Sikkerhed i Dropbox til virksomheder

En hvidbog fra Dropbox

Dropbox

Indhold

Oversigt

Digital transformation bliver i stigende grad en del af forskellige brancher, og det er vigtigt, at data, teams og enheder er beskyttet, uanset hvor de er. Organisationer, der er afhængige af cloud-løsninger som Dropbox Business til at muliggøre fjern- og distribuerede arbejdsgange, har brug for at strømline samarbejde, proaktivt styre skyrisici og implementere effektive kontroller, der sikrer fortroligheden af intellektuelle ejendom (IP), integriteten af lagrede og delte data og tilgængeligheden af data gennem administrerede og fleksible cloudtjenester.

Over 600.000 virksomheder og organisationer er afhængige af Dropbox til virksomheder som løsningen til sikkert samarbejde mellem eksterne og distribuerede teams. Den centrale Dropbox til virksomheder-løsning inkluderer smart workspace til samarbejde, filsynkronisering og delingsfunktioner. Vores løsninger understøttes af branchens førende infrastruktur samt funktioner til avanceret virksomhedssikkerhed, team- og indholdssikkerhed, elektronisk underskrift, sikker overførsel og dataforvaltning. Medmindre andet er angivet, gælder oplysningerne i denne hvidbog for alle Dropbox til virksomheder-produkter (Standard, Advanced og Enterprise) samt Dropbox Education. Paper er en funktion i Dropbox til virksomheder og Dropbox Education.

Kernen i Dropbox til virksomheder er Dropbox' tillidsprogram, vores omfattende sikkerhedsprogram, Dropbox Trust Program, som har en niveauinddelt tilgang til sikkerhed, som er særligt vigtig, efterhånden som globale tilgange til fjernarbejde udvikler sig.

Denne hvidbog beskriver produktsikkerhedsfunktioner for Dropbox til virksomheder, Dropbox' operationelle sikkerhedsforanstaltninger, vores forpligtelse til beskyttelse af personlige oplysninger og gennemsigtighed samt back-end-politikker, uafhængige certificeringer og lovgivningsmæssige overholdelsesforanstaltninger, der gør Dropbox til den sikre løsning for din organisation.

Medmindre andet er angivet, gælder oplysningerne i denne hvidbog for alle Dropbox til virksomheder-produkter (Standard, Advanced og Enterprise) samt Dropbox Education. Paper er en funktion i Dropbox til virksomheder og Dropbox Education.

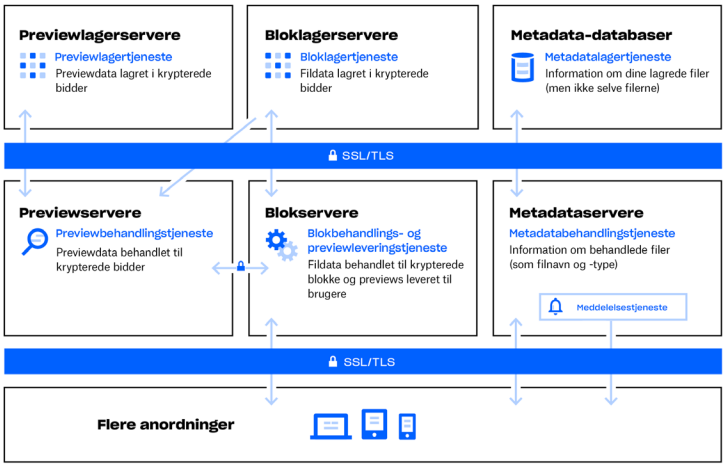
De tekniske detaljer

Vores brugervenlige grænseflader understøttes af en infrastruktur, som fungerer bag kulisserne for at sikre hurtig og pålidelig synkronisering, deling og samarbejde. Til det formål forbedrer vi hele tiden vores produkt og arkitektur for at gøre dataoverførsler hurtigere, forbedre driftssikkerheden og tilpasse os til ændringer i omgivelserne. I dette afsnit forklarer vi, hvordan data overføres, opbevares og behandles på sikker vis.

Filinfrastruktur

Dropbox-brugere kan få adgang til filer og mapper når som helst på stationære pc'er, internettet og mobilklienter eller via tredjepartsapplikationer, som er brugt til at oprette forbindelse til Dropbox. Alle disse klienter opretter forbindelse til krypterede servere, så brugerne kan få adgang til filer, dele filer med andre og opdatere tilknyttede enheder, når filerne tilføjes, ændres eller slettes.

Dropbox' filinfrastruktur består af følgende komponenter:



- ***Metadataservere***

  Visse grundlæggende oplysninger om brugerdata, der kaldes metadata, opbevares i deres egen særskilte lagertjeneste og fungerer som et indeks for dataene på brugernes konti. Metadataene indeholder grundlæggende konto- og brugeroplysninger, f.eks. e-mailadresse, navn og enhedsnavne. Metadataene indeholder også grundlæggende oplysninger om filer, f.eks. filnavne og -typer, der understøtter funktioner som versionshistorik, gendannelse og synkronisering.

- ***Databaser med metadata***

  Filmetadata lagres i en et transaktionsbaseret nøgleværdilager med kontrol af flere samtidige versioner og deles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

- ***Blokservere***

  Dropbox er designet med en unik sikkerhedsmekanisme, som beskytter brugerdata med mere end blot traditionel kryptering. Blokservere behandler filer fra Dropbox-applikationerne ved at dele hver enkelt fil op i blokke, kryptere hver enkelt fil ved hjælp af en stærk kode og kun synkronisere de blokke, som er ændret mellem gennemgange. Når en Dropbox-applikation registrerer en ny fil eller ændringer af en eksisterende fil, underretter applikationen blokserverne om ændringen, og nye eller ændrede filblokke behandles og overføres til bloklagerserverne. Blokservere bruges desuden til at levere filer og previews til brugere. For detaljerede oplysninger om den kryptering, der bruges af disse tjenester både ved overførsel og i hvile, se afsnittet Kryptering nedenfor.

- ***Bloklagerservere***

  Det faktiske indhold af brugernes filer lagres i krypterede blokke på bloklagerserverne.

  Før overførslen opdeler Dropbox-klienten filerne i filblokke som forberedelse til lagring. Bloklagerserverne fungerer som et CAS-system (Content-Addressable Storage), hvor hver enkelt krypteret filblok hentes på baggrund af dens hash-værdi.

- ***Forhåndsvisningsservere***

  Previewserverne danner forhåndsvisninger af filer. Forhåndsvisninger (previews) er en gengivelse af en brugers fil i et andet filformat, der er bedre egnet til hurtig visning på en slutbrugers enhed. Previewservere henter filblokke fra bloklagerserverne for at generere forhåndsvisninger. Når der anmodes om en forhåndsvisning af en fil, henter previewserverne den cachede forhåndsvisning fra previewlagerserverne og overfører det til blokserverne. Forhåndsvisninger leveres i sidste ende til brugerne af blokservere.

- ***Previewlagerservere***

  Cachede previews lagres i et krypteret format på previewlagerserverne.

- ***Meddelelsestjeneste***

  Denne separate tjeneste overvåger, om der foretages nogen ændringer i Dropbox-konti. Ingen filer eller metadata opbevares eller overføres her. Hver klient etablerer en lang forespørgselsforbindelse til meddelelsestjenesten og venter. Når der sker en ændring til en fil i Dropbox, giver meddelelsestjenesten besked om ændringen til den eller de pågældende klienter ved at lukke den lange forespørgselsforbindelse. Når forbindelsen lukkes, er det tegn til, at klienten skal oprette en sikker forbindelse til metadataserverne for at synkronisere eventuelle ændringer.

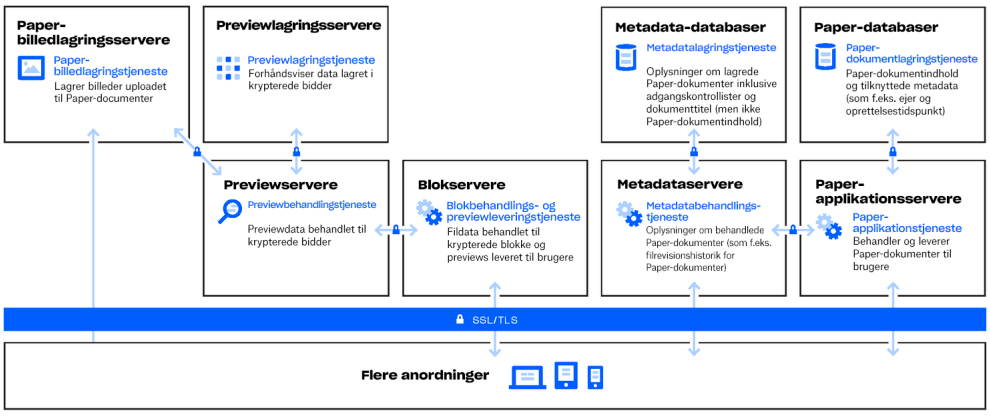
Opbevaring af fildata

Dropbox opbevarer primært to typer fildata: metadata om filer (f.eks. datoen og tidspunktet, hvor en fil sidst blev ændret) og filernes indhold (filblokke). Filers metadata gemmes på Dropbox-servere. Filblokke gemmes i enten Amazon Web Services (AWS) eller Magic Pocket, som er Dropbox' eget lagersystem. Magic Pocket fungerer ved hjælp af både patenteret software og hardware og er designet fra bunden til at være pålideligt og sikkert. I både Magic Pocket og AWS krypteres de lagrede filblokke, og begge systemer overholder krævende standarder for driftssikkerhed. Få flere oplysninger i afsnittet Driftssikkerhed nedenfor.

Paper-infrastruktur

Dropbox-brugere kan når som helst få adgang til Paper-dokumenter fra computer-, web- og mobilklienterne eller gennem tredjepartsapplikationer, der er forbundet med Dropbox Paper-applikationen. Alle disse klienter er forbundet til sikre servere for at give adgang til Paper-dokumenter, gøre det muligt at dele dokumenter med andre og at opdatere forbundne enheder, når dokumenter tilføjes, ændres eller slettes.

Dropbox Papers infrastruktur består af følgende komponenter:



- ***Paper-applikationsservere***

  Paper-applikationsserverne behandler brugeranmodninger, viser output af redigerede Paper-dokumenter tilbage til brugeren og kører meddelelsestjenester. Paper-applikationsservere skriver indgående brugerændringer til Paper-databaserne, hvor de gemmes i permanent lager. Kommunikationssessioner mellem Paper-applikationsservere og Paper-databaser er sikret med Secure Hypertext Transfer Protocol (HTTPS).

- ***Paper-databaser***

  Det faktiske indhold af brugernes Paper-dokumenter samt visse metadata om disse Paper-dokumenter krypteres i permanent lager i Paper-databaserne. Dette inkluderer oplysninger om et Paper-dokument (såsom titel, ejer, oprettelsestid og anden information) samt indhold i selve Paper-dokumentet, inklusive kommentarer og opgaver. Paper-databaserne opdeles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

- ***Metadataservere***

  Paper bruger de samme metadata-servere, der er beskrevet i Dropbox-infrastrukturdiagrammet til at behandle oplysninger om Paper-dokumenter, såsom revisionshistorik for Paper-dokumenter og medlemskab af delt mappe. Dropbox har direkte administration af metadata-servere, som findes i tredjepartsdatacentre på fælles lokalitet.

- ***Databaser med metadata***

  Paper bruger de samme metadata-databaser, der er beskrevet i Dropbox-infrastrukturdiagrammet til at gemme oplysninger, der er relateret til Paper-dokumenter, såsom deling, tilladelser og mappeassociationer. Dokumentmetadata for Paper lagres i en MySQL-understøttet databasetjeneste og deles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

- ***Paper-billedlagerservere***

  Billeder, der uploades til Paper-dokumenter, lagres og krypteres i hvile på Paper-billedlagerserverne. Overførsel af billeddata mellem Paper-applikationen og Paper-billedserverne foregår med en krypteret session.

- ***Forhåndsvisningsservere***

  Previewserverne producerer previews for både billeder, som uploades til Paper-dokumenter, og for hyperlinks, som er indlejret i Paper-dokumenter. For billeder, der uploades til Paper-dokumenter, henter previewserverne billeddata, der er lagret på Paper-billedlagerserverne, gennem en krypteret kanal. For hyperlinks, der er indlejret i Paper-dokumenter, henter previewservere billeddataene og viser et preview af billedet ved hjælp af kryptering, der er specificeret i kildelinket. Til sidst vises previewet for brugere af blokserverne.

- ***Previewlagerservere***

  Paper bruger de samme previewlagerservere, der er beskrevet i diagrammet over Dropbox-infrastrukturen, til at lagre cachede billedpreviews. Bidder af cachede previews lagres i et krypteret format på previewlagerserverne.

Opbevaring af Paper-dokumenter

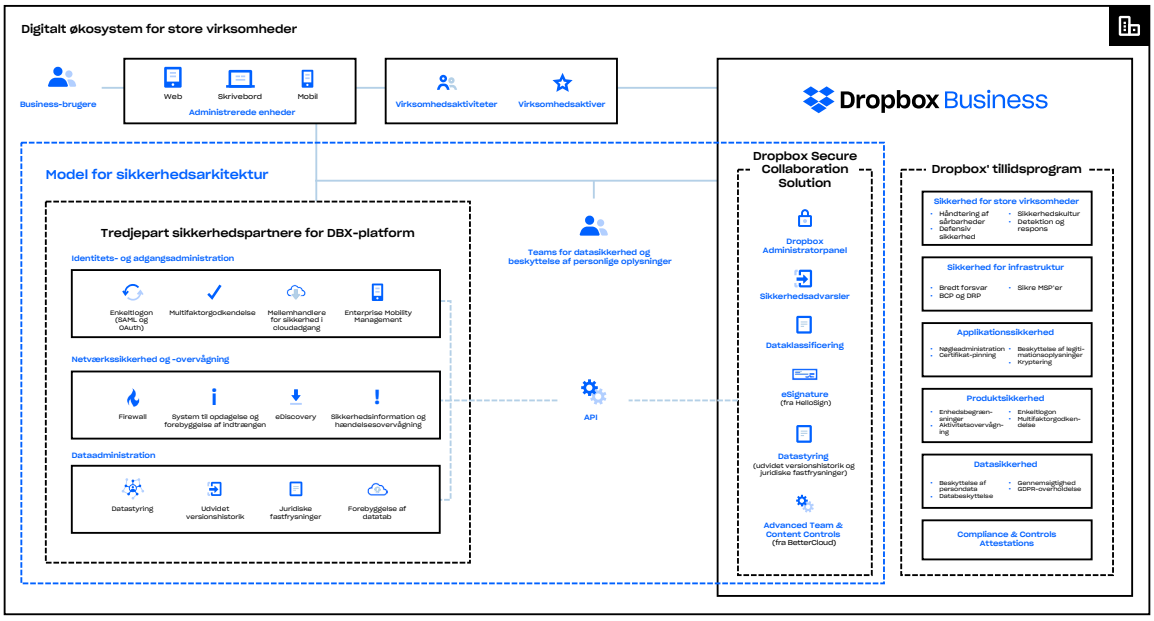
Dropbox gemmer primært de følgende datatyper i Paper-dokumenter: metadata om Paper-dokumenter (for eksempel et dokuments delte tilladelser) og det faktiske indhold af de Paper-dokumenter, som brugeren har uploadet. Disse kaldes under ét for Paper-dokumentdata, og billeder, der uploades til Paper-dokumenter, kaldes for Paper-billeddata. Hver af disse datatyper gemmes i Amazon Web Services (AWS). Paper-dokumenter krypteres i hvile i AWS, og AWS overholder høje standarder for driftssikkerheden. Du kan finde flere oplysninger i afsnittet Driftssikkerhed nedenfor.

Dropbox' tillidsprogram

Tillid er grundlaget for vores forhold til millioner af mennesker og virksomheder i hele verden. Vi værdsætter din tillid og tager ansvaret for at beskytte dine personlige oplysninger seriøst. For at gøre os værdige til din tillid har vi udviklet og fortsætter med at udvikle Dropbox med fokus på sikkerhed, persondata, gennemsigtighed og overholdelse.

Politikken for Dropbox' tillidsprogram etablerer en risikovurderingsproces, der er designet til at håndtere miljømæssige risici, fysiske risici, brugerrisici, tredjepartsrisici, risici ifm. gældende love og bestemmelser, risici ifm. kontraktmæssige forpligtelser og en lang række andre risici, der kan påvirke systemsikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelsen af personlige oplysninger. Udviklingen på de forskellige områder evalueres mindst én gang om året. Få flere oplysninger om Dropbox' tillidsprogram på www.dropbox.com/business/trust.

Vi følger en tilgang i flere lag for at sikre virksomhed, infrastruktur, applikationer og produkter, der påvirker din organisation.



Sikkerhed på virksomhedsniveau

Dropbox har retningslinjer for håndtering af informationssikkerhed, som omfatter formål, målsætning, principper og grundlæggende regler for, hvordan vi sikrer kundernes tillid til os. Dette opnås ved at vurdere risici og hele tiden forbedre Dropbox til virksomheder-systemernes sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger. Vi gennemgår og opdaterer regelmæssigt sikkerhedspolitikkerne, uddanner i sikkerhed, tester applikations- og netværkssikkerhed (herunder penetrationstests), overvåger overholdelse af sikkerhedspolitikker og udfører interne og eksterne risikovurderinger.

Vores politikker

Vi har omhyggeligt tilrettelagt et sæt sikkerhedspolitikker, som håndhæves af Dropbox' Security & Abuse-team. Alle sikkerhedspolitikker gennemgås og godkendes mindst én gang om året. Ansatte, praktikanter og leverandører deltager i obligatoriske sikkerhedskurser, når de bliver en del af virksomheden, og deltager i sikkerhedsorienterede kurser.

