Dropbox Business

Delat ansvar: Arbeta tillsammans för att hålla era data säkra

Dropbox arbetar med sina Business- och Dropbox Education-kunder för att hålla deras data säkert. Vi vidtar omfattande åtgärder för att skydda vår infrastruktur, vårt nätverk och våra program. Vi åstadkommer detta genom att utbilda de anställda i rutiner för säkerhet och sekretess, skapa en företagskultur där högsta prioritet är att förtjäna kundernas förtroende samt genom att låta våra system och rutiner genomgå rigorösa tester och granskningar av tredje part.

Dropbox ansvarar för att trygga varje del av tjänsten vi har har kontroll över, men kunderna har en viktig roll vad gäller att säkerställa att deras team och data skyddas och är säkra. Som administratör för Dropbox Business- eller Education-teamen har du möjlighet att konfigurera, använda och övervaka ditt konto på sätt som uppfyller din organisations behov av säkerhet, sekretess och efterlevnad.

Vi har sammanställt den här vägledningen för att informera dig om vad Dropbox gör i syfte att skydda ditt konto, och vad du kan göra för att bibehålla synligheten och kontrollen över ditt teams data.

Dropbox ansvar

Bygga en säker arkitektur

Tusentals företag över hela världen har gett oss förtroendet att skydda deras viktigaste arbete. För att förtjäna det förtroendet arbetar vi hårt med att skapa säkra produkter som administratörer som du kan lita på. Här följer några av sätten som vi skyddar vår arkitektur och våra nätverk på.

Distribuerad arkitektur

Dropbox-arkitekturen distribuerar olika nivåer av information för olika tjänster. Det innebär inte bara snabbare och tillförlitligare synkronisering, utan ökar även säkerheten. Dropbox arkitektur är uppbyggd på ett sätt som gör att åtkomst till en enskild tjänst inte kan användas för att återskapa filer eller Paper-dokument.

Säkra nätverk

Strikt begränsning upprätthålls mellan det interna Dropbox-nätverket och det offentliga internet. Internetbunden trafik till och från produktionsnätverket kontrolleras noggrant genom en dedikerad proxytjänst. Dessa skyddas i sin tur av restriktiva brandväggsregler. Åtkomst till produktionsmiljöer är begränsad till enbart auktoriserade IP-adresser och kräver flerfaktorsverifiering i alla slutpunkter.

Kryptera användardata

Dropbox Business- och Education-kunder interagerar med våra system genom våra mobilappar, dator- och webbprogram samt API:er. Oavsett vilket program du använder skyddar vi dina filer och Paper doc:s, både när de överförs och när de inte används.

Överföring av data

Dropbox använder Secure Sockets Layer (SSL)/Transport Layer Security (TLS) vid överföring av data för att skydda data som skickas mellan Dropbox-appar och våra servrar. Detta skapar en säker tunnel som skyddas av Advanced Encryption Standard-kryptering (AES) om 128 bitar eller högre. Fildata som skickas mellan en Dropbox-klient (för närvarande dator, mobil, API eller webb)

och värdtjänsten är krypterade via SSL/TLS. På liknande vis krypteras Paper-dokumentdata som skickas mellan en Paper-klient (för närvarande dator, mobil, API eller webb) och värdtjänsten alltid via SSL/TLS. För slutpunkter som vi kontrollerar (klient och mobil) samt moderna webbläsare använder vi starka chiffer och stödjer perfect forward secrecy och certificate pinning. Vi flaggar dessutom alla autentiseringscookies på webben som säkra och aktiverar HTTP Strict Transport Security (HSTS) med includeSubDomains aktiverat.

För att förhindra mellanhandsattacker verifieras Dropbox front-end-servrar via publika certifikat hos klienten. Innan några filer eller Paper-dokument förs över förhandlas en krypterad anslutning, vilket säkerställer en säker leverans till Dropbox front-end-servrar.

Vilande data

Dropbox-filer i vila krypteras med Advanced Encryption Standard (AES) om 256 bitar. Filer lagras i flera datacenter i diskreta filblock. Varje block är fragmenterat och krypterat med ett starkt chiffer. Endast block som modifierats mellan revideringar synkas. Paper-dokument i vila krypteras också med 256-bitars Advanced Encryption Standard (AES). Paper-dokument lagras över flera tillgänglighetszoner med tredjepartssystem.

