Dropbox Business

Gedeelde verantwoordelijkheid: samenwerken om je gegevens veilig te houden

Dropbox werkt samen met zijn Business- en Dropbox Education-klanten om hun gegevens veilig te houden. We nemen uitvoerige maatregelen om onze infrastructuur, ons netwerk en onze toepassingen te beschermen; werknemers te trainen op het gebied van beveiligings- en privacymethoden; een cultuur op te zetten waar betrouwbaar zijn de hoogste prioriteit heeft; en onze systemen en methoden op rigoureuze wijze te laten testen en controleren door derden.

Hoewel Dropbox verantwoordelijk is voor het beveiligen van elk aspect van de service die wordt beheerd, spelen klanten een belangrijke rol om ervoor te zorgen dat hun teams en gegevens beschermd en veilig zijn. Als beheerder van een Dropbox Business- of Dropbox Education-team kun je je account configureren, gebruiken en controleren op manieren die voldoen aan de privacy- en nalevingsbehoeften van je bedrijf.

We hebben deze handleiding opgesteld om uit te leggen wat Dropbox doet om je account veilig te houden, en wat jij kunt doen om zicht op, en controle over, de gegevens van je team te houden.

De verantwoordelijkheden van Dropbox

Beveiliging inbouwen in je architectuur

Duizenden bedrijven over de hele wereld vertrouwen op ons om hun belangrijkste werk te beschermen. We krijgen dat vertrouwen omdat we heel hard werken aan het ontwikkelen van veilige en betrouwbare producten voor beheerders zoals jij. Hier vind je enkele manieren waarop we onze architectuur en netwerken beveiligen.

Gedistribueerde architectuur

De architectuur van Dropbox distribueert verschillende informatieniveaus over verschillende services. Dit maakt synchroniseren niet alleen sneller en betrouwbaarder, het vergroot ook de veiligheid. Vanwege de manier waarop de Dropbox-architectuur is opgezet, kan de toegang tot een afzonderlijke service niet worden gebruikt om bestanden of Paper-documenten te reconstrueren.

Veilige netwerken

Er wordt een strikte scheiding gehandhaafd tussen het interne Dropbox-netwerk en internet. Er wordt zorgvuldig toegezien op het internetverkeer van en naar het productienetwerk via een speciaal daarvoor ingerichte proxy-service, die op zijn beurt weer wordt beschermd door restrictieve firewall-regels. De productieomgeving is uitsluitend toegankelijk voor geautoriseerde IP-adressen en meervoudige authenticatie is vereist op alle eindpunten.

Gegevens van gebruikers versleutelen

Business- en Education-klanten van Dropbox werken met onze systemen via onze mobiele, desktop- en webtoepassingen, maar ook via API's. Ongeacht welke app je gebruikt, wij beschermen je bestanden en de gegevens van Paper-documenten zowel tijdens verzending als in rust.

Gegevens tijdens verzending

Voor de bescherming van gegevens tijdens verzending tussen Dropbox-apps en onze servers, gebruikt Dropbox SSL/TLS (Secure Sockets Layer / Transport Layer Security). Hiermee wordt een veilige tunnel tot stand gebracht die wordt beschermd door 128-bits AES-versleuteling (Advanced Encryption Standard) of hoger. Bestandsgegevens tijdens verzending tussen een Dropbox-client (momenteel desktop, mobiel, API of web) en de gehoste service worden versleuteld via SSL/TLS. Op dezelfde manier worden gegevens van Paper-documenten op

doorvoer tussen een Paper-client (mobiel, API of web) en de gehoste services versleuteld via SSL/TLS. Voor de eindpunten die we beheren (desktop en mobiel) en moderne browsers, gebruiken we een sterke coderingsmethode en ondersteunen we Perfect Forward Secrecy en certificate pinning. Bovendien markeren we op internet alle authenticatiecookies als veilig en activeren we HTTP Strict Transport Security (HSTS) met includeSubDomains ingeschakeld.

Om zogenaamde man-in-the-middle-aanvallen te voorkomen, wordt de authenticatie van front-endservers van Dropbox uitgevoerd via openbare certificaten die door de client worden beheerd. Er wordt een versleutelde verbinding tot stand gebracht vóór de verzending van bestanden of Paper-documenten, zodat ze gegarandeerd veilig worden afgeleverd bij de front-endservers van Dropbox.