- ***Informationssikkerhed***

  Bruger- og Dropbox-oplysninger holdes sikre.

- ***Godkendelse***

  Beskriver, hvordan Dropbox-medarbejdere autentificerer sig selv for at få adgang til informationssystemer og data.

- ***Sikkerhed for enheder***

  Mindstekravene til mobilenheder, der bruges til at tilgå information i virksomheden.

- ***Logisk adgangskontrol***

  Beskyttelse af Dropbox-systemer, brugere og information. Dækker adgangskontrol for både virksomheds- og produktionsmiljøer.

- ***Datasikkerhed***

  Beskriver, hvordan Dropbox beskytter data gennem specifikke krav til opbevaring, adgang og brug.

- ***Rejsesikkerhed***

  Beskriver, hvad Dropbox-medarbejdere skal gøre, før de rejser til udlandet.

- ***Sikkerhedsretningslinjer for salg og kundeoplevelse (CX)***

  Brugeroplysninger holdes sikre, vi beskytter vores ansatte og yder support til vores brugere.

- ***Fysisk sikkerhed***

  Opretholdelse af et trygt og sikkert miljø for mennesker og ejendom hos Dropbox.

- ***Retningslinjer for fysisk sikkerhed i produktion***

  Håndtering af fysisk adgang til produktionsfaciliteter.

- ***Reaktion på hændelser***

  Skitserer, hvordan Dropbox håndterer rapporterede sikkerheds-, privatlivs- og websiteshændelser og dokumenterer hændelsesresponsplaner for hver af disse.

- ***Uautoriseret ophavsretligt beskyttet materiale***

  Forbyder medarbejdere at bruge Dropbox- eller Dropbox-systemer til at gemme eller dele uautoriseret indhold.

- ***Administration af ændringer***

  Håndtering af ændringer i produktionssystemer. Henvender sig til alle Dropbox-medarbejdere, leverandører og praktikanter med adgang til systemer.

- ***Beskyttelse af brugeroplysninger***

  Beskyttelse og håndtering af brugeroplysninger og brugerdata hos Dropbox til overholdelse af vores politik om beskyttelse af personlige oplysninger.

- ***Politik for forretningskontinuitet og administration af nødberedskab***

  Beskriver, hvad vi gør for opretholdelsen, beskyttelsen og sikringen af personer (Dropbox' medarbejdere), ejendom og (forretnings-)processer.

- ***Dropbox's persondataprogram***

  Formålet, principperne og ansvarligheden for Dropboxs persondataprogram.

- ***Dropbox' tillidsprogram***

  Beskriver, hvordan Dropbox driver sin virksomhed og gør sig fortjent til kundernes tillid (Worthy of Trust).

- ***Sikkerhed for betalingsmiljøet***

  Sikring og vedligeholdelse af det dedikerede betalingsmiljø, der bruges i Dropbox til modtagelse af kreditkortbetalinger.

Personalepolitik og -adgang

Ved ansættelsen skal alle Dropbox-medarbejderes baggrund kontrolleres, de skal underskrive en accept af sikkerhedspolitikken og en fortrolighedaftale, og de skal gennemføre et sikkerhedskursus. Kun personer, der har gennemført disse procedurer, får fysisk og logisk adgang til virksomheds- og produktionsmiljøerne, alt efter hvad der er nødvendigt for, at de kan udføre deres job. Desuden skal alle ansatte fuldføre et årligt sikkerhedskursus, og de får regelmæssigt uddannelsesmateriale om sikkerhed i form af e-mails med oplysninger, seminarer og præsentationer samt ressourcer på vores intranet.

Medarbejdernes adgang til Dropbox-miljøet administreres af en central mappe og godkendes ved hjælp af en kombination af stærke adgangskoder, SSH-nøgler med beskyttet adgangsudtryk og tofaktorbekræftelse. Fjernadgang kræver brug af VPN, der er beskyttet med totrinsbekræftelse, og alle særlige adgangshændelser gennemgås og vurderes af sikkerhedsteamet. Adgang til virksomheds- og produktionsnetværk er stærkt begrænset i henhold til definerede politikker. Adgang til produktionsnetværket er SSH-nøglebaseret og begrænset til udviklingsteams, der har brug for at få adgang for at udføre deres arbejdsopgaver. Konfiguration af firewalls kontrolleres omhyggeligt, og kun et lille antal administratorer har mulighed for at gøre dette.

Desuden kræver vores interne politikker, at de medarbejdere, der får adgang til produktions- og virksomhedsmiljøer, skal overholde retningslinjer for oprettelse og opbevaring af private SSH-nøgler. 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.

Dropbox benytter teknisk adgangskontrol og interne politikker til at forhindre ansatte i at opnå vilkårlig adgang til brugerfiler og til at begrænse adgang til metadata og andre oplysninger om brugernes konti. For at beskytte slutbrugernes personlige oplysninger og sikkerhed er det kun et lille antal teknikere, der er ansvarlige for at udvikle Dropbox' kerneydelser og har adgang til det miljø, hvor brugerfilerne opbevares. Medarbejderes adgang fjernes med det samme, når en medarbejder forlader virksomheden.

Eftersom Dropbox bliver en forlængelse af vores kunders infrastruktur, garanterer vi dem, at vi er ansvarlige vogtere af deres data. Se afsnittet Persondata herunder for at få flere oplysninger.

Håndtering af sårbarheder

Vores sikkerhedsteam udfører regelmæssige, automatiserede og manuelle sikkerhedsteste og rettelseshåndtering, og samarbejder med tredjepartsspecialister for at identificere og afhjælpe potentielle sikkerhedssårbarheder og fejl.

Som en nødvendig del af vores system til administration af informationssikkerhed rapporteres resultater og anbefalinger som følge af alle disse vurderingsaktiviteter til Dropbox-ledelsen, som vil evaluere dem og udføre de nødvendige handlinger, alt efter hvad der betragtes som nødvendigt. Alvorlige punkter dokumenteres, overvåges og håndteres af delegerede sikkerhedsteknikere.

Ændringsstyring

Alle udviklings-, problemrensnings- og rettelses-processer følger vores formelle politik til ændringsstyring, der er defineret af teknikerteamet hos Dropbox for at sikre, at systemændringer er blevet testet og godkendt inden implementering i produktionsmiljøerne. Ændringer i kildekode påbegyndes af udviklere, der gerne vil forbedre Dropbox-applikationen eller -tjenesten Ændringer gemmes i et system til versionskontrol og skal gennemgå automatiserede testprocedurer for kvalitetssikring (QA) for at bekræfte, at sikkerhedskravene er opfyldt. En vellykket kvalitetskontrol betyder, at ændringen vil blive implementeret. QA-godkendte ændringer implementeres automatisk i produktionsmiljøet. Vores livscyklus for udvikling af software (SDLC) kræver, at sikre retningslinjer for kodning overholdes, og kodeændringer gennemgås for sikkerhedsproblemer via vores processer til kvalitetskontrol og manuel gennemgang. Ændringer, der sættes i produktion, logges og arkiveres, og der gives automatisk besked til ledelsen hos Dropbox' teknikere.

Kun autoriseret personale må foretage ændringer i Dropbox' infrastruktur. Dropbox' sikkerhedsteam er ansvarlig for at vedligeholde infrastrukturens sikkerhed og sørge for, at server-, firewall- og andre sikkerhedskonfigurationer opdateres og opfylder branchens standarder. Firewallregelsæt og enkeltpersoner med adgang til produktionsservere gennemgås regelmæssigt.

Scanning og penetrationstests af sikkerheden (internt og eksternt)

Vores sikkerhedsteam udfører regelmæssig automatiseret og manuel test af applikationssikkerheden for at identificere og reparere potentielle sikkerhedshuller og -fejl i vores computer-, web- (Dropbox og Paper) og mobilapplikationer (Dropbox og Paper).

Derudover har Dropbox indgået samarbejde med tredjepartsudbydere om at udføre periodiske penetrations- og sårbarhedstests i produktionsmiljøet. Vi samarbejder med tredjepartseksperter, andre sikkerhedsteams i branchen og netværket for forskning i sikkerhed for at beskytte vores applikationer. Vi bruger også automatiske analysesystemer til at identificere sårbarheder. Denne proces omfatter internt udviklede systemer, open source-systemer, som vi tilpasser til vores behov, og eksterne udbydere, som vi hyrer til kontinuerlig automatiseret analyse.

Skadeligt indhold holdes ude af Dropbox

Vi har scanningsfunktioner, der sigter mod at forhindre lagring og distribution af skadeligt indhold i Dropbox. Vores scannere udnytter vores egen teknologi såvel som avancerede kapaciteter fra partnere som Microsoft og Google for at gøre Dropbox til et sikkert sted for vores kunder.

Dusører for detektion af fejl

Mens vi samarbejder med professionelle firmaer, når det drejer sig om penetrationstests, og udfører vores egne interne tests, tilbyder vi også dusører for opdagelse af fejl (eller belønningsprogrammer for identifikation af sårbarheder) for at få gavn af det bredere sikkerhedscommunitys ekspertise. Vores dusørprogram for opdagelse af fejl motiverer researchere til at afsløre softwarefejl på en ansvarlig måde. Vores inddragelse af det eksterne community giver vores sikkerhedsteam uafhængige analyser af vores applikationer, som bidrager til beskyttelsen af vores brugere. Vi bestræber os på at være blandt de førende i branchen, når det gælder dusørprogrammer samt reaktions- og afhjælpningstider.

Vi har udarbejdet instrukser til, hvilke typer fejl der kan gøres opmærksom på i forbindelse med de enkelte Dropbox-applikationer, og vi har suppleret dem med en ansvarlig offentliggørelsespolitik, der opfordrer til detektering og rapportering af sikkerhedssårbarheder for at øge brugersikkerheden. Politikken indeholder følgende retningslinjer:

- Giv os en detaljeret beskrivelse af sikkerhedsproblemet.
- Vis respekt for vores eksisterende applikationer. Spamming af formularer gennem automatiserede sårbarhedsscannere vil ikke resultere i nogen form for belønning eller tildeling, da disse eksplicit er uden for anvendelsesområdet.
- Giv os rimelig tid til at reagere på problemet, før du offentliggør oplysninger om sikkerhedsproblemet.
- Undlad at få adgang til eller ændre brugerdata uden tilladelse fra kontoens ejer.
- Dataene må ikke vises, ændres, gemmes, lagres, overføres eller på anden måde tilgås, og lokal information skal straks slettes, når du rapporterer sårbarheden til Dropbox.
- Handl i god tro for at undgå at krænke beskyttelse af personlige oplysninger eller afbrydelse eller forringelse af vores tjenester (herunder denial of service-angreb)

Problemer kan rapporteres til Bugcrowd på: bugcrowd.com/dropbox.

Fysisk sikkerhed

Infrastruktur

Fysisk adgang til underleverandørers faciliteter, hvor produktionssystemerne findes, er begrænset til personale, som Dropbox har godkendt, i det omfang det er nødvendigt for at udføre deres jobfunktion. Alle personer, der skal have yderligere adgang til produktionsmiljøets faciliteter, opnår denne adgang ved hjælp af udtrykkelig godkendelse fra den relevante ledelse.

Registrering af anmodningen om adgang, grunden til dette og godkendelsen heraf udføres af ledelsen, og de relevante personer giver adgang. Når godkendelsen er modtaget, vil et godkendt medlem af infrastrukturteamet kontakte den relevante underleverandør for at anmode om, at den godkendte person får adgang. Den eksterne leverandør indtaster brugerens oplysninger i sit eget system og giver det godkendte Dropbox-personale adgang ved hjælp af et adgangskort og biometrisk scanning (hvis det er muligt). Når godkendte personer har fået adgang, er det datacenterets opgave at sørge for, at det kun er godkendte personer, der har adgang.

Kontorer i store virksomheder

- ***Fysisk sikkerhed***

  Dropbox' team for fysisk sikkerhed har ansvaret for at håndhæve politikken for fysisk sikkerhed og føre tilsyn med sikkerheden på vores kontorer.

- ***Politik for besøgende og adgang***

  Politik for besøgende og adgang. Fysisk adgang til virksomhedens faciliteter udover offentlige indgange og forhaller er begrænset til autoriseret Dropbox-personale og registrerede besøgende, som er ledsaget af Dropbox-personale. Et adgangssystem med adgangskort sørger for, at kun godkendte personer har adgang til områder i virksomhedens faciliteter, hvor der er adgang forbudt.

- ***Serveradgang***

  Adgang til områder, hvor virksomhedens servere befinder sig, såsom serverrum, er begrænset til autoriseret personale gennem ophøjede roller, der gives i systemet med adgangskort. Listerne over autoriserede personer, der er godkendt til fysisk adgang til virksomheds- og produktionsmiljøer, gennemgås som minimum hvert kvartal.

Reaktion på hændelser

Vi har politikker for reaktion på hændelser og procedurer for håndteringen af problemer med tjenestens tilgængelighed, integritet, sikkerhed, beskyttelse af persondata og fortrolighed. Som en del af vores procedurer for reaktion på hændelser har vi dedikerede teams, der er uddannet til at:

- Reagere omgående på advarsler om potentielle hændelser.
- Bestemme, hvor alvorlig hændelsen er.
- Om nødvendigt udføre handlinger for at afhjælpe og begrænse problemer.

- Kommuniker med relevante interne og eksterne interessenter, f.eks. ved at sende meddelelser til berørte kunder, for at overholde kontraktmæssige forpligtelser samt relevante love og bestemmelser vedrørende underretning om misligholdelse eller andre hændelser.
- Indsamle og opbevare beviser som led i en efterforskning.
- Dokumentere det arbejde, der foretages efter en sikkerhedsbrist, og udarbejd en permanent prioriteringsplan.

Politikker og processer for hændelsessvar revideres som en del af vores SOC 2, ISO/IEC 27001 og andre sikkerhedsvurderinger.

Sikkerhed for infrastruktur

Netværkssikkerhed

Hos Dropbox sørger vi altid for at opretholde sikkerheden i vores basale netværk. Vores teknikker til netværkssikkerhed og -overvågning er udviklet til at levere adskillige lag af beskyttelse og forsvar. Vi anvender branchens standardteknikker til beskyttelse, herunder firewalls, scanning efter netværkssårbarheder, overvågning af netværkssikkerhed og systemer til registrering af indtrængen, for at sikre, at kun berettiget trafik er i stand til at nå vores infrastruktur.

Vores interne private netværk er segmenteret efter brug og risikoniveau. De primære netværk er:

- Internet-DMZ
- Prioritetsinfrastruktur-DMZ
- Produktionsnetværk
- Virksomhedsnetværk

Adgang til produktionsmiljøet er begrænset til autoriserede IP-adresser og kræver multifaktorgodkendelse for alle slutpunkter. IP-adresser med adgang er tilknyttet virksomhedsnetværket eller godkendt Dropbox-personale. Autoriserede IP-adresser gennemgås hvert kvartal for at sikre et sikkert produktionsmiljø. Adgang til ændring af listen over IP-adresser er begrænset til autoriserede personer.

Trafik fra internettet, der er rettet mod vores produktionsnetværk, beskyttes med flere lag, der består af firewalls og proxyer.

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 firewallregler.

Dropbox anvender sofistikerede værktøjssæt til at overvåge både bærbare og stationære computere med Mac- og Windows-operativsystemer og produktionssystemer for ondsindede hændelser. Sikkerhedslogs samles ét centralt sted til reaktion på og analyse af hændelser iht. branchestandarden for opbevaringspolitik.

Dropbox identificerer og reducerer risici via regelmæssig afprøvning af netværkssikkerheden og kontroller, der foretages af dedikerede interne sikkerhedsteams og eksterne sikkerhedseksperter.

Tilstedeværelsespunkter (PoP'er)

For at give brugerne den bedst mulige oplevelse med webstedet benytter Dropbox tredjepartsnetværk til levering af indhold (CDN'er) og Dropbox-hostede tilstedeværelsespunkter (PoP'er) på 31 steder i verden. Ingen brugerdata cachelagres i disse områder, og alle brugerdata, der overføres, krypteres med SSL/TLS. Fysisk og logisk adgang til Dropbox-hostede PoP'er begrænses til kun at omfatte personale, der er godkendt af Dropbox. Dropbox optimerer både transportlaget (TCP) og applikationslaget (HTTP).

Peering

Dropbox har en åben peering-politik, og alle kunder er velkommen til at udføre peering med os. Der er flere oplysninger på dropbox.com/peering.

Driftssikkerhed

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.

Filmetadata

Ekstra kopier af metadata fordeles på tværs af uafhængige enheder i et datacenter i mindst en N+2-tilgængelighedsmodel. Der udføres inkrementelle sikkerhedskopier mindst en gang i timen, og der tages komplette sikkerhedskopier hver 36. time. Metadata gemmes på servere, der hostes og administreres af Dropbox i USA.

Filblokke

Ekstra kopier af filblokke lagres uafhængigt i mindst to separate geografiske regioner og kopieres pålideligt inden for hver region. (**Bemærk:** For kunder, som vælger at have deres files lagret i vores tyske, australske, japanske eller britiske infrastruktur, kopieres filblokke kun inden for deres respektive regioner. For yderligere oplysninger se afsnittet Datacentre og udbydere af administrerede tjenester nedenfor.) Både Magic Pocket og AWS er beregnet til at levere en årlig datavarighed på mindst 99,999999999%.

