Säkerhet i Dropbox Business

En informationssammanställning från Dropbox

Dropbox

Innehåll

Översikt

Den digitala omvandlingen fortgår i många branscher, och det är viktigt att data, team och enheter skyddas var de än befinner sig. Organisationer som förlitar sig på molnlösningar som Dropbox Business för att möjliggöra distansbaserade och distribuerade arbetsflöden måste strömlinjeforma samarbete, hantera molnrisker proaktivt och implementera effektiva kontroller som säkerställer konfidentialitet för immateriell egendom (IP), integritet för lagrade och delade data, tillgänglighet för data genom hanterad och en robust molntjänst.

Över 600 000 företag och organisationer förlitar sig på Dropbox Business som lösning för att distansteam ska kunna samarbeta på ett säkert sätt. Den centrala Dropbox-företagslösningen innehåller en smart arbetsyta för samarbete, samt filsynknings- och delningsfunktioner. Våra lösningar understöds av branschledande infrastruktur samt funktioner för avancerad företagssäkerhet, team- och innehållssäkerhet, elektroniska signaturer, säker överföring och datastyrning. Om inget annat anges gäller informationen i denna informationssammanställning alla Dropbox-företagsprodukter (Standard, Advanced och Enterprise) samt Dropbox Education. Paper är en funktion i Dropbox Business och Dropbox Education.

Kärnan för Dropbox Business är vårt omfattande säkerhetsprogram, Dropbox-förtroendeprogrammet, som har en flerskiktsstrategi för säkerhet som är avgörande när globala metoder för distansarbete utvecklas.

Den här informationssammanställningen beskriver produktsäkerhetsfunktioner i Dropbox Business, Dropbox operativa säkerhetsåtgärder, vårt sekretess- och transparensåtagande samt backend-policyer, oberoende certifieringar och åtgärder för regelefterlevnad som gör Dropbox till den säkra lösningen för din organisation.

Om inget annat anges gäller informationen i denna informationssammanställning alla Dropbox-företagsprodukter (Standard, Advanced och Enterprise) samt Dropbox Education. Paper är en funktion i Dropbox Business och Dropbox Education.

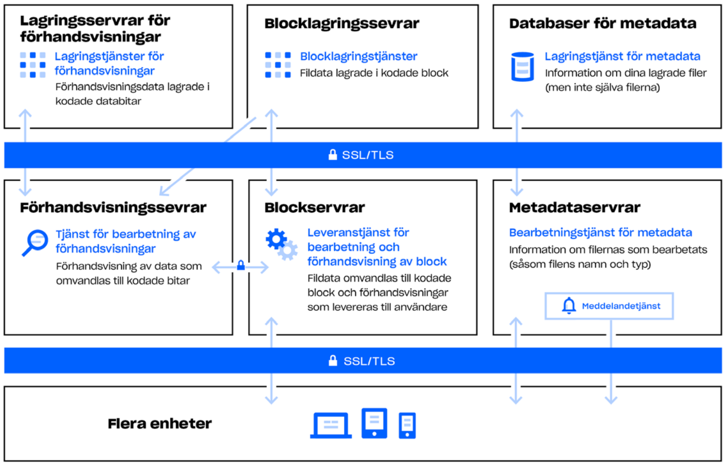
Under skalet

Våra användarvänliga gränssnitt stöds av en infrastruktur som arbetar i bakgrunden för att garantera snabb, pålitlig synkning och delning och ett smidigt samarbete. Vi förbättrar ständigt vår produkt och arkitektur för att skapa snabbare dataöverföring, öka tillförlitligheten och anpassa oss efter förändringar i miljön. I detta avsnitt förklarar vi hur data överförs, lagras och bearbetas på ett säkert sätt.

Filinfrastruktur

Dropbox-användare kan komma åt filer och mappar när som helst från datorn, webben och mobila klienter, eller genom tredjepartsappar som är kopplade till Dropbox. Alla dessa klienter ansluter till säkra servrar för att ge åtkomst till filer, möjliggöra fildelning med andra och uppdatera kopplade enheter när filer läggs till, ändras eller raderas.

Dropbox-filinfrastrukturen består av följande komponenter:



- ***Metadataservrar***

  Vissa grunduppgifter om användardata, så kallade metadata, lagras i sin egen diskreta lagringstjänst och fungerar som ett index för uppgifterna i användarnas konton. Metadata inkluderar grundläggande konto- och användarinformation som mejladress, namn och enhetsnamn. Metadata innefattar också basinformation om filer, inklusive filnamn och typ, vilket underlättar supportfunktioner som versionshistorik, återställning och synkronisering.

