Dropbox Business

Fælles ansvar: Samarbejd om at holde dine data sikre

Dropbox samarbejder med sine Business- og Dropbox Education-kunder om at beskytte deres data. Vi har omfattende foranstaltninger til beskyttelse af vores infrastruktur, netværk og applikationer; vi træner medarbejdere i praksis inden for sikkerhed og beskyttelse af personlige oplysninger; vi opbygger en kultur, hvor det at være tillidsbetroet er den største prioritet; og vi lader vores systemer og praksis gennemgå streng afprøvning og overvågning af tredjeparter.

Selvom Dropbox er ansvarlig for at sikre hvert eneste aspekt af tjenesten, der er under vores kontrol, spiller kunderne en vigtig rolle i at sikre, at deres teams og data er beskyttede og sikre. Som administrator for et Dropbox Business- eller Dropbox Education-team kan du konfigurere, bruge og overvåge din konto på måder, der overholder din organisations behov for sikkerhed, beskyttelse af personlige oplysninger samt overholdelse af regler og standarder.

Vi har udarbejdet denne vejledning for at hjælpe dig med at forstå, hvad Dropbox gør for at holde din konto sikker, og hvad du kan gøre for at opretholde synlighed og kontrol over dit teams data.

Dropbox' ansvar

Indbygning af sikkerhed i vores arkitektur

Tusindvis af virksomheder i hele verden stoler på, at vi beskytter deres allervigtigste filer. For at gøre os fortjent til denne tillid arbejder vi hårdt på at skabe sikre produkter, som administratorer som dig kan stole på. Her er nogle af de måder, hvorpå vi sikrer vores arkitektur og netværk.

Distribueret arkitektur

Dropbox' arkitektur distribuerer forskellige niveauer af information på tværs af flere tjenester. Dette gør ikke kun synkronisering hurtigere og mere pålidelig, men det øger også sikkerheden. Dropbox' arkitektur betyder, at adgang til en individuel tjeneste ikke kan bruges til at genskabe filer eller Paper-dokumenter.

Sikre netværk

Der opretholdes en streng afgrænsning mellem det interne Dropbox-netværk og det offentlige internet. Internetrelateret trafik til og fra produktionsnetværket kontrolleres nøje gennem en særlig proxytjeneste, som endvidere beskyttes af restriktive firewall-regler. Adgang til produktionsmiljøet er begrænset til autoriserede IP-adresser og kræver multifaktorgodkendelse for alle slutpunkter.

Krypterede brugerdata

Dropbox Business- og Dropbox Education-kunder interagerer med vores systemer via vores mobil-, computer- og webapplikationer samt API'er. Uanset hvilken app du bruger, beskytter vi dine data i filer og Paper-dokumenter, både under overførsel og opbevaring.

Data under overførsel

Til beskyttelse af data under overførsel mellem Dropbox-apps og vores servere bruger Dropbox Secure Sockets Layer (SSL)/Transport Layer Security (TLS), der skaber en sikker kanal, som er beskyttet af 128-bit eller højere Advanced Encryption Standard-kryptering (AES). De fildata, der er under overførsel mellem en Dropbox-klient (i øjeblikket computer, mobil, API eller web)

og den hostede tjeneste, krypteres altid ved hjælp af SSL/TLS. På samme måde krypteres Paper-dokumentdata, som overføres mellem en Paper-klient (i øjeblikket mobil, API eller web) og værtstjenesterne, vha. SSL/TLS. På slutpunkter, der administreres af os (computer og mobil) og moderne browsere, bruger vi stærke koder og understøtter Perfect Forward Secrecy og certifikat-pinning. På nettet markerer vi desuden alle godkendelsescookies som sikre og aktiverer HTTP Strict Transport Security (HSTS) med aktivering af "includeSubDomains".