Dropbox' arkitektur, applikationer og synkroniseringsmekanismer arbejder sammen om at beskytte brugerdata og gøre dem vidt tilgængelige. I det sjældne tilfælde at der skulle opstå problemer med tjenestens tilgængelighed, vil Dropbox-brugere stadig have adgang til de senest synkroniserede kopier af 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, driftsstop eller manglende internetforbindelse. Ændringer af filer og mapper synkroniseres til Dropbox, når der igen er adgang til tjenesten eller netværket.

Paper-dokumenter

Ekstra kopier af Paper-dokumentdata fordeles på tværs af uafhængige enheder i et datacenter i en N+1-tilgængelighedsmodel. Der tages også komplette sikkerhedskopier af Paper-dokumentdata hver dag. Til lagring af Paper-dokumenter bruger Dropbox AWS-infrastruktur i USA, som er designet til at give 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.

Filsynkronisering

Dropbox har den bedste filsynkronisering, som er anerkendt i resten af branchen. Vores synkroniseringsmekanismer giver hurtige, responsive filoverførsler og mulighed for adgang til data på tværs af enheder overalt. Dropbox-synkronisering er også modstandsdygtig. Hvis forbindelsen til Dropbox-tjenesten afbrydes, genoptager en klient hurtigt handlingen, så snart forbindelsen genoprettes. Filerne opdateres kun på den lokale klient, hvis de er synkroniseret fuldstændigt og valideret med Dropbox-tjenesten. Belastningsudjævning på tværs af flere servere sikrer redundans samt en ensartet synkroniseringsoplevelse for slutbrugerne.

Deltasynkronisering

Hvis man bruger denne synkroniseringsmetode, bliver kun ændrede dele af filer downloadet eller uploadet. Dropbox gemmer hver fil i separate, krypterede blokke og opdaterer kun de blokke, der er ændret.

Streamingsynkronisering

I stedet for at vente på at en filupload afsluttes, begynder streamingsynkroniseringen at downloade synkroniserede blokke til en anden enhed, før upload af alle blokkene fra den første enhed er afsluttet. Denne metode bruges automatisk, hvis separate computere forbindes til den samme Dropbox-konto eller når forskellige Dropbox-konti deler en mappe.

Sparer plads på harddisken

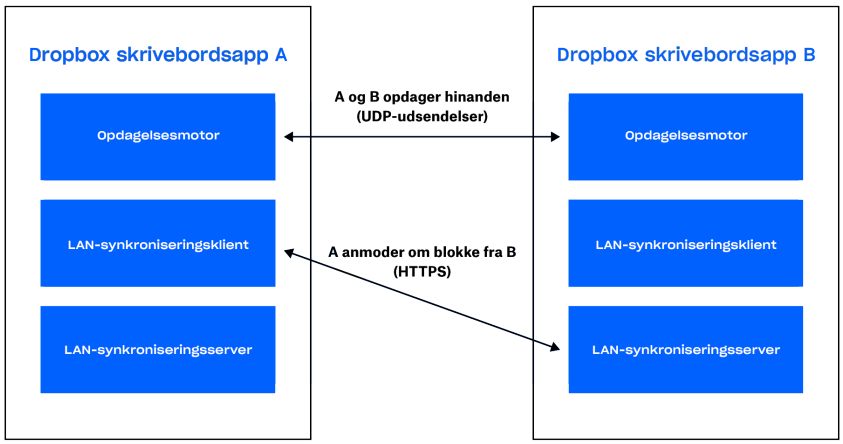
Brugere kan frigøre lagerplads på deres computere ved kun at gøre filer, de vil bruge på deres harddisk, tilgængelige offline. Dette giver mere plads på computeren, fordi alt det andet ligger online på dropbox.com.

LAN-synkronisering

Når denne funktion aktiveres, henter den nye og opdaterede filer fra andre computere på det samme lokale netværk (LAN), hvilket sparer tid og båndbredde i forhold til at downloade filerne fra Dropbox-servere.

Arkitektur

Der findes tre hovedkomponenter i LAN-synkroniseringssystemet, som kører på applikationen til stationære pc'er: søgeprogrammet, serveren og klienten. Søgeprogrammet finder enheder på netværket, som der kan synkroniseres med. Dette begrænses til enheder, som har godkendt adgang til de samme personlige eller delte Dropbox-mapper. Serveren håndterer anmodninger fra andre enheder på netværket og henter de filblokke, der anmodes om. Klienten anmoder om filblokke fra netværket.



Søgeprogram

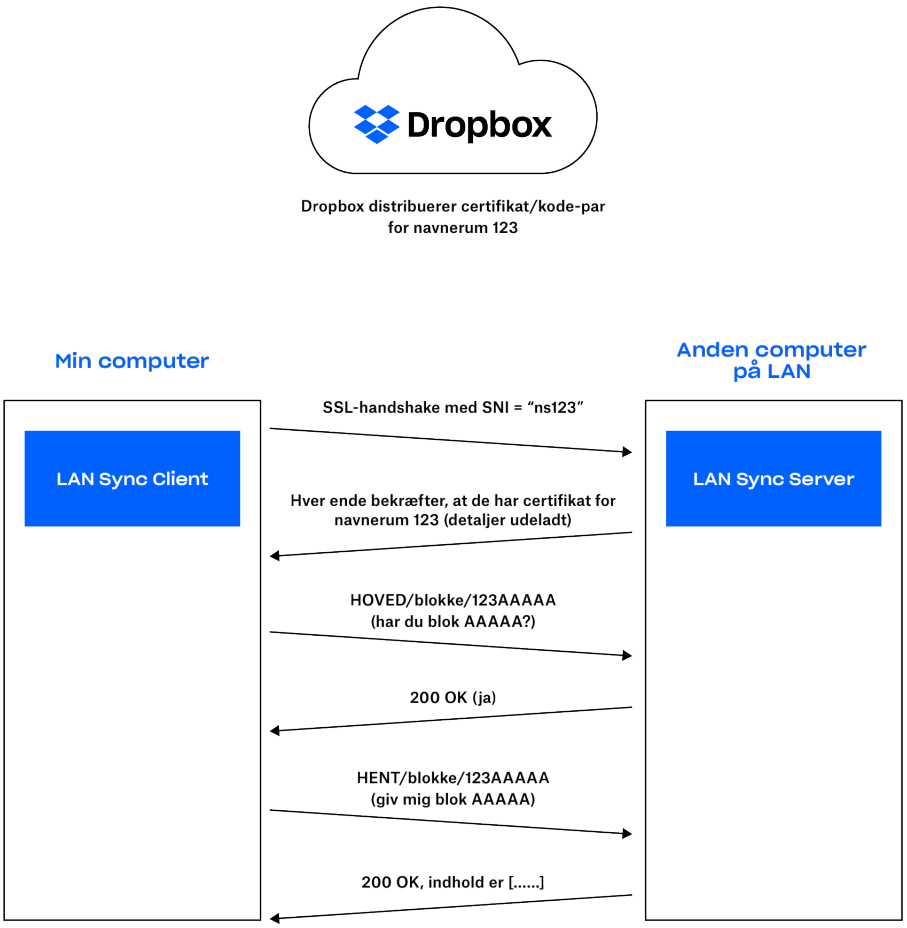
Hver enkelt enhed i det lokale netværk sender og lytter efter UDP-signalpakker via port 17500 (som reserveres af IANA til LAN-synkronisering). Disse pakker indeholder versionen af den protokol, der bruges af den pågældende computer, de personlige og delte Dropbox-mapper, der understøttes, den TCP-port, der bruges til at køre serveren (som kan være en anden end 17500, hvis den pågældende port ikke er tilgængelig) og en tilfældig identifikator til enheden. Når en pakke opdages, føjes enhedens IP-adresse til en liste for hver personlige eller delte mappe for at angive en potentiel destination.

Protokol

Selve overførslen af filblokke udføres via HTTPS. Hver enkelt computer kører en HTTPS-server med slutpunkter. En klient vil polle flere peers for at se, om de har blokkene, men downloader kun blokke fra en enkelt server.

For at beskytte alle dine data sørger vi for, at det kun er de klienter, som har adgang til en bestemt mappe, der kan anmode om filblokke. Vi sørger også for, at computere ikke kan udgive sig for at være servere til mapper, som de ikke har kontrol over. For at løse dette genererer vi SSL-nøgle-/-certifikatpar for hver enkelt personlige Dropbox-mappe eller delte mappe. Disse fordeles fra Dropbox-servere til de af brugerens computere, som har adgang til mappen. Nøgle-/certifikatparrene udskiftes, hver gang et medlemskab ændres (f.eks. når en person fjernes fra en delt mappe). Vi bruger begge ender af HTTPS-forbindelsen til at godkende ved hjælp af det samme certifikat (certifikatet for Dropbox-mappen eller den delte mappe). Dette beviser, at begge ender af forbindelsen har tilladelse.

Når vi opretter en forbindelse, fortæller vi serveren, hvilke personlige Dropbox-mapper eller mapper, vi forsøger at oprette forbindelse til, ved hjælp af Server Name Indication (SNI), så serveren bruger det korrekte certifikat.



Server/klient

Med den førnævnte protokol skal serveren blot vide, hvilke blokke der er til stede, og hvor de findes.

Ved hjælp af søgeprogrammets resultater opretholder klienten en liste over peers for hver enkelt personlige Dropbox-mappe eller delte mappe. Når LAN-synkroniseringssystemet modtager en anmodning om at hente en filblok, sender det en anmodning til et tilfældigt eksempel på de peers, som det har søgt efter for den personlige Dropbox-mappe eller delte mappe, og derefter anmoder det om blokken fra den første, der svarer, at den har blokken.

For at undgå forsinkelser benytter vi forbindelsespuljer, der gør det muligt at genanvende forbindelser, som allerede er oprettet. Vi åbner først en forbindelse, når det er nødvendigt, og når den er åbnet, holder vi den i gang, hvis vi skulle få brug for at benytte den igen. Vi begrænser også antallet af forbindelser til en enkelt peer.

Hvis en filblok ikke kan findes eller hentes, eller hvis forbindelsen er for langsom, henter systemet i stedet blokken fra Dropbox-servere.

Datacentre og leverandører af administrerede tjenester

Dropbox' erhvervs- og produktionssystemer drives fra eksterne underleverandørers datacentre og leverandører af administrerede tjenester med adresse forskellige steder i USA. SOC-rapporter for underleverandørers datacentre og/eller leverandørernes sikkerhedsspørgeskemaer og kontraktlige forpligtelser gennemgås mindst én gang om året for at sikre tilstrækkelig sikkerhedskontrol. Disse eksterne tjenesteudbydere er ansvarlige for de fysiske, omgivelsesmæssige og driftsmæssige sikkerhedskontroller ved Dropbox-infrastrukturens begrænsninger. Dropbox er ansvarlig for den logiske, netværksmæssige og applikationsmæssige sikkerhed i vores infrastruktur, der drives fra tredjeparters datacentre.

Vores leverandør af administrerede tjenester til behandling og lagring, Amazon Web Services (AWS), er ansvarlig for den logiske og netværksmæssige sikkerhed i Dropbox' tjenester, som leveres via deres infrastruktur. Forbindelser beskyttes ved hjælp af deres firewall, der konfigureres i en standardtilstand, hvor alt afvises. Dropbox begrænser adgangen til miljøet til et begrænset antal IP-adresser og medarbejdere.

Infrastruktur i Tyskland, Australien, Japan og Storbritannien

Dropbox tilbyder kvalificerede kunder lagring af filblokke i regioner udenfor USA. Vores infrastruktur hostes af Amazon Web Services (AWS) i Tyskland, Australien, Japan og Storbritannien og kopieres i den respektive region for at sikre redundans og beskytte mod datatab. Filmetadata lagres i USA på Dropbox' egne servere. Paper-dokumenter og -forhåndsvisninger lagres i USA for alle kunder.

Virksomhedskontinuitet

Dropbox har etableret et system til håndtering af virksomhedsdrift (BCMS), der skal løse problemet med at genoptage eller fortsætte med at tilbyde tjenester til brugere (og hvordan man kan fungere som en virksomhed), hvis virksomhedskritiske processer og aktiviteter afbrydes. Vi udfører en cyklisk proces, som består af følgende faser:

- ***Vurderinger af virksomhedskonsekvenser og risiko***

  Vi udfører en vurdering af virksomhedskonsekvenser (BIA) mindst én gang om året for at finde ud af, hvilke processer der er vigtige for Dropbox, vurdere de mulige konsekvenser ved afbrydelser, etablere prioriterede tidsfrister for gendannelse og identificere vigtige elementer, som vi er afhængige af, og leverandører. Vi udfører også risikovurdering i hele virksomheden mindst én gang årligt. Risikovurderingen hjælper os med systematisk at identificere, analysere og evaluere risikoen ved afbrydelser af Dropbox. Risikovurderingen og BIA er med til at fremhæve prioriteter i forbindelse med kontinuitet samt afhjælpnings- og gendannelsesstrategier for planer til at sikre virksomhedskontinuitet (BCP'er).

- ***Virksomhedskontinuitetsplaner***

  Teams, der ifølge BIA er kritiske for Dropbox' kontinuitet, bruger denne platform til at udvikle BCP'er for deres kritiske processer. Disse planer viser teams, hvem der er ansvarlig for at genoptage processer i nødstilfælde, hvem der i en anden Dropbox-afdeling kan overtage deres processer i tilfælde af en afbrydelse, og hvilke kommunikationsmetoder der skal bruges i tilfælde af afbrudt kontinuitet. Disse planer hjælper os også med at forberede os på en afbrydelse ved at centralisere vores gendannelsesplaner og andre vigtige oplysninger, f.eks. hvornår og hvordan planen skal bruges, kontakt- og mødeoplysninger, vigtige apps og gendannelsesstrategier. Dropbox' kontinuitetsplaner er en del af vores krisehåndteringsplan for hele virksomheden (CMP), der angiver Dropbox' krisehåndterings- og problemløsningsteams.

- ***Test/udøvelse af plan***

  Dropbox tester udvalgte elementer i sine virksomhedskontinuitetsplaner mindst én gang om året. Disse tests er i overensstemmelse med BCMS' omfang og målsætninger, de er baserede på relevante scenarier, og de er

gennemtænkte med tydeligt definerede målsætninger. Omfanget for disse tests kan være alt lige fra gruppeøvelser til omfattende simuleringer af virkelige begivenheder. Ved hjælp af resultaterne af testen og erfaring fra virkelige hændelser kan teams opdatere og forbedre deres planer for at afhjælpe problemer og blive bedre til at reagere på hændelser.

- ***Gennemgang og godkendelse af BCMS***

  Mindst én gang om året gennemgår vores ledelse BCMS som en del af gennemgangen af Dropbox' tillidsprogram.

Katastrofegenoprettelse

For at leve op til kravene om sikkerhed i tilfælde af en voldsom krise eller et nedbrud, der påvirker driften af Dropbox til virksomheder, følger vi altid en plan for gendannelse efter nedbrud. Dropbox' tekniske team gennemgår denne plan årligt og tester udvalgte elementer mindst én gang om året. Relevante problemstillinger dokumenteres og følges nøje, indtil de er løst.

Vores plan for gendannelse efter nedbrud (DRP) omfatter både holdbarheds- og tilgængelighedsnedbrud, der er defineret på følgende måder:

- Et holdbarhedsnedbrud består af en eller flere af følgende:
  - Et fuldstændigt eller permanent tab af et primært datacenter, hvor metadata gemmes, eller af flere datacentre, hvor filblokke opbevares.
  - Mistet evne til at kommunikere eller hente data fra et datacenter, hvor metadata opbevares, eller fra flere datacentre, hvor filindhold opbevares.
- Et tilgængelighedsnedbrud omfatter et eller flere af følgende:
  - Et nedbrud, der varer mere end 10 dage.
  - Manglende evne til at kommunikere eller hente data fra en lagertjeneste eller et datacenter, hvor metadata opbevares, eller fra flere lagertjenester eller datacentre, hvor filindhold opbevares.

Vi definerer et Recovery Time Objective (RTO), som er den tid, det tager at genoprette forretningsprocesser og tjenester til et bestemt serviceniveau efter en katastrofe, og et Recovery Point Objective (RPO), som er den længste acceptable periode, hvor data kan være mistet efter en afbrydelse af tjenesten. Vi måler også Recovery Time Actual (RTA) under testen af katastrofegenoprettelsen, som udføres mindst en gang om året.

Dropbox' planer for reaktion på hændelser, virksomhedskontinuitet og genoprettelse efter nedbrud testes i planlagte intervaller og efter betydelige organisatoriske og miljømæssige ændringer.

Programsikkerhed

Dropbox' brugergrænseflader

Dropbox-tjenesten kan udnyttes og tilgås via en række grænseflader. Hver enkelt grænseflade har sikkerhedsindstillinger og funktioner, der behandler og beskytter brugerdata og samtidig gør det let at få adgang.

- ***WEB***

  Denne grænseflade kan åbnes i alle moderne webbrowsere. Den giver brugere mulighed for at uploade, downloade, se og dele deres filer. Webgrænsefladen giver også brugere mulighed for at åbne eksisterende lokale versioner af filer via deres computers standardprogram.

- ***Computer***

  Dropbox' program til computere er en effektiv synkroniseringsklient, som opbevarer filer lokalt med henblik på offlineadgang. Den giver brugere fuld adgang til deres Dropbox-konti og kører på operativsystemerne Windows og Mac. Filer kan ses og deles direkte i operativsystemernes respektive filbrowsere.

- ***Mobil***

  Dropbox-appen kan fås til iOS- og Android-enheder og giver brugere adgang til alle deres filer, når de er på farten. Mobilappen giver også brugerne mulighed for at gøre filer tilgængelige til offlineadgang.