- ***Databaser för metadata***

  Alla metadata för filer lagras i ett värdelager med transaktionsnyckel med samtidighetskontroll för flera versioner, och partitioneras och replikeras efter behov för att leva upp till våra krav på prestanda och hög tillgänglighet.

- ***Blockservrar***

  Dropbox erbjuder en unik säkerhetsmekanism som överträffar traditionell kryptering för att skydda användardata. Blockservrar bearbetar filer från Dropbox-applikationerna genom att dela upp dem i block som krypteras med ett starkt chiffer. Endast block som har modifierats sedan den senaste versionen synkas. En Dropbox-applikation meddelar blockservrarna att en ändring genomförts när den upptäcker en ny fil eller ändringar i en befintlig fil. De nya eller modifierade filblocken bearbetas och överförs till blocklagringsservrarna. Blockservrarna används dessutom för att leverera filer och förhandsvisningar till användaren. Mer information om den kryptering som dessa tjänster använder, både vid överföring och lagring, finns i avsnittet Kryptering nedan.

- ***Blocklagringsservrar***

  Det faktiska innehållet i användarnas filer lagras i krypterade block på blocklagringsservrarna.

  Dropbox-klienten delar upp filerna i filblock innan överföringen för att förbereda dem inför lagringen. Lagringsservrarna fungerar som ett Content-Adressable Storage-system (CAS), där varje enskilt filblock tas emot baserat på dess hashvärde.

- ***Förhandsvisningsservrar***

  Förhandsvisningsservrarna framställer förhandsvisningar av filer. Förhandsvisningar är en framställning av en användares fil i ett annat filformat som är mer lämpat för att snabbt visas på en slutanvändares skärm. Förhandsvisningsservrar hämtar filblock från blocklagringsservrarna för att generera förhandsvisningar. När en förhandsvisning av en fil begärs hämtar förhandsvisningsservrarna den cachelagrade förhandsvisningen från förhandsvisningsservrarna och överför den till blockservrarna. I slutändan levereras förhandsvisningarna till användare via blockservrarna.

- ***Förhandsvisningens lagringsservrar***

  Cachelagrade förhandsvisningar lagras i ett krypterat format på lagringsservrarna för förhandsvisningar.

- ***Meddelandetjänst***

  Denna separata tjänst övervakar huruvida några ändringar har gjorts i Dropbox-konton eller inte. Inga filer eller metadata lagras eller överförs. Varje klient skapar en long poll-anslutning till meddelandetjänsten och avvaktar. När en fil i Dropbox modifieras signalerar meddelandetjänsten detta till de relevanta klienterna genom att stänga long poll-anslutningen. När anslutningen stängs signalerar detta att klienten måste ansluta till metadatatjänsten på ett säkert sätt för att synkronisera eventuella ändringar.

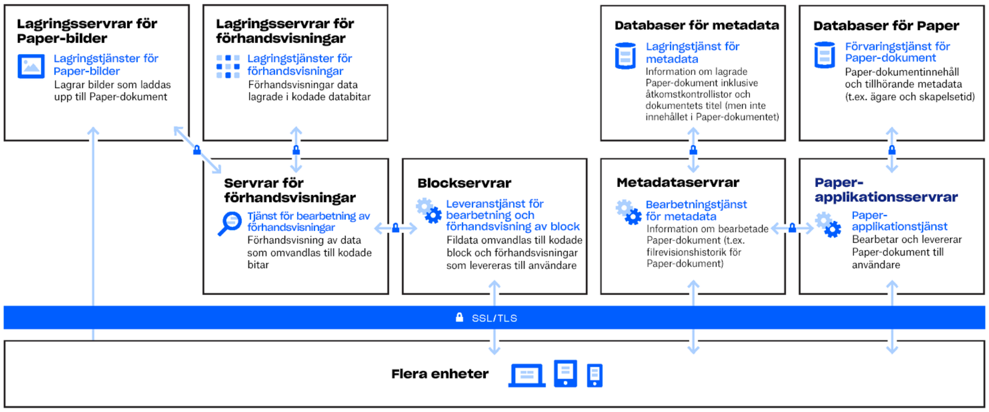
Fildatalagring

Dropbox lagrar huvudsakligen två slags metadata: metadata om filer (till exempel datum och tid för den senaste filändringen) och det faktiska filinnehållet (filblock). Metadatan om filerna lagras på Dropbox servrar. Filblock lagras i ett av två system: Amazon Web Services (AWS) eller Magic Pocket, Dropbox interna lagringssystem. Magic Pocket består av tillverkarspecifik program- och maskinvara och har designats från grunden för att vara tillförlitligt och säkert. I både Magic Pocket och AWS krypteras filblock när de är inaktiva, och båda systemen uppfyller höga krav på tillförlitlighet. Mer information finns i avsnittet Tillförlitlighet nedan.