Gegevens in rust

Dropbox-bestanden in rust worden versleuteld met 256-bits AES-versleuteling (Advanced Encryption Standard). Bestanden worden in meerdere datacenters opgeslagen in afzonderlijke bestandsblokken. Elk blok wordt gefragmenteerd en versleuteld met een sterke coderingsmethode. Alleen blokken die tussen twee revisies in zijn aangepast, worden gesynchroniseerd. Paper-documenten in rust worden ook versleuteld met de 256-bits Advanced Encryption Standard (AES). Paper-documenten worden opgeslagen in meerdere beschikbaarheidszones met behulp van systemen van derden.

Een betrouwbare service behouden

Elk opslagsysteem is zo goed als de betrouwbaarheid ervan. Daarom hebben we Dropbox ontwikkeld met verschillende redundantielagen om gegevensverlies te voorkomen en de beschikbaarheid te waarborgen. Redundante exemplaren van metagegevens worden verspreid over onafhankelijke apparaten in een datacenter volgens ten minste één N+2-beschikbaarheidsmodel. Er worden elk uur incrementele back-ups van metagegevens uitgevoerd, en om de drie dagen volledige back-ups. Metagegevens worden opgeslagen op servers die worden gehost en beheerd door Dropbox. Voor de opslag van bestandsblokken gebruikt Dropbox zowel interne als externe systemen die zijn ontworpen om jaarlijkse duurzaamheid van gegevens van ten minste 99,999999999% te bieden.

Ook als de service niet online is, wat zelden gebeurt, hebben Dropbox-gebruikers toegang tot de laatste gesynchroniseerde exemplaren van hun bestanden in de lokale Dropbox-map op gekoppelde computers. Kopieën van bestanden die zijn gesynchroniseerd met de Dropbox-desktopclient/lokale map zijn beschikbaar op de harde schijf van de gebruiker tijdens uitvaltijd, storingen of als ze offline zijn.

Redundante exemplaren van gegevens van Paper-documenten worden verspreid over onafhankelijke apparaten in een datacenter volgens een N+1-beschikbaarheidsmodel. Bovendien wordt dagelijks een volledige back-up gemaakt van de gegevens van Paper-documenten. Voor de opslag van Paper-documenten gebruikt Dropbox externe systemen die zijn ontworpen om jaarlijkse duurzaamheid van gegevens van ten minste 99,999999999% te bieden. Mocht een service uitvallen, hebben gebruikers nog gewoon toegang tot de laatste gesynchroniseerde exemplaren van hun Paper-documenten in de offlinemodus in de mobiele toepassing.

Toegang van medewerkers tot backend-systemen beperken

We weten dat wanneer jij als Dropbox Business- of Dropbox Education-klant je bestanden en Paper-documenten opslaat op Dropbox, je van ons verwacht dat wij je gegevens op een verantwoordelijke manier bewaren. Als onderdeel van deze verantwoordelijkheid zorgen wij ervoor dat toegang door Dropbox-medewerkers tot onze interne systemen streng wordt beheerd. Om te beginnen, is de toegang tot onze ondernemings- en productienetwerken sterk beperkt. De toegang tot het productienetwerk vindt bijvoorbeeld plaats op basis van een SSH-sleutel en wordt beperkt tot engineeringteams die uit hoofde van hun functie toegang moeten hebben. De firewallconfiguratie is aan strenge regels onderworpen en beperkt tot een klein aantal beheerders. Toegang tot andere bedrijfsmiddelen, waaronder datacenters, serverconfiguratietools, productieservers en ontwikkelingstools voor broncode, wordt toegekend na expliciete goedkeuring door het relevante management. Een dossier met het toegangsverzoek, de onderbouwing en de goedkeuring wordt door het management bijgehouden, en de toegang wordt verleend door hiervoor bevoegde mensen.