For at forhindre angreb fra tredjeparter udføres der godkendelse af Dropbox' front end-servere gennem offentlige certifikater, der er i klientens besiddelse. En krypteret forbindelse forhandles, før der overføres nogen filer eller Paper-dokumenter, og sørger for sikker levering til Dropbox' frontend-servere.

Data under opbevaring

Inaktive Dropbox-filer krypteres ved hjælp af 256-bit Advanced Encryption Standard-kryptering (AES). Filer gemmes i diskrete filblokke i flere datacentre. Hver blok fragmenteres og krypteres med en stærk kode. Kun de blokke, der er blevet ændret mellem versioner, synkroniseres. Paper-dokumenter i hvile krypteres også vha. 256-bit Advanced Encryption Standard-kryptering (AES). Paper-dokumenter gemmes på tværs af flere tilgængelighedszoner vha. tredjepartssystemer.

Vedligeholdelse af en pålidelig tjeneste

Et opbevaringssystem er kun godt, hvis det er driftssikkert, og vi har derfor udviklet Dropbox med adskillige sikkerhedslag for at beskytte mod tab af data og sikre, at disse data er tilgængelige. Ekstra kopier af metadata fordeles på tværs af uafhængige enheder i et datacenter i mindst en N+2-tilgængelighedsmodel. Der tages delvise sikkerhedskopier af metadata på timebasis, og der tages komplette sikkerhedskopier hver tredje dag. Metadata gemmes på servere, der hostes og administreres af Dropbox. Til lagring af filblokke bruger Dropbox både interne systemer og systemer fra tredjepartsudbydere, der er designede til at give en årlig datastabilitet på mindst 99,999999999 %.

Hvis der i sjældne tilfælde skulle opstå problemer med tjenestens tilgængelighed, vil Dropbox-brugere stadig have adgang til de senest synkroniserede kopier af deres filer i den lokale Dropbox-mappe på tilknyttede computere. De kopier af filer, der er synkroniseret i Dropbox-programmet på computeren eller den lokale mappe, er tilgængelige fra en brugers harddisk under nedetid, driftstop eller manglende internetforbindelse.

På samme måde fordeles ekstra kopier af Paper-dokumentdata på tværs af uafhængige enheder i et datacenter i en N+1-tilgængelighedsmodel, og vi har konfigureret daglige komplette sikkerhedskopier af Paper-dokumentdata. Til lagring af Paper-dokumenter benytter Dropbox tredjepartssystemer, der er designet til at yde en årlig datastabilitet på mindst 99,999999999 %. Hvis der i sjældne tilfælde skulle opstå problemer med en tjenestes tilgængelighed, har brugerne stadig adgang til deres Paper-dokumenter i “offlinetilstand” fra mobilapplikationen.

Begrænset medarbejderadgang til back end-systemer

Vi ved, at når du som Dropbox Business- eller Dropbox Education-kunde gemmer dine filer og Paper-dokumenter hos Dropbox, forventer du, at vi er ansvarlige forvaltere af dine data. Som en del af dette ansvar sikrer vi, at Dropbox-medarbejderes adgang til vores interne systemer er strengt kontrolleret. Adgang mellem vores erhvervs- og produktionsnetværk er f.eks. yderst begrænset. Adgang til produktionsnetværket er SSH-nøglebaseret og begrænset til udviklingsteams, der har brug for at få adgang for at udføre deres arbejdsopgaver. Firewallkonfigurering er tæt kontrolleret og begrænset til et lille antal administratorer. Adgang til andre ressourcer, herunder datacentre, programmer til serverkonfigurering, produktionsservere og programmer til udvikling af kildekode, tildeles udelukkende efter specifik godkendelse af den relevante ledelse. Registrering af anmodningen om adgang, begrundelsen herfor og godkendelsen heraf udføres af ledelsen, og de relevante personer giver adgang.