Paper-infrastruktur

Dropbox-användare kan komma åt Paper-dokument och mappar när som helst från webben och mobila klienter, eller genom tredjepartsappar som är kopplade till Dropbox Paper-appen. Alla dessa klienter ansluter till säkra servrar för att ge åtkomst till Paper-dokument, möjliggör dokumentdelning med andra och uppdaterar anslutna enheter när filer läggs till, ändras eller tas bort.

Dropbox Paper-infrastrukturen består av följande komponenter:



- ***Papers programservrar***

  Paper-applikationsservrar behandlar användarbegäranden, renderar redigerade Paper-dokument tillbaka till användaren och hanterar aviseringstjänster. Paper-applikationsservrar skriver inkommande användarredigeringar till Paper-databaser där de lagras permanent. Kommunikationssessionerna mellan Paper-applikationsservrar och Paper-databaser skyddas med Secure Hypertext Transfer Protocol (HTTPS).

- ***Paper-databaser***

  Det faktiska innehållet i användarnas Paper-dokument, samt vissa metadata om dessa Paper-dokument, lagras permanent i Paper-databaser. Detta omfattar informationen om Paper-dokumentet (som titel, ägare, skapelsetid och annan information) samt innehållet i själva Paper-dokumentet, inklusive kommentarer och uppgifter. Paper-databaser shardas och replikeras efter behov för att uppfylla höga krav på prestanda och tillgänglighet.

- ***Metadataservrar***

  Paper använder samma metadata-servrar som beskrivs i Dropbox-infrastrukturdiagrammet för att hantera information om Paper-dokument, till exempel filrevisionshistorik för Paper-dokument och delat mappmedlemskap. Dropbox hanterar metadata-servrarna direkt. Servarna är placerade i datacenter som drivs av tredje part.

- ***Databaser för metadata***

  Paper använder samma metadata-servrar som beskrivs i Dropbox-infrastrukturdiagrammet för att lagra information om Paper-dokument, till exempel delning, behörigheter och mappassociationer. Alla metadata för Paper-dokument lagras i en databastjänst med MySQL-stöd, samt delas och replikeras efter behov för att leva upp till våra krav på prestanda och hög tillgänglighet.

- ***Papers bildlagringsservrar***

  Bilder som laddas upp till Paper-dokument lagras och krypteras i vila på lagringsservrar för Paper-bilder. Överföringen av bilddata mellan Paper-applikationen och Paper-bildservrar sker över en krypterad session.

- ***Förhandsvisningsservrar***

  Förhandsvisningsservrar levererar förhandsvisningar av både bilder som laddats upp till Paper-dokument och hyperlänkar som bäddats in i Paper-dokument. För bilder som laddats upp i Paper-dokumentet hämtar förhandsvisningsservrarna bilddata som lagrats i lagringsservrarna för Paper-bilder via en krypterad kanal. För hyperlänkar som bäddats in i Paper-dokument hämtar förhandsvisningsservrarna bilddata och renderar en förhandsvisning av bilden med användning av kryptering i enlighet med källänkens specifikationer. I slutändan levereras förhandsvisningarna till användare via blockservrarna.

- ***Förhandsvisningens lagringsservrar***

  Paper använder sig av samma förhandsvisningsservrar som beskrivs i infrastrukturdiagrammet för Dropbox för att lagra cachelagrade förhandsvisningar av bilder. Cachelagrade förhandsvisningar lagras i ett krypterat format på lagringsservrarna för förhandsvisningar.