- ***API***

  Dropbox-API'er giver en fleksibel metode til at læse og skrive til Dropbox-brugerkonti og til at få adgang til avancerede funktioner såsom søgning, revideringer og gendannelse af filer. API'erne kan bruges til at administrere brugerlivscyklussen for en Dropbox til virksomheder-konto, udføre handlinger for alle medlemmer af teamet og give adgang til administratorfunktioner i Dropbox til virksomheder.

Brugergrænseflader i Paper

Du kan bruge og få adgang til Paper-tjenesten via en række grænseflader. Hver enkelt grænseflade har sikkerhedsindstillinger og funktioner, der behandler og beskytter brugerdata og samtidig gør det let at få adgang.

- ***WEB***

  Denne grænseflade kan åbnes i alle moderne webbrowsere. Den giver brugerne mulighed for at oprette, se, redigere, downloade og dele deres Paper-dokumenter.

- ***Mobil***

  Paper-mobilapplikationen er tilgængelig til iOS- og Android-mobilenheder og tablets, så brugerne kan få adgang til alle deres Paper-dokumenter, når de er på farten. Mobilapplikationen er oprettet som en hybridapplikation, der består af oprindelig kode (iOS eller Android), som er bygget omkring en intern webbrowser.

- ***API***

  Dropbox API'en, som er beskrevet ovenfor, omfatter slutpunkter og datatyper til administration af dokumenter og mapper i Dropbox Paper, herunder understøttelse af funktioner som f.eks. administration af tilladelser, arkivering og permanent sletning.

Kryptering

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".

Bemærk: Dropbox benytter udelukkende TLS og har udfaset brugen af SSLv3 på grund af kendte sårbarheder. Men TLS kaldes ofte for "SSL/TLS", så vi bruger denne betegnelse her.

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 filer eller Paper-dokumenter, for udføre sikker levering til Dropbox' frontend-servere.

Data under opbevaring

Dropbox-filer, som brugerne uploader, krypteres i hvile vha. 256-bit Advanced Encryption Standard-kryptering (AES). Filer gemmes på flere datacentre i diskrete filblokke. 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.

Nøgleadministration

Dropbox' infrastruktur til nøgleadministration er udviklet med driftsmæssig, teknisk og proceduremæssig sikkerhedskontrol med meget begrænset direkte adgang til nøgler. Generering, udveksling og opbevaring af krypteringsnøgler fordeles med henblik på decentraliseret behandling.

- ***Filkrypteringsnøgler***

  Dropbox er designet til at administrere filkrypteringsnøgler på brugernes vegne for at fjerne kompleksiteten og muliggøre avancerede produktfunktioner og stærk kryptografisk kontrol. Filkrypteringsnøgler oprettes, lagres og beskyttes af sikkerhedskontroller og sikkerhedspolitikker i produktionssystemets infrastruktur.

- ***Interne SSH-nøgler***

  Adgang til produktionssystemer er begrænset med unikke SSH-nøglepar. Sikkerhedspolitikker og -procedurer kræver beskyttelse vha. SSH-nøgler. Et internt system administrerer den sikre offentlige nøgleudvekslingsproces, og private nøgler opbevares sikkert. Interne SSH-nøgler kan ikke bruges til at få adgang til produktionssystemer uden en separat anden godkendelsesfaktor.

- ***Nøgledistribution***

  Dropbox automatiserer administrationen og distributionen af følsomme nøgler til systemer, der er påkrævede for handlinger.

Certifikat-pinning

Dropbox udfører certifikat-pinning i moderne browsere, der understøtter HTTP Public Key Pinning-specifikationen, og på vores klienter til mobilenheder og stationære computere. Certifikat-pinning er en ekstra kontrol, der sikrer, at den tjeneste, du opretter forbindelse til, er den, du forventer, og ikke er et forsøg på svindel. Vi bruger det til at beskytte dig mod andre metoder, som dygtige hackere kan bruge til at udspionere din aktivitet.

Beskyttelse af godkendelsesdata

Dropbox bruger mere end almindelig hashing til at beskytte brugernes logonoplysninger. I henhold til retningslinjerne i branchen "saltes" hver enkelt adgangskode med tilfældigt genereret "salt", som er unikt for hver bruger, og vi bruger gentagen hashing til at gøre beregningen langsommere. Disse metoder er med til at beskytte mod voldsomme forsøg på indtrængen, ordbogs- og regnbueangreb. Som en ekstra foranstaltning krypterer vi hashene med en nøgle, der gemmes et andet sted end i databasen, hvilket er med til at beskytte adgangskoder i tilfælde af, at det kun er databasen, der kompromitteres.

Malware-scanning

Vi har udviklet et automatiseret system, der scanner for malware på det tidspunkt, hvor indhold deles uden for den oprindelige brugers konto. Systemet udnytter både vores egen teknologi og detekteringssystemer af branchestandard og er designet til at forhindre spredning af malware.

Produktsikkerhed

Dropbox indeholder funktioner til administrativ kontrol og synlighed, som gør det muligt for både it-teams og slutbrugere at administrere og sikre data på en effektiv måde. Med Dropbox får du alt, hvad du har brug for til arbejdet – dine værktøjer, indhold og samarbejdspartnere – alt på ét sted. Dropbox er mere end sikker opbevaring – det er en smart, problemfri måde at optimere din eksisterende arbejdsgang på.

Nedenfor vises nogle højdepunkter blandt de funktioner, der er tilgængelige for administratorer og brugere, samt nogle tredjepartsintegrationer til administration af vigtige it-processer.

Bemærk: Tilgængeligheden af funktioner afhænger af abonnementet. Se dropbox.com/business/plans for yderligere information.

Indholdskontrol

Beskyttelse af følsomme forretningsaktiver – som intellektuel ejendomsret og personlig identificerbar information (PII) – er afgørende for it og datasikkerhedsteams. Fra niveauinddelte indholdstilladelser til politikker for opbevaring af data og juridisk fastfrysning giver Dropbox brancheførende løsninger til at administrere, overvåge og beskytte dit indhold. Nedenfor er de vigtigste Dropbox-produkter og funktioner, der understøtter indholdskontrol.

Detaljerede tilladelser til indhold og til filer og mapper

- ***Tilladelser til delte filer***

  Et teammedlem, der ejer en delt fil, kan fjerne bestemte brugeres adgang og deaktivere kommentarer til filen.

- ***Tilladelser til delte filer***

  Et teammedlem, der ejer en delt mappe, kan fjerne bestemte brugeres adgang til mappen, ændre visnings-/rediger-tilladelser for bestemte brugere og overføre mappeejerskab. Alt efter teamets globale delingstilladelser kan hver enkelt delt mappes ejer også bestemme, om den kan deles med ikke-teammedlemmer, om andre med tilladelse til redigering kan administrere medlemskab, og om links kan deles med personer uden tilknytning til mappen.

- ***Adgangskoder til delte links***

  Ethvert delt link kan beskyttes med en adgangskode, som vælges af ejeren. Før filer eller data overføres, bekræfter et lag til adgangskontrol, at den rigtige adgangskode er indtastet, og at alle øvrige krav (f.eks. team, gruppe eller mappe-ACL) er overholdt. Hvis dette er tilfældet, gemmes en sikker cookie i brugerens browser. Denne cookie husker, at adgangskoden tidligere er bekræftet. Med delingsfunktioner kan administratorer også indstille standardadgangskoder i stedet for at have dem som valgfri for bedre at beskytte deres teams indhold.

- ***Udløbsdatoer for delte links***

  Brugere kan angive en udløbsdato for alle delte links for at give midlertidig adgang til filer eller mapper. Med delingsfunktioner kan administratorer også indstille standardudløbsdatoer i stedet for at have dem som valgfri for bedre at beskytte deres teams indhold.

Tilladelser til Paper-dokument og delt Paper-mappe

- ***Tilladelser til Paper-dokumenter og delte Paper-mapper***

  Et teammedlem, der ejer et Paper-dokument eller en delt Paper-mappe, kan fjerne bestemte brugeres adgang og deaktivere redigering af Paper-dokumentet.

- ***Tilladelser til Paper-dokumenter***

  Et teammedlem, der ejer et Paper-dokument, kan fjerne adgangen for bestemte brugere, som eksplicit er angivet i delingspanelet. Både ejeren og redaktørerne for et Paper-dokument kan ændre visnings- og redigeringstilladelser for bestemte brugere samt ændre dokumentets linkpolitik. Linkpolitikken bestemmer, hvilke brugere der kan åbne dokumentet, samt deres tilladelser. Teamadministratoren kan angive politikker for dokumentdeling, der gælder for hele teamet.

- ***Tilladelser til Paper-mapper***

  Et teammedlem, der er medlem af mappen, kan dele mappens delingspolitik og fjerne adgangen for bestemte brugere, som var tilføjet specifikt til mappen.

Fil- og mappe-handlinger

- ***Teammapper til filer***

  Administratorer kan oprette teammapper, der automatisk giver grupper og andre kollegaer det rette adgangsniveau (se eller redigere) til det relevante indhold.

- ***Niveauinddelt adgang og delingskontroller***

  Med delingsfunktioner kan administratorer styre medlemskaber og tilladelser på det øverste niveau eller undermappeniveau, så personer i og uden for virksomheden udelukkende har adgang til de specifikke mapper, de har brug for.

- ***Administratorfunktion til teammappe***

  Administratorer kan få vist alle deres teammapper og tilpasse delingspolitikker fra en central placering for at forhindre deling af fortroligt materiale ved en fejltagelse.

- ***Delte mapper til Paper-dokumenter***

  Administratorer kan oprette delte Paper-mapper, der automatisk giver andre samarbejdspartnere det rette adgangsniveau – kommentering eller redigering – til det indhold, de har brug for.

- ***Fjernsletning***

  Når medarbejdere forlader teamet, eller hvis en enhed går tabt, kan administratorer fjernslette Dropbox-data og lokale kopier af filer. Filerne fjernes både fra computere og mobilenheder, næste gang de er online, og Dropbox-programmet kører.

- ***Kontooverførsel***

  Efter at have fjernet en bruger (enten manuelt eller via adresselister) kan administratorer overføre filer og ejerskab til Paper-dokumenter, som det tidligere teammedlem har oprettet, fra brugerens konto til en anden bruger på teamet. Funktionen til kontooverførsel kan bruges, når en bruger fjernes, eller på ethvert tidspunkt efter sletningen af en brugers konto.

De følgende funktioner er tilgængelige som tilføjelsesprogrammer (kontakt vores salgsafdeling for mere information).

- ***Scan indhold***

  Med tilføjelsen Advanced Team og Content Controls kan Dropbox til virksomheder Advanced- og Enterprise-kunder scanne efter nyt og eksisterende indhold i Dropbox for at lokalisere og undgå datasårbarheder.

- ***Konfigurer og udløs tilpassede arbejdsgange***

  Med tilføjelsen Advanced Team og Content Controls kan administratorer foretage handlinger, der kan tilpasses mod filer, der overtræder virksomhedens politikker.

- ***Indstil advarsler***

  Administratorer kan overvåge sikkerhedsproblemer i realtid og undgå datasårbarheder. Få advarsler om filer, der deles eksternt, og få følsomme data scannet.

Indholdssynlighed

Sikkerhedsadvarsler og -meddelelser

Administratorer på Dropbox Enterprise kan modtage meddelelser i realtid, når misbrugsrelateret aktivitet, risikabel aktivitet eller potentielle datalækager opdages på deres konti. Følgende hændelser kan overvåges:

- Massesletninger
- Masseflytninger af data
- Følsomt indhold, der deles eksternt
- Malware delt uden for dit team
- Malware, der deles i dit team
- For mange fejlslagne loginforsøg
- Login fra et højrisikoland
- Registrering af ransomware

Dropbox gav også mulighed for at konfigurere advarselsgrænser, justere underretningsmodtagere og udløse advarsler, når mapper med følsomme filer deles eksternt. Administratorer kan også markere advarsler som under gennemgang, løst eller afvist. Derudover viser en dashboard-widget overordnet indsigt og tendenser for teamalarmer for den sidste uge.

Rapport og side om ekstern deling

Dropbox giver ekstra synlighed med ekstern delingsrapport og -side. Administratorer kan oprette en rapport enten fra indsigtssiden eller den eksterne delingsside. Rapporten viser alle teamets filer og mapper, der deles uden for deres team, og alle delte links. Siden om ekstern deling er en ekstra side i administrationskonsollen, der giver administratorer mulighed for at se og filtrere gennem de filer og mapper, der blev delt direkte ud af teamet og delte links, f.eks. filtype, hvem der har delt, linkindstillinger o.m.m.

Delingsfunktioner

Delingsindstillinger giver teamadministratorer mere kontrol over delingen og adgang til deres teams indhold. Administratorer kan angive standardudløb på teamniveau, adgangsbegrænsninger eller begge dele. Disse begrænsninger reducerer risikoen for datatab ved at fjerne brugerens ansvar for at angive begrænsninger.

Dataklassificering

Teams på Dropbox Enterprise kan have personlige og følsomme data automatisk mærket for bedre at beskytte dem. Administratorer modtager advarsler om forebyggelse af datatab (DLP) via e-mail og i administrationskonsollen, når filer eller mapper, der er gemt i teammapper, der indeholder følsomme oplysninger, deles uden for deres team. Administratorer har mulighed for automatisk at identificere og klassificere følsomme data, der er gemt i delte mapper og teammedlemmers personlige mapper. Dropbox Enterprise-administratorer kan aktivere automatisk dataklassificering fra administrationskonsollen.

Tilføjelsesprogram til dataforvaltning

Dataforvaltning er det overordnede sæt processer, teknologier og teams, der går sammen om at styre og beskytte en organisations dataaktiver. Dette inkluderer muligheden for at gemme, identificere, opdage og hente virksomhedsdata efter behov.

Dropbox' tilføjelsesprogram til dataforvaltning samler et sæt funktioner, der giver organisationer mulighed for bedre at kontrollere og sikre deres data, samtidig med at de reducerer risici og omkostninger forbundet med at opfylde lovgivnings- og compliance-behov. I øjeblikket indeholder dette tilføjelsesprogram fire nøglefunktioner til teamadministratorer og compliance-administratorer.

- ***Udvidet versionshistorik***

  Din standard filversionshistorik afhænger af typen af din Dropbox-konto. Med Dropbox til virksomheder kan du dog købe en udvidet versionshistorik (EVH) særskilt eller som del af tilføjelsesprogrammet til dataforvaltning, der gør det muligt at gendanne filer, der er slettet eller ændret inden for de sidste 10 år.

- ***Juridiske fastfrysninger***

  Ved at placere en juridisk fastfrysning på et teammedlem, kan team- og compliance-administratorer se og eksportere indhold, der er oprettet eller ændret af det pågældende medlem. Medlemmer, der er berørt af en juridisk fastfrysning, får ikke besked om tilbageholdelsen og bevarer deres tilladelser til at oprette, redigere og slette filer.

- ***Dataopbevaring***

  Datalagring gør det muligt for teams og compliance-administratorer at forhindre utilsigtet sletning af indhold, der er påkrævet i henhold til reglerne, at blive tilbageholdt i en fastlagt periode. Denne funktion gør det muligt for kunder at bevare data i de sidste 10 år fra den seneste "revisionsdato".

- ***Dataforældelse***

  Datadisponering gør det muligt for team- og compliance-administratorer at slette data permanent på en bestemt dato for at overholde krav for dataopbevaring og disponering. Administratorer kan overvåge aktivitet ved at modtage rapporter, der advarer dem om kommende sletninger af filer.

Gendannelse og versionskontrol

Dropbox til virksomheder-kunder kan gendanne mistede filer og Paper-dokumenter og gendanne tidligere versioner af filer og Paper-dokumenter, så ændringer i vigtige data kan spores og hentes.

Datasikkerhed på mobile enheder

- ***Slet data***

  For at styrke sikkerheden har brugeren mulighed for at slette alle Dropbox-data fra enheden efter 10 mislykkede forsøg på at indtaste adgangskoden.

- ***Internt lager og offlinefiler***

  Som standard gemmes filer ikke i mobilenheders interne lagerplads. I Dropbox' mobilklienter er det muligt at gemme individuelle filer og mapper på enheden, så de kan ses offline. Når en enheds forbindelse til en Dropbox-konto afbrydes, enten via mobil- eller webgrænsefladen, slettes disse filer og mapper automatisk fra enhedens interne lagerplads.

- ***Offline Paper-dokumenter***

  Når en enheds forbindelse til Paper afbrydes via Dropbox-kontoens sikkerhedsside, bliver brugeren logget ud, og offline Paper-dokumenter bliver automatisk slettet fra enhedens interne lagerplads.

Team-kontroller

Ikke to virksomheder er ens, og derfor har vi udviklet en række værktøjer, der giver administratorer mulighed for at tilpasse Dropbox til virksomheder til deres afdelingers individuelle behov. Dropbox til virksomheder indeholder værktøjer, der giver slutbrugere mulighed for at beskytte deres konti og data. Godkendelse, gendannelse, logføring og øvrige sikkerhedsfunktioner nedenfor er tilgængelige via de forskellige Dropbox-brugergrænseflader.

Nedenfor ses flere af de kontrol- og synlighedsfunktioner, som kan benyttes via administratorkonsollen til Dropbox til virksomheder.

Niveauinddelte indholdstilladelser

- ***Niveaudelte administratorroller***

  Dropbox tilbyder opdelte administratorroller for at muliggøre mere effektiv teamadministration. Kontoadministratorer kan tildeles et af tre adgangsniveauer. Der er ingen grænse for, hvor mange administratorer et team kan have, og ethvert teammedlem kan tildeles en administratorrolle.