Medewerkers bewust laten blijven van beveiliging en privacy

Onderdeel van het veilig houden van onze service is ervoor zorgen dat mensen die bij Dropbox werken, begrijpen hoe ze zich bewust kunnen zijn van veiligheid en hoe ze verdachte activiteiten kunnen herkennen. Om dat te bereiken, moeten medewerkers van Dropbox vertrouwd zijn met het veiligheidsbeleid voordat ze toegang tot de systemen krijgen. Medewerkers moeten ook verplicht deelnemen aan een beveiligings- en privacytraining voor nieuwe medewerkers en jaarlijkse vervolgtrainingen. Ook krijgen ze regelmatig training op het gebied van beveiligingsbewustzijn via informatieve e-mails, gesprekken, presentaties en bronnen die beschikbaar zijn op ons intranet.

Onze methoden valideren

We maken gebruik van derden om de effectiviteit van onze beveiligingsmethoden te beoordelen en ons zo te helpen garanderen dat deze beveiligingsmethoden werken zoals bedoeld. Specialisten voeren periodieke penetratie- en kwetsbaarheidstesten uit op de ondernemings- en productieomgevingen van Dropbox. Problemen die worden geïdentificeerd, krijgen prioriteit en worden door onze beveiligingstechnici opgelost. Daarnaast beoordelen externe, onafhankelijke controleurs onze beveiligingspraktijken ten opzichte van internationale en industrienormen. Voor meer informatie over de methoden van Dropbox en om deze te beoordelen, kun je ons SOC 3-rapport en onze ISO 27001-, ISO 27017-, ISO 27018- en ISO 22301-certificaten online bekijken. Je kunt ook ons SOC 2-rapport, een toewijzings- en beoordelingsrapport voor HIPAA-eisen, een BSI C5-beoordeling en -rapport (beschikbaar in het Engels en Duits) en samenvattingen van penetratietestresultaten opvragen onder een geheimhoudingsovereenkomst (NDA).

Problemen aan jou communiceren

Status van de service

Dropbox maakt een externe site beschikbaar waarop de status van onze service voor Dropbox Business- en Dropbox Education-klanten wordt gecommuniceerd. Als huidige klant kun je op elk moment naar status.dropbox.com gaan om de huidige status van de site te bekijken, en eerdere storingen en onderhoudsactiviteiten te controleren.

Melding van inbreuk

Dropbox zal je bij inbreuk op gegevens hiervan op de hoogte stellen, zoals vereist door de wet. Wij hanteren beleidsrichtlijnen en procedures voor incidentrespons, waaronder een proces voor het melden van inbreuk, dat ons in staat stelt de betrokken klanten waar nodig op de hoogte te stellen. Als je een HIPAA-zakenpartnerovereenkomst of een gegevensverwerkingsovereenkomst van de EU bent aangegaan, word je op de hoogte gesteld zoals wordt beschreven in die overeenkomsten.

Tools die je nodig hebt om veilig te werken

We willen dat jij en andere Dropbox Business- en Dropbox Education-beheerders beschikken over de tools om verantwoorde, geïnformeerde beslissingen te nemen over de beveiliging van je team. Om je te helpen je account te configureren, gebruiken en controleren op een manier die voldoet aan jouw behoeften, is je beheerconsole voorzien van beveiligingsfuncties waarmee je namens je team kunt handelen. Met handleidingen als deze, onze whitepaper over beveiliging van Dropbox Business, het helpcentrum en ons supportteam, geven we je inzicht in hoe je met deze instellingen je account op een verantwoorde manier kunt configureren.

Verantwoordelijkheden van de klant

Meer informatie over onze praktijken

Bepalen of Dropbox Business of Dropbox Education het beste past bij de behoeften van jouw bedrijf is een belangrijk proces. We moedigen je aan de tijd te nemen om onze procedures te beoordelen, net zoals je met elke andere toepassing zou doen. Om je de tools te geven die je nodig hebt om onze beveiligingspraktijken te controleren, zijn onze ISO 27001-, ISO 27017-, ISO 27018- en ISO 22301-certificaten; ons SOC 3-garantierapport en onze CSA STAR Level 1 Self-Assessment en Level 2 Certification online beschikbaar. We kunnen ook toegang geven tot extra documentatie onder een geheimhoudingsovereenkomst, om je te helpen een weloverwogen besluit te nemen. Dit zijn onder andere onze SOC 1- en SOC 2-beoordelingsrapporten, ons C5-beoordelingsrapport (beschikbaar in het Engels en Duits) en een overzicht van onze interne praktijken en aanbevelingen voor klanten die willen voldoen aan de eisen van de beveiligings- en privacyregels en de regels omtrent melding van inbreuk van HIPAA/HITECH, maar ook samenvattingen van onze laatste toepassingspenetratietesten. Onze Servicevoorwaarden, gebruiksregels en Standaardbedrijfsovereenkomst zijn online beschikbaar, zodat je ze kunt lezen en je ervan kunt verzekeren dat Dropbox Business of Dropbox Education goed past bij je team.

