Sikkerhet for Dropbox Business

Et Whitepaper fra Dropbox

Dropbox

Innhold

Oversikt

Digitale transformasjoner fortsetter å ta tak i flere bransjer, og det er viktig at data, team og enheter er beskyttet uansett hvor de er. Organisasjoner som er avhengige av nettskybaserte løsninger som Dropbox Business for å aktivere eksterne og distribuerte arbeidsprosesser, må strømlinjeforme samarbeid, proaktivt håndtere risikoen i forbindelse med nettskytjenester og implementere effektive kontroller som sikrer konfidensialiteten til deres immaterielle eiendeler, integriteten (IM) til lagrede og delte data, tilgjengeligheten av data gjennom en styrt og robust nettskytjeneste.

Over 600 000 bedrifter og organisasjoner bruker Dropbox Business for å sikre at teammedlemmer som befinner seg på forskjellige steder kan samarbeide sikkert. Dropbox Business er kjernen i dette og er en løsning som består av Smart Workspace for samarbeid og funksjoner for filsynkronisering og -deling. Våre løsninger støttes av bransjeledende infrastruktur samt funksjoner for Advanced Enterprise sikkerhet, sikkerhet for team og innhold, elektronisk underskrift, sikker overføring og datastyring. Med unntak av der annet er oppgitt, gjelder informasjonen i dette dokumentet alle følgende Dropbox Business-produkter (Standard, Advanced og Enterprise) og Dropbox Education. Paper er en funksjon av Dropbox Business og Dropbox Education.

Dropbox i Dropbox Business er det omfattende sikkerhetsprogrammet vårt, Dropbox Trust-programmet, som tar en flerlags tilnærming til sikkerhet, noe som er avgjørende ettersom globale tilnærminger til eksternt arbeid utvikler seg.

Denne rapporten beskriver sikkerhetsfunksjonene i Dropbox Business, Dropbox' operative sikkerhetstiltak, vår forpliktelse om personvern og åpenhet samt administrative retningslinjer, uavhengige sertifiseringer og etterlevelse av forskrifter som gjør Dropbox til den sikre løsningen for enhver organisasjon.

Med unntak av der annet er oppgitt, gjelder informasjonen i dette dokumentet alle følgende Dropbox Business-produkter (Standard, Advanced og Enterprise) og Dropbox Education. Paper er en funksjon av Dropbox Business og Dropbox Education.

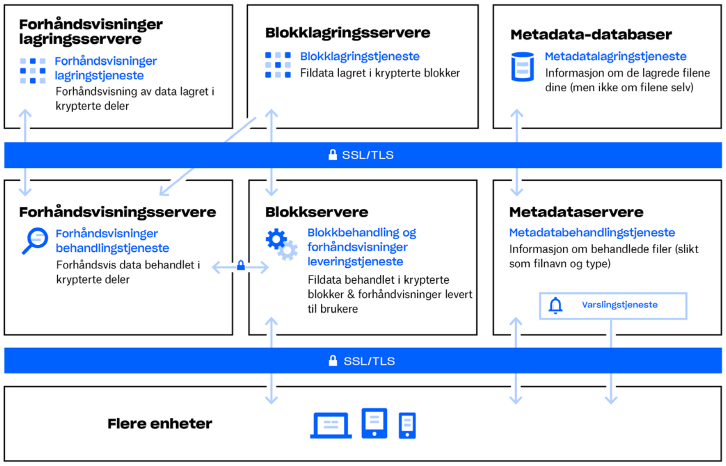
I dybden

De brukervennlige grensesnittene våre støttes av en infrastruktur som jobber bak kulissene for å sikre rask og pålitelig synkronisering, deling og samarbeid. Vi videreutvikler stadig produktet og arkitekturen for å gjøre dataoverføringene raskere og påliteligheten større, samt tilpasser oss endringer i miljøet. I dette avsnittet vil vi forklare hvordan data overføres, lagres og behandles på en sikker måte.

Filinfrastruktur

Dropbox-brukere kan åpne filer og mapper når som helst fra datamaskiner, nettet og mobilklienter eller gjennom tredjepartsapper som er koblet til Dropbox. Alle disse klientene er koblet til sikre servere for å gi tilgang til filer, tillate fildeling med andre og oppdatere tilkoblede enheter når filer legges til, endres eller slettes.

Dropbox sin filinfrastruktur består av følgende komponenter:



- ***Metadataservere***

  Visse typer grunnleggende informasjon om brukerdata, kalt metadata, oppbevares i en egen atskilte lagringstjeneste og fungerer som en indeks for dataene på brukernes kontoer. Metadata omfatter grunnleggende konto- og brukerinformasjon, som e-postadresse, navn og enhetsnavn. Metadata omfatter også grunnleggende informasjon om filer, inkludert filnavn og -typer, som hjelper støttefunksjoner som versjonshistorikk, gjenoppretting og synkronisering.

- ***Metadata-databaser***

  Filmetadata lagres i et verdilager for transaksjonsnøkler med samtidighetskontroll i flere versjoner og sønderdeles, og replikeres etter behov for å møte krav til ytelse og høy tilgjengelighet.

- ***Blokk-servere***

  Dropbox er designet med en unik sikkerhetsmekanisme for å beskytte brukerdata, som overgår tradisjonell kryptering. Blokkservere behandler filer fra Dropbox-programmer gjennom å dele hver enkelt fil inn i blokker der hver filblokk krypteres ved hjelp av en avansert kodenøkkel og ved å bare synkronisere blokker som er blitt endret fra versjon til versjon. Når Dropbox-programmet finner en ny fil eller oppdager endringer i en eksisterende fil, varsler programmet blokkserverne om endringen og nye eller modifiserte filblokker behandles og overføres til lagringsserverne. I tillegg brukes blokkservere til å levere filer og forhåndsvisninger til brukere. For detaljert informasjon om krypteringen som brukes av disse tjenestene både i transitt og ved stillstand, kan du se avsnittet om kryptering nedenfor.

- ***Lagringsservere***

  Det faktiske innholdet i brukernes filer lagres i krypterte blokker hos lagringsserverne.

  Før overføring deler Dropbox-klienten filene inn i filblokker for å forberede lagringen. Lagringsserverne fungerer som et Content-Addressable Storage-system (CAS), der hver enkelt krypterte filblokk hentes basert på hash-verdien dens.

- ***Forhåndsvisningsservere***

  Forhåndsvisningsserverne produserer forhåndsvisninger av filer. Forhåndsvisninger er en gjengivelse av en brukers fil i et annet filformat som er mer egnet for rask visning på en sluttbrukers enhet. Forhåndsvisningsservere gjenfinner filblokker fra lagringsservere å generere forhåndsvisning. Når det bes om forhåndsvisning av en fil, henter forhåndsvisningsservere den hurtigbufrede forhåndsvisningen fra lagringsservere for forhåndsvisning og overfører den til blokkservere. Forhåndsvisning leveres i siste intans av blokkservere til brukere

- ***Lagringsservere for forhåndsvisninger***

  Hurtigbufrede forhåndsvisninger lagres i et kryptert format på lagringsservere for forhåndsvisning.

- ***Varslingstjeneste***

  Denne separate tjenesten overvåker om det er gjort endringer av Dropbox-kontoer eller ikke. Ingen filer eller metadata lagres eller overføres her. Hver klient etablerer en «long poll»-tilkobling til varslingstjenesten og venter. Når en hvilken som helst fil i Dropbox endres, signaliserer varslingstjenesten endringen til de(n) aktuelle kunden(e) ved å lukke «long poll»-tilkoblingen. Når tilkoblingen lukkes, signaliserer dette at klienten på forsvarlig måte må koble til metadataserverne for å synkronisere eventuelle endringer.

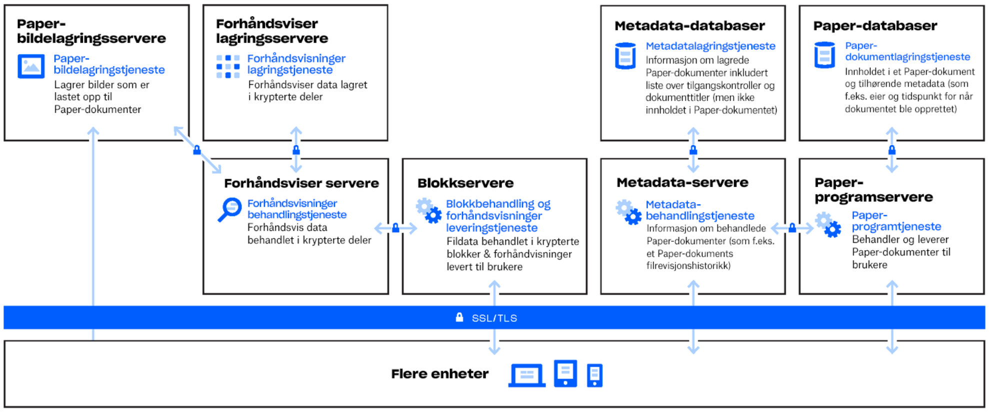
Lagring av fildata

Dropbox lagrer hovedsakelig to typer fildata: Metadata om filer (slik som tid og dato for siste endring av en fil) og det faktiske innholdet i filene (filblokker). Filmetadataene lagres på serverne til Dropbox. Filblokkene lagres i ett av to systemer: Amazon Web Services (AWS) eller Magic Pocket, som er det interne lagringssystemet til Dropbox. Magic Pocket omfatter både rettighetsbelagt programvare og maskinvare, og er utviklet med fokus på pålitelighet og sikkerhet i alle ledd. Både med Magic Pocket og AWS blir filblokkene krypterte mens de er inaktive, og begge systemene innfrir høye standarder for pålitelighet. Les avsnittet om pålitelighet nedenfor for å finne ut mer om dette.

Paper-infrastruktur

Dropbox-brukere har tilgang til Paper-dokumenter når som helst via nettbaserte og mobile klienter eller gjennom tredjeparts applikasjoner som er koblet til Dropbox Paper-programmet. Alle disse klientene kan kobles til sikre servere for å gi tilgang til Paper-dokumenter, tillate dokumentdeling med andre og oppdatere tilknyttede enheter når dokumenter legges til, endres eller slettes.

Dropbox Paper sin infrastruktur består av følgende komponenter:



- ***Paper-applikasjonservere***

  Programservere for Paper behandler brukerforespørsler, gjengir produksjon av redigerte Paper-dokumenter tilbake til brukeren og utfører varslingstjenester. Programservere for Paper skriver innkommende brukerredigeringer til Paper-databasene, der de blir plassert i vedvarende lagring. Kommunikasjonsøkter mellom programservere for Paper og Paper-databaser er kryptert med Secure Hypertext Transfer Protocol (HTTPS).

- ***Paper-databaser***

  Det faktiske innholdet til brukeres Paper-dokumenter, så vel som visse metadata om disse Paper-dokumentene, er kryptert i vedvarende lagring i Paper-databasene. Dette omfatter informasjon om et Paper-dokument (slik som tittel, opprettingstidspunkt og annen informasjon), så vel som innholdet i selve Paper-dokumentet, inkludert kommentarer og oppgaver. Paper-databasene fragmenteres og replikeres etter behov for å møte høye krav om ytelse og tilgjengelighet.

- ***Metadataservere***

  Paper bruker de samme metadataserverne som er beskrevet i infrastrukturdiagrammet i Dropbox for behandling av informasjon om Paper-dokumenter, for eksempel revisjonshistorikk og medlemskap i delte mapper. Dropbox administrerer direkte metadataservere som er lokalisert i tredjeparts samlokaliserte datasentre.

- ***Metadata-databaser***

  Paper bruker de samme databasene for metadata som er beskrevet i infrastrukturdiagrammet i Dropbox for å lagre informasjon om Paper-dokumenter som blant annet deling, tillatelser og mappetilknytninger. Metadata i Paper-dokumenter lagres i en MySQL-støttet databasetjeneste og fragmenteres og replikeres når nødvendig for å innfri høye krav til ytelse og tilgjengelighet.

- ***Paper-bildeservere***

  Bilder som lastes opp til Paper-dokumenter er lagret og kryptert i ro på bildeserverne til Paper. Overføring av bildedata mellom Paper-programmet og bildeserverne til Paper gjennomføres i løpet av en kryptert økt.

- ***Forhåndsvisningsservere***

  Forhåndsvisningsservere leverer bildeforhåndsvisninger både for bilder som er lastet opp i Paper-dokumenter og for hyperkoblinger som er innebygd i Paper-dokumenter. For bilder som er lastet opp til Paper-dokumenter, vil forhåndsvisningsservere hente bildedata lagret i bildelagringsserverne til Paper gjennom en kryptert kanal. For hyperkoblinger som er innebygd i Paper-dokumenter, vil forhåndsvisningservere hente bildedata og gjengi en forhåndsvisning av bildet ved hjelp av kryptering som er angitt av kildekoblingen. Forhåndsvisning leveres i siste intans av blokkservere til brukere

- ***Lagringsservere for forhåndsvisninger***

  Paper bruker de samme serverne for forhåndsvisningslagring som er beskrevet i diagrammet for Dropbox-infrastruktur for å lagre hurtigbufret forhåndsvisning av bilde. Hurtigbufrede deler av forhåndsvisning lagres i et kryptert format på forhåndsvisningservere.

Oppbevaring av papirdokumenter

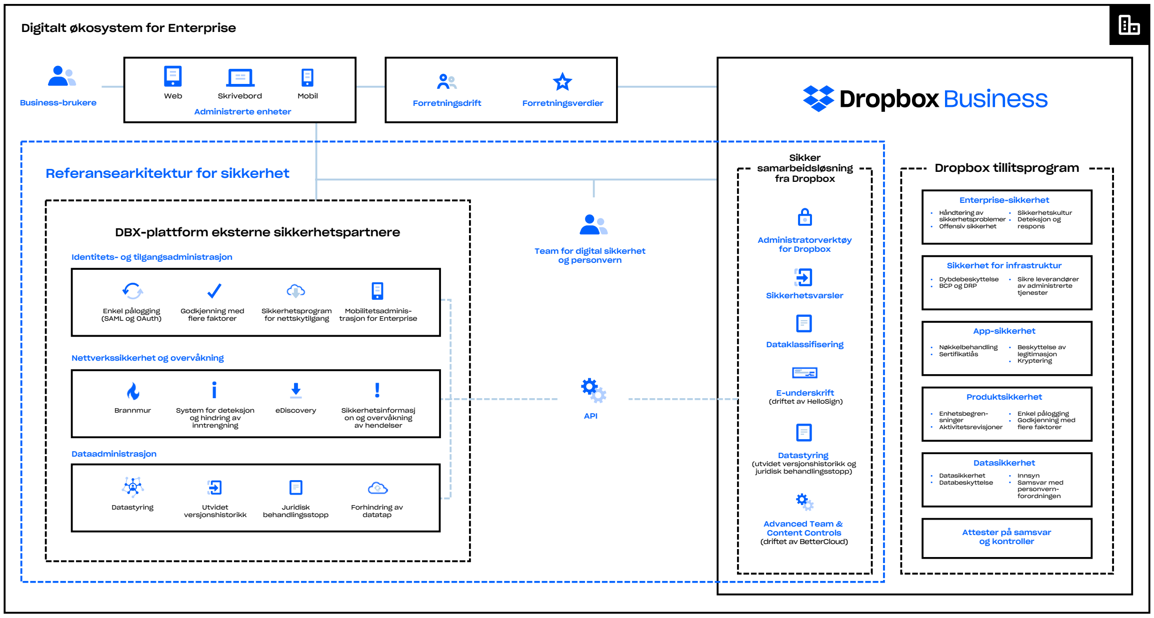
Dropbox lagrer primært følgende typer data i Paper-dokumenter: Metadata om Paper-dokumenter (slik som de delte tillatelsene til et dokument) og det faktiske innholdet til Paper-dokumenter lastet opp av brukeren. Dette er samlet referert til som Paper-dokumentdata og bilder lastet opp til Paper-dokumenter er referert til som Paper-bildedata. Hver av disse datatypene er lagret i Amazon Web Services (AWS). Paper-dokumenter er kryptert i stillstand i AWS og AWS møter høye standarder for pålitelighet. For mer informasjon, se avsnittet om pålitelighet nedenfor.

Dropbox Trust-program

Tillit er grunnlaget for forholdet vårt med flere millioner mennesker og bedrifter over hele verden. Vi setter pris på tiltroen du gir oss og tar ansvaret med å beskytte informasjonen din på alvor. For å gjøre oss fortjent til tilliten din, bygde vi og vil fortsette å utvikle Dropbox med vekt på sikkerhet, personvern og overholdelse.

Tillitsprogrammet til Dropbox etablerer en risikovurderingsprosess, som er utviklet for å håndtere miljømessige risikoer, fysiske risikoer, brukerrisikoer, risikoer fra tredjeparter, risikoer i forbindelse med gjeldende lover og forskrifter, risikoer i forbindelse med kontraktskrav og diverse andre risikoer som kan påvirke systemets sikkerhet, konfidensialitet, integritet, tilgjengelighet eller personvern. En gjennomgang av denne prosessen skjer minst én gang i året. Mer informasjon om tillitsprogrammet til Dropbox er tilgjengelig på www.dropbox.com/business/trust.

Vi benytter sikkerhet i flere lag for å sikre virksomheten, infrastrukturen, programmene og produktene som har innvirkning på organisasjonen.



Sikkerhet i bedriftsklassen

Dropbox har etablert et rammeverk for informasjonssikkerhet som beskriver hensikt, retning, prinsipper og grunnleggende regler for hvordan vi opprettholder tillit. Dette gjøres ved å vurdere risiko og kontinuerlig forbedre sikkerhet, konfidensialitet, integritet, tilgjengelighet og personvern for Dropbox Business-systemer. Med jevne mellomrom gjennomgår og oppdaterer vi retningslinjene om sikkerheten, gir opplæring i sikkerhet, utfører testing av applikasjoner og nettverk (inkludert utbredelsetesting), tilsynsføring av sikkerhetsretningslinjene, og vi gjennomfører interne og eksterne risikovurderinger.