- ***Teamadministrator***

  Kan angive sikkerheds- og delingstilladelser for hele teamet, oprette administratorer og administrere medlemmer. Teamadministratoren har alle tilgængelige administratortilladelser. Kun teamadministratorer kan tildele eller ændre administratorroller, og der skal altid være mindst én teamadministrator på en Dropbox til virksomheder-konto.

- ***Brugeradministrator***

  Kan håndtere de fleste teamadministrationsopgaver, herunder at tilføje og fjerne teammedlemmer, administrere grupper og få vist et teams aktivitetsfeed.

- ***Supportadministrator***

  Kan håndtere almindelige serviceanmodninger fra teammedlemmer, såsom at gendanne slettede filer eller hjælpe teammedlemmer, som ikke længere har adgang til totrinsgodkendelse. Supportadministratorer kan også nulstille ikke-administratoradgangskoder og eksportere en logfil over aktiviteter for et bestemt teammedlem.

- ***Faktureringsadministrator***

  Kan få adgang til faktureringssider i administratorpanelet.

- ***Indhold***

  Kan oprette og administrere teammapper i medlemsadministrator.

- ***Rapporteringsadministrator***

  Kan oprette rapporter i administratorpanel og har adgang til aktivitetssiden.

- ***Sikkerhedsadministrator***

  Kan administrere sikkerhedsadvarsler, ekstern deling og sikkerhedsrisici.

- ***Compliance-administrator (kun for teams med tilføjelsesprogrammet til dataforvaltning)***

  Kan administrere dataforvaltningssider (juridiske fastfrysninger, dataopbevaring og datadisponering) og også få adgang til medlemsadministrator.

- ***Grupper***

  Teams kan oprette og administrere medlemslister i Dropbox og nemt give dem adgang til bestemte mapper. Dropbox kan også synkronisere Active Directory-grupper ved hjælp af Active Directory Connector.

- ***Virksomhedsstyrede grupper***

  Kun administratorer kan oprette, slette og administrere medlemskabet for denne type gruppe. Brugere kan ikke anmode om at deltage i eller forlade en virksomhedsstyret gruppe.

- ***Brugeradministrerede grupper***

  Administratorer kan vælge, om brugere kan oprette og administrere deres egne grupper. Administratorer kan også til enhver tid ændre en brugeradministreret gruppe til en virksomhedsadministreret gruppe for at overtage kontrollen over den.

- ***Begrænsning af flere konti på computere***

  Administratorer kan forhindre teammedlemmer i at knytte en sekundær Dropbox-konto til computere, som er knyttet til deres arbejdsrelaterede Dropbox-konto.

- ***Brugertilstanden Suspenderet***

  Administratorer kan deaktivere en brugers adgang til vedkommendes konto, samtidig med at vedkommende beholder sine data- og delingsforhold, så virksomhedsoplysningerne beskyttes. Administratorer kan genaktivere eller slette kontoen senere.

- ***Log ind som bruger***

  Teamadministratorer kan logge ind som medlemmer af deres teams. Dette giver administratorer direkte adgang til filer, mapper og Paper-dokumenter på teammedlemmers konti, så de kan ændre, dele på vegne af teammedlemmer eller kontrollere hændelser på filniveau. "Log ind som bruger"-hændelser registreres i teamets aktivitets-logfil, og administratorer kan vælge, om medlemmer skal underrettes om disse hændelser.

- ***Delingstilladelser***

  Teamadministratorer har omfattende kontrol over deres teams muligheder for at dele ved hjælp af Dropbox, herunder om:

  - teammedlemmer kan dele filer og mapper med andre end teammedlemmer.
  - teammedlemmer kan redigere mapper, der ejes af andre end teammedlemmer.
  - delte links, der oprettes af teammedlemmer, kan bruges af andre end teammedlemmer.
  - teammedlemmer kan oprette filanmodninger og indsamle filer fra teammedlemmer og/eller andre end teammedlemmer.
  - andre kan se og kommentere filer, der ejes af teamet.
  - teammedlemmer kan dele Paper-dokumenter og Paper-mapper uden for teamet.
  - Der gives permanente slettetilladelser.

Teamadministratoren Teamadministratoren Dropbox til virksomheder-konto kan begrænse muligheden for at slette filer permanent, så kun teamadministratorer kan gøre dette.

Onboarding og brugerklargøring

Metoder til klargøring af brugere og identitetsstyring

- ***Invitation pr. e-mail***

  Et værktøj i administratorpanelet til Dropbox til virksomheder giver administratorer mulighed for manuelt at oprette en invitation pr. e-mail.

- ***Active Directory***

  Administratorer i Dropbox til virksomheder kan automatisere oprettelsen og fjernelsen af konti fra et nuværende Active Directory-system via vores forbindelse til Active Directory eller tredjeparts-identitetsudbyder. Når Active Directory er integreret, kan det bruges til at administrere medlemskaber.

- ***Enkeltlogon***

Dropbox til virksomheder kan konfigureres til at give teammedlemmer adgang ved at logge ind på en central identitetsudbyder. Vores SSO-implementering, der benytter Security Assertion Markup Language 2.0 (SAML 2.0), som er standard i branchen, gør klargøring mere enkelt og sikkert ved at gøre en pålidelig identitetsudbyder ansvarlig for godkendelse og give teammedlemmer adgang til Dropbox uden behov for at administrere endnu en adgangskode. Dropbox har også indgået et samarbejde med førende udbydere af identitetsadministration, så brugere automatisk kan klargøres og fjernes. Få flere oplysninger i Dropbox Business API-integrationer nedenfor.

- ***API***

  Dropbox Business API kan bruges af kunder til at oprette tilpassede løsninger til provisionering af brugere og administration af identitet. Få flere oplysninger i afsnittet Dropbox Business API-integrationer nedenfor.

Totrinsbekræftelse

Denne yderst anbefalede sikkerhedsfunktion føjer et ekstra beskyttelseslag til en brugers Dropbox-konto. Når totrinsbekræftelse er aktiveret, kræver Dropbox en sekscifret sikkerhedskode ud over en adgangskode, hver gang der logges på eller forbindes en ny computer, telefon eller tablet.

- Administratorer kan vælge at kræve totrinsbekræftelse for alle teammedlemmer eller kun for bestemte medlemmer.
- Kontoadministratorer kan kontrollere, hvilke teammedlemmer der har aktiveret totrinsbekræftelse.
- Koder til Dropbox-totrinsbekræftelse kan modtages via SMS eller i apps, der overholder algoritmestandarden TOTP (Time-based One-Time Password (tidsbaseret engangs-adgangskode)).
- Hvis en bruger ikke kan modtage sikkerhedskoder ved hjælp af disse metoder, kan vedkommende vælge at bruge en 16-cifret éngangs-reservekode til nødstilfælde. Brugeren kan også vælge at bruge et sekundært telefonnummer til at modtage en reservekode som SMS.
- Dropbox understøtter desuden den åbne standard FIDO Universal 2nd Factor (U2F), der giver brugere mulighed for at godkende med en USB-sikkerhedsnøgle, som de har opsat, i stedet for en 6-cifret kode.

Installationsprogram til store virksomheder

Administratorer med behov for skaleret provisionering kan bruge vores Enterprise-installationsprogram til Windows til at installere Dropbox-klienten til stationære pc'er diskret og via fjernadgang ved hjælp af administrerede softwareløsninger og implementeringsmekanismer.

Administrerede enheder og login

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

  Dropbox integrerer med tredjepartsudbydere af EMM, så administratorer af konti med Dropbox til virksomheder på et Enterprise-abonnement får mere kontrol over, hvordan teammedlemmer bruger Dropbox på mobilenheder. Administratorer kan begrænse brugen af mobilapps for Dropbox Enterprise-konti til kun administrerede enheder (uanset om de er til arbejde eller personlig brug), få overblik over brug af apps (herunder ledig lagerplads og adgangssteder) og benytte fjernsletning, hvis en enhed mistes eller bliver stjålet. Bemærk, at Paper-mobilappen ikke kan administreres vha. EMM.

- ***Godkendelse af enheder***

  Dropbox gør det muligt for administratorer af Dropbox Education og Dropbox til virksomheder på Advanced- og Enterprise-abonnementer at begrænse antallet af enheder, som en bruger kan synkronisere med Dropbox, og at vælge, om godkendelser er brugerstyrede eller administratorstyrede. Administratorer kan også oprette en undtagelsesliste over brugere, der ikke er begrænset til et bestemt antal enheder. Bemærk, at Paper-mobilappen ikke er inkluderet i enhedsgodkendelser.

- ***Krav om totrinsbekræftelse***

  Administratorer kan vælge at kræve totrinsbekræftelse for alle teammedlemmer eller kun for bestemte medlemmer. Andre krav til multifaktorgodkendelse kan håndhæves gennem teamets SSO-implementering.

- ***Adgangskodestyring***

  Administratorer af Education-, Advanced- og Enterprise-teams kan kræve, at medlemmerne angiver og opretholder stærke, komplekse adgangskoder til deres konti. Når denne funktion er aktiveret, bliver teammedlemmerne logget ud fra alle websessioner og bedt om at oprette nye adgangskoder, når de logger på. Et indbygget værktøj analyserer styrken af adgangskoder ved at sammenligne dem med en database over ofte benyttede ord, navne, mønstre og tal. En bruger, der indtaster en almindelig adgangskode, bliver bedt om at finde på noget mere særegent, der er svært at gætte. Administratorer kan også nulstille adgangskoder for hele teamet eller for enkelte brugere.

- ***Domæneadministration***

  Dropbox kan tilbyde virksomheder en række værktøjer til at forenkle og fremskynde onboarding af brugere og kontrollere brug af Dropbox.

  - **Domænebekræftelse.** Virksomheder kan kræve ejerskab af deres domæner og få adgang til andre værktøjer til domæneadministration.

  - **Håndhævelse af regler for invitation**
    Administratorer kan kræve, at individuelle Dropbox-brugere, som er inviteret med i virksomhedens Dropbox-team, skal migrere til teamet eller ændre e-mailadressen på deres personlige konto.

  - **Domæneindsigt.**
    Administrator kan se nøgleinformation, for eksempel hvor mange individuelle Dropbox-konti der bruger virksomhedens e-mailadresser.

  - **Kontoopsamling.**
    Administrator kan tvinge alle Dropbox-brugere, der benytter virksomhedens mailadresse, til at være med i virksomhedens team eller ændre mailadressen på deres privatkonto.

- ***Styring af websession***

  Administratorer kan styre, hvor længe teammedlemmer kan være logget på dropbox.com. Administratorer kan begrænse varigheden af alle websessioner og/eller inaktive sessioner. Sessioner, der overskrider disse grænser, bliver automatisk logget ud. Administratorer kan også holde øje med og afbryde enkelte brugeres websessioner.

- ***Programadgang***

  Administratorer kan se og tilbagekalde adgang til brugerkonti for tredjepartsapps.

- ***Afbrydelse af forbindelse til enheder***

  Administratorer kan fra administratorpanelet afbryde forbindelsen fra computere og mobilenheder til brugerkonti. Brugeren kan også afbryde forbindelsen i indstillingerne for kontosikkerhed. Når forbindelsen afbrydes på en computer, fjernes godkendelsesdata, og det er muligt at slette lokale kopier af filer, næste gang computeren er online (se **Fjernsletning**). Når forbindelsen afbrydes på mobilenheder, fjernes de filer, der er markeret som favoritter, cachelagrede data og logonoplysninger. Afbrydelse af forbindelsen

fjerner også offline Paper-dokumenter fra Paper-mobilapplikationen. Hvis totrinsbekræftelse er aktiveret, skal brugerne godkende enhederne igen, hvis forbindelsen genoprettes. Desuden er det muligt at angive i brugerens kontoindstillinger, at der automatisk skal sendes en e-mail til brugeren, hvis en ny enhed tilknyttes.

- ***Netværkskontrol***

  Administratorer af teams med Dropbox til virksomheder på et Enterprise-abonnement kan begrænse brugen af Dropbox på virksomhedens netværk til kun at ske via Enterprise-teamkontoen. Denne funktion integreres med virksomhedens udbyder af netværkssikkerhed for at blokere al trafik, der findes på computere uden for den tilladte konto. Bemærk, at Paper i øjeblikket ikke administreres via netværksstyring.

Mobilsikkerhed

- ***Fingeraftrykksscanning***

  Brugere kan aktivere Touch ID eller Face ID på iOS-enheder og oplåsning med fingeraftryk (hvis dette understøttes) på Android-enheder som en metode til at låse op for Dropbox-mobilappen.

Adgangssynlighed

- ***Identitetskontrol til teknisk support***

  Før Dropbox-support kan udlevere oplysninger om fejlfinding eller konti, skal kontoens administrator oplyse en tilfældigt genereret sikkerhedskode, der kun kan bruges én gang, for at bekræfte vedkommendes identitet. Denne kode kan kun ses i administratorpanelet.

Brugerkontoaktivitet

Hver bruger kan se følgende sider i sine kontoindstillinger og finde de mest opdaterede oplysninger om sin egen kontoaktivitet:

- ***Siden Deling***

  Denne side viser de delte mapper, der i øjeblikket findes i brugerens Dropbox, og delte mapper, som brugeren kan tilføje. En bruger kan fjerne deling af mapper og filer og vælge delingstilladelser.

- ***Siden Filer***

  Denne side viser de filer, der er delt med brugeren, og datoen for delingen af hver fil. Brugeren kan fjerne sin adgang til disse filer. Hvis brugeren vil se Paper-dokumenter, som andre har delt med brugeren, kan vedkommende navigere til siden “Delt med mig” i navigationsgrænsefladen til Paper-dokumenter.

- ***Siden Links***

  Denne side viser alle de aktive og delte links, som brugeren har oprettet, samt datoen for oprettelsen af hvert enkelt link. Den viser desuden alle de links, som deles med brugeren af andre. Brugeren kan deaktivere links eller ændre tilladelser.

- ***E-mailmeddelelser***

  En bruger kan vælge at modtage en e-mailmeddelelse, så snart en ny enhed eller app forbindes til vedkommendes Dropbox-konto.

Brugerkontotilladelser

- ***Forbundne enheder***

  I afsnittet **Enheder** i en brugers indstillinger for kontosikkerhed kan du se alle de computere og mobilenheder, der er forbundet til brugerens konto. For hver computer vises IP-adresse, land og det anslåede tidspunkt for seneste aktivitet. En bruger kan afbryde forbindelsen til enhver enhed, med mulighed for at slette filer på forbundne computere, næste gang de er online.

- ***Aktive websessioner***

  I afsnittet **Sessioner** kan du se alle de webbrowsere, der i øjeblikket er logget på en brugers konto. For hver af disse vises IP-adresse, land og logontidspunkt for den seneste session samt det anslåede tidspunkt for den seneste aktivitet. En bruger kan fjernafslutte enhver session fra vedkommendes indstillinger for kontosikkerhed.

- ***Forbundne apps***

  Afsnittet **Forbundne apps** indeholder en liste over alle apps fra tredjeparter med adgang til en brugers konto og den type adgang, hver app har. En bruger kan tilbagekalde en hvilken som helst apps tilladelse til at få adgang til brugerens Dropbox.

Aktivitetsfeed

Dropbox til virksomheder registrerer bruger- og administratorhandlinger i teamets aktivitetsfeed, som kan tilgås fra administratorpanelet. Aktivitetsfeedet tilbyder fleksible filtreringsindstillinger, der gør det muligt for administratorer at udføre målrettede undersøgelser af konto-, fil- og Paper-dokumentaktivitet. De kan f.eks. se den komplette historik for en fil eller et Paper-dokument, og hvordan brugere har interageret med filen, eller se al aktivitet for teamet i løbet af en bestemt tidsperiode. Aktivitetsfeedet kan eksporteres som en rapport, der kan downloades i CSV-format, og også integreres direkte i et SIEM-produkt (Security Information and Event Management (administration af sikkerhedsoplysninger og hændelser)) eller et andet analyseværktøj via tredjepartspartnerløsninger. Følgende hændelser registreres i aktivitetsfeedet:

- ***Deling for filer, mapper og links***

  Rapporterer, hvis det er relevant, om handlinger har vedrørt personer, som ikke er teammedlemmer

  Delte filer

  - Tilføjede eller fjernede et teammedlem eller et ikke-teammedlem.
  - Ændrede tilladelser for et teammedlem eller ikke-teammedlem.
  - Tilføjede eller fjernede en gruppe.
  - Føjede en delt fil til brugerens Dropbox.
  - Så indholdet i en fil, som blev delt via en fil- eller mappeinvitation.
  - Kopierede delt indhold til brugerens Dropbox.
  - Hentede delt indhold.
  - Skrev en kommentar til en fil.
  - Håndterede eller håndterede ikke en kommentar.

- Slettede en kommentar.
- Abonnerede eller afmeldte abonnement på kommentarmeddelelser.
- Godkendte en invitation til en fil, som ejes af teamet.
- Anmodede om adgang til en fil, der ejes af teamet.
- Fjernede deling af en fil.

Delte mapper

- Oprettede en ny delt mappe.
- Tilføjede eller fjernede et teammedlem, et ikke-teammedlem eller en gruppe.
- Føjede en delt mappe til brugerens Dropbox, eller brugeren fjernede sin egen adgang til en delt mappe.
- Tilføjede en delt mappe fra et link.
- Ændrede et teammedlems eller ikke-teammedlems tilladelser.
- Overførte mappeejerskab til en anden bruger.
- Afbrød deling af en mappe.
- Godkendte medlemskab til en delt mappe.
- Anmodede om adgang til en delt mappe.
- Føjede en bruger, der har anmodet om det, til en delt mappe.
- Blokerede eller fjernede blokering af ikke-teammedlemmers mulighed for at blive føjet til en mappe.
- Gav alle teammedlemmer eller kun ejeren mulighed for at føje personer til en mappe.
- Ændrede gruppeadgang til en delt mappe.