Lagring av Paper-dokument

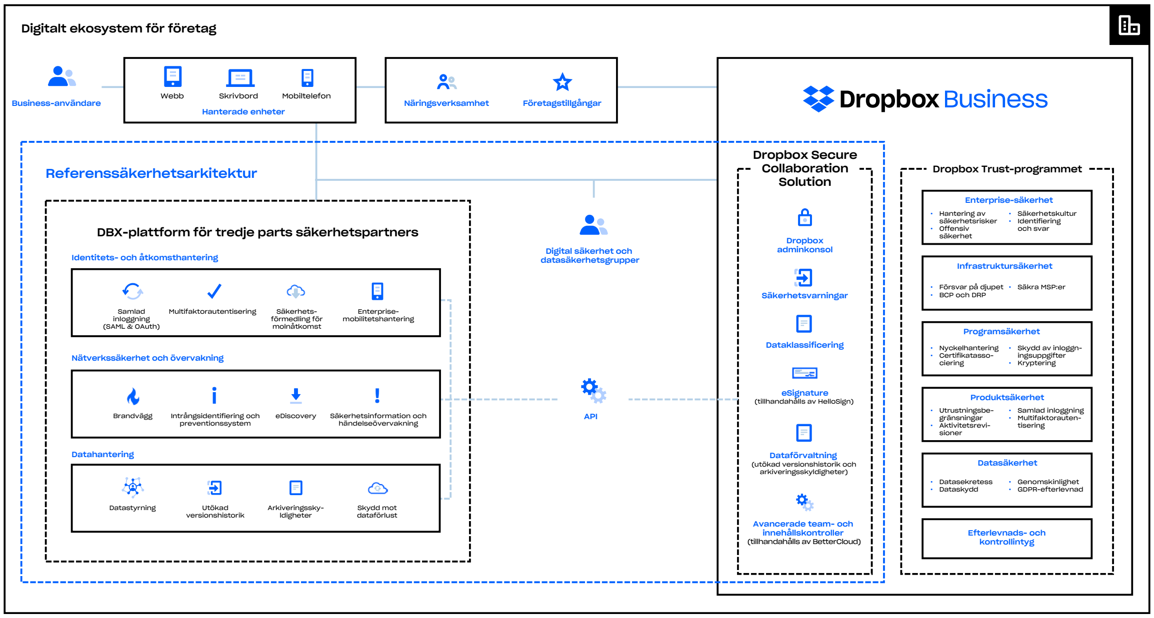
Dropbox lagrar huvudsakligen följande datatyper i Paper-dokument: metadata om Paper-dokument (som ett dokuments delade tillstånd) och det faktiska innehållet i Paper-dokumentet som laddats upp av användaren. Dessa data benämns gemensamt som Paper-dokumentdata, och bilder som laddats upp till Paper-dokument benämns Paper-bilddata. Var och en av dessa datatyper lagras i Amazon Web Services (AWS). Paper-dokument är krypterade i vila AWS, och AWS uppfyller kraven i stränga standarder med avseende på pålitlighet. För mer information, se avsnittet Tillförlitlighet nedan.

Dropbox-Dropbox förtroendeprogram

Förtroende utgör grunden för vårt förhållande med miljontals människor och företag världen över. Vi värdesätter det förtroende du gett oss och tar vårt ansvar att skydda din information på yttersta allvar. För att förtjäna ditt förtroende, skapade vi Dropbox med tyngdpunkt på säkerhet, sekretess, transparens och efterlevnad.

Policyn för Dropbox förtroendeprogram etablerar en riskutvärderingsprocess som är utformad för att ta upp gällande lagar och förordningar för miljö, fysiska faktorer, användare och tredje part, kontraktsmässiga krav och olika andra risker som kan påverka systemsäkerhet, konfidentialitet, integritet, tillgänglighet eller sekretess. Prestandagranskningar genomförs minst en gång om året. Mer information om Dropbox förtroendeprogram finns på: dropbox.com/business/trust.

Vi följer en flerskiktsstrategi för att säkra företag, infrastruktur, applikationer och produkter som påverkar din organisation.



Företagssäkerhet

Dropbox har fastställt ett ramverk för hanteringen av informationssäkerhet. Detta ramverk beskriver syftet, inriktningen, principerna och de grundläggande reglerna för hur vi bibehåller vårt förtroende. Detta uppnås genom att bedöma risker och att ständigt förbättra säkerheten, sekretessen, integriteten, tillgängligheten och sekretessen för Dropbox-företagssystemen. Vi granskar och uppdaterar regelbundet våra säkerhetspolicyer, erbjuder säkerhetsutbildning, utför tester av applikations- och nätverkssäkerhet (inklusive intrångstester), övervakar hur alla säkerhetspolicyer efterlevs samt utför interna och externa riskbedömningar.

Våra policyer

Vi har upprättat en omfattande uppsättning säkerhetspolicyer som upprätthålls av säkerhets- och missbruksteamet på Dropbox. Alla säkerhetspolicyer granskas och godkänns minst en gång per år. Medarbetare, praktikanter och underleverantörer deltar i en obligatorisk säkerhetsutbildning när de ansluter sig till företaget och får kontinuerlig utbildning i säkerhetsmedvetenhet.

- ***Informationssäkerhet***

  Hålla användar- och Dropbox-information säker.

- ***Autentisering***

  Beskriver hur Dropbox-personal autentiserar sig för att komma åt informationssystem och data.

- ***Enhetssäkerhet***

  Minsta säkerhetskrav för mobila enheter som används för att få åtkomst till företagsinformation.

- ***Logisk åtkomstkontroll***

  Håller åtkomst till Dropbox-system, användare och information säker. Omfattar åtkomstkontroll för både företags- och produktionsmiljöer.

- ***Datasäkerhet***

  Beskriver hur Dropbox skyddar data genom specifika krav för lagring, åtkomst och användning.