Bibeholdelse af medarbejderes opmærksomhed på sikkerhed og beskyttelse af personlige oplysninger

Som en del af at holde vores tjeneste sikker sørger vi for, at de personer, der arbejder hos Dropbox, har forståelse for, hvordan de er opmærksomme på sikkerhed og genkender mistænkelig aktivitet. Til dette formål kræves det, at Dropbox-medarbejdere har kendskab til sikkerhedspolitikkerne, inden de får adgang til systemer. Medarbejdere deltager også i obligatorisk træning af nyansatte inden for sikkerhed og beskyttelse af personlige oplysninger og årlig opfølgningstræning og modtager regelmæssig træning inden for opmærksomhed på sikkerhed via informations-e-mails, foredrag, præsentationer og ressourcer på vores intranet.

Validering af vores praksis

For at hjælpe os med at sikre, at vores sikkerhedspraksis fungerer, som den skal, bruger vi tredjeparter til at vurdere effektiviteten. Specialister udfører periodiske penetrations- og sårbarhedstests på Dropbox' erhvervs- og produktionsmiljøer. De problemer, der opdages, prioriteres og løses af vores sikkerhedsudviklingsteam. Derudover evaluerer tredjepartsauditører vores sikkerhedspraksis i forhold til internationale og branchemæssige standarder. For at hjælpe dig med at lære mere om og evaluere Dropbox' praksis offentliggør vi vores SOC 3-rapport og ISO 27001-, 27017-, 27018- og 22301- certifikater online. Du kan også anmode om vores SOC 2-rapport, en oversigts- og vurderingsrapport over HIPAA-krav, en BSI C5-vurdering og -rapport (tilgængelig på engelsk og tysk) samt resultatsammendrag for penetrationstests i forbindelse med en fortielsesaftale (NDA).

Kommunikation af problemer til dig

Status for tjenesten

Dropbox har et tredjepartswebsted, der viser status for vores tjeneste for Dropbox Business- og Dropbox Education-kunder. Som nuværende kunde kan du gå til status.dropbox.com når som helst for at se den aktuelle webstedsstatus samt tidligere afbrydelser og vedligeholdelse.

Meddelelse om lækage

Dropbox giver dig besked i tilfælde af en datalækage som påkrævet ved lov. Vi har politikker og procedurer for reaktion på hændelser, herunder en meddelelsesproces for lækager, som gør os i stand til at give påvirkede kunder besked efter behov. Hvis du har indgået en HIPAA Business Associate-aftale eller en EU Data Processing-aftale, får du besked som angivet i disse aftaler.

Du får de værktøjer, du har brug for til konstant at være sikret

Vi vil gerne have, at du og andre Dropbox Business- og Dropbox Education-administratorer har de værktøjer, I har brug for til at træffe ansvarlige, informerede beslutninger om jeres teams sikkerhed. For at hjælpe dig med at konfigurere, bruge og overvåge din konto på en måde, der opfylder dine behov, er dit Administratorpanel udstyret med sikkerhedsfunktioner, som du kan aktivere på vegne af dit team. Via vejledninger som denne, vores Dropbox Business-sikkerhedshvidbog, hjælpecenteret og vores supportteam kan vi give oplysninger, der kan hjælpe dig med at forstå, hvordan du med disse indstillinger kan konfigurere din konto på en ansvarlig måde.

Kundeansvar

Oplysninger om vores praksis

Det er vigtigt at fastslå, om Dropbox Business eller Dropbox Education er det rette valg for din virksomheds behov. Vi opfordrer dig til at bruge samme tid og nøje opmærksomhed på at validere vores praksis, som du ville med enhver anden applikation. For at give dig de værktøjer, du behøver til at bekræfte vores sikkerhedspraksis, findes vores ISO 27001-, 27017- , 27018- og 22301- certifikater, SOC 3-sikkerhedsrapport og CSA STAR-selvevaluering på niveau 1 og certificering på niveau 2 online. Vi kan også give adgang til yderligere dokumentation under en fortielsesaftale (NDA) som hjælp til at træffe en informeret beslutning. Dette omfatter vores SOC 1- og SOC 2-overvågningslogs, vores C5-vurderingsrapport (tilgængelig på engelsk og tysk), en oversigt over vores interne praksis og anbefalinger til kunder, der vil overholde HIPAA/HITECH-kravene til sikkerhed, beskyttelse af personlige oplysninger og information om sikkerhedsbrud, samt sammendrag af vores seneste applikationspenetrationstests. Vores servicebetingelser, politik for acceptabel brug og standardvirksomhedsaftale findes også online, så du kan gennemlæse disse og sikre, at Dropbox Business eller Dropbox Education er det rette valg for dit team.