Våre retningslinjer

Vi har etablert et grundig sett med sikkerhetspolicyer som håndheves av Dropbox Security and Abuse Team. Alle retningslinjer for sikkerhet blir gjennomgått og godkjent minst én gang i året. Ansatte, praktikanter og entreprenører deltar i obligatorisk sikkerhetsopplæring når de begynner i bedriften og får løpende opplæring innen sikkerhetsbevissthet.

- ***Informasjonssikkerhet***

  Beskytte bruker- og Dropbox-informasjon.

- ***Godkjenning***

  Beskriver hvordan Dropbox-ansatte autentiserer seg for å få tilgang til informasjonssystemer og data.

- ***Enhetssikkerhet***

  Minstekravene til sikkerhet for mobile enheter som brukes til å få tilgang til firmainformasjon.

- ***Logisk tilgangskontroll***

  Beskytte tilgangen til Dropbox-systemer, -brukere og -informasjon. Dekke tilgangskontroll til både bedrifts- og produksjonsmiljøer.

- ***Datasikkerhet***

  Beskriver hvordan Dropbox beskytter data gjennom spesifikke krav til lagring, tilgang og bruk.

- ***Reisesikkerhet***

  Beskriver hva Dropbox-ansatte bør gjøre før de reiser utenlands.

- ***Retningslinjer for sikring av salg- og kundeopplevelser (CX)***

  Sikring av brukerinformasjon, beskytte våre ansatte og sørge for kundestøtte for brukerne våre.

- ***Fysisk sikkerhet***

  Opprettholde et trygt og sikkert miljø for personer og eiendom hos Dropbox.

- ***Retningslinjer for fysisk sikkerhet for produksjon***

  Administrere fysisk tilgang til produksjonsanlegg.

- ***Hendelsesrespons***

  Skisserer måten Dropbox håndterer rapportert sikkerhet, personvern og nettstedhendelser på og dokumenterer hendelsesresponsplaner for hver.

- ***Uautorisert, opphavsrettsbeskyttet materiale***

  Forhindrer ansatte i å bruke Dropbox- eller Dropbox-systemer til å lagre eller dele uautorisert innhold.

- ***Endringsstyring***

  Håndtere endringer av produksjonssystemer. Beregnet for alle Dropbox-ansatte, kontraktører og praktikanter med tilgang til systemer.

- ***Personvern for brukerdata***

  Beskytte og håndtere brukerinformasjon og brukerdata i Dropbox i samsvar med vår personvernerklæring.

- ***Retningslinjer for forretningskontinuitet og krisehåndtering***

  Beskriver bevaring, beskyttelse og sikkerhet til mennesker (Dropbox-ansatte), eiendom og (forretnings-)prosesser.

- ***Dropbox personvernprogram***

  Hensikten, prinsippene og ansvaret for Dropbox personvernprogram.

- ***Dropbox Trust-program***

  Beskriver hvordan Dropbox fungerer og er tilliten verdig.

- ***Betalinger for miljøsikkerhet***

  Sikre og opprettholde det dedikerte betalingsmiljøet som brukes i Dropbox for å akseptere betaling med kredittkort.

Retningslinjer og tilgang for ansatte

Ved ansettelse må hver Dropbox-ansatt godta at det gjennomføres en bakgrunnssjekk og må signere en bekreftelse av sikkerhetsreglene og en taushetserklæring, samt få opplæring i sikkerhet. Kun personer som har fullført disse prosedyrene gis fysisk og logisk tilgang til bedrifts- og produksjonsmiljøer, som kreves for at de skal kunne gjøre jobben sin. I tillegg deltar alle som ansettes på obligatorisk sikkerhetsopplæring hvert år, og får jevnlig sikkerhetsbevisshetstrening via informerende e-poster, foredrag og presentasjoner og ressurser tilgjengelige på intranettet.

Ansattes tilgang til Dropbox-miljøet vedlikeholdes av en sentral katalog og autentiseres ved hjelp av en kombinasjon av sterke passord, passordbeskyttede SSH-nøkler og tofaktorautentisering. Fjerntilgang krever bruk av VPN beskyttet med to-faktors autentisering, og all spesiell tilgang gjennomgås og sikkerhetsklareres av sikkerhetsteamet. Tilgang til bedrifts- og produksjonsnettverk er strengt begrenset basert på angitte retningslinjer. For eksempel er produksjonsnettverkstilgang SSH-nøkkelbasert og begrenset til ingeniørteam som trenger tilgang for å utføre oppgavene sine. Brannmurkonfigurasjonen er strengt kontrollert og begrenset til et lite antall administratorer.

I tillegg krever våre interne retningslinjer at ansatte med tilgang til produksjon- og bedriftsmiljøer følger mønsterpraksis for etablering og lagring av private SSH-nøkler. Tilgang til andre ressurser, inkludert datasentre, konfigureringsverktøy for servere, produksjonsservere og verktøy for utvikling av kildekode gis ved eksplisitt godkjenning av aktuell ledelse. En oppføring av tilgangsforespørselen, rettferdiggjørelsen og godkjenningen blir registrert av ledelsen, og tilgang blir gitt av egnede personer.

Dropbox anvender tekniske tilgangskontroller og interne retningslinjer som forbyr de ansatte fra vilkårlig tilgang til brukerfiler og dette begrenser tilgangen til metadata og annen informasjon om brukernes kontoer. For å beskytte sluttbrukers personvern og sikkerhet har vi kun et lite antall ingeniører med ansvar for å utvikle kjernetjenestene til Dropbox som har tilgang til miljøet der brukerfiler lagres. Ansatte sin tilgang fjernes raskt når vedkommende forlater selskapet.

Ettersom Dropbox er en forlengelse av våre kunders infrastruktur, kan kundene være trygge på at vi er ansvarlige forvaltere av dataene deres. Se avsnittet Personvern nedenfor for å få mer informasjon.

Sårbarhetsadministrasjon

Sikkerhetsteamet vårt utfører automatisk og manuell testing av sikkerheten og korreksjonsrutinene og samarbeider med eksterne spesialister for å identifisere og eliminere potensielle sikkerhetssårbarheter og feil.

Som en nødvendig del av vårt system for administrasjon av informasjonssikkerhet, blir funn og anbefalinger som følger av alle disse vurderingene sendt til Dropbox-ledelsen, evaluert og nødvendige tiltak blir truffet, i den grad det anses nødvendig. Problemer med høy alvorlighetsgrad dokumenteres, spores og løses av utnevnte sikkerhetsteknikere.

Endringsadministrasjon

All utvikling, problemløsning og alle korreksjonsrutiner følger vår formelle retningslinjer for endringsstyring som er definert av Dropbox' tekniske team for å sikre at programendringer er testet og godkjent før implementering i produksjonsmiljøene. Endringer av kildekoden blir iverksatt av utviklere som ønsker å forbedre Dropbox-appen eller -tjenesten. Endringer lagres i et versjonskontrollsystem og er pålagt å gå gjennom automatiserte testprosedyrer for kvalitetskontroll (QA) for å sikre at sikkerhetskravene oppfylles. Vellykket gjennomføring av kvalitetsprosedyrer fører til at endringen implementeres. Endringer som godkjennes etter kvalitetssjekken, blir automatisk implementert i produksjonsmiljøet. Livssyklusen for programvareutvikling (SDLC) krever tilslutning til sikre retningslinjer for koding, samt screening av kodeendringer for potensielle sikkerhetsproblemer gjennom vår kvalitetssjekk og manuelle gjennomgangsprosesser. Endringer som slippes ut i produksjonen loggføres og arkiveres, og varsler sendes automatisk til Dropbox Engineering-teamledelsen.

Endringer av infrastrukturen i Dropbox er begrenset til autorisert personell. Sikkerhetsteamet hos Dropbox har ansvar for å vedlikeholde sikkerheten i infrastrukturen samt sikre at server, brannmur og andre sikkerhetsrelaterte konfigurasjoner holdes oppdaterte etter industristandarden. Regelsett for brannmuren og enkeltpersoner som har tilgang til produksjonsservere gjennomgås regelmessig.

Skanning og testing av sikkerheten (intern og ekstern)

Sikkerhetsteamet vårt utfører regelmessig automatisk og manuell sikkerhetstesting av programvaren for å identifisere og eliminere potensielle sikkerhetssårbarheter og feil i programmene for skrivebord, nett (Dropbox og Paper) og mobile (Dropbox og Paper) applikasjoner.

I tillegg inngår Dropbox kontrakter med tredjepartsleverandører for å utføre periodiske penetrasjons- og sårbarhetstester i produksjonsmiljøene. Vi samarbeider med tredjepartsspesialister, andre sikkerhetsteam i industrien og forskningsmiljøet som jobber med sikkerhet, for å sørge for at programmene våre er sikre. Vi benytter også automatiske analysesystemer for å identifisere sårbarheter. Dette inkluderer systemer vi utvikler internt, systemer med åpen kildekode som vi modifiserer etter våre behov og eksterne leverandører vi leier inn for kontinuerlig automatisert analyse.

Holde skadelig innhold vekk fra Dropbox

Vi har skannemuligheter som tar sikte på å forhindre lagring og distribusjon av skadelig innhold i Dropbox. Våre skannere benytter egenutviklet teknologi så vel som banebrytende funksjoner fra partnere som Microsoft og Google for å gjøre Dropbox til et trygt sted for kundene våre.

Bug-dusører

Selv om vi arbeider med profesjonelle firmaer for deltakelse i penetrasjonstesting og utfører våre egne tester internt, lar vi dusørjegere (bug bounties hvor enkeltpersoner belønnes for å finne sårbarheter) få innblikk i ekspertisen i det utvidede sikkerhetsfellesskapet. Vårt belønningsprogram for å finne feil gir forskere motivasjon til identifisere og å fortelle oss om programvarefeil på en ansvarlig måte. Ved å involvere det eksterne samfunnet får sikkerhetsteamet vårt en uavhengig gransking av våre programmer, noe som bidrar til å holde brukerne trygge. Vi bestreber oss på å være ledende in bransjen innen både belønninger og respons- og opprettingstider.

Vi har etablert en ramme for kvalifiserte innleveringer og Dropbox-programmer. Vi har også utformet ansvarlige retningslinjer som fremmer oppdagelse og rapportering av sikkerhetsproblemer, noe som øker sikkerheten for brukeren. Disse retningslinjene er som følger:

- Opplys om sikkerhetsproblemet i detalj
- Vis respekt for våre eksisterende applikasjoner. Spamming av skjemaer gjennom automatiserte sårbarhetsskannere vil ikke føre til noen form for belønning eller anerkjennelse fordi disse eksplisitt er utenfor omfanget.
- Gi oss rimelig tid til å svare før du offentliggjør informasjon om sikkerhetsproblemet.
- Ikke forsøk å få tilgang til eller endre brukerdata uten tillatelse fra kontoinnehaveren.
- Ikke vis, endre, lagre, oppbevar, overføre eller på annen måte åpne dataene, og fjern umiddelbart lokal informasjon når du rapporterer sårbarheten til Dropbox
- Handle i god tro for å unngå brudd på personvernet, ødeleggelse av data og avbrudd eller forringelse av tjenestene våre (inkludert tjenestenekt)

Problemer kan rapporteres ved å sende en rapport til Bugcrowd på: bugcrowd.com/dropbox.

Fysisk sikkerhet

Infrastruktur

Fysisk tilgang til fasiliteter til undertjenesteorganisasjoner der produksjonssystemer er plassert, er begrenset til Dropbox-autorisert personell som trenger tilgang for å utføre arbeidspliktene sine. Eventuelle enkeltpersoner som krever ytterligere tilgang til fasiliteter knyttet til produksjonsmiljøer, gis tilgang gjennom eksplisitt godkjenning av en egnet administrator.

En oppføring for tilgangsforespørsel, grunnlaget for forespørselen og eventuell godkjenning blir registrert av ledelsen, og tilgang blir gitt av egnede personer. Når godkjenning er mottatt vil et autorisert medlem av infrastrukturteamet kontakte den aktuelle undertjenesteorganisasjonen for å be om tilgang for personen som fikk godkjenning. Undertjenesteorganisasjonen legger inn brukerens informasjon i sitt eget system og gir det godkjente Dropbox-personellet tilgang med kodet navneskilt og om mulig tilgang med biometrisk skanning. Når godkjente personer har fått tilgang, er det datasenterets ansvar å sørge for at tilgangen er begrenset til kun de personene som fikk autorisasjon.

Bedriftens kontorer

- ***Fysisk sikkerhet***

  Teamet for fysisk sikkerhet hos Dropbox er ansvarlig for å håndheve fysiske sikkerhetsretningslinjer og kontrollere sikkerheten på våre kontorer.

- ***Retningslinjer for besøkende og tilgang***

  Fysisk tilgang til bedriftens fasiliteter, annet enn offentlige innganger og resepsjoner, er begrenset til autorisert Dropbox-personell og registrerte besøkende som har følge av Dropbox-personell. Et system for tilgang med kodete navneskilt sikrer at kun autoriserte personer får tilgang til bedriftens fasiliteter.

- ***Servertilgang***

  Tilgang til områder der bedriftens servere og nettverksutstyr befinner seg er begrenset til autorisert personell i høytstående stillinger, gitt gjennom det kodete navneskiltsystemet. Listene over autoriserte personer som er godkjent for fysisk tilgang til bedrifts- og produksjonsmiljøer gjennomgås minst hvert kvartal.

Hendelsesrespons

Vi har retningslinjer for hendelsesrespons og prosedyrer for å håndtere problemer med tilgjengelighet, integritet, sikkerhet, personvern og konfidensialitet i tjenesten. Som en del av prosedyren vår for hendelsesrespons har vi dedikerte team som er opplært til å:

- Raske svar på varsler om potensielle hendelser
- Vurdering av alvorlighetsgraden til en hendelse
- Om nødvendig, utføre tiltak for å begrense og forhindre ytterligere skade

- Kommunikasjon med relevante interne og eksterne interessenter, inkludert varsling til berørte kunder for å møte kontraktsmessige forpliktelser til brudd- eller hendelsevarsling, samt overholdelse av relevante lover og forskrifter.
- Innsamling og sikring av bevis for granskning
- Dokumentering av post mortem og utvikling av en permanent håndteringsplan

Retningslinjene og prosessene for hendelsesresponser revideres som en del av SOC 2+, ISO/IEC 27001 og andre sikkerhetsvurderinger.

Infrastruktursikkerhet

Nettverkssikkerhet

Dropbox opprettholder iherdig sikkerheten til det underliggende nettverket. Våre metoder for nettverkssikkerhet og overvåking er utviklet for å gi flere lag med beskyttelse og forsvar. Vi benytter standardiserte beskyttelsesteknikker, inkludert brannmurer, skanning av sårbarheter i nettverket, overvåking av nettverkssikkerhet og systemer for oppdagelse av inntrenging for å sikre at bare kvalifisert og ikke-skadelig trafikk er i stand til å nå infrastrukturen vår.

Vårt interne privatnettverk er segmentert i henhold til bruk og risikonivå. De primære nettverkene er:

- Internett-orientert DMZ
- Prioritert infrastruktur-DMZ
- Produksjonsnettverk
- Bedriftsnettverk

Tilgang til produksjonsmiljøet er utelukkende begrenset til autoriserte IP-adresser og krever autentisering med flere faktorer på alle endepunkter. IP-adresser med tilgang er knyttet til bedriftens nettverk eller godkjent Dropbox-personell. Autoriserte IP-adresser blir inspisert hvert kvartal for å sikre et sikkert produksjonsmiljø. Tilgang til endring av IP-adresselisten er begrenset til autoriserte personer.

Trafikk fra Internett som skal til vårt produksjonsnettverk er beskyttet ved hjelp av flere lag av brannmurer og proxier.

Det opprettholdes en streng atskillelse mellom det interne Dropbox-nettverket og det offentlige nettet. Trafikk som skal via nettet, og som kommer til og fra produksjonsnettverket, kontrolleres nøye gjennom en egen proxy-tjeneste som igjen er beskyttet av restriktive brannmurregler.

Dropbox bruker avanserte verktøysett til å overvåke bærbare maskiner og skrivebord med Mac- og Windows-operativsystemer og produksjonssystemer for å fange opp ondsinnede hendelser.bærbar Sikkerhetslogger samles et sentralt sted for rettsmedisinsk og hendelsesrespons etter bransjestandarden for oppbevaringsretningslinjer.

Dropbox identifiserer og reduserer risikoen via regelmessig sikkerhetstesting av nettverket og revisjon utført av både tilegnede interne sikkerhetsteam og tredjeparts sikkerhetsspesialister.

Lokale tilknytningspunkt (PoPs)

For å optimalisere nettstedets ytelse for brukerne bruker Dropbox tredjepartsnettverk for innholdslevering (ILN) og lokale tilknytningspunkt (PoPs) som Dropbox er vert for på 31 steder rundt om i verden. Ingen brukerdata lagres på disse lokaliseringene og alle brukerdata som overføres krypteres med SSL/TLS. Fysisk og logisk tilgang til lokale tilknytningspunkt (PoPs) som Dropbox er vert for, er begrenset til autorisert personell. Dropbox utfører optimaliseringer både i transportlaget (TCP) og programlaget (HTTP).

Node-til-node-overføring

Dropbox har åpne retningslinjer for node-til-node-overføring, og alle kunder kan bruke node-til-node-overføring med oss. For detaljer, se dropbox.com/peering.

Pålitelighet

Et lagringssystem er bare så godt som det er pålitelig, og på grunn av dette utviklet vi Dropbox med flere lag av redundans for å beskytte mot tap av data og for å sikre tilgjengelighet.

