompliziert hinzugefügt, entfernt und überprüft werden. Überprüfen Sie diese Liste häufig, um sicherzugehen, dass nur berechtigte Nutzer Zugriff auf vertrauliche Daten in Ihrem Dropbox Business- oder Dropbox Education-Konto haben. Wenn Personen aus Ihrem Unternehmen ausscheiden oder durch eine Veränderung ihrer Rolle keinen Zugriff mehr benötigen, können Sie diesen Nutzern die Zugriffsberechtigung entziehen. Außerdem können Sie die Rollen der einzelnen Teammitglieder über die Verwaltungskonsole anpassen, um jedem Nutzerkonto den passenden Zugriff zu gewähren.

Geräte

Sie und Ihre Teammitglieder sollten häufig überprüfen, welche Geräte mit Ihrem Konto verknüpft sind, und nicht mehr genutzte oder nicht autorisierte Geräte entfernen. Sowohl die Teammitglieder selbst als auch die Team-Administratoren können die Verknüpfung von Geräten aufheben. Sie und Ihre Teammitglieder haben auch die Option, Dropbox-Inhalte beim Aufheben der Verknüpfung remote von Ihrem Gerät zu löschen. Durch das Aufheben der Verknüpfung und das Löschen der Daten von den Geräten bleiben Ihre Daten geschützt, wenn ein Gerät verloren geht oder gestohlen wird oder ein Mitglied das Team verlässt.

Apps von Drittanbietern

Es stehen zahlreiche Drittanbieter-Apps zur Verfügung, die Sie mit Ihrem Dropbox Business- oder Dropbox Education-Konto verknüpfen können, um dessen Funktionsumfang zu erweitern. Integrationsmöglichkeiten für Dienste wie SIEM, DLP oder Identitätsmanagement können die Sicherheit Ihrer bisherigen Verfahren erhöhen. Doch auch wenn diese Apps und Integrationsmöglichkeiten eine hilfreiche Ergänzung für Ihr Konto sind, sollten Sie stets bedenken, dass es sich dabei nicht um Angebote von Dropbox handelt. Für sie gelten die Geschäftsbedingungen und der Unternehmensvertrag von Dropbox nicht. Auch mögliche Partnervereinbarungen oder Vereinbarungen zur Datenverarbeitung, die Sie mit Dropbox getroffen haben, greifen hier nicht. Je nach Serviceangebot werden Sie von den Apps möglicherweise aufgefordert, ihnen in einem bestimmten Umfang Zugriff auf Ihre Informationen zu gewähren. Als Administrator können Sie Team-Apps, die sich auf Ihr gesamtes Konto beziehen, verknüpfen oder entfernen. Das Gleiche gilt für persönliche Apps, die Teammitglieder ihrem eigenen Konto hinzugefügt haben. Apps von Drittanbietern und deren Zugriffsberechtigungen können über die Verwaltungskonsole überprüft und geändert werden.

Überwachung im Hinblick auf ungewöhnliche Aktivitäten

Als Team-Administrator können Sie Berichte anzeigen und exportieren, aus denen die Dateiereignisse, Freigaben, Authentifizierungen und Administratorenaktivitäten Ihres Teams hervorgehen. Als Beitrag zur Sicherheit ihres Teams sollten Administratoren diese Aktivitätsberichte regelmäßig überprüfen und dabei auf ungewöhnliche Aktivitäten achten. Unter Umständen empfiehlt sich zur Funktionserweiterung die Integration einer SIEM- oder anderweitigen Überwachungslösung von einem Drittanbieter.

Ermittlung des Bedarfs an Verschlüsselung

Dropbox speichert standardmäßig eine lokale Kopie Ihrer Dateien auf Ihrem Computer, damit Sie die benötigten Dateien jederzeit zur Hand haben. Diese lokalen Kopien Ihrer Dateien sind genauso geschützt wie alle anderen Dateien auf Ihrem Computer. Um sie optimal zu schützen, empfehlen wir Ihnen, wenn immer möglich die Dateiverschlüsselung auf Ihren Geräten zu aktivieren und ein starkes, einzigartiges Kennwort für Ihren Laptop, Ihr Telefon, Tablet oder ein anderes Gerät einzurichten, das den Zugriff auf Ihr Dropbox-Konto ermöglicht. Ein starkes und einzigartiges Kennwort auf Ihren Geräten sichert außerdem den Zugriff auf Ihre Paper-Dokumente.

Dropbox schützt Dateien, die Sie in Ihr Konto hochladen, indem es diese Dateien in separate Blöcke unterteilt und jeden dieser Blöcke mit 256-Bit-AES-Verschlüsselung (Advanced Encryption Standard) verschlüsselt. Dropbox sichert Paper-Dokumente auf ähnliche Weise, indem sie bei der dauerhaften Speicherung im Ruhezustand mit 256-Bit-AES-Verschlüsselung (Advanced Encryption Standard) verschlüsselt werden. Die Verschlüsselungsschlüssel werden von Dropbox im Auftrag der Kunden verwaltet, um diesen Vorgang für die Nutzer zu vereinfachen und bestimmte Funktionen zu ermöglichen.

Nutzer von Dropbox Business und Dropbox Education können Dateien vor dem Dropbox-Upload selbst oder mithilfe einer integrierten Drittanbieterlösung verschlüsseln. In diesem Fall sind die Nutzer selbst für die Verwaltung der entsprechenden Verschlüsselungsschlüssel verantwortlich. Unter Umständen wird durch eine Dateiverschlüsselung vor dem Upload der Funktionsumfang bestimmter Elemente eingeschränkt.

Wenn Sie als Kunde mehr über die Sicherheitsansätze von Dropbox erfahren möchten, lesen Sie das Sicherheits-Whitepaper oder sehen Sie auf unserer Website nach: dropbox.com/business/trust. Wenn Sie weitere Informationen über Dropbox Business oder Dropbox Education wünschen oder im Rahmen einer Vertraulichkeitsvereinbarung externe Prüfberichte anfordern möchten, wenden Sie sich an sales@dropbox.com.