- ***Resesäkerhet***

  Beskriver vad Dropbox-personal bör göra innan de reser utomlands.

- ***Säkerhetsriktlinjer för sälj- och kundupplevelse (CX)***

  Hålla användarinformationen säker, skydda våra anställda och ge support till våra användare.

- ***Fysisk säkerhet***

  Bibehålla en trygg och säker miljö för personer och egendom på Dropbox.

- ***Riktlinjer för fysisk säkerhet i produktion***

  Hantera fysisk åtkomst till produktionsanläggningar.

- ***Incidenthantering***

  Beskriver hur Dropbox hanterar rapporterade säkerhets-, sekretess- och platshändelser och dokumenterar händelseplaner för var och en.

- ***Obehörigt upphovsrättsskyddat material***

  Förbjuda personal från att använda Dropbox eller Dropbox-system för att lagra eller dela otillåtet innehåll.

- ***Förändringshantering***

  Hantera ändringar i produktionssystem. Avsedd för alla Dropbox-medarbetare, konsulter och praktikanter med åtkomst till system.

- ***Sekretess för användardata***

  Skydda och hantera användarinformation och användaruppgifter på Dropbox i enlighet med vår integritetspolicy.

- ***Policy för verksamhetskontinuitet och nödfallshantering***

  Beskriver bevarande, skydd och säkerhet hos och av människor (Dropbox-personal), egendom och (affärs)processer.

- ***Dropbox-sekretessprogram***

  Syftet, principerna och ansvarsförhållandena för Dropbox-sekretessprogrammet.

- ***Dropbox-förtroendeprogrammet***

  Beskriver hur Dropbox arbetar och är trovärdigt.

- ***Säkerhet för betalningsmiljön***

  Säkra och underhålla den dedikerade betalningsmiljön som används på Dropbox för att acceptera kreditkortsbetalningar.

Policy och åtkomst för medarbetare

Efter anställningen måste samtliga Dropbox-medarbetare genomgå en bakgrundskontroll och underteckna en bekräftelse av säkerhetspolicyn och ett sekretessavtal, samt genomgå säkerhetsutbildning. Endast personer som har slutfört dessa procedurer får fysisk och logisk åtkomst till företagets och produktionens miljöer, utifrån vad deras ansvarsområden kräver. Dessutom måste samtliga medarbetare slutföra en obligatorisk årlig säkerhetsutbildning och de får regelbunden utbildning om säkerhetskännedom via informationsmejl, samtal och presentationer och resurser som finns på intranätet.

Medarbetaråtkomst till Dropbox-miljön upprätthålls av en central mapp och autentiseras med en kombination av starka lösenord, lösenfrasskyddade SSH-nycklar och tvåfaktorautentisering. Fjärråtkomst kräver VPN som skyddas av tvåfaktorsautentisering och all specialåtkomst granskas och behandlas av vårt säkerhetsteam. Åtkomsten till företags- och produktionsnätverk är strikt begränsad baserat på fastställda policyer. Åtkomsten till produktionsnätverk är exempelvis baserad på SSH-nycklar och är begränsad till ingenjörsteam som måste ha åtkomst för att kunna utföra sina arbetsuppgifter. Brandväggskonfiguration sker under rigorös kontroll och är begränsad till ett fåtal administratörer.

Våra interna policyer kräver dessutom att medarbetare som använder produktions- och företagsmiljöer följer bästa praxis för skapande och lagring av privata SSH-nycklar. Åtkomst till andra resurser, inklusive datacenter, funktioner för serverkonfiguration, produktionsservrar och funktioner för utveckling av källkod tilldelas genom uttryckligt godkännande från lämplig chef. En kopia av åtkomstförfrågan, motivering och godkännande registreras av ledningen och åtkomsten beviljas av lämpliga personer.

Dropbox använder tekniska åtkomstkontroller och interna policyer för att hindra medarbetare från att godtyckligt komma åt användares filer och för att begränsa åtkomsten till metadata och andra uppgifter om användarnas konton. För att skydda slutanvändarnas sekretess och säkerhet har endast ett mindre antal tekniker, som är ansvariga för att utveckla Dropbox kärntjänster, åtkomst till miljön där användarnas filer lagras. Medarbetaråtkomst återkallas omedelbart när en medarbetare lämnar företaget.

När Dropbox blir en förlängning av våra kunders infrastruktur kan de lita på att vi förvaltar deras data ansvarsfullt. Se vårt Sekretessavsnitt nedan för mer information.

Sårbarhetshantering

Vårt säkerhetsteam utför regelbundna automatiska och manuella säkerhetstester och hantering av korrigeringar, och samarbetar med tredjepartsexperter för att identifiera och åtgärda eventuella sårbarheter och buggar.