Filmetadata

Overflødige kopier av metadata er fordelt over selvstendige enheter innenfor et datasenter i minst en N+2-tilgjengelighetsmodell. Inkrementelle sikkerhetskopier utføres minst hver time, og full sikkerhetskopiering utføres hver 36. time. Metadata er lagret på servere som Dropbox administrerer og er vert for i USA.

Filblokker

Redundante kopier av filblokker lagres uavhengig i minst to separate geografiske områder og replikeres pålitelig innenfor hver region. (**Merk:** For kunder som velger å ha filene sine lagret i vår tyske, australske, japanske eller britiske infrastruktur, replikeres filblokker kun innenfor deres respektive regioner. For mer informasjon, se Datasentre og administrerte tjenesteleverandører nedenfor.) Både Magic Pocket og AWS er designet for å gi en årlig dataholdbarhet på minst 99,999999999 %.

Dropbox-arkitekturen, -programmene og -synkroniseringsmekanismene fungerer sammen for å beskytte brukerdata og gjøre dem svært tilgjengelige. Dersom det mot formodning skulle forekomme tjenesteavbrudd, har Dropbox-brukere fremdeles tilgang til den siste synkroniserte kopien av filene sine i den lokale Dropbox-mappen på tilkoblede datamaskiner. Kopier av filer som synkroniseres i skrivebordsklienten / den lokale mappen for Dropbox, vil være tilgjengelige fra brukernes harddisk under nedetider, avbrudd eller når de er frakoblet Internett. Endringer av filer og mapper synkroniseres til Dropbox så snart tjenesten eller tilkoblingen gjenopprettes.

Paper-dokumenter

Overflødige kopier av Paper-dokumentdata er fordelt over selvstendige enheter innenfor et datasenter i en N+1-tilgjengelighetsmodell. Fullstendige sikkerhetskopier av Paper-dokumentdata utføres også daglig. For lagring av Paper-dokumenter bruker Dropbox AWS-infrastruktur i USA, som er utformet til å levere en årlig dataholdbarhet på minst 99,999999999 %. Dersom det mot formodning skulle forekomme tjenesteavbrudd, har brukere fremdeles tilgang til de siste synkroniserte kopiene av Paper-dokumentene sine i «offline»-modus i mobilappen.

Filsynkronisering

Dropbox tilbyr brukerne filsynkronisering anerkjent av bransjen. Synkroniseringsmekanismene våre sikrer raske, responsive filoverføringer og gir tilgang til data hvor som helst, og fra ulike enheter. Dropbox sin synkronisering er også motstandsdyktig. Hvis hendelsen til Dropbox-tjenesten avbrytes, gjenopptar den aktuelle klienten driften sømløst når tilkoblingen er etablert igjen. Filene oppdateres bare på den lokale klienten hvis de er helt synkronisert og er godkjent med Dropbox-tjenesten. Belastningsfordeling over flere servere sikrer redundans og en konsekvent synkroniseringsopplevelse for sluttbrukerne.

Deltasynkronisering

Denne synkroniseringsmetoden vil bare laste ned/opp modifiserte deler av filer. Dropbox lagrer hver opplastede fil i diskrete, krypterte blokker og oppdaterer kun de blokkene som er endret.

Streamingsynkronisering

I stedet for å vente på at en filopplasting fullføres, vil streamingsynkroniseringen begynne å laste ned synkroniserte blokker til en annen enhet før filene er ferdig opplastet fra den første enheten. Dette gjøres automatisk når separate datamaskiner er koblet til den samme Dropbox-kontoen eller når forskjellige Dropbox-kontoer deler en mappe.

Sparer harddiskplass

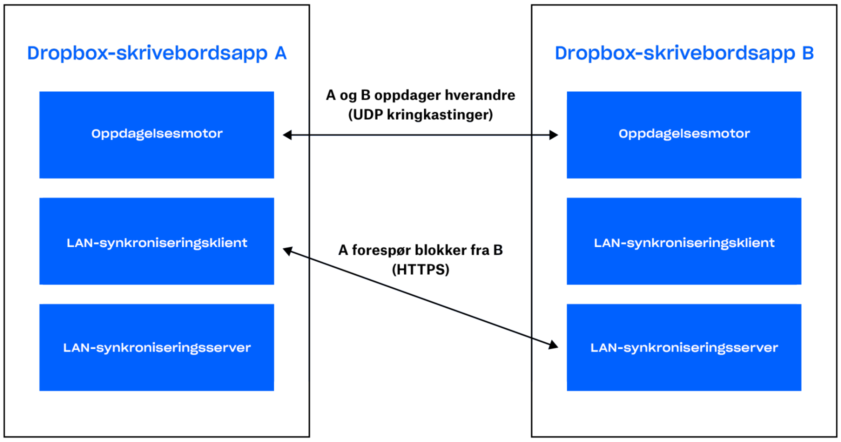
Brukere kan frigjøre lagringsplass på datamaskinene sine ved å gjøre bare filene de vil ha på harddisken tilgjengelig offline. Dette frigjør plass på datamaskinen ved å holde alt annet bare online på dropbox.com.

LAN-synkronisering

Når denne funksjonen er aktivert, lastes nye og oppdaterte filer fra andre datamaskiner ned på det samme lokale nettverket (LAN), noe som sparer tid og båndbredde sammenlignet med filnedlasting fra Dropbox-serverne.

Arkitektur

Tre hovedkomponenter i systemet for LAN-synkronisering kjører i skrivebordsappen: oppdagelsesmotoren, serveren og klienten. Utforskningsmotoren finner maskiner på nettverket å synkronisere med. Dette begrenses til maskiner som har godkjent tilgang til de samme personlige eller delte Dropbox-mappene. serveren behandler forespørsler fra andre maskiner i nettverket og leverer forespurte filblokker. Klienten ber om filblokker fra nettverket.



Oppdagelsesmotoren

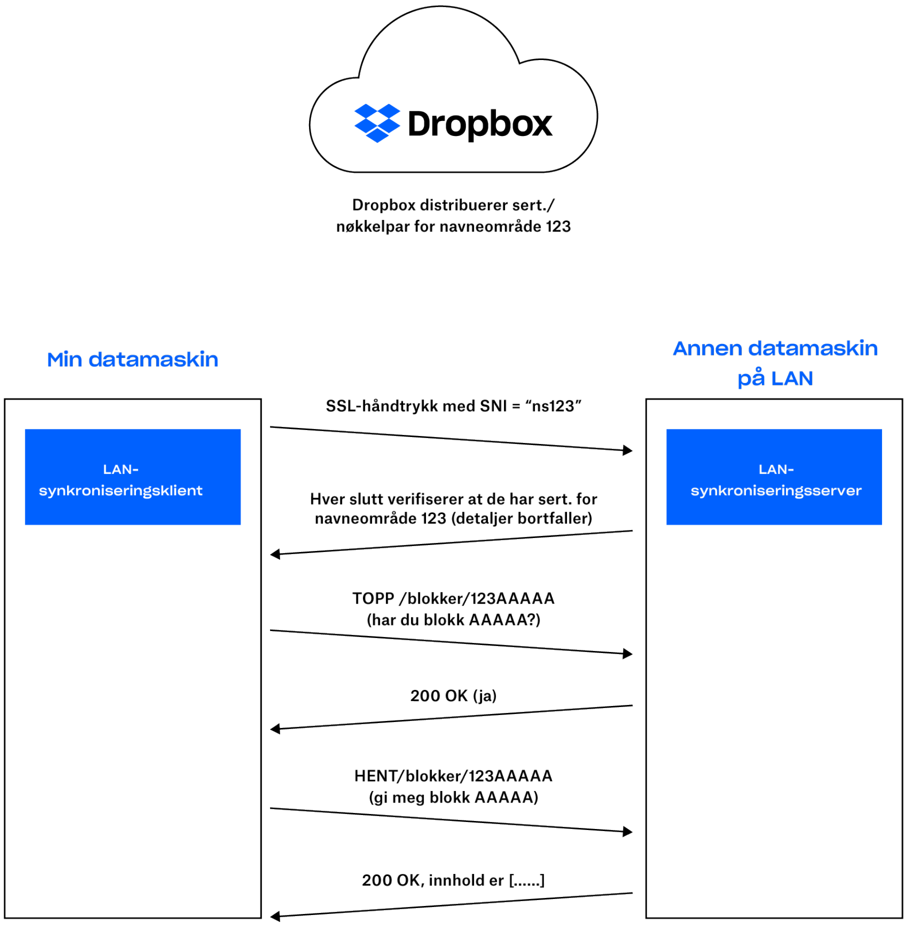
Hver maskin i det lokale nettverket sender jevnlig ut og søker etter UDP-kingkastingspakker via port 17500 (som IANA reserverer for LAN-synkronisering). Disse pakkene inneholder versjonen av protokollen som brukes av den aktuelle datamaskinen, de personlige og delte Dropbox-mappene som støttes, TCP-porten som brukes til å kjøre tjeneren (kan være en annen enn 17500 dersom denne porten er utilgjengelig), samt en tilfeldig maskinidentifikator. Når en pakke oppdages, legges IP-adressen til maskinen til i en liste for hver personlige eller delte mappe og indikerer dermed et potensielt mål.

Protokoll

Selve filblokkoverføringen skjer via en HTTPS-tilkobling. Hver datamaskin kjører en HTTPS-server med endepunkter. En klient sender forespørsler til flere noder for å sjekke om de har blokkene, men laster bare ned blokker fra én server.

For å beskytte dataene dine sikrer vi at bare klienter som er godkjente for en gitt mappe, kan be om filblokker. Vi sørger også for at datamaskiner ikke kan utgi seg for å være servere for mapper de ikke styrer. Dette gjøres ved bruk av SSL-nøkkelpar eller -sertifikatpar for hver private Dropbox eller delte mappe. Disse distribueres fra Dropbox-servere til brukerdatamaskiner som er godkjente for mappen. SSL-nøkkelparene eller -sertifikatparene roteres hver gang det skjer endringer i medlemskap (for eksempel når noen fjernes fra en delt mappe). Vi krever at begge endene av HTTPS-tilkoblingen godkjennes med det samme sertifikatet (sertifikatet for den private Dropbox-mappen eller den delte mappen). Dette sikrer at begge endene av tilkoblingen er godkjente.

Når vi oppretter en tilkobling, forteller vi serveren hvilken personlig Dropbox eller mappe vi prøver å koble til ved å bruke Server Name Indication (SNI) slik at serveren bruker riktig sertifikat.



Server/klient

Med protokollen beskrevet over trenger serveren bare å vite hvilke blokker som er tilgjengelige, for å finne dem.

Basert på resultatene fra oppdagelsesmotoren vedlikeholder klienten en liste over noder for hver private Dropbox-mappe og hver delte mappe. Når systemet for LAN-synkronisering får en forespørsel om å laste ned en filblokk, sender det en forespørsel til et tilfeldig utvalg av nodene som er oppdaget for den private Dropbox-mappen eller den delte mappen, og forespør deretter blokken fra den første noden som svarer at den har blokken.

For å unngå forsinkelser bruker vi tilkoblingsutvalg som lar oss bruke allerede opprettede tilkoblinger på nytt. Vi etablerer ikke en tilkobling før det er nødvendig, og når den er etablert, holder vi den aktiv i tilfelle vi trenger den igjen. Vi begrenser også antall tilkoblinger til én enkelt node.

Hvis en filblokk ikke blir funnet eller lastet ned, eller hvis tilkoblingen viser seg å være for treg, går systemet tilbake til å hente blokken fra Dropbox-servere.

Datasentre og administrerte tjenesteleverandører

Bedrifts- og produksjonssystemene til Dropbox er plassert i tredjeparts datasentre tilhørende undertjenesteorganisasjoner og administrerte tjenesteleverandører i ulike områder av USA. SOC-rapporter fra datasentre for undertjenesteorganisasjoner og/eller sikkerhetsundersøkelser for leverandører og kontraktmessige obligasjoner gjennomgås minst én gang i året for tilstrekkelige sikkerhetskontroller. Disse tredjeparts tjenesteleverandørene er ansvarlige for de fysiske, miljømessige og driftsmessige sikkerhetskontrollene ved overgangene til infrastrukturen til Dropbox. Dropbox er ansvarlig for den logiske sikkerheten, nettverkssikkerheten og programsikkerheten til infrastrukturen som ligger i tredjeparts datasentre.

Vår administrerte tjenesteleverandør for behandling og lagring, Amazon Web Services (AWS), er ansvarlig for logisk sikkerhet og nettverkssikkerhet for Dropbox-tjenester som leveres via deres infrastruktur. Tilkoblingene beskyttes av deres brannmur som er konfigurert i en standardmodus som blokkerer alt. Dropbox begrenser tilgangen til miljøet til et begrenset antall IP-adresser og ansatte.

Infrastruktur i Tyskland, Australia, Japan og Storbritannia

Dropbox tilbyr lagring av filblokker i regioner utenfor USA for kvalifiserte kunder. Infrastrukturen vår blir driftet av Amazon Web Services (AWS) i Tyskland, Australia, Japan og Storbritannia og blir replisert i hver enkelt region for å sikre redundans og beskytte mot datatap. Filmetadata blir lagret i Dropbox' egne servere i USA. Paper-dokumenter og forhåndsvisninger blir for tiden lagret i USA for alle kunder.

Driftskontinuitet

Dropbox bruker et administrasjonssystem for driftskontinuitet for å se hvordan vi kan gjenoppta eller fortsette å levere tjenester til brukere – samt hvordan vi kan fungere som bedrift – hvis bedriftskritiske prosesser og aktiviteter forstyrres. Vi gjennomfører en syklus bestående av følgende faser:

- ***Bedriftspåvirkning og risikovurderinger***

  Vi gjennomfører en konsekvensutredning for bedriften (BIA) minst én gang i året for å identifisere prosesser som er kritiske for Dropbox, vurdere de mulige konsekvensene av avbrudd, angi prioriterte tidsrammer for gjenoppretting og identifisere viktige faktorer vi er avhengige av, samt viktige leverandører. Vi gjennomfører også en bedriftsomfattende risikovurdering minst én gang i året. Risikovurderingen bidrar til å systematisk identifisere, analysere og vurdere risikoen for forstyrrende hendelser i Dropbox. Sammen gir risikovurderingen og konsekvensutredningen informasjon som legges til grunn for kontinuitetsprioriteringer, samt skadebegrensnings- og gjenopprettingsstrategier for bedriftskontinuitetsplaner (BCPs).

- ***Driftskontinuitetsplaner***

  Team som identifiseres som kritiske for Dropbox driftskontinuitet i konsekvensutredningen for bedriften, bruker denne informasjonen til å utvikle driftskontinuitetsplaner for viktige prosesser. Disse planene hjelper teamene med å få oversikt over hvem som er ansvarlige for å gjenoppta prosesser i nødssituasjoner, hvem som på et annet Dropbox-kontor eller beliggenhet kan ta over prosessene ved avbrudd og hvilke metoder for kommunikasjon som bør brukes under ved et kontinuitetsproblem. Disse planene bidrar også til å forberede oss for forstyrrende hendelser ved å sentralisere gjenopprettingsplanene og annen viktig informasjon, for eksempel når og hvordan planen bør brukes, kontakt- og møteinformasjon, viktige programmer og gjenopprettingsstrategier. Kontinuitetsplanene til Dropbox er knyttet til vår bedriftsomfattende krisehåndteringsplan (CMP), som beskriver Dropbox-teamene for krisehåndtering og hendelsesrespons.

- ***Plantesting/-trening***

  Dropbox tester utvalgte elementer i driftskontinuitetsplanene minst én gang i året. Disse testene er i tråd med omfanget av og målene i administrasjonssystemet for driftskontinuitet. De er også basert på passende scenarioer og er godt utviklet med tydelige målsettinger. Testene kan være alt fra vurderingsmøter til fullstendige simuleringer av realistiske hendelser. Basert på resultatene av testingen og erfaring fra faktiske hendelser, oppdaterer og forbedrer teamene planene sine for å håndtere utfordringer og styrke responsevnen.

- ***Gjennomgang og godkjenning av administrasjonssystemet for driftskontinuitet***

  Ledelsen vår går gjennom administrasjonssystemet for driftskontinuitet minst én gang i året som en del av Dropbox' Trust-program.

Katastrofegjenoppretting

For å overholde sikkerhetskrav for informasjon i krise- eller katastrofesituasjoner som påvirker driften til Dropbox for bedrifter, har vi en plan for gjenoppretting etter katastrofer. Dropbox Engineering Team vurderer denne planen årlig og tester utvalgte elementer minst årlig. Relevante funn dokumenteres og jobbes med inntil en løsning er funnet.

Planen vår for gjenoppretting etter katastrofer gjelder for både holdbarhets- og tilgjengelighetsrelaterte kriser. Disse krisetypene er definert nedenfor:

- En holdbarhetskatastrofe innebærer ett eller flere av disse scenariene:
  - Fullstendig eller permanent tap av et primærdatasenter som lagrer metadata, eller av flere datasentre som lagrer filblokker.
  - Tapt evne til å kommunisere eller levere data fra et datasenter som lagrer metadata, eller fra flere datasentre som lagrer filinnhold.
- En tilgjengelighetskatastrofe innebærer ett eller flere av disse scenariene:
  - Et strømbrudd på mer enn ti dager.
  - Tapt evne til å kommunisere eller levere data fra en lagringstjeneste eller et datasenter som lagrer metadata, eller fra flere lagringstjenester eller datasentre som lagrer filblokker.

Vi angir et mål for gjenopprettingstiden – varigheten i tid og tjenestenivået der bedriftsprosesser eller -tjenester må gjenopprettes etter en katastrofe, samt et mål for gjenopprettingsperioden – den maksimale akseptable perioden der data kan gå tapt fra et tjenesteavbrudd. Vi måler også Recovery Time Actual (RTA) under testing for katastrofegjenoppretting, som blir utført minst én gang i året.

Dropbox-planene for hendelsesrespons, driftskontinuitet og gjenoppretting etter katastrofe testes i planlagte intervaller og ved betydelige organisatoriske endringer eller miljøendringer.