Delte links

- Oprettede eller fjernede et link.
- Gjorde indholdet fra et link synligt for alle med linket eller kun for teammedlemmer.
- Beskyttede et links indhold med en adgangskode.
- Angav eller fjernede et udløb af et link.
- Fik vist et link.
- Hentede indholdet fra et link.
- Kopierede indholdet fra et link til brugerens Dropbox.
- Oprettede et link til en fil via en API-app.
- Delte et link med et teammedlem, et ikke-teammedlem eller en gruppe.
- Blokerede eller fjernede ikke-teammedlemmers mulighed for at se links til filer i en delt mappe.
- Delte et album.

Filforespørgsler

- Oprettede, ændrede, lukkede eller slettede en filanmodning.
- Føjede brugere til en filanmodning.
- Tilføjede eller fjernede en tidsfrist for en anmodning om en fil.
- Ændrede en filanmodningsmappe.
- Modtog filer via en filanmodning.
- Modtog filer til Dropbox via e-mail.

Individuelle fil- og mappehændelser

- Føjede en fil til Dropbox.
- Oprettede en mappe.
- Fik vist en fil.
- Redigerede en fil.
- Downloadede en fil.
- Kopierede en fil eller mappe.
- Flyttede en fil eller mappe.
- Omdøbte en fil eller mappe.
- Gendannede en fil til en tidligere version.
- Tilbageførte ændringer i filer.
- Gendannede en slettet fil.
- Slettede en fil eller mappe.
- Slettede en fil eller mappe permanent.

Vellykkede og mislykkede logons.

- Vellykket eller mislykket logonforsøg.
- Mislykkede forsøg på logon eller fejl via Single Sign-On (SSO).
- Mislykket logonforsøg eller fejl via EMM.
- Loggede af.
- Ændring af IP-adresse for websession.

Adgangskoder

Ændring af indstillinger for adgangskoder eller totrinsbekræftelse. Administratorer kan ikke se brugernes faktiske adgangskoder.

- Ændret eller nulstillet adgangskode.
- Aktiverede, nulstillede eller deaktiverede totrinsbekræftelse.

- Konfigurerede eller ændrede totrinsbekræftelse til brug af SMS eller en mobilapp.
- Tilføjede, redigerede eller fjernede en reservetelefon til totrinsbekræftelse.
- Tilføjede eller fjernede en sikkerhedsnøgle til totrinsbekræftelse.

Medlemskab

Tilføjelse og fjernelse af teammedlemmer.

- Inviterede et teammedlem.
- Blev medlem af teamet.
- Fjernede et teammedlem.
- Suspenderede eller fjernede suspenderingen af et teammedlem.
- Genoprettede et fjernet teammedlem.
- Anmodede om at blive en del af et team ud fra kontodomæne.
- Godkendte eller afviste en anmodning om at blive en del af et team ud fra kontodomæne.
- Sendte domæneinvitationer til nuværende domænekonti.
- Bruger blev en del af teamet som følge af kontoopsamling.
- Bruger forlod domænet som følge af kontoopsamling.
- Blokerede eller fjernede blokering af teammedlemmers mulighed for at foreslå nye teammedlemmer.
- Foreslog et nyt teammedlem.

Apps

Forbindelser mellem apps fra tredjeparter og Dropbox-konti.

- Godkendte eller fjernede et program
- Godkendte eller fjernede en team-applikation.

Enheder

Forbindelser mellem computere eller mobilenheder og Dropbox-konti.

- Tilknyttede eller fjernede tilknytning af en enhed.
- Brugte fjernsletning og slettede alle filer eller lykkedes ikke med at slette nogle filer.
- Ændrede IP-adresse for stationær pc eller mobilenhed.

Administratorhandlinger

Ændring af indstillinger i administratorpanelet, såsom tilladelser for delte mapper.

- ***Godkendelse og enkelt-logon (SSO)***
  - Nulstillede teammedlems adgangskode.

- Nulstillede alle teammedlemmers adgangskoder.
- Blokerede eller fjernede blokering af teammedlemmers mulighed for at deaktivere totrinsbekræftelse.
- Aktiverede eller deaktiverede SSO.
- Gjorde logon via SSO påkrævet.
- Ændrede eller fjernede webadresse til SSO.
- Opdaterede SSO-certifikatet.
- Ændrede SSO-identitetstilstanden.

- ***Medlemskab***
  - Blokerede eller fjernede blokering af brugeres mulighed for at anmode om at blive en del af teamet ud fra kontodomæne.
  - Indstillede anmodninger om medlemskab af team til at blive godkendt automatisk eller kræve manuel administratorgodkendelse.

- ***Administration af medlemskonto***
  - Ændrede et teammedlems navn.
  - Ændrede et teammedlems e-mailadresse.
  - Tildelte eller fjernede administratorstatus eller ændrede administratorrollen.
  - Loggede ind eller loggede ud som et teammedlem.
  - Overførte eller slettede indholdet på et fjernet medlems konto.
  - Slettede permanent indholdet på et fjernet medlems konto.

- ***Globale delingsindstillinger***
  - Blokerede eller fjernede teammedlemmers mulighed for at tilføje delte mapper, som ejes af ikke-teammedlemmer.
  - Blokerede eller fjernede blokering af teammedlemmers mulighed for at dele mapper med ikke-teammedlemmer.
  - Aktiverede advarsler, der vises til brugere, før de deler mapper med ikke-teammedlemmer.
  - Blokerede eller fjernede blokering af muligheden for, at ikke-teammedlemmer kan se delte links.
  - Indstillede delte links til kun at være for team som standard.
  - Blokerede eller fjernede blokering af personers mulighed for at kommentere filer.
  - Blokerede eller fjernede teammedlemmers mulighed for at oprette filanmodninger.
  - Tilføjede, ændrede eller fjernede et logo for sider med delt link.
  - Blokerede eller fjernede blokering af teammedlemmers mulighed for at dele Paper-dokumenter og Paper-mapper med ikke-teammedlemmer.

- ***Administration af teammappe til filer***
  - Oprettede en teammappe.
  - Omdøbte en teammappe.
  - Arkiverede eller fjernede arkivering af en teammappe.

- Slettede en teammappe permanent.
- Nedgraderede en teammappe til en delt mappe.

- ***Domæneadministration***
  - Forsøgte at bekræfte eller bekræftede et domæne eller fjernede et domæne.
  - Dropbox Support bekræftede eller fjernede et domæne.
  - Aktiverede eller deaktiverede muligheden for at sende domæneinvitationer.
  - Aktiverede eller deaktiverede "Inviter automatisk nye brugere".
  - Ændrede kontoopsamlingstilstand.
  - Dropbox-support gav mulighed for eller annullerede kontoopsamling.

- ***EMM (Enterprise Mobility Management)***
  - Aktiverede EMM for testtilstand (valgfrit) eller implementeringstilstand (påkrævet).
  - Genindlæste EMM-token.
  - Tilføjede eller fjernede teammedlemmer fra liste over brugere, der er ekskluderet fra EMM.
  - Deaktiverede EMM.
  - Oprettede en rapport med en EMM-undtagelsesliste.
  - Oprettede en rapport over brug af EMM-mobilapp.

- ***Ændringer i andre teamindstillinger***
  - Sammenlagde teams.
  - Opgraderede teamet til Dropbox til virksomheder eller nedgraderede til et gratis team.
  - Ændrede teamnavnet.
  - Oprettede en rapport for teamaktivitet.
  - Blokerede eller fjernede en blokering af teammedlemmers mulighed for at have mere end én konto knyttet til en computer.
  - Gav alle teammedlemmer eller kun administratorer mulighed for at oprette grupper.
  - Blokerede eller fjernede blokering af teammedlemmers muligheder for at slette filer permanent.
  - Påbegyndte eller afsluttede en Dropbox-supportsession for en forhandler.

Grupper

Oprettelse, sletning og oplysninger om medlemskab for grupper.

- Oprettede, omdøbte, flyttede eller slettede en gruppe.
- Tilføjede eller fjernede et medlem.
- Ændrede et gruppemedlems adgangstype.
- Ændrede gruppe til teamadministreret eller administratoradministreret.
- Ændrede en gruppes eksterne ID.

Paper-aktivitetslog

Administratorer kan vælge en Paper-aktivitetstype på aktivitetsfeeden eller downloade en komplet aktivitetsrapport. Paper-hændelser registreres for:

- Paper aktiveret eller deaktiveret.
- Oprettelse, redigering, eksport, arkivering, permanent sletning og gendannelse af Paper-dokument.
- Kommentering af Paper-dokument og løsning af kommentarer.
- Deling og ophævelse af deling af Paper-dokument med teammedlemmer og ikke-teammedlemmer.
- Anmodninger om adgang til Paper-dokument fra teammedlemmer og ikke-teammedlemmer.
- Omtaler af Paper-dokument for teammedlemmer og ikke-teammedlemmer.
- Paper-dokument set af teammedlemmer og ikke-teammedlemmer.
- Paper-dokument fulgt.
- Ændringer af medlemstilladelser for Paper-dokument (rediger, kommenter eller skrivebeskyttet).
- Ændringer til politik for ekstern deling af Paper-dokument.
- Oprettelse, arkivering og permanent sletning af Paper-mappe.
- Paper-dokument tilføjet i eller fjernet fra en mappe.
- Paper-mappe omdøbt.
- Overførsler af Paper-dokument og -mappe.

Dropbox Passwords

Dropbox Passwords er en sikker og enkel metode til lagring, synkronisering og automatisk udfyldelse af brugernavne, adgangskoder og kredit-/betalingskort på tværs af enheder, så du kan beskytte dine logonoplysninger på nettet. Dropbox Passwords beskytter dine følsomme brugernavne, adgangskoder og kredit- og betalingskort til onlinekonti med vidensløs kryptering i skyen og på dine enheder. Vores produkter er bygget til daglig brug og er designet til at være sikre.

Vidensløs kryptering

Dropbox Passwords gemmer dine krypterede data i skyen, men nøglerne til dekryptering af disse data gemmes kun på dine enheder. **Dropbox har aldrig adgang til dem.** Nøglerne er lange og tilfældige og genereres på din enhed. De forlader aldrig din enhed, undtagen når du beslutter dig for at parre eller tilmelde en ny enhed. Ved denne overførsel anvendes kryptografi med offentlige nøgler til både at underskrive og beskytte nøglerne kryptografisk under overførslen, så du kan være sikker på, at ingen andre kan dekryptere dem, mens du også får bekræftet deres ægthed. Denne egenskab kaldes ofte for vidensløs kryptering, fordi de krypterede data er ubrugelige for alle, der ikke har nøglerne, heriblandt Dropbox. Det betyder, **at kun du kan se dine oplysninger,** og i den usandsynlige situation, at Dropbox bliver hacket, er dine oplysninger stadig sikre. De krypterede data er adskilt fra synlige Dropbox-mapper og kan ikke tilgås af Dropbox-klienter eller -API'er.

Oplysninger om kryptering

Dropbox krypterer dine data ved hjælp af XChaCha20-Poly1305 i kombineret tilstand for implicit godkendelse. Vores browserudvidelser og mobilapplikationer bruger alle krypteringsimplementeringer, der understøttes af libsodium, som er en revideret og bredt distribueret gren af NaCl.

Hver krypteringshandling genererer en tilfældig 192-bits nonce, som gemmes sammen med de krypterede nyttedata, der senere skal dekrypteres. I modsætning til AES-GCM understøtter XChaCha20-Poly1305 tilfældige nonces. Ved dekryptering læses den 192-bit nonce fra nyttedataene og bruges til at dekryptere de krypterede nyttedata. Enhver efterfølgende kryptering genererer en tilfældig 192-bit nonce, der er uafhængig af den tidligere nonce. Dropbox Passwords genererer tilfældige tal ved hjælp af libsodium, der som standard skifter til en kryptografisk sikker generator af tilfældige tal på hver af de platforme, som vi understøtter.

Nøgler og genoprettelsesord

Vi genererer en symmetrisk nøgle på 256 bit (krypteringsnøglen) ved hjælp af 128 bits entropi (brugernøglen) via Blake2-hashing. Denne krypteringsnøgle forbliver kun på ejerens enheder, og når det er muligt, forbliver den i det mest sikre lager, som vi har adgang til på disse enheder. På iPhones gemmer vi f.eks. krypteringsnøglen i iOS-nøgleringen.

Vi bruger 128 bits entropi som kilde, fordi det giver tilstrækkelig sikkerhed, samtidig med at det kun kræver 12 genoprettelsesord, når vi bruger BIP-39-standarden til backup. BIP-39 giver en brugervenlig måde at repræsentere store tilfældige nøgler på ved at omdanne disse nøgler til en liste med 12 ord. Enhver 128-bit nøgle har en tilsvarende liste med ord, og hver liste med 12 ord identificerer entydigt 128 bits. Det eneste forbehold er, at de 12 ord faktisk svarer til 132 bits, så de ekstra fire bits bruges som en kontrolsum, der bruges til at identificere fejl. Genoprettelsesordene giver dig mulighed for at gendanne din krypteringsnøgle, hvis din enhed bliver væk eller bliver stjålet. Vi anbefaler, at du udskriver dem og opbevarer dem et sikkert sted. Du kan også overveje at give dem til en ven eller et familiemedlem, du har tillid til, eller gemme dem på et USB-drev.

Registrering af enhed

Når en bruger logger på Dropbox Passwords på en ny enhed, skal den pågældende enhed fuldføre en sikker registreringsprocedure for at få adgang til brugerens adgangskodeoplysninger. Denne procedure er med til at sikre, at en brugers hemmelige nøgle og Passwords-data kun er tilgængelige for brugerens tilmeldte enheder. Det er også med til at sikre, at en bruger kun kan tilmelde yderligere enheder, hvis brugeren har adgang til en eksisterende tilmeldt enhed eller til sine genoprettelsesord. Proceduren for registrering af enheder foregår på nedenstående måde.

En ny enhed, der skal tilmeldes, genererer tilfældigt et 256-bit offentligt/privat enhedsnøglepar og uploader den offentlige nøgle til Dropbox-serveren. Derefter opstår enten scenariet **A**, **B** eller **C**.

A: Hvis brugeren ikke tidligere har tilmeldt en enhed, genererer den tilmeldende enhed tilfældigt en 128-bit hemmelig brugernøgle. Både brugernøglen og enhedens nøglepar gemmes på et sikkert sted afhængigt af operativsystemet, som det beskrives i følgende afsnit om nøgleopbevaring. Enheden initialiserer brugerens Passwords-data, krypterer dem og uploader de krypterede nyttedata til Dropbox-serveren.

B: Hvis brugeren har en eller flere tidligere tilmeldte enheder, sendes der en anmodning om godkendelse af tilmeldingen til hver af disse enheder. Den tilmeldte enheds offentlige nøgle er vedhæftet til anmodningen. Brugeren skal derefter godkende anmodningen på en af sine tilmeldte enheder. Hvis anmodningen godkendes, krypterer den tilmeldte enhed brugerens nøgle ved hjælp af sin private nøgle og den tilmeldende enheds offentlige nøgle via X25519 ECDH med XSalsa20-Poly1305. Den tilmeldte enhed uploader den krypterede brugernøgle til Dropbox-serveren, så den sendes til den tilmeldende enhed. Den tilmeldte enhed downloader og dekrypterer brugernøglen ved hjælp af sin private nøgle og den tilmeldte enheds offentlige nøgle. Den tilmeldte enhed downloader derefter de krypterede Passwords nyttedata og dekrypterer dem med brugernøglen.

C: Hvis brugeren tidligere har tilmeldt en enhed, men ikke længere kan få adgang til den, kan brugeren indtaste sine 12 gendannelsesord og dermed lokalt rekonstruere brugernøglen. Den tilmeldte enhed downloader derefter de krypterede Passwords nyttedata og dekrypterer dem med brugernøglen.

Opbevaring af nøgler

Browserudvidelser

I webbrowsere gemmes brugernøglen i browserudvidelsens område for lokal opbevaring. Lokale lagerværdier for browserudvidelser er kun tilgængelige fra udvidelsen. Eventuel kode på websites, som brugeren besøger, kan ikke læse fra browserudvidelsens lokale lageromrade. Desuden forhindrer browserudvidelser, at der afvikles kode, der ikke er inkluderet i den signerede udvidelsespakke, hvorfor der ikke er nogen risiko for XSS-sårbarhed, der ville få adgang til lokale lagerværdier.

En angriber med ubegrænset adgang til brugerens enhed kan få adgang til brugerens nøgle ved at læse den lokale lagringsfil på disken. Eksempler på sådanne trusler er: en angriber med fysisk adgang til enheden eller en angriber, der kører skadelig malware på enheden. For at beskytte sig mod disse scenarier kan brugeren konfigurere et adgangsudtryk til den lokale enhed.

Når der er konfigureret et adgangsudtryk, krypteres brugernøgle inaktivt i browserudvidelsens lokale lager. Krypteringsnøglen udledes af adgangsudtrykket ved hjælp af Argon2-adgangskodehashing, og den anvendte krypteringsmetode er XChaCha20-Poly1305. Hver gang browserudvidelsen genstartes, skal brugeren angive sit adgangsudtryk for at dekryptere brugernøglen og låse sine data op. Derfor kan en angriber uden adgangsudtryk ikke dekryptere den brugernøgle, der er gemt i den lokale lagringsfil på disken.

iOS

På iOS gemmes brugernøglen i iOS-nøgleringen, som er en krypteret databasefil på disken. Denne fil krypteres med en hemmelig nøgle, der er gemt i Secure Enclave-hardwaremodulet med AES256-GCM som krypteringsmetode. Kun den signerede Dropbox Passwords-app til iOS kan tilgå til de elementer, som den har gemt i nøgleringen. Dette forhindrer anden kode, der kører på brugerens enhed, i at få adgang til brugerens nøgle.