Som en nödvändig komponent i vårt system för hantering av informationssäkerhet rapporteras resultat och rekommendationer från alla dessa utvärderingar till Dropbox ledning, som utvärderar informationen och vidtar lämpliga åtgärder efter behov. Allvarliga ärenden dokumenteras, spåras och åtgärdas av tilldelade säkerhetstekniker.

Förändringshantering

Alla processer för utveckling, åtgärdande av problem och rättelser följer vår formell policy för förändringshantering som har utarbetats av Dropbox ingenjörsteam för att säkerställa att systemändringar har testats och auktoriserats innan de implementeras i produktionsmiljöerna. Källkodsändringar initieras av utvecklare som vill förbättra Dropbox-appen eller -tjänsten. Alla ändringar lagras i ett versionskontrollsystem och måste genomgå en automatiserad kvalitetskontroll (Quality Assurance, QA) för att verifiera att säkerhetskraven uppfylls. När QA-testen har godkänts implementeras ändringen. QA-godkända ändringar implementeras automatiskt i produktionsmiljön. Vår livscykel för programvaruutveckling (SDLC) kräver att riktlinjerna för säker kodning efterlevs. Man måste även söka efter kodändringar för att hitta potentiella säkerhetsproblem via våra processer för QA och manuell granskning. Ändringar som går vidare till produktion loggas och arkiveras och varningar skickas automatiskt ut till Dropbox-teknikerteamledningen.

Ändringar i Dropbox infrastruktur kan endast utföras av behörig personal. Dropbox-säkerhetsteamet ansvarar för att upprätthålla infrastrukturens säkerhet och säkerställa att servrar, brandväggar och andra säkerhetsrelaterade konfigurationer alltid är uppdaterade och efterlever aktuell branschstandard. Vi utför regelbundna granskningar av brandväggsregler och personer med åtkomst till produktionsservrar.

Skanning och testning av säkerhetspenetrering (intern och extern)

Vårt säkerhetsteam utför regelbundna automatiserade och manuella säkerhetstester av applikationer för att identifiera och åtgärda potentiella säkerhetsluckor och buggar i våra applikationer för dator, webben (Dropbox och Paper) och mobilapplikationer (Dropbox och Paper).

Dessutom har Dropbox kontrakt med tredjepartssäljare för att utföra periodvisa penetrerings- och sårbarhetstester i produktionsmiljöer. Vi samarbetar även med externa säkerhetsspecialister, andra säkerhetsteam i branschen samt säkerhetsforskare för att se till att våra applikationer förblir säkra. Vi använder också automatiska analyssystem för att identifiera sårbarheter. Detta inkluderar system som vi utvecklar internt, system med öppen källkod som vi modifierar efter våra behov och externa leverantörer som vi anlitar för kontinuerliga, automatiserade analyser.

Hålla skadligt innehåll borta från Dropbox

Vi har skanningsfunktioner som syftar till att förhindra att skadligt innehåll lagras och distribueras i Dropbox. Våra skanningsfunktioner utnyttjar vår egenutvecklade teknik samt avancerade funktioner från partnerföretag som Microsoft och Google för att göra Dropbox till en säker plats för våra kunder.

Buggpremier

Även om vi arbetar med professionella företag för testning och även utför testning internt kan vi med buggpremier (eller belöningsprogram för sårbarheter) få tillgång till expertisen hos ett bredare säkerhetscommunity. Vårt buggpremieprogram ger ett incitament för utredare att på ett ansvarsfullt sätt identifiera och avslöja programvarubuggar. Detta engagemang hos ett externt community ger vårt säkerhetsteam fristående granskning av våra applikationer som hjälper oss att hålla användarna säkra. Vi strävar efter att vara en branschledare i buggpremiearbetet även vad gäller svars- och åtgärdstider.

Vi har etablerat en omfattning för kvalificerande överföringar och Dropbox-applikationer, samt en policy för ansvarsfullt avslöjande som gynnar upptäckten och rapporteringen av säkerhetssårbarheter och ökar användares säkerhet. Denna policy fastställer följande riktlinjer:

- Berätta för oss i detalj om säkerhetsproblemet.
- Respektera våra befintliga applikationer. Att masskicka formulär genom automatiska sårbarhetsskannrar leder inte till någon bonus eftersom de uttryckligen är uteslutna.
- Ge oss rimlig tid att svara innan du offentliggör någon information om säkerhetsproblemet.
- Försök inte komma åt eller modifiera användardata utan kontoägarens tillstånd.
- Du ska inte visa, ändra, spara, lagra, överföra eller på annat sätt öppna informationen, och omedelbart rensa all lokal information när du rapporterar sårbarheten till Dropbox.
- Handla i god tro så att du undviker sekretessöverträdelser, förstörelse av data eller avbrott eller försämringar av våra tjänster (inklusive funktionsförlust, även kallat ”denial of service”).