Applikasjonssikkerhet

Dropbox-brukergrensesnitt

Dropbox-tjenesten er tilgjengelig og kan benyttes på en rekke grensesnitt. Hvert grensesnitt har sikkerhetsinnstillinger og funksjoner som behandler og beskytter brukerdata og samtidig sikrer enkel tilgang.

- ***Web***

  Dette grensesnittet er tilgjengelig i alle moderne nettlesere. Det gjør at brukerne kan laste opp, laste ned, vise og dele filene sine. Med nettgrensesnittet kan brukere også åpne eksisterende lokale versjoner av filer via datamaskinens standardprogram.

- ***Skrivebord***

  Skrivebordprogrammet til Dropbox er en kraftig synkroniseringsklient som lagrer filer lokalt for frakoblet tilgang. Det gir brukerne full tilgang til Dropbox-kontoene og fungerer på operativsystemene Windows, Mac og Linux. Filer vises og kan deles direkte i operativsystemets filnettlesere.

- ***Mobilt***

  Dropbox-appen er tilgjengelig for iOS- og Android-, enheter slik at brukerne kan få tilgang til alle filene sine uansett hvor de er. Mobilappen lar også brukere gjøre filer tilgjengelige for frakoblet tilgang.

- ***API***

  Dropbox API-ene gjør at data kan skrives til og fra Dropbox-brukerkontoer på en fleksibel måte. I tillegg gir de tilgang til avansert funksjonalitet som søk, revisjoner og gjenoppretting av filer. API-ene kan brukes til å administrere brukerlivssyklusen for en Dropbox Business-konto, utføre handlinger for alle medlemmene i et team, og gi tilgang til admin-funksjonalitet i Dropbox Business.

Paper-brukergrensesnitt

Paper-tjenesten er tilgjengelig og kan benyttes på en rekke grensesnitt. Hvert grensesnitt har sikkerhetsinnstillinger og funksjoner som behandler og beskytter brukerdata og samtidig sikrer enkel tilgang.

- ***Web***

  Dette grensesnittet er tilgjengelig i alle moderne nettlesere. Det gjør at brukere kan opprette, vise, redigere, laste ned og dele Paper-dokumentene sine.

- ***Mobilt***

  Den mobile Paper-applikasjonen er tilgjengelig for iOS og mobile Android-enheter og -nettbrett slik at brukere kan få tilgang til alle Paper-dokumentene sine på farten. Den mobile applikasjonen er bygget som en hybrid applikasjon som består av native kode (iOS eller Android) pakket rundt en intern webview-nettleser.

- ***API***

  API-en for Dropbox beskrevet over inneholder sluttpunkter og datatyper for administrering av dokumenter og mapper i Dropbox Paper, inkludert støtte for funksjonalitet, slik som administrering av tillatelser, arkivering og permanent sletting.

Kryptering

Data under overføring

For å beskytte data under overføring mellom Dropbox-apper og serverne, bruker Dropbox Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for dataoverføring, som oppretter en sikker tunnel som beskyttes av 128-bits AES-kryptering eller høyere. Fildata i transitt mellom en Dropbox-klient (for tiden skrivebord, mobil, API eller nett) og den vertsbaserte tjenesten, blir kryptert med SSL/TLS. På liknende vis vil Paper-dokumentdata i transitt mellom en Paper-klient (for tiden mobil, API eller nett) og de vertsbaserte tjenestene krypteres via SSL/TLS. For sluttpunkt som vi kontrollerer (skrivebord og mobil) og moderne nettlesere, bruker vi avanserte kodenøkler og støtter fullkomment hemmelighold av videresending og sertifikatlås. I tillegg flagger vi alle informasjonskapsler for autentisering på nettet som sikre og aktiverer HTTP Strict Transport Security (HSTS) med includeSubDomains aktivert.

Merk: Dropbox bruker kun TLS og har frarådet bruken av SSLv3 på grunn av kjente sårbarheter. Imidlertid omtales TLS ofte som «SSL/TLS», så vi bruker den betegnelsen her.

For å forhindre mellomleddsangrep blir autentisering av Dropbox-frontservere utført via offentlige sertifikater hos klienten. En kryptert tilkobling forhandles før overføringen av filer eller Paper-dokumenter, noe som sørger for sikker levering av filer til Dropbox sine frontservere.

Inaktive data

Dropbox-filer lastet opp av brukere er kryptert i stillstand med bruk av 256-bit Advanced Encryption Standard (AES). Filer lagres i flere datasentre i separate filblokker. Hver blokk blir fragmentert og kryptert ved hjelp av en kraftig chiffer. Bare blokker som har blitt endret mellom revisjoner, blir synkronisert. Paper-dokumenter i stillstand krypteres også med bruk av 256-bit Advanced Encryption Standard (AES). Paper-dokumenter lagres i flere tilgjengelighetssoner med bruk av tredjepartssystemer.

Nøkkelbehandling

Dropbox-infrastrukturen for nøkkelbehandling er konstruert med driftsmessige, tekniske og prosedyremessige sikkerhetskontroller med svært begrenset direkte tilgang til nøkler. Generering, utveksling og lagring av krypteringsnøkler blir distribuert for desentralisert behandling.

- ***Filkrypteringsnøkler***

  Dropbox administrerer filkrypteringsnøkler på vegne av brukere for å fjerne kompleksitet og muliggjøre avanserte produktfunksjoner og sterk kryptografisk kontroll. Filkrypteringsnøkler opprettes, lagres og beskyttes av produksjonssystemets infrastruktur for sikkerhetskontroller og sikkerhetsregler.

- ***Interne SSH-nøkler***

  Tilgang til produksjonssystemer begrenses med unike SSH-nøkkelpar. Sikkerhetsreglene og -prosedyrene krever at SSH-nøklene beskyttes. Et internt system styrer en sikker, offentlig nøkkelutvekslingsprosess og private nøkler lagres på en sikker måte. Interne SSH-nøkler kan ikke brukes for å få tilgang til produksjonssystemer uten en separat andre faktor for godkjenning.

- ***Nøkkeldistribusjon***

  Dropbox automatiserer bare administrasjon og distribusjon av sensitive nøkler til de systemene som er nødvendig for driften.

Sertifikatlås

Dropbox tilbyr sertifikatfesting i moderne nettlesere som støtter HTTP Public Key Pinning-spesifikasjonen, og på våre stasjonære og mobile klienter. Sertifikatfesting er en ekstra sjekk for å sikre at tjenesten du kobler til er den du forventer og ikke en bedrager. Vi bruker den til å beskytte mot andre metoder som dyktige hackere kan benytte for å spionere på aktiviteten din.

Beskytte autentiseringsdata

Dropbox bruker mer enn bare vanlig nøkkeltransformering for å beskytte påloggingsinformasjonen til brukerne. I tråd med beste praksis i bransjen, er alle passord kryptert med en tilfeldig generert, brukerunik kryptering, og vi bruker iterativ nøkkeltransformering til å redusere beregningshastigheten. Disse metodene bidrar til å beskytte mot rå-makt-angrep, ordbokangrep og regnbuetabellangrep. Som en ekstra forholdsregel, krypterer vi nøkkeltransformeringer med en nøkkel som oppbevares atskilt fra databasen, noe som bidrar til å holde passordet beskyttet hvis databasen alene utsettes for et sikkerhetsbrudd.

Skanning av skadelig programvare

Vi har utviklet et automatisert system som skanner etter skadelig programvare når alt innhold deles utenfor den opprinnelige brukerens konto. Systemet utnytter både proprietær teknologi og deteksjonsmotorer av industristandard og er designet for å stoppe skadelig programvare fra å spres.

Produktsikkerhet

Dropbox leverer administrative funksjoner for kontroll og innsyn som gjør det mulig for både IT-avdelingen og sluttbrukerne å administrere og sikre data på en effektiv måte. Med Dropbox får du alt du trenger til jobb – verktøy, innhold og samarbeidspartnere – på ett sted. Dropbox er mer enn bare en sikker lagringsplass – det er en smart og effektiv måte å optimalisere eksisterende arbeidsflyter på.

Nedenfor er et utvalg av funksjoner som er tilgjengelig for administratorer og brukere, samt tredjepartsintegreringer for administrasjon av sentrale IT-prosesser.

Merk: Tilgjengelige funksjoner avhenger av type abonnement. Du finner mer informasjon på dropbox.com/business/plans .

Innholdskontroller

Beskyttelse av sensitive bedriftsverdier, som intellektuell eiendom og personlig identifiserbar informasjon (PII), er avgjørende for IT- og datasikkerhetsteam. Dropbox tilbyr bransjeledende løsninger for å administrere, overvåke og beskytte innhold, fra omfattende innholdstillatelser til retningslinjer for oppbevaring av data og juridisk behandlingsstopp. Du kan se de viktigste Dropbox-produktene og -funksjonene som støtter innholdskontroll nedenfor.

Granulære innholdstillatelser og delte fil- og mappetillatelser

- ***Tillatelser for delte mapper***

  Et teammedlem som eier en delt fil, kan fjerne tilgangen for bestemte brukere og deaktivere kommentarer i filen.

- ***Tillatelser for delte filer***

  Et teammedlem som eier en delt mappe, kan oppheve mappetilgang for bestemte brukere, endre visnings- og redigeringstillatelser for bestemte brukere og overføre mappeeierskap. Avhengig av teamets globale delingstillatelser kan eieren av hver delte mappe også kontrollere om mappene kan deles med personer utenfor teamet, om andre med redigeringsrettigheter skal kunne administrere medlemskapet og om koblinger kan deles med personer utenfor mappen.

- ***Passord for delte koblinger***

  Alle delte koblinger kan beskyttes med et eierdefinert passord. Før fil- eller mappedata overføres, bekrefter et lag for tilgangskontroll at riktig passord er angitt og at alle andre krav (for eksempel team-, gruppe- eller mappe-ACL) er innfridd. Når dette er bekreftet, blir en sikker informasjonskapsel lagret i brukerens nettleser for å huske at passordet har blitt bekreftet tidligere. Med delingskontroller kan administratorer også angi standard passord, i stedet for valgfrie, for å sikre teaminnholdet bedre.

- ***Utløpsdatoer for delte koblinger***

  Brukere kan angi en utløpsdato for alle delte koblinger for å gi midlertidig tilgang til filer eller mapper. Med delingskontroller kan administratorer også angi standard utløpsdatoer, i stedet for valgfrie, for å sikre teaminnholdet bedre.

Paper-dokumenter og delte Paper-mappetillatelser

- ***Tillatelser for Paper-dokumenter og delte Paper-mapper***

  Et teammedlem som eier et Paper-dokument eller en delt Paper-mappe, kan fjerne tilgangen for bestemte brukere og deaktivere kommentarer i Paper-dokumentet.

- ***Tillatelser for Paper-dokumenter***

  Et teammedlem som eier et Paper-dokument kan fjerne tilgangen for bestemte brukere som er eksplisitt opplistet i delingspanelet. Både eieren og redaktørene av et Paper-dokument kan endre tillatelser for skrivebeskyttelse/redigering for bestemte brukere, samt endre retningslinjene for kobling av dokumentet. Retningslinjene for kobling styrer hvilke brukere som kan åpne dokumentet og tillatelsen de gis. Teamadministratoren kan angi retningslinjer for koblinger og dokumentdeling som gjelder hele teamet.

- ***Tillatelser for Paper-mapper***

  Et teammedlem som er medlem av mappen kan endre retningslinjene for deling i mappen og fjerne tilgang for bestemte brukere som eksplisitt ble lagt til mappen.

Aktiviteter i filer og mapper

- ***Teammapper for filer***

  Administratorer kan opprette teammapper som automatisk gir grupper og andre bidragsytere riktig tilgangsnivå (se eller endre) til innholdet de trenger.

- ***Detaljert tilgangs- og delingskontroll***

  Delingskontroller lar administratorer håndtere medlemskap og tillatelser på topp- eller undermappenivå slik at personer og grupper innenfor og utenfor virksomheten kun har tilgang til enkelte mapper.

- ***Administrator av teammappe***

  Administratorer kan se alle teammappene og tilpasse retningslinjer for deling fra sentralt hold for å unngå feildeling av konfidensielt materiale.

- ***Delte mapper for Paper-dokumenter***

  Administratorer kan opprette delte Paper-mapper som automatisk gir andre bidragsytere riktig tilgangsnivå—kommentere eller redigere—til innholdet de trenger.

- ***Ekstern sletting***

  Når ansatte forlater teamet eller hvis enheten mistes, kan administratorer eksternt slette Dropbox-data og lokale kopier av filer. Filene blir slettet fra både datamaskiner og mobile enheter når de kommer på nett og Dropbox-programmet kjører.

- ***Kontooverføring***

  Etter at en bruker har blitt fjernet (enten manuelt eller via katalogtjenester), kan administratorer overføre filene og eierskap av Paper-dokumenter opprettet av tidligere teammedlemmer fra brukerens konto til en annen bruker i teamet. Kontooverføringsfunksjonen kan brukes samtidig som man fjerner en bruker eller til enhver tid etter å ha slettet en brukerkonto.

Følgende funksjoner er tilgjengelige som tilleggsfunksjoner (kontakt salgsavdelingen for mer informasjon).

- ***Skann innhold***

  Med tilleggsprogrammet Advanced Team and Content Controls kan brukere av Dropbox Business Advanced og Enterprise skanne etter nytt og eksisterende innhold i Dropbox for å finne og unngå datasårbarhet.

- ***Konfigurere og utløse tilpassede arbeidsprosesser***

  Med tilleggsprogrammet Advanced Team and Content Controls kan administratorer foreta tilpassede handlinger for filer som bryter med bedriftens retningslinjer.

- ***Konfigurere varsler***

  Administratorer kan overvåke sikkerhetsproblemer i sanntid og unngå datasårbarhet. Bli varslet om filer som deles eksternt og sensitive data som skannes.

Innholdssynlighet

Sikkerhetsvarsler og -meldinger

Administratorer på Dropbox Enterprise kan motta sanntidsvarsler når misbrukende aktiviteter, risikofylt aktivitet eller potensielle datalekkasjer oppdages på kontoene deres. Disse hendelsene kan overvåkes:

- Masseslettinger
- Massedataflytting
- Sensitivt innhold delt eksternt
- Skadelig programvare som blir delt utenfor teamet
- Skadelig programvare delt med teamet ditt
- For mange mislykkede påloggingsforsøk
- Pålogging fra et høyrisikoland
- Deteksjon av løsepengevirus

Dropbox gjør det også mulig å konfigurere varslingsterskler, endre mottakere av varsler og utløse varsler ved ekstern deling av mapper som inneholder sensitive filer. Administratorer kan også merke varsler som «undersøkes», «løst» eller «avvist». I tillegg gir et kontrollprogram i administratorpanelet en samlet oversikt over teamvarslinger og trender den siste uken.

Ekstern delingsrapport og side

Dropbox tilbyr økt innsikt med en rapport og side for ekstern deling. Administratorer kan opprette en rapport enten fra innsiktssiden eller fra siden for ekstern deling. Denne rapporten gir en oversikt over alle teamfiler og -mapper som blir delt utenfor teamet og alle delte koblinger. Siden for ekstern deling er en tilleggsside i administratorverktøyet hvor administratorer kan se og filtrere (etter filtype, hvem som har delt, koblingsinnstillinger og mye mer) filene og mappene som blir delt direkte fra teamkoblinger og delte koblinger.

Del kontroller

Med delingsinnstillinger har administratorer bedre kontroll over deling, og tilgang til teaminnhold. Administratorer kan angi standard utløpsdato og/eller passordbegrensninger på teamnivå. Disse begrensningene reduserer risikoen for datatap fordi de fritar brukerne for ansvaret for å angi begrensninger.

Dataklassifisering

Team som bruker Dropbox Enterprise har mulighet for automatisk merking av personlige og sensitive data for å gi bedre beskyttelse mot eksponering. Administratorer får varsler om forhindring av datatap (DLP) på e-post og i administratorverktøyet når filer eller mapper som er lagret i teammappene og som inneholder sensitiv informasjon blir delt utenfor teamet. Administratorer har mulighet for automatisk identifisering av sensitive data som er lagret i delte mapper og i teammedlemmenes personlige mapper. Dropbox Enterprise-administratorer kan aktivere automatisk dataklassifisering fra administratorverktøyet.

Tilleggsprogram for datastyring

Datastyring er det overordnede settet med prosesser, teknologier og team som kommer sammen for å administrere og beskytte en organisasjons dataressurser. Dette inkluderer muligheten til å lagre, identifisere, gjenkjenne og gjenopprette bedriftsdata ved behov.

Dropbox' tilleggsprogram for datastyring er et sett med funksjoner som lar organisasjoner kontrollere og sikre data på en bedre måte og samtidig redusere risikoer og kostnader knyttet til innfrielse av forskriftsmessige krav og samsvarskrav. For øyeblikket inkluderer dette tilleggsprogrammet fire hovedfunksjoner for teamadministratorer og samsvarsadministratorer.

- ***Utvidet versjonshistorikk***

  Standard filversjonshistorikk avhenger av typen Dropbox-konto du har. Men med Dropbox Business kan du kjøpe et utvidet versjonshistorikk (EVH)-tilleggsprogram separat eller som en del av Data Governance-tilleggspakken som tillater gjenoppretting av alle filer som er slettet eller endret i løpet av de siste ti årene.

- ***Juridisk behandlingsstopp***

  Hvis et teammedlem blir satt i juridisk behandlingsstopp, kan team- og samsvarsadministratorer se og eksportere innhold som det medlemmet har opprettet eller endret. Medlemmer som berøres av en juridisk behandlingsstopp, vil ikke bli varslet om dette og vil fortsatt opprettholde sine tillatelser til å opprette, redigere og slette filer.