Android

På Android gemmes brugernøglen i et EncryptedSharedPreferences-objekt, som er en krypteret præferencefil på disken. Denne fil krypteres med en hovednøgle, der er gemt i Android Keystore-sikkerhedshardwaren med AES256-GCM som krypteringsmetode. Kun den signerede Dropbox Passwords-app til Android kan tilgå hovednøglen, der bruges til at dekryptere præferencefilen.

Lokal godkendelse

Dropbox Passwords tilbyder valgfrie lokale godkendelsesforanstaltninger, der yderligere begrænser adgangen til en brugers Passwords-data på brugerens fysiske enhed. For mobilapps kan den lokale godkendelsesbevægelsen for det lokale operativsystem genbruges (dvs. et adgangsudtryk med supplerende biometrisk godkendelse). For browserudvidelser kan der konfigureres et valgfrit adgangsudtryk. Disse mekanismer giver et ekstra lag af applikationssikkerhed, når operativsystemet på brugerens enheden er låst op. Dette giver brugeren mulighed for at sikre sine Passwords-data i tilfælde, hvor en anden bruger har adgang til enheden, f.eks. et familiemedlem eller en kollega.

Forslag til adgangskodestyrke

Dropbox har udviklet open source-værktøjet zxcvbn, som bruges af flere adgangskodeadministratorer til at vurdere adgangskoders styrke. Værktøjet sammenligner adgangskoder med en database med 30.000 almindelige adgangskoder, almindelige navne og efternavne i henhold til amerikanske folketællingsdata, populære engelske ord fra Wikipedia og amerikansk tv og film samt andre almindelige mønstre som datoer, gentagelser (aaa), sekvenser (abcd), tastaturmønstre (qwertyuiop) og Leetspeak (1337). Hvis den adgangskode, som en bruger forsøger at indtaste, er almindelig, opfordrer værktøjet brugeren til at indtaste noget, der er mere unikt og svært at gætte. Ved at bruge indstillingen **Meget stærk** kan du sikre det højeste niveau af kontosikkerhed for brugerne.

Datasikkerhed, beskyttelse af persondata og gennemsigtighed

Enkeltpersoner og organisationer overlader Dropbox deres vigtigste arbejdsfiler hver eneste dag, og det er vores ansvar at beskytte disse oplysninger og sikre, at de forbliver private.

Persondatapolitik

Vores politik om beskyttelse af personlige oplysninger kan ses på www.dropbox.com/privacy. Dropbox' Politik om beskyttelse af personlige oplysninger, Serviceaftale, Servicebetingelser og Politik om acceptabel brug indeholder oplysninger om følgende vilkår:

- Hvilken slags data vi indsamler og hvorfor.
- Hvem vi kan dele oplysninger med.
- Hvordan vi beskytter disse oplysninger, og hvor længe vi opbevarer dem.
- Hvor vi opbevarer og overfører dine oplysninger.
- Hvad der sker, hvis politikken ændres, eller hvis du har spørgsmål.

Gennemsigtighed

Dropbox bestræber sig på gennemsigtighed i forbindelse med håndtering af politiets anmodninger om udlevering af brugeroplysninger såvel som disse anmodningers antal og typer. Vi gennemgår nøje alle anmodninger om udlevering af data for at sikre, at de er i overensstemmelse med loven, og vi bestræber os på at give brugere besked i henhold til loven, når deres konti identificeres i forbindelse med en anmodning fra politiet.

Disse bestræbelser understreger vores engagement i beskyttelsen af vores brugeres privatliv og data. Vi har tillige offentliggjort en gennemsigtighedsrapport og etableret en række principper for dataanmodninger fra myndighederne. Vi overholder følgende principper, når vi modtager, undersøger og reagerer på myndigheders anmodninger om vores brugeres data:

- ***Være åbne***

  Vi er af den opfattelse, at onlinetjenester skal have tilladelse til at offentliggøre antallet og arterne af de anmodninger, de modtager fra myndighederne, og at give enkeltpersoner besked, når der anmodes om oplysninger om dem. Denne form for åbenhed styrker brugerne ved at give dem bedre viden om tilfælde og mønstre af myndighedskontrol. Vi vil fortsat offentliggøre detaljerede oplysninger om disse anmodninger og tale for retten til at levere flere af disse vigtige oplysninger.

- ***Bestride for brede anmodninger***

  Myndighedernes dataanmodninger bør være begrænset til bestemte personer og legitime undersøgelser. Vi vil bestride generelle og for brede anmodninger.

- ***Beskytte alle brugere***

  Love, der giver mennesker forskellig beskyttelse, afhængigt af hvor de bor eller deres statsborgerskab, er forældede og afspejler ikke onlinetjenesters globale natur. Vi vil fortsætte med at tale for ændringer af sådanne love.

- ***Levere tjenester, man kan have tillid til***

  Myndigheder bør aldrig installere bagdøre til onlinetjenester eller kompromittere infrastrukturen for at indhente brugerdata. Vi fortsætter vores arbejde for at beskytte vores systemer og ændre lovene for at gøre det klart, at denne type aktivitet er ulovlig.

Vores gennemsigtighedsrapporter kan ses på dropbox.com/transparency.

Integritetscertifikater, attester og lovgivningsmæssig overholdelse

Personer og organisationer betror deres vigtigste arbejdsfiler til Dropbox hver eneste dag. Det er vores ansvar at beskytte disse filer og at sikre, at de forbliver fortrolige. Vores forpligtelse til beskyttelse af dine personlige oplysninger er kernen i enhver beslutning, vi træffer.

ISO/IEC 27018 (Kodeks for beskyttelse af personlige data i skyen) og ISO/IEC 27701 (udvidelse til IS/IEC 27001 og ISO/IEC 27002 til styring af oplysninger om beskyttelse af personlige oplysninger)

Dropbox til virksomheder var en af de første større udbydere af cloudtjenester, der opnåede certificering med ISO/IEC 27018 og ISO/IEC 27701.

ISO/IEC 27018 er en global standard for beskyttelse af persondata og databeskyttelse i skyen og blev offentliggjort i august 2014 for specifikt at adressere brugernes fortrolighed og databeskyttelse.

ISO/IEC 27701 er den første certificerbare globale standard for systemer til administration af persondata og blev offentliggjort i 2019 for at give en ramme for udvidelse af systemet til administration af informationssikkerhed (ISMS) fra ISO/IEC 27001 til et system til administration af persondata (PIMS) ved at omfatte overvejelser om beskyttelse af persondata.

Standarderne indeholder en række krav til, hvordan Dropbox bruger og ikke bruger din organisations oplysninger:

- ***Din organisation kontrollerer dine data***

  Vi bruger kun de personlige oplysninger, som du giver os, til at levere den tjeneste, du er tilmeldt. Du kan tilføje, ændre eller slette filer og Paper-dokumenter fra Dropbox, når du har brug for det.

- ***Fuld åbenhed om dine data***

  Vi er fuldt åbne om, hvor dine data befinder sig på vores servere. Vi fortæller også, hvem der er vores betroede partnere. Vi giver dig besked om, hvad der sker, hvis du lukker en konto eller sletter en fil eller et Paper-dokument, og vi underretter dig, hvis der sker ændringer på nogen af områderne.

- ***Dine data er i sikre hænder***

  ISO/IEC 27018 og ISO/IEC 27701 blev designet som supplementer til og udvidelser af ISO/IEC 27001, som er en af verdens mest accepterede standarder for informationssikkerhed. Vi modtog ISO/IEC 27001 certificeringsfornyelse i oktober 2021.

- ***Vores retningslinjer gennemgås regelmæssigt***

  Som en del af vores overholdelse af ISO/IEC 27018, ISO/IEC 27701 og ISO/IEC 27001 kontrolleres vi hvert år af en uafhængig tredjepart, så vi fortsat er kvalificerede til disse certificeringer. Du kan se alle vores ISO-certificeringer her.

Dataoverførsler

Under overførsel af data fra Den Europæiske Union, Det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz benytter Dropbox en række forskellige juridiske midler, såsom kontrakter med vores kunder og associerede selskaber, standardkontraktbestemmelser og Europa-Kommissionens beslutninger om et tilstrækkeligt beskyttelsesniveau om visse lande, alt efter hvad der er relevant.

Dropbox overholder rammerne for EU og USA's privatlivsskjold (Privacy Shield) samt Schweiz og USA's privatlivsskjold som fastsat af det amerikanske Department of Commerce vedrørende indsamling, brug

og opbevaring af persondata, der overføres fra EU, det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz til USA, selvom Dropbox ikke forlader sig på EU og USA's privatlivsskjold (Privacy Shield) eller Schweiz og USA's privatlivsskjold som et juridisk grundlag for overførsel af persondata. Dropbox har certificeret over for USA's handelsministerium, at det og overholder principperne for privatlivsskjoldet med hensyn til disse data. Du kan få flere oplysninger om Privacy Shield på https://www.privacyshield.gov.

Klager og tvister i relation til vores Privacy Shield-overholdelse undersøges og løses gennem JAMS, en uafhængig tredjepart. Du kan finde flere oplysninger i vores politik for beskyttelse af personlige oplysninger (dropbox.com/privacy).

EU's generelle forordning om databeskyttelse (GDPR)

Databeskyttelsesforordningen (GDPR) er en EU-forordning fra 2018, der fastlægger omfattende rammer for håndtering og beskyttelse af personlige data.

Dropbox har en permanent forpligtelse, når det drejer sig om sikkerheden og beskyttelsen af vores brugeres data i overensstemmelse med lovkrav og bedste praksis. I overensstemmelse med vores forpligtelse over for vores brugere har vi arbejdet hårdt for at sikre, at Dropbox er kompatibel med GDPR, herunder udnævnelse af en databeskyttelsesansvarlig, omstrukturering af vores privatlivsprogram for at sikre, at brugere kan udøve deres rettigheder som dataemner, dokumentation af vores databehandlingsaktiviteter og styrkelse af vores interne processer i tilfælde af et brud på sikkerheden. Efterhånden som databeskyttelsesmyndigheder giver yderligere vejledning, fortsætter vi med at foretage justeringer for at sikre, at vores proces og praksis opfylder eller mere end opfylder specifikke elementer af de nye regler.

EU Cloud Code of Conduct

EU Cloud Code of Conduct er et frivilligt redskab, der giver leverandører af cloudtjenester, som f.eks. Dropbox, mulighed for at vise, at vi forpligter os til at overholde GDPR. Dropbox til virksomheder, som består af planerne Standard, Advanced, Enterprise og Education til teams, er blevet erklæret i overensstemmelse med EU Cloud Code of Conduct og har modtaget et "Compliance Mark på “Niveau 2”, som betyder, at disse tjenester har implementeret tekniske, organisatoriske og kontraktmæssige foranstaltninger i overensstemmelse med kravene i EU Cloud Code of Conduct. Du kan få mere at vide om EU Cloud Code of Conduct og Dropbox' overholdelse af den på det officielle website for EU Cloud Code of Conduct.

Du kan finde flere oplysninger om vores praksisser og politikker for beskyttelse af personlige oplysninger i Dropbox' hvidbog om beskyttelse af personlige oplysninger og data.

Compliance

Der er forskellige lovgivningsmæssige og branche-specifikke krav til sikkerhed og beskyttelse af persondata, som din organisation kan være påkrævet at overholde. Vores tilgang er at kombinere de mest anerkendte standarder med foranstaltninger, der er tilpasset de specifikke behov i vores kunders virksomheder eller brancher.

ISO

International Organization for Standardization (ISO) har udviklet en række standarder for informations- og samfundsmæssig sikkerhed for at hjælpe virksomheder med at udvikle pålidelige og innovative produkter og tjenester. Dropbox har certificeret sine datacentre, systemer, programmer, medarbejdere og processer via en række revisioner udført af en uafhængig tredjepart, EY CertifyPoint i Nederlandene. EY CertifyPoint opretholder sine ISO-akkrediteringer fra Raad voor Accreditatie (det nederlandske akkrediteringsråd).

ISO/IEC 27001 (informationssikkerhed)

ISO/IEC 27001 er anerkendt som verdens førende ISMS-standard (Information Security Management System). Standarden anvender også den bedste praksis for sikkerhed, der er beskrevet i ISO/IEC 27002. For at gøre os fortjent til din tillid har vi fokus på løbende og omfattende administration af vores fysiske, tekniske og juridiske kontrol hos Dropbox.

Se ISO/IEC 27001-certifikatet for Dropbox til virksomheder og Dropbox Education.

ISO/IEC 27017 (cloudbaseret sikkerhed)

ISO/IEC 27017 er en international standard for cloudbaseret sikkerhed, der giver retningslinjer for sikkerhedskontroller, der gælder for levering og brug af cloudtjenester. Vores Vejledning til fælles ansvar forklarer en række af de krav til sikkerhed, beskyttelse af personlige oplysninger og krav til regler og standarder, som Dropbox og dets kunder kan løse i fællesskab.

Se ISO/IEC 27017-certifikatet for Dropbox til virksomheder og Dropbox Education

ISO/IEC 27018 (cloudbaseret beskyttelse af personlige oplysninger og data)

ISO/IEC 27018 er en international standard for beskyttelse af data og personlige oplysninger. Standarden finder anvendelse for udbydere af cloudtjenester som Dropbox, der behandler personlige oplysninger på vegne af deres kunder, og udgør grundlaget for vores kunders almindelige krav eller spørgsmål i forbindelse med lovgivningsmæssige og kontraktmæssige forhold.

Se ISO/IEC 27018-certifikatet for Dropbox til virksomheder og Dropbox Education.

ISO/IEC 22301 (Kontinuitet i virksomheden)

ISO/IEC 22301 er en international standard for kontinuitet i virksomheden, der vejleder virksomheder i at reducere risikoen for forstyrrende hændelser og reagere korrekt på dem, hvis de opstår, ved at minimere den potentielle skade. Dropbox Business continuity management system (BCMS) er en del af vores overordnede risikostyringsstrategi til beskyttelse af personer og driften under nedbrud.

Se ISO/IEC 22301-certifikatet for Dropbox til virksomheder og Dropbox Education.

ISO/IEC 27701 (administration af persondata)

ISO 27701 er en international standard for administration af persondata. Standarden giver en ramme til forbedring og udvidelse af systemet til sikkerhedsadministration under ISO 27001 til et system til administration af persondata (PIMS). Dropbox til virksomheder og Dropbox Education har modtaget denne certificering som PII-processor.

Se ISO 27701-certifikatet for Dropbox til virksomheder og Dropbox Education.

SOC

Service Organization Controls (SOC)-rapporter, der kaldes SOC 1, SOC 2 eller SOC 3, er ordninger, der er etableret af American Institute of Certified Public Accountants (AICPA) til rapportering af interne kontrolfunktioner, der er implementeret i en virksomhed. Dropbox har valideret sine systemer, programmer, medarbejdere og processer via en række revisioner udført af en uafhængigt tredjepartsvirksomhed, Ernst & Young LLP.

SOC 3 for sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger

SOC 3-kontrolrapporten dækker de fem TSC'er (Trust Service Criteria): sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger (TSP sektion 100). Dropbox' rapport om almindelig brug er en sammenfatning af SOC 2-rapporten og omfatter tredjepartsrevisorens udtalelse om den effektive udformning og drift af vores kontroller.

Se SOC 3-undersøgelsen om Dropbox til virksomheder og Dropbox Education.

SOC 2 for sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger

SOC 2-rapporten giver kunderne et detaljeret niveau af kontrolbaseret forsikring og dækker alle fem Trust Service Criteria: Sikkerhed, tilgængelighed, behandlingsintegritet, fortrolighed og beskyttelse af personlige oplysninger (TSP sektion 100). SOC 2-rapporten omfatter en detaljeret gennemgang af Dropbox' processer og mere end 100 kontrolforanstaltninger, som vi anvender til at beskytte dit indhold. Ud over vores uafhængige tredjepartsrevisors udtalelser om vores effektive design og brug af vores kontrolforanstaltninger indeholder rapporten revisorens testprocedurer og resultater for hver kontrolforanstaltning. Vores SOC 2-rapport (undertiden kaldet en SOC 2+-rapport) omfatter også en revideret sammenknytning mellem vores kontrolforanstaltninger og de ovenfor nævnte ISO-standarder, hvilket giver vores kunder yderligere gennemskuelighed. SOC 2-undersøgelsen af Dropbox til virksomheder og Dropbox Education kan fås ved anmodning.

SOC 1 / SSAE 18 / ISAE 3402 (tidligere SSAE 16 eller SAS 70)

SOC 1-rapporten giver specifik sikkerhed for kunder, som har besluttet, at Dropbox til virksomheder eller Dropbox Education er et centralt element i deres interne kontrol med økonomisk rapportering (ICFR-programmer). Disse specifikke forsikringer bruges primært til vores kunders Sarbanes-Oxley-overholdelse (SOX). Den uafhængige tredjepartsundersøgelse er udført i overensstemmelse med Standards for Attestation Engagements No. 18 (SSAE 18) og International Standard on Assurance Engagements No. 3402 (ISAE 3402). Disse standarder har erstattet de forældede Statement on Standards for Attestation Engagement No. 16 (SSAE16) og Statement on Auditing Standards No. 70 (SAS 70). SOC 1-undersøgelsen for Dropbox til virksomheder og Education fås efter anmodning.