Upprätthålla en tillförlitlig tjänst

Ett lagringssystem är aldrig bättre än dess tillförlitlighet. Därför har vi gett Dropbox flera redundanta lager som skyddar mot dataförluster och säkerställer tillgänglighet. Överblivna metadatakopior fördelas över oberoende enheter inom ett datacenter i en N+2-tillgänglighetsmodell (som minimum). Inkrementella säkerhetskopieringar utförs varje timme, och fullständiga säkerhetskopieringar utförs var tredje dag. Metadata lagras på servrar som Dropbox är värd för och hanterar. Dropbox använder både interna lagringssystem och lagringssystem från tredje part för lagring av filblock. Dessa har utformats för att ge en årlig datahållbarhet på minst 99,999999999 %.

I de sällsynta fall då en tjänst inte är tillgänglig kan Dropbox-användare fortfarande komma åt de senaste synkade kopiorna av filerna i den lokala Dropbox-mappen på kopplade datorer. Kopior av filer som synkroniserats i Dropbox-skrivbordsklienten/lokala mappen kan nås från din hårddisk under driftstörningar, strömavbrott eller när datorn är offline.

På liknande vis så fördelas redundanta kopior av Paper-doc:s över oberoende enheter inom ett datacenter i en N+1-tillgänglighetsmodell, och vi har konfigurerat dagliga fullständiga säkerhetskopieringar av Paper-doc:sdata. För lagring av Paper-doc:s använder sig Dropbox av tredje-partssystem som har utformats för att ge en årlig datahållbarhet på minst 99,999999999 %. I de sällsynta fall en tjänst inte är tillgänglig har Dropbox-användare fortfarande åtkomst till de senaste synkade kopiorna av sina Paper-dokument via ”offline”-läget i mobilapplikationen.

Begränsa personalens åtkomst till backend-system

Vi vet att när du lagrar dina filer med Dropbox som Business- eller Education-kund, förväntar du dig att vi skyddar dina data på ett ansvarsfullt sätt. Som en del av det ansvaret ser vi till att Dropbox-anställdas åtkomst till våra interna system är fullständigt kontrollerad. Till att börja med är åtkomsten mellan våra företags- och produktionsnätverk strängt begränsad. Åtkomsten till produktionsnätverk är exempelvis baserad på SSH-nycklar och är begränsad till ingenjörsteam som måste ha åtkomst för att kunna utföra sina arbetsuppgifter. Brandväggskonfiguration sker under rigorös kontroll och är begränsad till ett fåtal administratörer. Åtkomst till andra resurser, inklusive datacenter, funktioner för serverkonfiguration, produktionsservrar och funktioner för utveckling av källkod tilldelas genom uttryckligt godkännande från lämplig chef. En kopia av av åtkomstförfrågan, motivering och godkännande registreras av ledningen och åtkomsten beviljas av lämpliga personer.

Utbilda personalen i säkerhet och sekretess

En del av säkerhetsarbetet tjänsten består i att se till att personer som jobbar på Dropbox förstår vad det innebär att vara säkerhetsmedveten och känna igen misstänkt aktivitet. Av den anledningen måste Dropbox-anställda acceptera våra säkerhetspolicyer innan de beviljas systemåtkomst. De anställda deltar även i obligatoriska utbildningar i säkerhet och sekretess samt en årlig fortbildning. De får dessutom regelbunden utbildning i säkerhetsmedvetenhet via e-post och genom möten, presentationer och resurser på intranätet.

Validera våra rutiner

I syfte att säkerställa att våra säkerhetsrutiner fungerar som de ska använder vi tredjeparter för att utvärdera deras effektivitet. Specialister utför regelbundna penetrations- och sårbarhetstester på Dropbox företags- och produktionsmiljöer. Identifierade problem prioriteras och åtgärdas av vårt säkerhetstekniska team. Dessutom utvärderar tredjepartsgranskare våra säkerhetsrutiner mot internationella och branschmässiga standarder. För att du ska lära dig mer om Dropbox rutiner och utvärdera dem finns vår SOC 3-rapport och våra ISO 27001-, 27017-, 27018- och 22301-certifikat tillgängliga på nätet. Du kan också begära att få vår SOC 2-rapport, en utvärderingsrapport och en sammanställning av HIPAA-krav, en BSI C5-utvärdering och rapport (tillgänglig på engelska och tyska) samt en sammanfattning av resultaten från penetrationstester under ett sekretessavtal.

Informera dig om problem

Tjänstestatus

Dropbox tillgängliggör en webbplats från tredje part, varifrån statusen på vår tjänst meddelas till Dropbox Business- och Education-kunder. Som kund hos oss kan du besöka status.dropbox.com när du vill för att visa den aktuella webbplatsstatusen samt tidigare avbrott och underhållsperioder.