Konfiguration af tilladelser for deling og visning

Dropbox Business og Dropbox Education giver dig fleksibilitet til at konfigurere din konto, så den understøtter dine behov for sikkerhed, samarbejde og beskyttelse af personlige oplysninger. Administratorer kan se og ændre disse indstillinger via deres Administratorpanel, så de afspejler deres miljø for deling og overholdelse af lovmæssige krav. Konti kan f.eks. konfigureres, så mapper, links og Paper-dokumenter ikke kan deles med personer uden for dit team. Når teammedlemmer opretter delte mapper til Dropbox-filer, kan de desuden tilpasse mappernes indstillinger og vælge det rette adgangsniveau – redigering eller skrivebeskyttet.

Stærk godkendelsespraksis

En stærk godkendelsespraksis hjælper med at holde dit teams data sikre. Administratorer bør gennemgå tilgængelige godkendelsesindstillinger og aktivere dem, der bedst beskytter deres konti. Dropbox Business- og Dropbox Education-konti har følgende indstillinger:

Totrinsbekræftelse

Teamadministratorer kan kræve, at medlemmer bruger totrinsbekræftelse til at logge på deres konti. Denne yderst anbefalede sikkerhedsfunktion føjer et ekstra beskyttelseslag til brugeres Dropbox-konti. Når den er aktiveret, kræver Dropbox en sekscifret sikkerhedskode eller en sikkerhedsnøgle ud over adgangskoden, når der oprettes forbindelse til en ny computer, telefon eller tablet.

Enkeltlogon

Hvis din virksomhed allerede administrerer adgangskodepolitikker og godkendelse via en central identitetsudbyder, vil du muligvis også gerne aktivere enkeltlogon for dit Dropbox Business- eller Dropbox Education-team. Ved at bruge din eksisterende udbyder af enkeltlogon behøver dine teammedlemmer ikke at skulle huske endnu en adgangskode. Endnu vigtigere er, at godkendelse af adgang til Dropbox administreres ved hjælp af samme adgangskodepolitikker som andre tjenester i din virksomhed.

Udførelse af regelmæssig adgangsgennemgang

Adgang til dit teams konto bør ændres, efterhånden som medlemmer i dit team, deres interne roller og enheder ændres. Du bør regelmæssigt kontrollere, at kun de rette personer, enheder og apps har adgang til din konto, så dine oplysninger er i de rette hænder. Du kan nemt ændre eller fjerne adgang via dit Administratorpanel.

Teammedlemmer

Teammedlemmer kan nemt tilføjes, fjernes og gennemgås fra dit Administratorpanel. For at sikre, at der kun er adgang til følsomme data på din Dropbox Business- eller Dropbox Education-konto for de rette personer, anbefaler vi, at du regelmæssigt gennemgår denne liste. Du kan derefter fjerne adgang, når nogen forlader din organisation eller ikke længere har brug for adgang grundet et rolleskift. På samme måde kan du ændre teammedlemmers roller i dit Administratorpanel, så hver brugerkonto har det rette adgangsniveau.