- ***Oppbevaring av data***

  Med datalagring kan team- og samsvarsadministratorer sørge for at innhold som skal lagres i en fastsatt tidsperiode i henhold til forskrifter ikke blir slettet ved et uhell. Med denne funksjonen kan kunder oppbevare data lenger enn ti år fra siste «revisjonsdato».

- ***Datadisponering***

  Med fjerning av data kan team- og samsvarsadministratorer slette data permanent på en fastsatt dato for å være i samsvar med krav til datalagring og -disponering. Administratorer kan overvåke aktivitet ved å motta rapporter som varsler dem om forestående sletting av filer.

Gjenoppretting og versjonskontroll

Alle Dropbox Business-kunder kan gjenopprette tapte filer og Paper-dokumenter og gjenopprette tidligere versjoner av filene og Paper-dokumentene for å sikre at endringer i viktige data kan spores og gjenopprettes.

Datasikkerhet på mobile enheter

- ***Sletting av data***

  For å få ekstra sikkerhet kan en bruker aktivere dette alternativet for å slette alle Dropbox-data automatisk fra enheten etter ti mislykkede passordforsøk.

- ***Intern lagring og offline-filer***

  Som standard blir ingen filer lagret internt på mobile enheter. Dropbox-mobilklienter har muligheten til å lagre individuelle filer og mapper på enheten for visning i frakoblet modus. Når en enhet kobles fra en Dropbox-konto, enten fra mobilen eller Internett-grensesnittet, slettes de lagrede filene og mappene automatisk fra enhetens interne lagringsplass.

- ***Paper-dokumenter i frakoblet modus***

  Når en enhet kobles fra Paper, fra Dropbox-kontoens sikkerhetsside, logges brukeren av og Paper-dokumenter i frakoblet modus slettes automatisk fra enhetens interne lagringsplass.

Teamkontrollerer

Ingen organisasjoner er helt like, så vi utviklet en rekke verktøy som gjør det mulig for administratorer å tilpasse Dropbox Business etter det aktuelle teamets spesielle behov. Dropbox Business inneholder verktøy som gjør det mulig for sluttbrukere å beskytte sine kontoer og data ytterligere. Godkjenning, gjenoppretting, loggføring og andre sikkerhetsfunksjoner nedenfor er tilgjengelige fra de ulike brukergrensesnittene i Dropbox.

Nedenfor er flere funksjoner for kontroll og synlighet. De er tilgjengelige via administratorverktøyet for Dropbox Business.

Detaljerte innholdstillatelser

- ***Trinnvis ordnede administratorroller***

  Dropbox tilbyr lagdelte administratorroller for å muliggjøre mer effektiv administrering av team. Kontoadministratorer kan tildeles én av tre tilgangsnivåer. Det er ingen grense for antall administratorer et team kan ha og hvert gruppemedlem kan tildeles en administratorrolle.

- ***Teamadministrator***

  Kan konfigurere sikkerhets- og delingstillatelser, opprette administratorer og administrere medlemmer. Teamadministratoren har alle tilgjengelige administratortillatelser. Kun teamadministratorer kan tildele eller endre administratorroller og det må alltid være minst én teamadministrator i en Dropbox Business-konto.

- ***Administrator for brukerhåndtering***

  Kan håndtere de fleste administrasjonsoppgavene til teamet, inklusive å legge til og fjerne teammedlemmer, administrere grupper og se på aktivitetslisten til teamet.

- ***Støtteadministrator***

  Kan håndtere vanlige tjenesteforespørsler fra teammedlemmer, som å gjenopprette slettede filer eller hjelpe medlemmer som ikke får tilgang grunnet to-trinns verifiseringen. Brukerstøtteadministratorer kan også tilbakestille passord for andre enn administratorer og eksportere aktivitetsloggen for et bestemt teammedlem.

- ***Faktureringsadministrator***

  Har tilgang til faktureringssider i administratorverktøyet.

- ***Innholdsadministrator***

  Kan opprette og administrere teammapper i funksjonen for innholdsbehandling.

- ***Rapportadmin***

  Kan opprette rapporter i administratorverktøyet og få tilgang til aktivitetssiden.

- ***Sikkerhetsadmin***

  Kan administrere sikkerhetsvarsler, ekstern deling og sikkerhetsrisikoer.

- ***Samsvarsadministrator(kun tilgjengelig for team med tilleggsprogram for datastyring)***

  Kan administrere datastyringssider (juridisk behandlingsstopp, datalagring og datadisponering) og også få tilgang til innholdsbehandling.

- ***Grupper***

  Team kan opprette og administrere lister med medlemmer i Dropbox og enkelt gi dem tilgang til bestemte mapper. Dropbox kan også synkronisere Active Directory-grupper ved bruk av Active Directory Connector.

- ***Selskapsadministrerte grupper***

  Kun administratorer kan opprette, slette og administrere medlemskap for denne typen gruppe. Brukere kan ikke sende forespørsel om å bli med i eller forlate en foretaksstyrt gruppe.

- ***Brukeradministrerte grupper***

  Administratorer kan velge om brukere kan opprette og administrere sine egne grupper. Administratorer kan også endre en brukeradministrert gruppe til en bedriftsadministrert gruppe når som helst for å ta kontroll over den.

- ***Begrensning av flere kontoer på samme datamaskin***

  Administratorer kan hindre teammedlemmer i å koble en sekundær Dropbox-konto til datamaskiner som allerede er koblet til en jobbrelatert Dropbox-konto.

- ***Opphevet brukerstatus***

  Administratorer har mulighet til å deaktivere en brukers tilgang til brukerkontoen og fortsatt bevare data- og delingsforholdet for å beskytte virksomhetens informasjon. Administratorene kan senere slette kontoene eller aktivere dem på nytt.

- ***Logg på som bruker***

  Teamadministratorer kan logge inn som medlemmer av teamene sine. Dette gir administratorene direkte tilgang til filene, mappene og Paper-dokumenter i teammedlemkontoer slik at de kan gjøre endringer, dele på vegne av teammedlemmer eller gjennomgå hendelser på filnivå. «Pålogging som bruker»-hendelser registreres i teamets aktivitetslogg og administratorer kan avgjøre om medlemmene skal varsles om disse hendelsene eller ikke.

- ***Delingstillatelser***

  Teamadministratorer har omfattende kontroll over delingsfunksjonene teamet kan bruke i Dropbox, inkludert følgende:

  - Teammedlemmer kan dele filer og mapper med personer utenfor teamet.
  - Teammedlemmer kan redigere mapper som eies av personer utenfor teamet.
  - Delte lenker opprettet av teammedlemmer vil fungere for personer utenfor teamet.
  - Teammedlemmer kan opprette filforespørsler og samle inn filer fra teammedlemmer og/eller personer utenfor teamet.
  - Folk kan se og kommentere filer som eies av teamet.
  - Teammedlemmer kan dele papirdokumenter og papirmapper utenfor teamet.
  - Permanente slettingstillatelser er gitt.

Teamadministratoren for en Dropbox Business-konto kan begrense muligheten til å permanent slette filer og Paper-dokumenter, til kun teamadministratorer.

Legge til nyansatte og nye brukere

Brukerklargjøring og metoder for identitetshåndtering

- ***E-postinvitasjon***

  Et verktøy i administratorverktøyet for Dropbox Business gjør det mulig for administratorer å generere en e-postinvitasjon manuelt.

- ***Aktiv katalog***

  Administratorer for Dropbox Business kan automatisere oppretting og fjerning av kontoer fra et eksisterende Aktiv katalog-system via vår Aktiv katalog-konnektor eller en tredjeparts identitetsleverandør. Når det er integrert, kan Aktiv katalog brukes til å administrere medlemskap.

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

Dropbox Business kan konfigureres for å gi teammedlemmer tilgang ved å logge på en sentral identitetsleverandør. Vi har en SSO-implementering som bruker bransjestandarden Security Assertion Markup Language 2.0 (SAML 2.0) og som gjør tildelinger enklere og sikrere fordi en pålitelig identitetsleverandør har ansvaret for godkjenning og fordi teammedlemmer har tilgang til Dropbox uten tilleggspassord. Dropbox har også inngått partnerskap med ledende leverandører av identitetsbehandling, slik at brukere kan legges til og fjernes automatisk. Se delen for API-integrasjoner for Dropbox Business nedenfor.

- ***API***

  Kundene kan bruke API for Dropbox Business for å skape tilpassede løsninger for brukerklargjøring og identitetshåndtering. Se avsnittet om integrering av API for Dropbox Business nedenfor.

Totrinns verifisering

Denne høyt anbefalte sikkerhetsfunksjonen gir et ekstra lag med beskyttelse på en brukers Dropbox-konto. Når to-trinns verifisering er aktivert, krever Dropbox en sekssifret sikkerhetskode i tillegg til passord når du logger på eller tilknytter en ny datamaskin, mobiltelefon eller nettbrett.

- Administratorer kan velge å kreve to-trinns verifisering for alle teammedlemmer eller bare bestemte medlemmer.
- Kontoadministratorer kan spore hvilke gruppemedlemmer som har to-trinns bekreftelse aktivert.
- Godkjenningskoder for Dropbox to-trinns verifisering kan mottas via tekstmelding eller apper som overholder algoritmestandardene for tidsbaserte engangspassord (TOTP)
- Hvis en bruker ikke kan motta sikkerhetskoder ved hjelp av disse metodene, kan vedkommende velge å bruke en 16-sifret engangskode som sikkerhetskode i nødsituasjoner. Alternativt kan vedkommende bruke et annet telefonnummer for å få en sikkerhetskode via tekstmelding.
- Dropbox støtter også den åpne standarden FIDO Universal 2nd Factor (U2F), som gjør brukergodkjenning mulig med en USB-sikkerhetsnøkkel i stedet for et sekssifret kode.

Enterprise-installatør

Administratorer som krever skalert klargjøring, kan bruke bedriftsinstallatøren vår for Windows for å fjerninstallere Dropbox-klienten for stasjonære maskiner via administrerte programvareløsninger og distribusjonsmekanismer.

Administrerte enheter og pålogging

- ***Enterprise mobility management (mobilitetsadministrasjon for bedrifter)***

  Dropbox integreres med tredjepartsleverandører av EMM for å gi administratorer av Dropbox Business-team med et Enterprise-abonnement mer kontroll over hvordan teammedlemmene bruker Dropbox på mobilenheter. Administratorer kan begrense mobilappbruk for Dropbox Enterprise-kontoer til bare administrerte enheter (jobbrelaterte eller private), få innsikt i appbruk (inkludert tilgjengelig lagringsplass og tilgangssteder) og utføre ekstern sletting for en mistet eller stjålet enhet. Vær oppmerksom på at Paper-mobilappen ikke administreres av EMM.

- ***Enhetsgodkjennelser***

  Dropbox lar administratorer av Dropbox Education- og Dropbox Business-team med Advanced- og Enterprise-abonnementer begrense antall enheter som en bruker kan synkronisere med Dropbox, samt velge om godkjenninger skal være administrator- eller brukerstyrte. Administratorer kan også opprette en unntaksliste med brukere som ikke er begrenset til et gitt antall enheter. Vær oppmerksom på at Paper-mobilappen ikke er inkludert i enhetsgodkjenninger.

- ***Krav om to-trinns verifisering***

  Administratorer kan velge å kreve to-trinns verifisering for alle teammedlemmer eller bare bestemte medlemmer. Andre krav om multi-faktor-godkjenning kan håndheves via teamets SSO-implementering.

- ***Passordkontroll***

  Administratorer for team i Education, Advanced og Enterprise kan kreve at medlemmer oppretter og opprettholder sterke og komplekse passord for kontoene sine. Når denne funksjonen er aktivert vil teammedlemmer logges ut av alle økter på nett og pålegges å opprette nye passord når de logger inn. Et innebygd verktøy analyserer passordstyrken ved å sammenligne dem opp mot en database med ofte brukte ord, navn, mønstre og tall. En bruker som skriver inn et ofte brukt passord bes om å komme opp med noe mer unikt og vanskelig å gjette. Administratorer kan også tilbakestille passord for hele teamet eller for hver enkelt bruker.

- ***Administrasjon av domener***

  Dropbox tilbyr et sett med verktøy som bedrifter kan bruke til å forenkle og fremskynde prosessen med registrering av brukere og kontrollere Dropbox-bruk.

  - **Domenebekreftelse.**
    Bedrifter kan hevde eierskap av domenene sine og få tilgang til andre verktøy for domeneadministrasjon.

  - **Invitasjonshåndhevelse.**
    Administratorer kan kreve at individuelle Dropbox-brukere som er invitert til selskapets Dropbox-team, overføres til teamet eller endrer e-postadressen i sin privatkonto.

  - **Domeneinnsikt.**
    Administratorer kan se nøkkelinformasjon, slik som hvor mange individuelle Dropbox-kontoer som bruker bedrifts-e-postadresser.

  - **Kontoinnhenting.**
    Administratorer kan tvinge alle Dropbox-brukere som bruker bedrifts-e-postadresser til å bli med i selskapets team eller endre e-postadressen i privatkontoene sine.

- ***Nettøktkontroll***

  Administratorer kan styre hvor lenge teammedlemmer kan forbli logget inn på dropbox.com. Administratorer kan begrense varigheten av alle nettøkter og/eller inaktive økter. Økter som når disse grensene vil logges av automatisk. Administratorer kan også spore og avslutte nettøkter til enkeltbrukere.

- ***App-tilgang***

  Administratorer har muligheten til å se på og inndra tredjeparters apptilgang til brukerkontoer.

- ***Fjerning av koblinger mellom enheter***

  Datamaskiner og mobile enheter som er tilknyttet brukerkontoer, kan bli frakoblet av administrator gjennom administratorverktøyet eller av brukeren gjennom individuelle kontosikkerhetsinnstillinger.

Ved frakobling via datamaskin fjernes godkjenningsdata og du får mulighet til å slette lokale kopier av filer neste gang maskinen er tilkoblet nettverket (se **ekstern sletting**). Ved frakobling via mobile enheter slettes filer som er markert som favoritter, lagrede data og påloggingsinformasjon. Frakobling fjerner også offline Paper-dokumenter fra Paper-mobilprogrammet. Hvis to-trinns verifisering er aktivert, må brukerne oppgi passord for enhver enhet ved eventuell ny tilknytting. I tillegg får brukerne muligheten til å sende en e-postmelding automatisk når enheter tilknyttes, ved hjelp av kontoinnstillingene.

- ***Nettverksstyring***

  Administratorer av Dropbox Business-team med et Enterprise-abonnement kan begrense Dropbox-bruk i bedriftens nettverk til kun Enterprise-teamkontoen. Denne funksjonen integreres med selskapets nettverkssikkerhetsleverandør for å blokkere all trafikk som eksisterer utenfor den sanksjonerte kontoen på datamaskiner. Merk at Paper for tiden ikke er administrert gjennom nettverksstyring.

Mobilsikkerhet

- ***Skanning av fingeravtrykk***

  Brukere kan aktivere Touch ID eller Face ID på iOS-enheter og fingeravtrykklås (der det støttes) på Android-enheter som en metode for å låse opp Dropbox-appen.

Tilgangsinnsyn

- ***Teknisk støtte for identitetsbekreftelse***

  Før kundestøtte hos Dropbox kan feilsøke eller utlevere kontoinformasjon, må kontoadministrator oppgi en tilfeldig generert engangskode for å bekrefte sin identitet. Denne PIN-koden er kun tilgjengelig via administratorverktøyet.

Brukerkontoaktivitet

Hver bruker kan se følgende sider fra kontoinnstillingene sine for å få oppdatert informasjon om egen kontoaktivitet:

- ***Delingsside***

  Denne siden viser de delte mappene som er i brukerens Dropbox, samt delte mapper brukeren kan legge til. En bruker kan oppheve deling av mapper og filer og angi deletillatelser.

- ***Filside***

  Denne siden viser filer som er delt med brukeren og datoen hver fil ble delt. Brukeren har muligheten til å fjerne tilgangen sin til disse filene. For å se Paper-dokumenter som har blitt delt med brukeren av andre, kan brukeren navigere til siden «Delt med meg» i grensesnittet for navigasjon av Paper-dokument.

- ***Koblingside***

  Denne siden viser alle aktive delte koblinger som brukeren har opprettet, samt opprettelsesdato for hver av dem. Den viser også alle koblinger som er delt med brukeren av andre. Brukeren kan deaktivere lenker eller endre tillatelser.

- ***E-postvarslinger***

  En bruker kan velge å motta en e-postmelding umiddelbart når en ny enhet eller app knyttes til Dropbox-kontoen.

Tillatelser for brukerkontoer

- ***Tilknyttede enheter***

  Enhets-delen av brukerens innstillinger for kontosikkerhet viser alle datamaskiner og mobile enheter som er tilknyttet brukerens konto. For alle datamaskiner vises IP-adresse, land og omtrentlig tidspunkt for siste aktivitet. En bruker kan koble fra en hvilken som helst enhet, med muligheten til å slette filer på tilknyttede datamaskiner neste gang de kobles til nettet.

- ***Aktive nettøkter***

  Nettøkt-delen viser alle nettlesere som til enhver tid er logget inn på en brukers konto. For hver av dem vises IP-adressen, landet, innloggingstidspunktet til siste økt og omtrentlig tidspunkt for siste aktivitet. En bruker kan avslutte alle økter eksternt fra brukerkontoens sikkerhetsinnstillinger.

- ***Tilknyttede apper***

  Delen **tilknyttede apper** inneholder en liste over alle tredjepartsapplikasjoner som har tilgang til brukerens konto og hvilken type tilgang hver app har. Brukeren kan oppheve appenes tilgang til brukerens Dropbox.