De configuratie van delen en machtigingen voor weergave

Met Dropbox Business en Dropbox Education heb je de flexibiliteit om je account zo te configureren dat het voldoet aan je vereisten voor beveiliging, samenwerking en privacy. Beheerders kunnen deze instellingen controleren en aanpassen via de beheerconsole om ze af te stemmen op de omgevingsvereisten voor delen en naleving. Accounts kunnen bijvoorbeeld worden geconfigureerd zodat mappen, links en Paper-documenten niet kunnen worden gedeeld met mensen buiten je team. Als teamleden gedeelde mappen voor Dropbox-bestanden maken, kunnen ze de instellingen van de mappen verder aanpassen en het passende toegangsniveau kiezen: bewerken of alleen-lezen.

Authenticatie versterken

Strenge authenticatiemethoden helpen bij het veilig houden van de gegevens van je team. Beheerders moeten de beschikbare authenticatie-instellingen controleren en de instellingen inschakelen waarmee hun accounts het beste worden beveiligd. Dropbox Business- en Dropbox Education-accounts bevatten de volgende opties:

Tweestapsverificatie

Teambeheerders kunnen vereisen dat leden gebruikmaken van tweestapsverificatie om zich aan te melden bij hun accounts. Deze sterk aanbevolen beveiligingsfunctie voegt een extra beschermingslaag toe aan de Dropbox-accounts van gebruikers. Nadat deze functie is ingeschakeld, vraagt Dropbox naast een wachtwoord om een zescijferige beveiligingscode of beveiligingssleutel bij het aanmelden of bij het koppelen met een nieuwe computer, telefoon of tablet.

Eenmalige aanmelding (SSO)

Als je bedrijf wachtwoordbeleidsregels en authenticatie al beheert met een centrale identiteitsprovider, is het wellicht verstandig om eenmalige aanmelding in te stellen voor je Dropbox Business- of Dropbox Education-team. Door gebruik te maken van je bestaande SSO-provider, hoeven je teamleden niet nóg een wachtwoord te onthouden. En wat nog belangrijker is: de authenticatie van toegang tot Dropbox wordt beheerd met dezelfde wachtwoordbeleidsregels als voor andere services in je bedrijf.

Regelmatige toegangscontroles uitvoeren

De toegang tot het account van je team ontwikkelt zich naarmate de teamleden, interne rollen en apparaten veranderen. Daarom moet je regelmatig controleren of alleen de juiste mensen, apparaten en apps toegang hebben tot je account om zo je informatie in de juiste handen te houden. Via de beheerconsole kun je de toegang eenvoudig aanpassen of verwijderen.

Teamleden

Je kunt teamleden eenvoudig toevoegen, verwijderen en weergeven via de beheerconsole. Om te garanderen dat alleen de juiste mensen toegang hebben tot gevoelige gegevens in je Dropbox Business- of Dropbox Education-account, raden we je aan deze lijst regelmatig te controleren. Je kunt vervolgens toegang verwijderen als iemand je organisatie verlaat of geen toegang meer nodig heeft. Je kunt ook de rollen van teamleden in de beheerconsole aanpassen, zodat elk gebruikersaccount het juiste toegangsniveau heeft.

Apparaten

Jij en je teamleden moeten apparaten die aan je account zijn gekoppeld, regelmatig controleren en ongebruikte of niet-geautoriseerde apparaten verwijderen. Apparaten kunnen worden losgekoppeld door teamleden en teambeheerders. Tijdens het loskoppelen van het apparaat kunnen jij en je teamleden ook het Dropbox-materiaal op afstand verwijderen. Het loskoppelen en opschonen van je apparaten kan je gegevens veilig houden bij verlies of diefstal, of als iemand het team verlaat.