Meddelanden om uppgiftsbrott

Dropbox meddelar dig i händelse av uppgiftsbrott enligt gällande lagstiftning. Vi har förfaranden för incidenthantering, däribland rutiner för meddelande om uppgiftsbrott, vilket gör att vi kan informera berörda kunder. Om du har tecknat ett affärsavtal i enlighet med HIPAA eller ett avtal om databehandling i EU, meddelas du enligt bestämmelserna i de avtalen.

Ger dig de verktyg du behöver för att vara säker

Vi vill att du och andra Dropbox Business- och Education-administratörer ska ha de verktyg ni behöver för att fatta ansvarsfulla och välinformerade beslut gällande teamets säkerhet. För att hjälpa dig att konfigurera, använda och övervaka kontot på ett sätt som tillgodoser alla behov, är administratörskonsolen utrustad med säkerhetsfunktioner som du kan aktivera för teamet. Genom vägledningar som denna, Dropbox Business-vitboken över säkerhet, hjälpcentret och vårt supportteam får du information som hjälper dig förstå hur du kan använda dessa inställningar till att konfigurera kontot på ett ansvarsfullt sätt.

Kundens ansvar

Lär dig om våra rutiner

Att avgöra om Dropbox Business eller Education passar ditt företag är en viktig process. Vi rekommenderar att du tar dig tid att granska våra metoder på samma sätt som du gör med andra applikationer. Eftersom vi vill ge dig de verktyg du behöver för att kontrollera våra säkerhetsrutiner finns våra ISO 27001-, 27017-, 27018- och 22301-certifikat, vår SOC 3-styrkande rapport och vår CSA STAR Nivå 1-självutvärdering och Nivå 2-certifiering finns tillgängliga på nätet. Vi kan också erbjuda åtkomst till ytterligare dokumentation under ett sekretessavtal för att hjälpa dig att fatta ett välgrundat beslut. Detta inkluderar våra SOC 1- och SOC 2-granskningsrapporter, vår C5-granskningsrapport (tillgänglig på engelska och tyska), en kartläggning av våra interna rutiner, rekommendationer för kunder som vill uppfylla kraven på säkerhet och sekretess i HIPAA och HITECH samt kraven för databrottsmeddelanden och sammanfattningar av våra senaste tester av applikationspenetration. Våra tjänstevillkor, vår policy för godkänd användning och vårt standardavtal för företag finns tillgängliga på nätet om du vill granska och se om Dropbox Business, Enterprise eller Education passar ditt team.

Konfigurera delning och visningsåtkomst

Med Dropbox Business och Education kan du konfigurera ditt konto på sätt som uppfyller dina behov av säkerhet, samarbete och sekretess. Administratörer kan granska och ändra inställningarna via administratörskonsolen så att de passar deras miljö beträffande delning och regler. Till exempel kan konton konfigureras så att mappar, länkar och Paper doc:s inte kan delas med personer utanför ditt team. När gruppmedlemmar skapar delade mappar för Dropbox-filer kan de anpassa mapparnas inställningar ytterligare och välja lämplig åtkomst nivå – redigering eller skrivskydd.

Stärka autentisering

Starka rutiner för autentisering bidrar till att skydda ditt teams data. Administratörer bör granska autentiseringsinställningarna och aktivera dem som på bästa sätt skyddar kontona. Dropbox Business- och Education-konton omfattar följande alternativ:

Tvåstegsverifiering

Teamadministratörer kan kräva att teammedlemmarna använder tvåstegsverifiering för kontoinloggning. Denna starkt rekommenderade säkerhetsfunktion skapar ett extra skyddslager för en användares Dropbox-konto. När tvåstegsverifieringen har aktiverats måste användarna ange en sexsiffrig säkerhetskod eller ett lösenord när de loggar in eller ansluter till en ny dator, telefon eller surfplatta.

Samlad inloggning (SSO)

Om ditt företags lösenordsrutiner och autentisering redan hanteras av en central identitetsleverantör vill du kanske installera samlad inloggning för ditt Dropbox Business- eller Dropbox Education-team. Genom att använda din nuvarande leverantör av samlad inloggning behöver dina teammedlemmar inte komma ihåg ytterligare ett lösenord. Men framförallt hanteras autentiseringsåtkomsten till Dropbox med samma lösenordsrutiner som för andra tjänster inom ditt företag.

Utföra regelbundna granskningar av åtkomst

Åtkomst till ditt teams konto bör utvecklas i takt med att förändringar sker med avseende på teammedlemskap, interna roller och enheter. Du bör regelbundet kontrollera att endast rätt personer, enheter och appar har åtkomst till ditt konto för att information inte ska hamna i fel händer. Det är enkelt att ändra eller ta bort åtkomst via administratörskonsolen.