Aktivitetsstrøm

Dropbox Business registrerer filaktiviteter i teamets aktivitetsstrøm som er tilgjengelig via administratorverktøyet. Aktivitetsstrømmen tilbyr fleksible filtermuligheter som lar administratorer undersøke målrettet aktivitet på kontoer, filer og Paper-dokumenter. De kan for eksempel se en fullstendig historikk for filer eller Paper-dokumenter og hvordan brukere har påvirket den, eller de kan se hele teamets aktivitet i en gitt tidsperiode. Aktivitetsstrømmen kan eksporteres og lastes ned som en rapport i CSV-format og integreres direkte i et SIEM-produkt (sikkerhetsinformasjon og hendelsesadministrasjon) eller annet analyseverktøy via tredjeparts partnerløsninger. Følgende innholdshendelser registreres i aktivitetsstrømmen:

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

  Hvis aktuelt, spesifiserer rapportene hvorvidt aktiviter involverte personer som ikke tilhører teamet.

  Delte filer

  - La til eller fjernet et teammedlem eller ikke-teammedlem.
  - Endret tillatelsene for et teammedlem eller ikke-teammedlem.
  - Tillegging eller fjerning av gruppe.
  - La til en delt fil til brukerens Dropbox.
  - Viste innholdet til en fil som var delt via en fil- eller mappeinvitasjon.
  - Kopierte delt innhold til brukerens Dropbox.
  - Delt innhold lastet ned.

- Fil kommentert.
- Kommentar løst eller ikke løst.
- Kommentar slettet.
- Abonnerte eller fjernet abbonnement til kommentarvarslinger.
- Aksepterte en invitasjon til en fil eid av teamet.
- La inn forespørsel om tilgang til en fil eid av teamet.
- Trakk tilbake deling av en fil.

Delte mapper

- Opprettet en ny delt mappe.
- La til eller fjernet et teammedlem, ikke-teammedlem eller gruppe.
- La til en delt mappe til brukerens Dropbox, eller brukeren fjernet deres egen tilgang til en delt mappe.
- La til en delt mappe fra en lenke.
- Endret tillatelsene til et teammedlem eller ikke-teammedlem.
- Overførte mappeeierskap til en annen bruker.
- Deling av en mappe opphevet.
- Påberopet seg medlemskap til en delt mappe.
- Forespurte tilgang til en delt mappe.
- La til en forespurt bruker til en delt mappe.
- Blokkerte eller fjernet blokkering for ikke-teammedlemmer fra å bli lagt til en mappe.
- Tillot alle teammedlemmer eller kun eieren å legge folk til en mappe.
- Endret gruppetilgang til en delt mappe.

Delte koblinger

- Opprettet eller fjernet en lenke.
- Gjorde innholdet til en lenke synlig for alle med lenken eller kun for teammedlemmer.
- Passordbeskyttet innholdet til en lenke.
- Satte eller fjernet en utløpsdato for en lenke.
- En lenke åpnet.
- Lastet ned innholdet i en lenke.
- Kopierte innholdet til en lenke til brukerens Dropbox.
- Opprettet en lenke til en fil via en API-app.
- Delt en kobling med et teammedlem, ikke-teammedlem eller gruppe.
- Blokkering eller oppheving av blokkering for visning av lenker til filer i en delt mappe.
- Delte et album.

Filforespørsler

- Opprettet, endret, lukket eller slettet en filforespørsel.
- La brukere til en filforespørsel.
- La til eller fjernet tidsfrist for en filforespørsel
- Endret filforespørselsmappe
- Mottok filer via en filforespørsel
- Filer mottatt via E-post til Dropbox

Individuelle fil- og mappehendelser

- Fil lagt til i Dropbox
- Opprettet en mappe.
- Fil åpnet.
- Redigerte en fil
- Fil nedlastet.
- Fil eller mappe kopiert.
- Fil eller mappe flyttet.
- Ga nytt navn til en fil eller mappe.
- Endret en fil tilbake til en tidligere versjon.
- Filendringer reversert.
- Slettet fil gjenopprettet.
- Fil eller mappe slettet.
- Slettet en fil eller mappe permanent.

Vellykkede og mislykkede pålogginger

- Vellykket eller mislykket påloggingsforsøk.
- Mislykket påloggingsforsøk eller feil med Single Sign-On (SSO).
- Mislykket påloggingsforsøk eller feil via EMM.
- Logget ut.
- Endring av IP-adresse for nettøkt.

Passord

Endring av innstillinger for passord eller to-trinns verifisering. Administratorer kan ikke se brukernes faktiske passord.

- Endret eller tilbakestilt passord.
- Aktivert, nullstilt eller deaktivert to-trinns verifisering.

- Konfigurert eller endret to-trinns verifisering for bruk av SMS eller mobilapp.
- Lagt til, redigert eller fjernet reservetelefon for to-trinns verifisering.
- Lagt til eller fjernet sikkerhetsnøkkel for to-trinns verifisering.

Medlemskap

Tilleggsprogrammer for og fjerninger fra teamet.

- Inviterte et teammedlem.
- Ble medlem av teamet.
- Fjernet et teammedlem.
- Et teammedlem ble suspendert eller fikk opphevet suspensjonen.
- Gjenopprettet et fjernet teammedlem.
- Forespørsel om teammedlemskap basert på kontodomene.
- Godkjent eller avvist forespørsel om teammedlemskap basert på kontodomene.
- Domeneinvitasjoner sendt til eksisterende domenekontoer.
- Bruker ble med i teamet som resultat av kontoinnhenting.
- Bruker forlot domenet som resultat av kontoinnhenting.
- Blokkering eller oppheving av blokkering for forslag fra teammedlemmer om nye medlemmer.
- Nytt teammedlem foreslått.

Apper

Kobling av tredjepartsapper til Dropbox-kontoer.

- App godkjent eller fjernet.
- Godkjent eller fjernet en teamapp.

Enheter

Kobling av datamaskiner eller mobilenheter til Dropbox-kontoer.

- Koblet til eller frakoblet en enhet.
- Ekstern sletting brukt – alle filene ble slettet eller noen filer ble ikke slettet.
- Endring av IP-adresse for stasjonær datamaskin eller mobil enhet.

Administratorhandlinger

Endringer av innstillingene i administratorverktøyet, som f.eks. delte mappetillatelser.

- ***Godkjenning og Single Sign-On (SSO)***
  - Tilbakestill passordet til teammedlemmet.

  - Tilbakestill alle teammedlemmers passord.
  - Blokkering eller oppheving av blokkering for deaktivering av to-trinns verifisering gjort av teammedlemmer.
  - Aktivert eller deaktivert SSO.
  - Innlogging via SSO kreves.
  - Endret eller fjernet SSO-URL-en-
  - SOO-sertifikat oppdatert.
  - SSO-identitetsmodus endret.

- ***Medlemskap***
  - Brukere blokkert eller blokkering opphevet for forespørsel om teammedlemskap basert på kontodomene.
  - Angivelse av at forespørsler om teammedlemskap skal godkjennes automatisk eller om det kreves manuell godkjennelse fra administrator.

- ***Administrator av medlemskonto***
  - Endret et teammedlems navn.
  - Teammedlems e-postadresse endret.
  - Administratorstatus gitt eller fjernet, eller endring i administratorrollen.
  - På- eller avlogging som teammedlem.
  - Sletting eller overføring av innholdet i kontoen til et fjernet medlem.
  - Permanent sletting av innholdet i kontoen til et fjernet medlem.

- ***Globale delingsinnstillinger***
  - Blokkerte eller fjernet blokkering for teammedlemmer fra å legge til delte mapper eid av ikke-teammedlemmer.
  - Blokkerte eller fjernet blokkering for teammedlemmer fra å dele mapper med personer som ikke er teammedlemmer.
  - Aktiverte varslinger som vises til brukerne før de deler mapper med folk som ikke er i teamet.
  - Blokkerte eller fjernet blokkering for visning av delte koblinger for ikke-teammedlemmer.
  - Satt delte koblinger kun for team som standard.
  - Blokkerte eller fjernet blokkering for folk til å kommentere på filer.
  - Blokkerte eller fjernet blokkering for teammedlemmers oppretting av filforespørsler.
  - La til, endret eller fjernet en logo for delte koblingssider.
  - Blokkering eller oppheving av blokkering for teammedlemmer til å dele Paper-dokumenter og Paper-mapper med personer som ikke er teammedlemmer.

- ***Filadministrering for teammapper***
  - Oppretting av teammappe.
  - Nytt navn på teammappe.
  - Arkiverte eller opphevet arkivering av en teammappe.

  - Permanent sletting av teammappe.
  - Nedgraderte en teammappe til en delt mappe.

- ***Domeneadministrasjon***
  - Forsøkte å verifisere, eller verifiserte et domene eller fjernet et domene.
  - Dropbox-kundestøtten godkjente eller fjernet et domenenavn.
  - Aktiverte eller deaktiverte utsending av domeneinvitasjoner.
  - Skrudde på eller av «Automatisk inviter nye brukere».
  - Endret kontoinnhentingsmodus.
  - Dropbox kundestøtte godkjente eller avviste kontoinnhenting.

- ***Mobilitetsstyring for bedrifter (EMM)***
  - Aktiverte EMM for testmodus (alternativ) eller distribusjonsmodus (påkrevd).
  - EMM-pollett oppdatert.
  - La til eller fjernet teammedlemmer fra listen over EMM-ekskluderte brukere.
  - EMM deaktivert.
  - Opprettet en rapport for EMM-unntaksliste.
  - Opprettet en EMM-bruksrapport for mobilapp.

- ***Endringer i andre teaminnstillinger***
  - Sammenslåtte team.
  - Oppgraderte teamet til Dropbox Business eller nedgraderte til gratisteam.
  - Endring av teamnavnet.
  - Rapport for teamaktivitet opprettet.
  - Blokkerte eller fjernet blokkering for teammedlemmer fra å tilknytte flere kontoer til samme datamaskin.
  - Tillot alle teammedlemmer eller kun administratorer til å opprette grupper.
  - Blokkerte eller fjernet blokkering for teammedlemmer fra å slette filer permanent.
  - Startet eller avsluttet en Dropbox-kundestøtteøkt for en forhandler.

Grupper

Oppretting, sletting og medlemskapsinformasjon for grupper.

- Opprettet, endret navn på, flyttet eller slettet en gruppe.
- Medlem slettet eller fjernet.
- Endret et gruppemedlems tilgangstype.
- Endret gruppen til teamadministriert eller administrator-administrert.
- Endret den eksterne gruppe-ID-en.

Aktivitetslogg for Paper

Administratorer kan velge en type Paper-aktivitet i aktivitetsstrømmen eller laste ned en fullstendig aktivitetsrapport. Aktiviteter i Paper registreres for:

- Paper aktivert eller deaktivert.
- Oppretting, redigering, eksportering, arkivering, permanent sletting og gjenoppretting av Paper-dokument.
- Kommentering og oppløsning av kommentarer i Paper-dokument.
- Deling og avbrutt deling av Paper-dokument med teammedlemmer og ikke-teammedlemmer.
- Tilgangsforespørsler for Paper-dokumenter fra teammedlemmer og ikke-teammedlemmer.
- Omtaler i Paper-dokumenter for teammedlemmer og ikke-teammedlemmer
- Paper-dokumenter sett av teammedlemmer og ikke-teammedlemmer.
- Paper-dokument fulgte.
- Endringer i medlemstillatelser i Paper-dokumenter (redigering, kommentering eller skrivebeskyttet).
- Endringer i retningslinjer for ekstern deling av Paper-dokumenter.
- Oppretting, arkivering og permanent sletting av Paper-mapper.
- Paper-dokument lagt til eller fjernet fra en mappe.
- Paper-mappe endret navn.
- Overføring av Paper-dokument og mappe.

Dropbox Passwords

Dropbox Passwords er en sikker, enkel måte å lagre, synkronisere og autofylle brukernavn, passord og kreditt- og debetkort på tvers av enheter på, slik at du kan beskytte påloggingsinformasjonen din på nettet. Dropbox Passwords beskytter dine sensitive brukernavn, passord og kreditt- og debetkort på nettkontoen din med null-kunnskapskryptering i nettskyen og på enhetene dine. Våre produkter er bygget for daglig bruk og sikre ved design.

Nullkunnskapskryptering

Dropbox Passwords lagrer de krypterte dataene dine i nettskyen, men nøklene for å dekryptere disse dataene lagres kun på enhetene dine. **Dropbox har aldri tilgang til dem.** Disse tastene er lange, tilfeldige og generert på enheten din. De forlater aldri enheten din bortsett fra når du bestemmer deg for å pare eller registrere en ny enhet. Denne overføringen bruker offentlig nøkkelkryptering både for å signere og beskytte nøklene kryptografisk under overføring, slik at du kan være sikker på at ingen andre kan dekryptere dem samtidig som du bekrefter at de er autentiske. Denne egenskapen kalles ofte nullkunnskapskryptering fordi de krypterte dataene er ubrukelige for alle som ikke har nøklene, inkludert Dropbox. Dette betyr **at bare du kan se på informasjonen din**, og i det usannsynlige tilfellet at Dropbox ble hacket, vil informasjonen din fortsatt være trygg. De krypterte dataene er atskilt fra synlige Dropbox-mapper og kan ikke krysses ved hjelp av Dropbox-klienter eller API-er.

Krypteringsdetaljer

Dropbox krypterer dataene dine ved hjelp av XChaCha20-Poly1305 i kombinert modus for implisitt autentisering. Våre nettleserutvidelser og mobilapplikasjoner bruker alle krypteringsimplementeringer støttet av libsodium, som er et revidert og vidt distribuert tilleggsprogram av NaCl.

Hver krypteringsoperasjon genererer en tilfeldig 192-bits nonce, som lagres med den krypterte nyttelasten for senere dekryptering. I motsetning til AES-GCM, støtter XChaCha20-Poly1305 tilfeldige noncer. Ved dekryptering leses 192-bits nonce fra nyttelasten og brukes til å dekryptere den krypterte nyttelasten. Enhver påfølgende kryptering genererer en tilfeldig 192-bits nonce uavhengig av den forrige nonce. Dropbox Passwords genererer tilfeldige tall ved hjelp av libsodium, som standard er en kryptografisk, sikker tilfeldig tallgenerator på hver av plattformene vi støtter.

Nøkler og gjenopprettingsord

Vi genererer en 256-bits symmetrisk nøkkel (krypteringsnøkkelen) fra 128 bits entropi (brukernøkkelen) via Blake2-hashing. Denne krypteringsnøkkelen forblir bare på eierens enheter, og når det er mulig, forblir den i den sikreste lagringsplassen som vi har tilgang til på disse enhetene. På iPhone lagrer vi for eksempel krypteringsnøkkelen i iOS-nøkkelringen.

Vi bruker 128 biter med entropi som kilden vår fordi den tilbyr tilstrekkelig sikkerhet mens den bare krever tolv gjenopprettingsord ved å bruke BIP-39-standarden for sikkerhetskopiering. BIP-39 gir en menneskevennlig måte å representere store tilfeldige nøkler på ved å transformere disse nøklene til en liste med tolv ord. Enhver 128-bits nøkkel har en tilsvarende liste med ord, og hver liste på tolv ord identifiserer unikt 128 bits. Det eneste forbeholdet er at de tolv ordene faktisk tilsvarer 132 bits, så de fire ekstra bits brukes som en kontrollsum for å identifisere feil. Gjenopprettingsordene gir deg en måte å gjenopprette krypteringsnøkkelen på i tilfelle enheten mistes eller blir stjålet. Vi anbefaler å skrive dem ut og oppbevare dem på et trygt sted. Du kan også vurdere å gi dem til en pålitelig venn eller et familiemedlem, eller lagre dem på en minnepinne.

Enhetsregistrering

Når en bruker logger på Dropbox Passwords på en ny enhet, må den enheten fullføre en sikker registreringsprosedyre for å få tilgang til brukerens passorddata. Denne prosedyren bidrar til å sikre at en brukers hemmelige nøkkel og passorddata bare er tilgjengelig blant brukerens registrerte enheter. Det bidrar også til å sikre at en bruker bare kan registrere flere enheter hvis de har tilgang til en eksisterende registrert enhet eller gjenopprettingsordene deres. Prosedyren for enhetsregistrering skjer som følger.

En ny registreringsenhet genererer tilfeldig et 256-bits offentlig/privat enhetsnøkkelpar, og laster opp den offentlige nøkkelen til Dropbox-serveren. Deretter oppstår enten scenario **A**, **B** eller **C.**

A: Hvis brukeren ikke tidligere har registrert en enhet, genererer den registrerende enheten tilfeldig en 128-bits hemmelig brukernøkkel. Både brukernøkkelen og enhetsnøkkelparet er lagret på en sikker OS-spesifikk plassering som beskrevet i følgende nøkkellagringsseksjon. Enheten initialiserer brukerens passorddata, krypterer dem og laster opp den krypterte nyttelasten til Dropbox-serveren.

B: Hvis brukeren har noen tidligere registrerte enheter, sendes en forespørsel om registreringsgodkjenning til hver av disse enhetene. Registreringsenhetens offentlige nøkkel er vedlagt forespørselen. Brukeren må da godkjenne forespørselen på en av sine registrerte enheter. Hvis den er godkjent, krypterer den registrerte enheten brukernøkkelen ved å bruke dens private nøkkel og registreringsenhetens offentlige nøkkel via X25519 ECDH med XSalsa20-Poly1305. Den registrerte enheten laster opp den krypterte brukernøkkelen til Dropbox-serveren for å sende den til den registrerte enheten. Registreringsenheten laster ned og dekrypterer brukernøkkelen ved å bruke dens private nøkkel og den registrerte enhetens offentlige nøkkel. Registreringsenheten laster deretter ned de krypterte nyttelastdataene for passord og dekrypterer dem med brukernøkkelen.

C: Hvis brukeren tidligere har registrert en enhet, men ikke lenger har tilgang til dem, kan de skrive inn sine tolv gjenopprettingsord for å rekonstruere brukernøkkelen lokalt. Registreringsenheten laster deretter ned de krypterte passorddataene og dekrypterer dem med brukernøkkelen.