Apps van derden

Er is een sterk ecosysteem van apps van derden die je kunt koppelen aan je Dropbox Business- of Dropbox Education-account voor extra functionaliteit. Integraties die services zoals SIEM, DLP en identiteitsbeheer leveren, kunnen krachtige tools zijn bij het versterken van je bestaande beveiligingsmethoden. Hoewel deze apps van derden en integraties geweldige aanvullingen kunnen zijn op je account, is het belangrijk te onthouden dat ze geen deel uitmaken van onze inbegrepen diensten. Ze vallen daarom niet onder de Gebruiksvoorwaarden of Bedrijfsovereenkomst van Dropbox, waaronder een Zakenpartnerovereenkomst of Gegevensverwerkingsovereenkomst, die je eventueel hebt ondertekend met Dropbox. Afhankelijk van hun serviceaanbod kunnen apps je om verschillende niveaus van toegang tot je informatie vragen. Als beheerder kun je teamapps—die van toepassing zijn op je gehele account—koppelen of verwijderen en afzonderlijke apps verwijderen die teamleden eventueel hebben toegevoegd aan hun eigen account. Apps van derden en toegang kun je controleren en aanpassen via de beheerconsole.

Ongebruikelijke activiteiten in de gaten houden

Als teambeheerder kun je rapporten bekijken en exporteren waarin gedetailleerde informatie wordt gegeven over bestandsgebeurtenissen en activiteiten van jouw team op het gebied van delen, authenticatie en beheer. Beheerders moeten deze activiteitenrapporten regelmatig bekijken om een oogje in het zeil te houden wat betreft ongebruikelijke activiteit en te helpen je team veilig te houden. Je kunt je mogelijkheden ook uitbreiden met een SIEM-oplossing van derden of een andere controle-integratie.

Versleutelingsbehoeften vaststellen

Dropbox slaat standaard een lokale kopie van je bestanden op je computer op om ervoor te zorgen dat je de bestanden die je nodig hebt meteen bij de hand hebt. De lokale kopieën van je bestanden zijn net zo goed beveiligd als alle andere bestanden op je computer. Om ze veilig te houden, raden we je aan schijfversleuteling in te schakelen op je apparaten als dat mogelijk is, en een sterk en uniek wachtwoord te gebruiken voor toegang tot je laptop, telefoon, tablets of enig ander apparaat dat toegang biedt tot je Dropbox-account. Met een sterk en uniek wachtwoord op je apparaten wordt bovendien de toegang tot je Paper-documenten beveiligd.

Dropbox beschermt bestanden die je uploadt naar je account door die bestanden automatisch op te splitsen in aparte blokken en elk blok te versleutelen door middel van 256-bits AES-versleuteling (Advanced Encryption Standard). Op dezelfde manier beschermt Dropbox Paper-documenten door deze in rust te versleutelen in permanente opslag door middel van 256-bits AES-versleuteling. Dropbox beheert de versleutelingscodes namens onze klanten om dit proces eenvoudig te houden voor gebruikers en om bepaalde functies mogelijk te maken.

Dropbox Business- en Dropbox Education-leden kunnen ervoor kiezen om bestanden ook zelf of via een integratie van derden te versleutelen voordat ze worden geüpload naar Dropbox. Gebruikers die gegevens versleutelen voordat deze worden geüpload naar Dropbox, zijn echter zelf verantwoordelijk voor het beheren van die versleutelingscodes. Mogelijk werken sommige functies niet optimaal als bestanden eerst worden versleuteld voordat ze worden geüpload naar Dropbox.

Klanten die graag meer willen weten over de beveiligingsaanpak van Dropbox, kunnen het beste de whitepaper over beveiliging lezen of onze website doornemen: dropbox.com/business/trust. Voor meer informatie over Dropbox Business of Dropbox Education en om auditrapporten van derden onder een geheimhoudingsovereenkomst aan te vragen, kun je contact opnemen met sales@dropbox.com.