Problem kan rapporteras genom att en rapport skickas till Bugcrowd på: bugcrowd.com/dropbox.

Fysisk säkerhet

Infrastruktur

Fysisk åtkomst till underleverantörernas anläggningar för produktionssystem är begränsad till personal som auktoriserats av Dropbox för att kunna utföra sina arbetsuppgifter. Alla personer som behöver ytterligare åtkomst till produktionsanläggningar tilldelas detta endast efter uttryckligt godkännande från ansvarig ledning.

En kopia av åtkomstförfrågan, motivering och godkännande registreras av ledningen och åtkomsten beviljas av lämpliga personer. När godkännandet mottagits kontaktar infrastrukturteamets behöriga medlem den aktuella underleverantören för att begära åtkomst för den godkända individen. Underleverantören anger användarens uppgifter i sitt eget system och beviljar den godkända Dropbox-personalen åtkomst genom en ID-bricka och, om möjligt, biometrisk skanning. När godkända individer har beviljats åtkomst är det datacentrets ansvar att se till att åtkomsten begränsas till endast dessa behöriga individer.

Företagskontor

- ***Fysisk säkerhet***

  Dropbox team för fysisk säkerhet bär ansvaret för att genomdriva den fysiska säkerhetspolicyn och att övervaka säkerheten på kontoret.

- ***Policy för besökare och åtkomst***

  Fysisk åtkomst till företagsanläggningar, utöver allmänna ingångar och receptioner, begränsas till behörig Dropbox-personal och registrerade besökare som åtföljs av Dropbox-personal. Ett system för åtkomst med ID-bricka säkerställer att endast behöriga individer har åtkomst till begränsade områden inom företagsanläggningarna.

- ***Serveråtkomst***

  Åtkomst till områden med företagsservrar (som serverrum) begränsas till behörig personal med rätt behörighetsnivå som ges via systemet med ID-brickor. Listan över behöriga personer som är godkända för fysisk åtkomst till företags- och produktionsmiljöer granskas minst en gång i kvartalet.

Incidenthantering

Vi har policyer och rutiner för incidenthantering som fastställer hur vi ska hantera problem med tillgänglighet, integritet, säkerhet, sekretess och konfidentialitet för tjänsten. Som del av våra incidenthanteringsprocedurer har vi särskilda team som är utbildade för att kunna:

- Reagera snabbt på varningar om potentiella incidenter.
- Fastställ incidentens allvarlighetsgrad.

- Vidta åtgärder för minimering och begränsning vid behov.
- Kommunicera med relevanta interna och externa intressenter, inklusive meddela drabbade kunder för att uppfylla kontraktsenliga förpliktelser om brott eller incidenter och följa relevanta lagar och förordningar.
- Samla in och lagra bevis för utredningsarbete.
- Dokumentera en efterhandsutredning och ta fram en permanent prioriteringsplan.

Regler och processer för incidentrespons revideras inom ramarna för SOC 2, ISO/IEC 27001 och andra säkerhetsutvärderingar.

Säkerhet för infrastruktur

Nätverkssäkerhet

Dropbox upprätthåller omsorgsfullt säkerheten i våra backend-nätverk. Vår teknik för nätverkssäkerhet och övervakning är utformad för att ge ett skydd som består av flera lager. Vi använder skyddstekniker som utgör branschstandarder, inklusive brandväggar, genomsökning av nätverkets sårbarhet, övervakning av nätverkets säkerhet, system för intrångsavkänning för att se till att bara kvalificerad och icke-skadlig trafik kan nå vår infrastruktur.

Vårt interna privata nätverk delas upp efter användning och risknivå. De primära nätverken är följande:

- DMZ mot internet
- DMZ med prioriterad infrastruktur
- Produktionsnätverk
- Företagsnätverk

Åtkomst till produktionsmiljöer är begränsad till auktoriserade IP-adresser och kräver flerfaktorsautentisering på alla slutpunkter. IP-adresser med åtkomst associeras med företagsnätverket eller godkänd Dropbox-personal. Auktoriserade IP-adresser granskas kvartalsvis för att säkerställa en säker produktionsmiljö. Åtkomst till modifiering av listan med IP-adresser är begränsad till behöriga personer.

Trafik från internet som är riktad mot vårt produktionsnätverk skyddas av flera brandväggs- och proxyskikt.

Strikt begränsning upprätthålls mellan det interna Dropbox-nätverket och det offentliga internet. Internetbunden trafik till och från produktionsnätverket kontrolleras noggrant genom en dedikerad proxytjänst. Denna skyddas i sin tur av restriktiva brandväggsregler.