Oppbevaring av nøkkel

Nettleserutvidelser

På nettlesere lagres brukernøkkelen i nettleserutvidelsens lokale lagringsområde. Nettleserutvidelsens lokale lagringsverdier er bare tilgjengelige fra utvidelsen. Eventuell kode som kjører på nettsteder som brukeren besøker, kan ikke lese fra nettleserutvidelsens lokale lagringsområde. Videre tillater nettleserutvidelser kjøring av kode som ikke er inkludert i den signerte utvidelsespakken, og eliminerer risikoen for en XSS-sårbarhet som vil få tilgang til lokale lagringsverdier.

En angriper med ubegrenset tilgang til brukerens enhet kan få tilgang til brukernøkkelen ved å lese den lokale lagringsfilen på disken. Eksempler på slike trusler inkluderer: en angriper med fysisk tilgang til enheten eller en angriper som kjører skadelig programvare på enheten. For å beskytte mot disse scenariene kan brukeren konfigurere en lokal enhetspassordfrase.

Når en passordfrase er konfigurert krypteres brukernøkkelen i hvile i nettleserutvidelsens lokale lagring. Krypteringsnøkkelen er avledet fra passordfrasen gjennom Argon2-passordhashing, og krypteringsmetoden som brukes er XChaCha20-Poly1305. Hver gang nettleserutvidelsen starter på nytt, må brukeren oppgi passordfrasen for å dekryptere brukernøkkelen og låse opp dataene deres. Følgelig kan ikke en angriper uten passordfrasen dekryptere brukernøkkelen som er lagret i den lokale lagringsfilen på disken.

iOS

På iOS lagres brukernøkkelen i iOS-nøkkelringen, som er en kryptert databasefil på disken. Denne filen er kryptert med en hemmelig nøkkel som er lagret i Secure Enclave-maskinvaremodulen, med AES256-GCM som krypteringsmetode. Bare den signerte Dropbox Passwords iOS-appen kan få tilgang til elementene den har lagret i nøkkelringen. Dette forhindrer annen kode som kjører på brukerens enhet fra å få tilgang til brukernøkkelen.

Android

På Android lagres brukernøkkelen i et EncryptedSharedPreferences-objekt, som er en kryptert preferansefil på disk. Denne filen er kryptert med en hovednøkkel som er lagret i Android Keystore sikker maskinvare, med AES256-GCM som krypteringsmetode. Bare den signerte Dropbox Passwords Android-appen kan få tilgang til hovednøkkelen som brukes til å dekryptere preferansefilen.

Lokal autentisering

Dropbox Passwords gir valgfrie lokale autentiseringstiltak for ytterligere å begrense tilgangen til en brukers passorddata på deres fysiske enhet. For mobilapplikasjoner kan den lokale OS-autentiseringsbevegelsen gjenbrukes (dvs. et passord med supplerende biometrisk autentisering). For nettleserutvidelser kan du konfigurere en valgfri passordfrase. Disse mekanismene gir et ekstra lag med applikasjonssikkerhet når brukerens enhets-OS er låst opp. Dette lar brukeren sikre passorddataene sine når en annen bruker kan ha tilgang til enheten deres, for eksempel et familiemedlem eller en kollega.

Forslag til passordstyrke

Dropbox bygde åpen kildekode zxcvbn-verktøyet som brukes av flere passordbehandlere for å estimere passordstyrken. Verktøyet sammenligner passord mot en database med 30 000 vanlige passord, vanlige navn og etternavn i henhold til amerikanske folketellingsdata, populære engelske ord fra Wikipedia og amerikansk TV og filmer, og andre vanlige mønstre som datoer, repetisjoner (aaa), sekvenser (abcd), tastaturmønstre (qwertyuiop) og Leet (1337) Speak. Hvis passordet som en bruker prøver å skrive inn er vanlig, ber verktøyet dem om å skrive inn noe mer unikt og vanskelig å gjette. Ved å bruke innstillingen **Veldig sterkt** bidrar du til å sikre det høyeste nivået av kontosikkerhet for brukere.

Datasikkerhet, personvern og åpenhet

Personer og organisasjoner stoler på at Dropbox tar vare på deres viktigste arbeid hver dag, og det er ansvaret vårt å beskytte denne informasjonen og holde den privat.

Personvernerklæring

Vår personvernerklæring er tilgjengelig på www.dropbox.com/privacy. Personvernerklæringen til Dropbox, forretningsavtalen, bruksvilkårene og retningslinjene for akseptabel bruk varsler deg om følgende vilkår:

- Hva slags data vi samler inn og hvorfor.
- Hvem vi kan dele informasjon med.
- Hvordan vi beskytter disse dataene og hvor lenge vi oppbevarer dem.

- Hvor vi oppbevarer og overfører dataene dine.
- Hva skjer hvis retningslinjene endres eller du lurer på noe.

Åpenhet

Dropbox har forpliktet seg til åpenhet i håndtering av forespørsler rundt rettshåndhevelse av brukerinformasjon samt antall og type forespørsler. Vi går nøye gjennom alle dataforespørsler for å være sikre på at de overholder loven, og vi varsler brukerne når kontoene deres identifiseres i en forespørsel fra rettsinstanser, med mindre dette forbys ved lov.

Dette arbeidet understreker vår forpliktelse til å beskytte personvernet til våre brukere og deres data. For å oppnå dette opprettholder vi en åpenhetsrapport og har etablert en rekke myndighetsbegjærte prinsipper. Følgende prinsipper styrer våre handlinger når vi mottar, gransker og svarer på forespørsler fra myndighetene for brukernes data:

- ***Vis åpenhet***

  Vi mener at nettbaserte tjenester burde tillates å publisere antall og typer av mottatte statlige forespørsler og å varsle individer når informasjon om dem etterspørres. Denne type åpenhet bemyndiggjør brukerne ved å hjelpe dem med å bedre forstå hendelser og mønstre av statlige inngrep. Vi vil fortsette å publisere detaljert informasjon om disse forespørslene og jobber for retten til å gi mer av denne viktige informasjonen.

- ***Bekjemp altfor brede forespørsler***

  Statlige dataforespørsler burde begrenses til spesifikke personer og legitime undersøkelser. Vi vil motstå generelle og altfor brede forespørsler.

- ***Beskytt alle brukere***

  Lover som gir personer ulik beskyttelse basert på hvor de bor eller statsborgerskap er foreldet og reflekterer ikke den globale karakteren til nettbaserte tjenester. Vi vil fortsette å jobbe for reform av disse lovene.

- ***Levér tjenester brukerne kan stole på***

  Myndigheter burde aldri installere bakdører til nettjenester eller infiltrere infrastruktur for å innhente brukerdata. Vi kommer til å fortsette å jobbe for å beskytte systemene våre og endre lovene for å gjøre det klart at denne typen aktivitet er ulovlig.

Innsynsrapportene våre kan sees på dropbox.com/transparency.

Personvernsertifiseringer, attester og overholdelse av forskrifter.

Hver eneste dag overlater personer og organisasjoner til Dropbox å ta vare på de viktigste jobbfilene deres. Derfor er det vårt ansvar å beskytte disse filene og sørge for at uvedkommende ikke får tilgang til dem. Vår forpliktelse til personvernet ditt er kjernen i enhver beslutning vi tar.

ISO/IEC 27018 Retningslinjer for beskyttelse av personopplysninger i nettskyen og ISO/IEC 27701 (utvidelse til ISO/IEC 27001 og ISO/IEC 27002 for personverninformasjonsstyring)

Dropbox Business var en av de første store nettskytjenesteleverandørene som oppnådde sertifisering med ISO/IEC 27018 og ISO/IEC 27701.

ISO / IEC 27018 er en global standard for personvern og databeskyttelse i nettskyen og er publisert i august 2014 for spesifikt å adressere brukernes personvern og databeskyttelse.

ISO / IEC 27701 er den første sertifiserbare globale standarden for personverninformasjonsstyring og er publisert i 2019 for å gi et rammeverk for utvidelse av informasjonssikkerhetsstyringssystemet (ISMS) fra ISO / IEC 27001 til et personverninformasjonsstyringssystem (PIMS) ved å inkludere hensyn til personverndata.

Standardene stiller mange krav til hvordan Dropbox vil og ikke vil bruke informasjon til organisasjonen din:

- ***Organisasjonen din har kontroll over dataene dine***

  Vi bruker kun den personlige informasjonen du gir oss for å levere deg de tjenestene du har registrert deg for. Du kan legge til, endre eller slette filer og Paper-dokumenter fra Dropbox når du trenger det.

- ***Vi vil være åpne om dataene dine***

  Vi er åpne om hvor dataene dine ligger på våre servere. Vi informerer deg også om hvem våre betrodde partnere er. Vi informerer deg om hva som skjer når du stenger en konto eller sletter en fil eller et Paper-dokument. Til slutt, vi informerer deg dersom noe av dette endres.

- ***Dataene dine er trygge og sikre***

  ISO/IEC 27018 og and ISO/IEC 27701 er utformet som tillegg og utvidelser til ISO/IEC 27001, en av de mest aksepterte standardene for informasjonssikkerhet i verden. Vi mottok ISO/IEC 27001-fornyelse av sertifisering i oktober 2021.

- ***Våre retningslinjer gjennomgås regelmessig***

  Som en del av vår tilslutning til ISO/IEC 27018, ISO/IEC 27701 og ISO/IEC 27001, vil vi gjennomgå årlige revisjoner utført av en uavhengig tredjepart for å opprettholde disse sertifiseringene. Du kan se alle ISO-sertifiseringene våre her.

Dataoverføringer

Ved overføring av data fra EU, EØS, Storbritannia og Sveits, er Dropbox avhengig av en rekke juridiske mekanismer, for eksempel kontrakter med våre kunder og tilknyttede selskaper, standard kontraktklausuler og EU-kommisjonens beslutninger om tilstrekkelighet om visse land, som aktuelt.

Dropbox overholder EU–US og Swiss–US Privacy Shield Frameworks som fastsatt av US Department of Commerce angående innsamling, bruk og oppbevaring av personopplysninger overført fra EU, Det europeiske økonomiske samarbeidsområdet, Storbritannia og Sveits til USA, selv om Dropbox ikke er avhengig av EU-US Privacy Shield eller Swiss-US Privacy Shield Frameworks som juridisk grunnlag for overføring av personopplysninger. Dropbox har sertifisert overfor handelsdepartementet at de overholder Privacy Shield-prinsippene med hensyn til slike data. Du kan også lære mer om Privacy Shield på https://www.privacyshield.gov.

Klager og tvister knyttet til vår Privacy Shield-overholdelse etterforskes og løses gjennom JAMS, en uavhengig tredjepart. For å få vite mer, se personvernerklæringen vår (dropbox.com/privacy).

EUs personvernforordning (GDPR)

General Data Protection Regulation (GDPR) er en EU-forordning fra 2018 som etablerer et omfattende rammeverk for håndtering og beskyttelse av personopplysninger.

Dropbox er forpliktet til sikkerhet og beskyttelse av våre brukeres data i tråd med juridiske krav og beste fremgangsmåter til enhver tid. I tråd med vår forpliktelse overfor våre brukere har vi jobbet hardt for å sikre at Dropbox er GDPR-kompatibelt, inkludert å utnevne en ansvarlig for databeskyttelse som gir vårt personvernprogram ny design og konfigurasjon for å sikre at brukerne kan utøve sine datasubjektrettigheter, som dokumenterer våre databehandlingsaktiviteter; og støtter våre interne prosesser i tilfelle av et sikkerhetsbrudd. Vi fortsetter å gjøre justeringer for å sikre at, ettersom ytterligere veiledning fortsetter å dukke opp fra databeskyttelsesmyndighetene, vår prosess og praksis overholder eller overgår bestemte elementer i de nye reglene.

EU-retningslinjer for skyløsninger

EUs Cloud Code of Conduct er et frivillig instrument som gjør det mulig for en nettskytjenesteleverandør, som for eksempel Dropbox, å demonstrere vår forpliktelse til GDPR-overholdelse. Dropbox Business, som består av Standard-, Advanced-, Enterprise- og Education-abonnementene for team, har blitt erklært å følge EUs Cloud Code of Conduct og mottatt et samsvarsmerke på «Nivå 2», som betyr at disse tjenestene har implementert teknisk, organisatoriske og kontraktsmessige tiltak i tråd med kravene i retningslinjene. For mer informasjon om EUs Cloud Code of Conduct og Dropboxs overholdelse av koden, besøk kodens offisielle nettsted.

For mer informasjon om retningslinjene våre for personvern og politikk, se Dropbox sitt hvitbok for personvern og databeskyttelse.

Overholdelse av standarder

Det finnes mange forskjellige lovpålagte og bransjespesifikke forskrifter for sikkerhet og personvern som en organisasjon må oppfylle. Vår tilnærmingen er å kombinere de mest aksepterte standardene med samsvarstiltak innrettet mot de spesifikke behovene til våre kunders bedrifter eller bransjer.

ISO

Den internasjonale standardiseringsorganisasjonen (ISO) har utarbeidet en serie standarder i verdensklasse for informasjons- og samfunnssikkerhet for å hjelpe organisasjoner med å utvikle pålitelige og innovative produkter og tjenester. Dropbox har sertifisert sine datasentre, systemer, applikasjoner, personer og prosesser gjennom en rekke revisjoner av en uavhengig tredjepart, EY CertifyPoint, Nederland. EY CertifyPoint opprettholder sine ISO-akkrediteringer fra Raad voor Accreditatie (det nederlandske akkrediteringsrådet).

ISO/IEC 27001 (informasjonssikkerhet)

ISO/IEC 27001 er anerkjent som hovedstandarden for informasjonssikkerhet (ISMS) rundt om i verden. Standarden tar i bruk de beste fremgangsmåtene for sikkerhet detaljert i ISO/IEC 27002. For å gjøre oss fortjent til tilliten din jobber vi hele tiden med omfattende administrasjon av våre fysiske, tekniske og juridiske kontroller hos Dropbox.

Se ISO/IEC 27001-sertifikatet for Dropbox Business og Dropbox Education.

ISO/IEC 27017 (nettskysikkerhet)

ISO/IEC 27017 er en internasjonal standard for nettskysikkerhet som gir retningslinjer for sikkerhetskontroller rundt tillegg og bruk av nettskytjenester. Vår guide for felles ansvar forklarer kravene til sikkerhet, personvern og samsvar som Dropbox og deres kunder kan løse sammen.

Se ISO/IEC 27017-sertifikatet for Dropbox Business og Dropbox Education.

ISO/IEC 27018 (personvern i nettsky og databeskyttelse)

ISO/IEC 27018 er en internasjonal standard for personvern og databeskyttelse. Den gjelder for leverandører av nettskytjenester som Dropbox som behandler personlig informasjon på vegne av kundene sine og gir et grunnlag for kundene våre for vurdering av vanlige forskriftsmessige og kontraktsmessige krav eller spørsmål.

Se ISO/IEC 27018-sertifikatet for Dropbox Business og Dropbox Education.

ISO/IEC 22301 (driftskontinuitet)

ISO/IEC 22301 er en internasjonal standard for driftskontinuitet som veileder organisasjoner rundt hvordan man kan minske sannsynligheten for forstyrrende hendelser, og håndtere dem ved å minimere potensiell skade hvis de oppstår. Administrasjonssystemet for driftskontinuitet for Dropbox Business (BCMS) er en del av vår generelle strategi for risikostyring for å beskytte personer og operasjoner i krisetider.

Se ISO/IEC 22301-sertifikatet for Dropbox Business og Dropbox Education.

ISO / IEC 27701 (personverninformasjonsstyring)

ISO 27701 er en internasjonal standard for personverninformasjonsstyring. Standarden gir en ramme for å forbedre og utvide informasjonssikkerhetsstyringssystemet under ISO 27001 til et personverninformasjonsstyringssystem (PIMS). Dropbox Business og Dropbox Education har mottatt denne sertifiseringen som PII-behandler.

Se Dropbox Business og Dropbox Education ISO 27701-sertifikat.

SOC

SOC-rapportene, kjent som SOC 1, SOC 2 eller SOC 3, er rammeverk opprettet av American Institute of Certified Public Accountants (AICPA) for rapportering av interne kontroller gjennomført i en organisasjon. Dropbox har sertifisert sine systemer, programmer, personer og prosesser gjennom en rekke revisjoner av en uavhengig tredjepartsrevisor, Ernst & Young LLP.

SOC 3 for sikkerhet, konfidensialitet, tilgjengelighet og personvern

SOC 3-garantirapporten dekker alle fem kriteriene for tjenestetillit; sikkerhet, konfidensialitet, integritet, tilgjengelighet og personvern. (TSP avsnitt 100). Rapporten for generell bruk for Dropbox er et sammendrag av SOC 2-rapporten, og inkluderer vår uavhengige tredjeparts revisors oppfatning av effektiviteten i design og drift av kontrollene våre.

Se SOC 3-undersøkelsen for Dropbox Business og Dropbox Education.

SOC 2 for sikkerhet, konfidensialitet, integritet, tilgjengelighet og personvern

SOC 2-rapporten gir kundene et detaljert innsyn i kontrollbaserte forsikringer, og dekker de fem kriteriene for tjenestetillit; sikkerhet, tilgjengelighet, prosesseringsintegritet, konfidensialitet og personvern (TSP avsnitt 100). SOC 2-rapporten vår inkluderer en detaljert beskrivelse av prosessene våre og de nærmere 100 kontrollene på plass for å beskytte tingene dine. I tillegg til vår uavhengige tredjeparts revisors oppfatning av effektiviteten i design og drift av våre kontroller inkluderer den også deres testprosedyrer og resultater for hver eneste kontroll. SOC 2-rapporten vår (noen ganger referert til som en SOC 2+-rapport) inkluderer også en revidert kartlegging av kontrollene våre til ISO-standardene nevnt ovenfor, noe som gir ytterligere gjennomsiktighet for kundene våre. SOC 2-undersøkelsen for Dropbox Business og Dropbox Education er tilgjengelig på forespørsel.