Enheder

Du og dine teammedlemmer bør regelmæssigt gennemgå de enheder, der er tilknyttet din konto, og fjerne ubrugte eller ikke-godkendte enheder. Tilknytningen til enheder kan fjernes af både teammedlemmer og -administratorer. Du og dine teammedlemmer har også mulighed for at fjernslette Dropbox-indhold fra enheder under fjernelse af tilknytning. Fjernelse af tilknytning og fjernsletning på enheder kan holde dine data sikre i tilfælde af tab eller tyveri, eller hvis nogen forlader dit team.

Tredjepartsapps

Der findes et robust økosystem af tredjepartsapps, som du kan tilknytte din Dropbox Business- eller Dropbox Education-konto for at få yderligere funktioner. Integrationer til tjenester som SIEM, DLP og identitetsstyring kan være nyttige til at styrke din eksisterende sikkerhedspraksis. Mens disse tredjepartsapps og -integrationer kan komplimentere din konto godt, er det vigtigt at huske på, at de ikke er en del af vores inkluderede tjenester. De er derfor ikke dækket af Dropbox' vilkår for brug eller virksomhedsaftale, herunder eventuelle Business Associate-aftaler eller Data Processing-aftaler, du har underskrevet med Dropbox. Apps kan bede dig om forskellige adgangsniveauer for dine oplysninger afhængigt af tjenestetilbuddet. Som administrator kan du tilknytte eller fjerne team-apps – der gælder for hele din konto – og fjernslette individuelle apps, som teammedlemmer måtte have føjet til deres egen konto. Tredjepartsapps og adgang kan gennemgås og ændres via administratorpanelet.

Overvågning af usædvanlig aktivitet

Som teamadministrator kan du se og eksportere rapporter, der viser dit teams filhændelser, deling-, godkendelse- og administratoraktiviteter. Administratorer bør regelmæssigt gennemgå disse aktivitetsrapporter for at holde øje med usædvanlig aktivitet og hjælpe med at holde teamet sikkert. Du kan overveje at bruge en tredjeparts-SIEM eller en anden overvågningsintegration til at forbedre dine funktioner.

Fastlægning af krypteringsbehov

Dropbox gemmer som standard en lokal kopi af dine filer på din computer for at sikre, at du har de filer, du har brug for, lige ved hånden. De lokale kopier af dine filer er beskyttet som alle andre filer på din computer. For at hjælpe med at beskytte dem anbefaler vi, at du aktiverer diskkryptering på dine enheder, når det er muligt, og kræver en stærk og unik adgangskode til at få adgang til din bærbare computer, telefon, tablets eller enhver anden enhed, der giver adgang til din Dropbox-konto. Ved at bruge stærke og unikke adgangskoder beskytter du også adgangen til dine Paper-dokumenter.

Dropbox beskytter de filer, du uploader til din konto, ved automatisk at dele filerne i adskilte blokke og kryptere hver blok ved hjælp af 256-bit Advanced Encryption Standard-kryptering (AES). På samme måde beskytter Dropbox Paper-dokumenter ved at kryptere dem under lagring ved at kryptere dem i permanent lager vha. 256-bit Advanced Encryption Standard (AES). Dropbox administrerer krypteringsnøglerne på kundernes vegne for at holde denne proces så enkel som mulig for brugerne og for at aktivere visse funktioner.

Dropbox Business- og Dropbox Education-medlemmer kan også vælge at kryptere filer, før de uploades til Dropbox, alene eller via en tredjepartsintegration. Men brugere, der krypterer data, inden de uploades til Dropbox, er selv ansvarlige for at administrere disse krypteringsnøgler. Kryptering af filer, inden de uploades til Dropbox, kan også mindske funktionaliteten for visse funktioner.

Kunder, som gerne vil vide mere om, hvordan Dropbox' tilgang til sikkerhed er, kan læse sikkerhedshvidbogen på vores websted: dropbox.com/business/trust. Kontakt sales@dropbox.com, hvis du vil vide mere om Dropbox Business eller Dropbox Education og anmode om tredjepartsovervågningsrapporter under en fortielsesaftale (NDA).