Teammedlemmar

Teammedlemmar kan enkelt läggas till, tas bort och granskas i administratörskonsolen. För att säkerställa att endast rätt personer har åtkomst till känsliga data i ditt Dropbox Business- eller Education-konto, rekommenderar vi att du granskar den här listan regelbundet. Du kan sedan ta bort åtkomsten när någon lämnar organisationen eller inte längre behöver ha åtkomst på grund av en förändrad arbetsroll. Du kan också ändra teammedlemmarnas roller i administratörskonsolen så att varje användarkonto har en lämplig åtkomstnivå.

Enheter

Du och dina teammedlemmar bör regelbundet granska enheter kopplade till ert konto och ta bort oanvända eller obehöriga enheter. Kopplingen till enheter kan tas bort av både teammedlemmar och teamadministratörer. Du och dina teammedlemmar har också möjlighet att fjärrensa Dropbox-innehåll från enheten när kopplingen tas bort. Att ta bort kopplingen till enheter eller rensa dem kan skydda data i händelse av förlust eller stöld, eller om någon lämnar ditt team.

Appar från tredje part

Det finns ett kraftfullt ekosystem av appar från tredje part som du kan koppla till ditt Dropbox Business- eller Dropbox Education-konto för att få fler funktioner. Integrationer med tjänster såsom SIEM, DLP och identitetshantering kan vara användbart för att stärka befintliga säkerhetsrutiner. Även om dessa appar och integrationer från tredje part kan vara bra ett komplement till ditt konto, är det viktigt att komma ihåg att de inte är en del av våra tjänster. Därför omfattas de inte av Dropbox användarvillkor eller affärsavtal, till exempel ett affärsavtal eller databehandlingsavtal som du kan ha undertecknat med Dropbox. Appar kan be dig om olika åtkomstnivåer till din information beroende på vilka tjänster som tillhandahålls genom dem. Som administratör kan du koppla eller ta bort teamappar, vilket gäller för hela kontot, och ta bort enskilda appar som en teammedlem kan ha lagt till i sitt eget konto. Appar från tredje part och åtkomst kan granskas och ändras i administratörskonsolen.

Övervaka ovanlig aktivitet

Som teamadministratör kan du granska och exportera rapporter med information om ditt teams filhändelser, delning, autentisering och administratörsaktiviteter. Administratörer bör regelbundet granska dessa aktivitetsrapporter för att hålla utkik efter ovanliga aktiviteter och skydda teamet. Du kanske också ska överväga att använda en SIEM från tredje part eller en annan typ av integrationsövervakning för att förbättra säkerheten.

Fastställa krypteringsbehov

Som standard lagrar Dropbox en lokal kopia av dina filer på datorn för att säkerställa att du alltid har de filer du behöver till hands. De lokala kopiorna av dina filer är lika skyddade som övriga filer på datorn. För att skydda dem rekommenderar vi att du aktiverar diskkryptering på dina enheter när det är möjligt. Det är också viktigt att du har ett starkt och unikt lösenord för att komma åt din bärbara dator, telefon, surfplatta eller andra enheter som ger åtkomst till ditt Dropbox-konto. Att använda ett starkt och unikt lösenord på dina enheter skyddar även tillgången till dina Paper docs.

Dropbox skyddar filer som du överför till ditt konto genom att automatiskt dela filerna i diskreta block och kryptera varje block med Advanced Encryption Standard (AES) om 256 bitar. Dropbox skyddar även Paper docs genom att kryptera dem i vila på beständig lagring genom användandet av 256-bit Advanced Encryption Standard (AES). Dropbox hanterar krypteringsnycklarna på uppdrag av våra kunder för att denna process ska vara enkel för användarna och för att tillhandahålla vissa funktioner.

Dropbox Business- och Education-medlemmar kan välja att även kryptera filerna innan de överför dem till Dropbox på egen hand eller genom en integration från tredje part. Men användare som krypterar data innan överföringen till Dropbox är ansvariga för hanteringen av dessa krypteringsnycklar. Att kryptera filer innan de överförs till Dropbox kan också minska funktionaliteten av vissa funktioner.

Kunder som är intresserade av att lära sig mer om hur Dropbox hanterar säkerhet kan läsa säkerhetsvitboken eller ta del av innehållet på vår hemsida: dropbox.com/business/trust. Om du vill veta mer om Dropbox Business- eller Education och begära granskningsrapporter från tredje part i enlighet med ett sekretessavtal kontaktar du sales@dropbox.com.