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

SOC 1-rapporten gir spesifikke forsikringer for kunder som mener at Dropbox Business eller Dropbox Education er et nøkkelelement i deres interne kontroll over programmer for finansiell rapportering (ICFR). Disse spesifikke forsikringene brukes hovedsaklig for våre kunders Sarbanes-Oxley-samsvar (SOX). Den uavhengige tredjepartens revisjon utføres i samsvar med Statement on Standards for Attestation Engagements, nr. 18 (SSAE 18) og International Standard on Assurance Engagements, nr. 3402 (ISAE 3402). Disse standardene har erstattet den frarådede Statement on Standards for Attestation Engagement, nr. 16 (SSAE 16) og Statement on Auditing Standards, nr. 70 (SAS 70). SOC 1-undersøkelsen for Dropbox Business og Education er tilgjengelig på forespørsel.

CSA

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

CSA Security, Trust & Assurance Registry (STAR) er et gratis og offentlig tilgjengelig register som tilbyr et sikkerhetsforsikringsprogram for nettskytjenester. Programmet hjelper brukere med å vurdere sikkerhetstilstanden til nettskyleverandører de bruker eller som de vurderer å inngå avtale med.

Dropbox Business og Dropbox Education har både CSA STAR Level 2-sertifisering og Level 2-attestering. CSA STAR nivå 2 krever en uavhengig tredjepartsvurdering av sikkerhetskontrollene våre av EY CertifyPoint (for sertifisering) og Ernst & Young LLP (for attestasjon), basert på kravene for ISO 27001, SOC 2 for tjenesteklarering og CSA Cloud Controls Matrix (CCM) v4.0.2.

Se vår CSA STAR Level 2-sertifisering og Attestation på CSA-nettstedet.

HIPAA/HITECH

Dropbox vil signere Business Associate Agreements (BAAs) med Dropbox Business eller Dropbox Education-kunder som krever dem for å overholde Health Insurance Portability and Accountability Act (HIPAA) og Health Information Technology for Economic and Clinical Health Act (HITECH). Se Dropbox og HIPAA/HITECH for mer informasjon.

Dropbox gjør tilgjengelig en tredjeparts forsikringsrapport som evaluerer kontrollene våre for reglene til HIPAA og HITECH for sikkerhet, personvern og bruddvarsling, i tillegg til en kartlegging over våre interne praksiser og anbefalinger for kunder som vil innfri sikkerhet- og personvernreglene i HIPAA/HITECH med Dropbox Business eller Dropbox Education.

Kunder som er interessert i disse dokumentene eller ønsker å lære mer om kjøp av Dropbox Business eller Dropbox Education, kan kontakte vårt salgsteam. Hvis du allerede er teamadministrator for Dropbox Business eller Dropbox Education, kan du signere en BAA elektronisk fra kontosiden i administratorverktøyet.

Vær oppmerksom på at muligheten til å signere en BBA elektronisk via administratorverktøyet kun er tilgjengelig for kunder i USA.

NIST 800-171

US National Institute of Standards and Technology (NIST) fremmer og vedlikeholder standarder og retningslinjer for å beskytte informasjonssystemer. NIST Special Publication (SP) 800171 Revisjon 2 (R2) gir retningslinjer for beskyttelse av kontrollert uklassifisert informasjon (CUI) i ikke-føderale informasjonssystemer og organisasjoner. Enhver enhet som behandler eller lagrer amerikanske myndigheters CUI, for eksempel forskningsinstitusjoner og utdanningssektoren, bør overholde NIST SP 800-171 R2. Dropbox sine CUI-systemer, prosesser og kontroller ble validert av en uavhengig tredjepartsrevisor, Ernst & Young LLP.

NIST SP 800-171 R2-rapporten for Dropbox Business og Dropbox Education er tilgjengelig på forespørsel gjennom salgsteamet vårt eller (for eksisterende Dropbox Business-kunder) kundestøtte.

Vær oppmerksom på at Dropbox Paper ikke er inkludert i omfanget av NIST SP 800-171 R2-rapporten.

FERPA og COPPA (studenter og barn)

Dropbox Business og Dropbox Education lar kundene bruke tjenestene i overensstemmelse med leverandørforpliktelser pålagt av US Family Education Rights and Privacy Act (FERPA). Utdanningsinstitusjoner med elever under 13 år kan også bruke Dropbox Business eller Dropbox Education i tråd med Children's Online Privacy Protection Act (COPPA), forutsatt at de samtykker til spesifikke kontraktsbestemmelser som krever at institusjonen må få foreldrenes samtykke ved bruk av tjenestene våre.

FDA 21 CFR del 11

Tittel 21 i Code of Federal Regulations (CFR) regulerer mat og medisiner i USA for Food and Drug Administration (FDA), Drug Enforcement Administration og Office of National Drug Control Policy. Del 11 av tittel 21 angir kriteriene der FDA anser elektroniske poster og signaturer som ansvarlige, pålitelige og generelt likeverdig med fysiske registreringer og håndskrevne signaturer utført på papir.

Se Dropbox og FDA 21 CFR del 11 hvitebokog hjelpesenterartikkel for mer informasjon om hvordan Dropbox kan hjelpe deg med aktivitetene for etterleve 21 CFR del 11.

PCI DSS

Dropbox som bedrift overholder Payment Card Industry Data Security Standard (PCI DSS). Imidlertid er Dropbox Business, Dropbox Education og Dropbox Paper ikke beregnet for behandling eller lagring av kredittkorttransaksjoner. PCI Attestation of Compliance (AoC) for vår handelsstatus er tilgjengelig på forespørsel.

Mer informasjon om Dropbox Business og Dropbox Education-overholdelse, besøk dropbox.com/business/trust/compliance.

Applikasjoner for Dropbox

DBX Platform består av et robust økosystem av utviklere som bygger videre på de fleksible API-ene (Application Programming Interface). Mer enn 750 000 utviklere har bygget programmer og tjenester på plattformen for produktivitet, samarbeid, sikkerhet, administrasjon med mer.

Forhåndsbygde komponenter

Chooser, Saver, og Embedder er ferdigbygde komponenter for nett og mobil som gir enkel tilgang til Dropbox i tredjeparts apper/nettsteder med bare noen få kodelinjer.

- Chooser gjør det mulig å velge filer fra Dropbox.
- Saver gjør det mulig for brukere å lagre filer direkte til Dropbox.
- Embedder gjør det mulig for brukerne å se filer og mapper fra Dropbox.

All godkjennelse til disse komponentene går utelukkende gjennom Dropbox. Apper gis tilgang til filer valgt av velgeren via delte lenker fra Dropbox eller kortvarige nedlastingslenker. Disse ferdigbygde komponentene kan brukes uavhengig, eller i forbindelse med API, som beskrevet nedenfor.

Dropbox Business API-integrasjoner

Den offentlig tilgjengelige Dropbox API gir tredjepartsutviklere muligheten til å få tilgang til og samhandle med Dropbox i applikasjonene deres. Dette inkluderer fil- og metadata-utveksling, deling og teamfunksjonalitet.

Autorisasjon

Dropbox bruker OAuth, en standardisert protokoll for autorisasjon, for at brukerne skal kunne gi apper ulike nivåer av kontotilgang uten å utlevere påloggingsinformasjonen for kontoen. Vi støtter OAuth 2.0 for å godkjenne alle API-forespørsler. Forespørsler godkjennes gjennom Dropbox-nettstedet eller mobilappen. Dropbox støtter OAuth beste fremgangsmåter, inkludert kortvarige tilgangspolletter og PKCE for distribuerte apper.

Brukertillatelser.

Apper som bruker Dropbox-API kan utvikles med følgende nivå på innholdstilgang for sluttbrukerens Dropbox:

- ***App-mappe.***

  En egen mappe med samme navn som appen opprettes i appmappen i brukerens Dropbox. Appen får lese- og skrivetilgang til denne mappen og brukerne kan gi innhold til appen ved å flytte filer til denne mappen. I tillegg kan appen be om fil/mappe-tilgang via Chooser eller Saver (se nedenfor).

- ***Full Dropbox.***

  Appen får fullstendig tilgang til alle filene og mappene i brukerens Dropbox, samt fil-/mappetilgang via velger eller lagrer.

Programmer kan også be om spesifikke omfang, begrense oppførselen ved hjelp av tilgang til undergrupper av API-endepunkter. Programmene kan for eksempel være begrenset til skrivebeskyttet tilgang til filer - eller muligheten til å laste opp innhold, men ikke til å opprette delinger.

Teamtillatelser

Administratorer av Dropbox Business kan godkjenne programmer for administrativ funksjonalitet som befinner seg i teamets administratorverktøy. Handlingene teamtilknyttede apper kan utføre er begrenset ved hjelp av omfang, og spesifiserer hvilke teaminnstillinger appen kan lese eller styre.

Vanlige kombinasjoner av omfang inkluderer:

- ***Teaminformasjon***

  Skrivebeskyttet informasjon om teamet og bruk på høyt nivå.

- ***Teamrevisjon***

  Skrivebeskyttet tilgang til teaminfo og detaljert hendelseslogg.

- ***Tilgang til teammedlemmers filer***

  Muligheten til å utføre handlinger på vegne av brukere i teamet, som for eksempel å administrere filer og mapper.

- ***Administrasjon av teammedlemmer***

  Legge til og fjerne medlemmer til og fra teamet.

Webhooks

Webhooks er en måte for nettprogrammer å få varsler i sanntid om endringer i en brukers Dropbox. Når en URI er registrert for å motta webhooks, sendes en HTTP-forespørsel til denne URI-en hver gang det er en endring for noen av appens registrerte brukere. Ved å bruke API for Dropbox Business kan webhooks også brukes til å opprette varsler om endringer i teammedlemskap. Mange sikkerhetsapper bruker webhooks for å hjelpe administratorer med å spore og administrere teamaktiviteter.

Utvidelser

Apper kan registrere utvidelses-URI-er, slik at handlinger kan vises i menyene 'Del' og 'Åpne' i Dropbox' brukergrensesnitt. Utvidelser gjør det mulig for brukerne å starte arbeidsprosesser fra tredjeparter direkte fra en fil i en Dropbox-flate. Når en handling utløses, vil Dropbox omdirigere brukere til den angitte URI-en, og gi en filidentifikator som kan brukes med API for å utføre en hvilken som helst filoperasjon. En app må autoriseres før en registrert utvidelse er synlig for brukeren. Vi kan markedsføre et utvalgt sett med utvidelsesintegrasjoner i «Del»- og «Åpne»-menyene, selv om disse appene ikke vil ha tilgang til innhold før brukeren autoriserer det.

Retningslinjer for Dropbox-utviklere

Vi har en rekke retningslinjer og praksiser for å hjelpe utviklere å lage API-apper som respekterer og beskytter brukernes personvern og samtidig forbedrer brukernes Dropbox-opplevelse.

- ***Appnøkler***

  For hver app som utvikles, må det brukes en unik Dropbox-appnøkkel. Hvis en app tilbyr tjenester eller programvare som omfatter at andre utviklere bruker DBX Platform, må hver utvikler i tillegg registrere seg for å bruke en egen Dropbox-appnøkkel.

- ***Applikasjonstillatelser***

  Utviklere er informert om at apper bør ha så begrensede tillatelser som mulig. Når en utvikler sender inn en app for godkjenning av produksjonsstatusen, sjekker vi at appen ikke ber om en unødvendig bred tillatelse i henhold til funksjonaliteten i appen.

- ***Vurderingsprosess for apper***

  - **Utviklingsstatus.**
    Når en Dropbox-API-app blir laget, får den status som «under utvikling». Appens funksjoner vil fungere på samme måte som en hvilken som helst produksjonsstatus-app, bortsett fra at den kun kan kobles opp med 500 Dropbox-brukere. Så snart en app kobler 50 Dropbox-brukere, har utvikleren to uker på å søke på og motta produksjonsstatustillatelse, før appens evne til å koble til ytterligere Dropbox-brukere fryses.

  - **Produksjonstatus og godkjenning.**
    For å kunne motta produksjonstatusgodkjenning, må alle apper overholde våre utviklerretningslinjer for merkevarebygging samt vilkår og betingelser, som omfatter forbudte bruksområder for DBX Platform. Disse forbudte bruksområdene inkluderer: fremming av brudd på IP- eller opphavsrett, oppretting av fildelingsnettverk og nedlasting av ulovlig innhold. Før den blir sendt inn til vurdering, blir utviklere først bedt om ytterligere informasjon om appens funksjonalitet og hvordan den bruker Dropbox-API. Når appen er godkjent for produksjonstatus, kan et ubegrenset antall Dropbox-brukere koble seg til appen.

Team App-administrasjon

Inne i teamadministrasjonskonsollen kan administratorer av Dropbox Business administrere tilknyttede apper og integrasjoner for teamet sitt.

API-partnerskap

Dropbox har jobbet tett med sine teknologipartnere for å gjøre dem i stand til å utvikle integrasjoner med deres populære programvarepakker. Disse partnerne bygger applikasjoner ved hjelp av Dropbox API-er, og jobber tett med Dropbox-arkitekter for å følge beste sikkerhet og UX-praksis. Disse inkluderer en rekke apper for sluttbrukerproduktivitet, samt sikkerhets- og administrasjonsverktøy som:

- ***Sikkerhetsinformasjon, hendelsesbehandling (SIEM) og analyse***

  Koble sammen Dropbox Business-kontoen med SIEM og analyseverktøy for å overvåke og evaluere brukerdeling, påloggingsforsøk, administratorhandlinger og mer. Få tilgang til og administrer de ansattes aktivitetslogger og sikkerhetsrelevante data via det sentrale administrasjonsverktøyet for logger.

- ***Forhindring av datatap (DLP)***

  Automatisk skanning av metadata og innhold i filer for å utløse varsler, rapportering og handlinger når viktige endringer utføres i Dropbox Business-kontoen. Ta i bruk selskapets retningslinjer for Dropbox Business-implementering og hjelp med å innfri forskriftsmessige krav til overholdelse.

- ***eDiscovery and juridisk behandlingsstopp***

  Svar på søksmål, megling, og forskriftsmessige undersøkelser med data fra Dropbox Business-kontoen. Søk etter og samle inn relevant elektronisk lagret informasjon og sikre dataene med eDiscovery-prosessen, som sparer bedriften både tid og penger.

- ***Administrasjon av digitale rettigheter (DRM)***

  Få ekstra sikkerhet for sensitiv eller opphavsrettsbeskyttet data som er lagret på ansattes kontoer, ved hjelp av tredjepartsbeskyttelse. Få tilgang til kraftige DRM-funksjoner, inkludert klientside-kryptering, vannmerking, revisjonsspor, tilbakekalling av tilgang og blokkering av bruker/enhet.

- ***Dataflytting og lokal sikkerhetskopiering***

  Overføre data til Dropbox fra eksisterende servere eller andre nettskyløsninger og spare tid, penger og krefter. Automatisere sikkerhetskopiering fra Dropbox Business-kontoen til lokale servere.

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

  Automatisere prosessen for klargjøring og fjerning, og fremskynde tiltredelse av nye medarbeidere. Effektivisere administrasjonen og stramme inn sikkerheten ved å integrere Dropbox Business med et eksisterende identitetssystem.

- ***Tilpasset arbeidsflyt***

  Lag interne apper som integrerer Dropbox med eksisterende bedriftsprosesser for å effektivisere den interne arbeidsflyten.

Se siden med appintegrasjoner for Dropbox for en oversikt over disse teknologipartnerne. Sluttbrukere kan finne utvalgte første- og tredjepartsapper og -integrasjoner i App Center.

Dropbox-integrasjoner

Vi har også samarbeidet med noen av våre topp teknologipartnere for å bygge integrasjoner som man finner i Dropbox-flater. Disse dypere integrasjonene er utviklet i et samarbeid mellom Dropbox og partneren. Disse inkluderer:

Dropbox-utvidelser

Disse integrasjonene gjør at du kan bruke forskjellige typer apputvidelser for å utføre handlinger sømløst, for eksempel å publisere en video, legge til filer i e-post og meldinger, sende en fil til e-underskrift med mer, direkte fra Dropbox. Disse applikasjonene er bygget av partneren, mens Dropbox gjør det mulig å finne utvalgte utvidelsespartnere gjennom menyene 'Åpne med' og 'Del med'.

Slack, Zoom og Trello

Disse integrasjonene er utviklet av Dropbox, slik at brukere kan starte Slack-samtaler og møter og opprette oppgaver i Dropbox. Sluttbrukere blir godkjent for disse verktøyene via OAuth.

Microsoft Office for mobile enheter og nett

Med Microsoft Office-integrasjonene kan brukere åpne Word-, Excel- og PowerPoint-filer som er lagret i Dropboxen. De kan gjøre endringer i Office-apper for mobil og nett, og lagre disse endringene direkte tilbake til Dropboxen. Brukere blir bedt om å godkjenne tilgang på første forsøk når de åpner en Dropbox-fil i hver Office-mobilapp eller enhver Office-webapp. Senere oppstarter vil bevare disse koblingene.

Adobe Acrobat og Acrobat Reader

Integrasjonene våre med datamaskin- og mobilversjoner (Android og iOS) av disse programmene gjør det mulig for brukere å se, redigere og dele PDF-filer som er lagret i Dropbox. Brukere blir bedt om å gi tilgang ved første forsøk på å åpne en Dropbox-fil i hver av appene. Endringer i PDF-filer lagres i Dropbox automatisk.

Oppsummering

Dropbox Business tilbyr et verktøy som er enkelt å bruke, slik at det blir lettere for team å samarbeide effektivt, samtidig som det sikrer overholdelse av sikkerhetstiltakene og sertifiseringen organisasjoner krever. Med en flerlagstilnærming som kombinerer en robust underliggende infrastruktur med et tilpasset sett med retningslinjer, gir vi bedrifter en kraftig løsning som kan skreddersys til deres unike behov. Hvis du vil vite mer om Dropbox for bedrifter, kan du ta kontakt med salgsteamet på sales@dropbox.com.