CSA

Cloud Security Alliance: CSA STAR (Security, Trust and Assurance Registry)

CSA STAR (Security, Trust & Assurance Registry) er et gratis offentligt tilgængeligt register, der tilbyder et sikkerhedsprogram til cloudtjenester og dermed hjælper brugere med at vurdere sikkerhedskvaliteten hos cloudleverandører, de bruger i øjeblikket eller overvejer at indgå kontrakt med.

Dropbox til virksomheder og Dropbox Education har modtaget både CSA STAR Level 2-certificering og Level 2-godkendelse. CSA STAR Level 2 kræver en uafhængig tredjeparts vurdering af vores sikkerhedskontroller ved EY CertifyPoint (for certificering) og Ernst & Young LLP (for attestering), baseret på kravene i ISO/IEC 27001, SOC 2 Trust Service Criteria og CSA Cloud Controls Matrix (CCM) v.4.0.2.

Se vores CSA STAR Level 2-certificering og -attestering på CSA's website.

HIPAA/HITECH

Dropbox vil underskrive Business Associate Agreements (BAA'er) med Dropbox til virksomheder- eller Dropbox Education-kunder, som kræver det for at overholde HIPAA-loven (Health Insurance Portability and Accountability Act) og HITECH-loven (Health Information Technology for Economic and Clinical Health Act). Se Dropbox og HIPAA/HITECH for at få flere oplysninger.

Dropbox stiller en tredjeparts vurderingsrapport, der evaluerer vores kontrolforanstaltninger vedrørende HIPAA-/HITECH-reglerne for sikkerhed, beskyttelse af personlige oplysninger og notifikation i tilfælde af sikkerhedsbrud, til rådighed sammen med en oversigt over vores interne praksis og anbefalinger for kunder, som skal opfylde kravene til datasikkerhed og fortrolighed i HIPAA/HITECH med Dropbox til virksomheder eller Dropbox Education.

Kunder, som er interesseret i at anmode om disse dokumenter eller få flere oplysninger om køb af Dropbox til virksomheder eller Dropbox Education, kan kontakte vores salgsteam.Hvis du er en aktuel Dropbox til virksomheder- eller Dropbox Education-teamadministrator, kan du underskrive en BAA elektronisk fra kontosiden i Administratorkonsollen.

Bemærk, at muligheden for at signere en elektronisk BAA fra Administratorkonsollen kun er tilgængelige for kunder i USA.

NIST 800-171

U.S. National Institute of Standards and Technology (NIST) fremmer og vedligeholder standarder og retningslinjer for at beskytte informationssystemer. NIST Special Publication (SP) 800171 Revision 2 (R2) indeholder retningslinjer for beskyttelse af kontrollerede ikke-klassificerede oplysninger (Controlled Unclassified Information (CUI)) i ikke-føderale informationssystemer og organisationer. Alle enheder, der behandler eller opbevarer CUI fra den amerikanske regering, f.eks. forskningsinstitutioner og uddannelsessektoren, bør overholde NIST SP 800-171 R2. Dropbox' CUI-systemer, -processer og -kontroller blev valideret af en uafhængig tredjepartsrevisor, Ernst & Young LLP.

NIST SP 800-171 R2-rapporten for Dropbox til virksomheder og Dropbox Education kan rekvireres ved anmodning via vores salgsteam eller (for eksisterende Dropbox til virksomheder-kunder) support.

Bemærk, at Dropbox Paper ikke er omfattet af NIST SP 800-171 R2-rapporten.

FERPA og COPPA (studerende og børn)

Med Dropbox til virksomheder og Dropbox Education kan kunder bruge tjenesterne i overensstemmelse med de leverandørforpligtelser, som den amerikanske lov FERPA (Family Education Rights and Privacy Act) har fastlagt. Uddannelsesinstitutioner med elever under 13 år kan også bruge Dropbox til virksomheder eller Dropbox Education i overensstemmelse med COPPA (Children's Online Privacy Protection Act), hvis de accepterer bestemte kontraktmæssige krav om indhentning af forældres samtykke til brugen af vores tjenester.

FDA 21 CFR del 11

Afsnit 21 i Code of Federal Regulations (CFR) regulerer mad og medicin i USA for Food and Drug Administration (FDA), Drug Enforcement Administration og Office of National Drug Control Policy. Afsnit 21, del 11, angiver de kriterier, hvorunder FDA anser elektroniske poster og underskrifter for at være troværdige, pålidelige og generelt tilsvarende skriftlige registreringer og håndskrevne underskrifter, der udføres skriftligt.

Se vores Dropbox og FDA 21 CFR del 11 hvidbog og artikel i hjælpecenter for at få flere oplysninger om, hvordan Dropbox kan hjælpe med at hjælpe dig med at overholde 21 CFR del 11.

PCI DSS

Dropbox er en forhandler, som overholder Payment Card Industry Data Security Standard (PCI DSS). Dropbox til virksomheder, Dropbox Education og Dropbox Paper er dog ikke beregnet til at behandle eller gemme kreditkorttransaktioner. PCI Attestation of Compliance (AoC) for vores forhandlerstatus er tilgængelig efter anmodning.

Du kan få flere oplysninger om overholdelse vedrørende Dropbox til virksomheder og Dropbox Education på dropbox.com/business/trust/compliance.

Apps til Dropbox

DBX-platformen består af et solidt system af udviklere, der udbygger vores fleksible Application Programming Interfaces (API'er). Mere end 750.000 udviklere har oprettet applikationer og tjenester på platformen til produktivitet, samarbejde, sikkerhed, administration og meget mere.

Færdigbyggede komponenter

Chooser, Saver og Embedder er forudbyggede web- og mobilkomponenter, der giver nem adgang til Dropbox i tredjepartsapps/-websteder på bare et par kodelinjer.

- Chooser aktiverer valg af filer fra Dropbox.
- Saver giver mulighed for at vælge filer fra Dropbox.
- Embedder giver brugerne mulighed for at se filer og mapper fra Dropbox.

Autorisationen til disse komponenter er udelukkende via Dropbox. Apps får adgang til filer, der er valgt af Chooser via Dropbox-delte links eller kortvarige download-links. Disse færdigbyggede komponenter kan bruges uafhængigt eller i forbindelse med API'en som beskrevet nedenfor.

Dropbox Business API-integrationer

Den offentlige Dropbox API giver tredjepartsudviklere mulighed for at få adgang til og interagere med Dropbox i deres applikationer. Dette inkluderer fil- og metadata-interaktion, deling og teamfunktionalitet.

Godkendelse

Dropbox bruger protokollen OAuth, som er standard i branchen, til godkendelse, så brugerne får mulighed for at give apps adgang til konti uden at afsløre deres loginoplysninger til disse konti. Vi understøtter OAuth 2.0 til godkendelse af API-anmodninger. Anmodninger godkendes via Dropbox' website eller mobilapp. Dropbox understøtter OAuth-bedste praksis, bla. kortvarige adgangstokener og PKCE til distribuerede apps.

Brugertilladelser

Apps, der bruger Dropbox API, kan bygges med følgende niveau af indholdsadgang til en slutbrugers Dropbox:

- ***App-mappe.***
  Der oprettes en dedikeret mappe med samme navn som appen i mappen Apps i en brugers Dropbox. Appen får kun læse- og skriveadgang til denne mappe, og brugere kan stille indhold til rådighed for appen ved at flytte filer til denne mappe. Appen kan desuden anmode om fil-/mappeadgang via Chooser eller Saver.

- ***Fuld Dropbox.***
  Appen får fuld adgang til alle filer og mapper i en brugers Dropbox og kan også anmode om fil-/mappeadgang via Chooser eller Saver.

Ansøgninger kan også anmode om specifikke anvendelsesområder, som begrænser deres adfærd ved adgang til undergrupper af API-slutpunkter. F.eks. kan applikationer være begrænset til skrivebeskyttet adgang til filer – eller mulighed for at uploade indhold, men ikke til at oprette delinger.

Teamtilladelser

Administratorer for Dropbox til virksomheder kan godkende applikationer til administrationsfunktionalitet, som er i teamets administrationskonsol. De handlinger, som teamlinkede apps kan udføre, er begrænset gennem omfang, der specificerer, hvilke teamindstillinger appen kan læse eller administrere.

Almindelige kombinationer af omfangs-kombinationer inkluderer:

- ***Teamoplysninger***
  Skrivebeskyttet information om teamet og høj anvendelse.

- ***Teamovervågning***
  Skrivebeskyttet adgang til teaminfo og den detaljerede begivenhedslog.

- ***Filadgang som teammedlem***
  Muligheden for at udføre handlinger på vegne af brugere i teamet, f.eks. styring af deres filer og mapper.

- ***Administration af teammedlemmer***
  Tilføjelse og fjernelse af medlemmer til og fra teamet.

Webhooks

Webhooks er en måde, hvormed webapps kan modtage meddelelser i realtid om ændringer i en brugers Dropbox. Når en URI registreres til at modtage webhooks, sendes der en HTTP-anmodning til den pågældende URI, hver gang der sker en ændring for en af appens registrerede brugere. Med Dropbox Business API kan webhooks også bruges til at generere meddelelser om ændringer i teammedlemskab. Mange sikkerhedsapps bruger webhooks til at hjælpe administratorer med at spore og administrere teamaktiviteter.

Udvidelser

Apps kan registrere udvidelses-URI'er, så aktiveringer kan vises i menuerne "Del" og "Åben" i Dropbox UI. Udvidelser giver brugerne mulighed for at starte tilpassede arbejdsgange fra tredjepart direkte fra en fil i en Dropbox-overflade. Når en handling udløses, vil Dropbox omdirigere brugere til den specificerede URI, og sende en filidentifikation, der kan bruges med API til at udføre enhver filoperation. En app skal autoriseres, før en registreret udvidelse er synlig for brugeren. Vi kan promovere et udvalgt sæt udvidelsesintegrationer i menuerne "Del" og "Åbn", men disse apps har ikke adgang til indholdet, før brugeren godkender det.

Retningslinjer for Dropbox-udviklere

Vi har udarbejdet en række retningslinjer og fremgangsmåder til at hjælpe udviklere med at oprette API-apps, der respekterer og beskytter brugernes personlige oplysninger og forbedrer brugernes Dropbox-oplevelse.

- ***Appnøgler***

  Til hver enkelt app, som en udvikler opretter, skal der bruges en unik Dropbox-appnøgle. Hvis en app leverer tjenester eller software, der indkapsler DBX-platformen, således at andre udviklere kan bruge den, skal hver enkelt udvikler desuden anskaffe en individuel Dropbox-appnøgle.

- ***App-tilladelser***

  Udviklere får besked om, at en app skal bruge tilladelsen med færrest mulige tilladelser. Når en udvikler indsender en app til produktionsstatusgodkendelse, kontrollerer vi, at appen ikke anmoder om en unødvendigt bred tilladelse baseret på den funktionalitet, som appen udfører.

- ***Gennemsyn af apps***

  - **Udviklingsstatus**
    Når en Dropbox API-app udvikles, får den udviklingsstatus. Appen fungerer på samme måde som enhver produktionsstatus-app bortset fra, at den kun kan knyttes til maks. 500 Dropbox-brugere. Når en app tilknytter 50 Dropbox-brugere, har udvikleren to uger til at ansøge om og få produktionsstatusgodkendelse, før appens mulighed for at tilknytte yderligere Dropbox-brugere suspenderes.

  - **Produktionsstatus og godkendelse**
    For at opnå godkendelse til produktionsstatus skal alle API-apps overholde vores retningslinjer for branding samt vilkår og betingelser for udviklere, som indeholder eksempler på ulovlig anvendelse af DBX-platformen. Disse anvendelser omfatter: Opfordring til krænkelse af intellektuel ejendomsret eller ophavsret, oprettelse af fildelingsnetværk og ulovligt download af indhold. Udviklere bliver bedt om at give yderligere oplysninger om deres apps funktionalitet, og hvordan den bruger Dropbox API'en, før den indsendes til gennemgang. Når appen er godkendt til produktionsstatus, kan et hvilket som helst antal Dropbox-brugere oprette forbindelse til appen.

Administration af teamapps

I teamadministrationskonsollen kan administratorer af Dropbox til virksomheder administrere de forbundne apps og integrationer for deres team.

API-partnerskaber

Dropbox har arbejdet tæt sammen med sine teknologipartnere for at gøre det muligt for dem at udvikle integrationer med deres populære softwarepakker. Disse partnere udvikler applikationer ved hjælp af Dropbox API'er og arbejder tæt sammen med Dropbox' arkitekter for at følge de bedste fremgangsmåder for sikkerhed og brugeroplevelse. Disse omfatter en række produktivitetsapps til slutbrugerne samt sikkerheds- og administrationsværktøjer som f.eks.:

- ***Sikkerhedsoplysninger og begivenhedsstyring (SIEM) og analyse***

  Knyt din Dropbox til virksomheder-konto til SIEM- og analyseværktøjer, så du kan overvåge og evaluere brugerdeling, forsøg på at logge på, administratorhandlinger og meget mere. Få adgang til og administrer logs for medarbejderaktivitet og sikkerhedsrelevante data via dit centrale administrationsværktøj for logfiler.

- ***Forebyggelse af datatab (DLP)***

  Scan automatisk metadata og indhold af filer, så der udløses advarsler, rapportering og handlinger, når der foretages vigtige ændringer på din Dropbox til virksomheder-konto. Integrer virksomhedens politikker i din implementering af Dropbox til virksomheder, så du hjælper med til at overholde alle krav og regler.

- ***eDiscovery og fastfrysning af data***

  Besvar søgsmål, voldgifter og lovmæssige høringer med data fra din Dropbox til virksomheder-konto. Søg efter og indsaml relevante elektronisk gemte oplysninger, og bevar dine data gennem hele eDiscovery-processen, så du kan spare din virksomhed tid og penge.

- ***Administration af digitale rettigheder (DRM)***

  Tilføj tredjepartsprogrammer som beskyttelse af følsomme og ophavsretligt beskyttede data, der er gemt på medarbejderkonti. Få adgang til effektive DRM-funktioner, inklusive klientbaseret kryptering, vandmærkning, revisionsspor, tilbagekaldelse af adgangsrettigheder og blokering af brugere/enheder.

- ***Dataoverførsel og sikkerhedskopiering på stedet***

  Overførsel af data til Dropbox fra eksisterende servere eller andre cloudbaserede løsninger, så du sparer tid, penge og besvær. Automatisering af sikkerhedskopiering fra din Dropbox til virksomheder-konto til lokale servere.

- ***Identitetsadministration og Single Sign-On (SSO)***

  Automatisering af klargørings- og fjernelsesprocessen for brugere, og nemhed ved onboarding af nye medarbejdere. Optimering af administrationen, og styrkelse af sikkerheden ved at integrere Dropbox til virksomheder med et eksisterende identitetssystem.

- ***Brugerdefinerede arbejdsgange***

  Udvikl interne apps, der integrerer Dropbox i eksisterende forretningsprocesser, for at forbedre virksomhedens interne arbejdsgange.

Se siden for Dropbox-appintegrationer for en liste over disse teknologipartnere. Slutbrugere kan opdage udvalgte applikationer og integrationer fra 1. og 3. part i App Center.

Dropbox-integrationer

Vi har også samarbejdet med nogle af vores bedste teknologipartnere om at opbygge integrationer i Dropbox-overflader. Disse dybere integrationer er fællesudviklet af Dropbox og partneren.
Disse omfatter:

Dropbox Extensions

Med disse integrationer kan du bruge forskellige typer appudvidelser til problemfrit at udføre handlinger såsom at offentliggøre en video, tilføje filer til e-mails og chats, sende en fil til e-signering og mere, direkte fra Dropbox. Disse applikationer er bygget af partneren, mens Dropbox fremmer opdagelsen af udvalgte udvidelsespartnere gennem menuerne "Åbn med" og "Del med".

Slack, Zoom og Trello

Disse integrationer er bygget første part af Dropbox, så brugere kan starte Slack-samtaler, starte møder og oprette opgaver inden for Dropbox. Slutbrugere godkender disse værktøjer via OAuth.

Microsoft Office til mobilenheder og web

Vores Microsoft Office-integrationer giver brugere mulighed for at åbne Word-, Excel- og PowerPoint-filer, der er gemt i deres Dropbox, foretage ændringer i Office-mobilapps eller -webapps og gemme disse ændringer direkte i Dropbox. Brugerne skal give adgang den første gang, hvor en Dropbox-fil åbnes i en Office-mobilapp eller -webapp. Når de senere åbnes igen, bevares disse links.

Adobe Acrobat og Acrobat Reader

Vores integrationer med versioner af disse apps til stationær pc og mobil (Android og iOS) giver brugere mulighed for at se, redigere og dele PDF-filer, som er gemt i deres Dropbox. Brugere bliver bedt om at give adgang ved første forsøg på at åbne en Dropbox-fil i hver enkelt app. Ændringer i PDF-filer gemmes automatisk i Dropbox.

Resumé

Dropbox til virksomheder tilbyder brugervenlige værktøjer, der hjælper teams med at samarbejde effektivt, samtidig med at der tilbydes de sikkerhedsforanstaltninger og overholdelsescertificeringer, som organisationer kræver. Ved hjælp af en fremgangsmåde i flere lag, der kombinerer en solid, grundlæggende infrastruktur med en række politikker, der kan tilpasses, giver vi virksomheder en avanceret løsning, der kan skræddersys til deres unikke behov. Få flere oplysninger om Dropbox til virksomheder ved at kontakte os på sales@dropbox.com.