Dropbox skapar sofistikerade verktygsuppsättningar för att övervaka bärbara och stationära datorer med Mac- och Windows-operativsystem och produktionssystem för skadliga händelser. Alla säkerhetsloggar samlas på en central plats för rättsvårdande respons och incidenthantering i enlighet med den retentionspolicy som är branschstandard.

Dropbox identifierar och minskar risker via regelbunden testning och granskning av nätverkssäkerhet av både dedikerade interna säkerhetsteam och säkerhetsspecialister från tredje part.

Närvaropunkter (PoP)

I syfte att optimera webbplatsprestanda för användare utnyttjar Dropbox tredjepartsnätverk för innehållsleverans (CDN:er) och närvaropunkter (PoP:er) som Dropbox är värd för på 31 platser runtom i världen. Inga användardata cachas på dessa platser och alla användardata som överförs krypteras med SSL/TLS. Fysisk och logisk åtkomst till PoP:er som Dropbox är värd för är begränsad till behörig Dropbox-personal. Dropbox utför optimeringar av både transportlagret (TCP) och applikationslagret (HTTP).

Peering

Dropbox har en öppen peeringpolicy och samtliga kunder är välkomna att skapa peerförbindelser med oss. För mer information, gå till dropbox.com/peering.

Tillförlitlighet

Ett lagringssystem är aldrig bättre än dess tillförlitlighet. Därför har vi gett Dropbox flera redundanta lager som skyddar mot dataförlust och säkerställer tillgänglighet.

Filmetadata

Överblivna metadatakopior fördelas över oberoende enheter inom ett datacenter i en N+2-tillgänglighetsmodell som minimum. Inkrementella säkerhetskopieringar utförs minst varje timme, och fullständiga säkerhetskopieringar utförs var 36:e timma. Metadata lagras på servrar som Dropbox driver och hanterar i USA.

Filblock

Redundanta kopior av filblock lagras separat i minst två olika geografiska regioner och replikeras på ett säkert sätt i varje region. (**Observera:** För kunder som har sina filer lagrade i vår infrastruktur i Tyskland, Australien, Japan eller Storbritannien replikeras filblocken enbart inom sina respektive regioner. Mer information finns i Datacenter och funktionstjänstleverantörer nedan.) Både Magic Pocket och AWS är utformade för att ge en årlig datahållbarhet på minst 99,999999999 %.

Dropbox arkitektur, applikationer och synkningsmekanismer bildar tillsammans ett skydd för användardata och gör dem lättillgängliga. I de sällsynta fall då en tjänst inte är tillgänglig kan Dropbox-användare fortfarande komma åt de senaste synkade kopiorna av filerna i den lokala Dropbox-mappen på anslutna datorer. Kopior av filer som synkroniserats i Dropbox-skrivbordsklienten/lokala mappen kan nås från en användares hårddisk under driftstörningar, strömavbrott eller när datorn är offline. Ändringar som görs i filer och mappar synkroniseras till Dropbox när tjänsten eller anslutningen fungerar igen.

Paper-dokument

Redundanta kopior av Paper-dokumentdata fördelas över oberoende enheter inom ett datacenter i en N+1-tillgänglighetsmodell. Fullständiga säkerhetskopieringar av Paper-dokumentdata genomförs också dagligen. För Paper-dokumentlagring använder Dropbox AWS-infrastruktur i USA som har utformats för att ge en årlig datahållbarhet på minst 99,999999999 %. I de sällsynta fall en tjänst inte är tillgänglig har Dropbox-användare fortfarande åtkomst till de senaste synkade kopiorna av sina Paper-dokument via ”offline”-läget i mobilapplikationen.

Filsynkning

Dropbox erbjuder branschens bästa filsynkning. Våra synkmekanismer garanterar snabba, responsiva filöverföringar och möjliggör åtkomst till data oavsett plats och enhet. Dropbox-synkningen är dessutom mycket robust. Om anslutningen till Dropbox-tjänsten misslyckas återupptar en klient smidigt åtgärden när anslutningen återupprättas. Filer uppdateras endast på den lokala klienten om de har synkats och validerats helt med Dropbox-tjänsten. Genom att sprida ut belastningen över flera servrar säkerställer vi redundans och enhetlig synkning för slutanvändare.

Delta-synkning

Med den här synkningsmetoden laddas bara ändrade delar av filer ner eller upp. Dropbox lagrar varje fil i diskreta, krypterade block och uppdaterar bara de block som har ändrats.

Strömmande synkning

I stället för att vänta på att en filuppladdning ska slutföras börjar strömmande synkronisering att ladda ner synkade block till en annan enhet innan alla block har laddats upp helt från den första enheten. Detta tillämpas automatiskt när separata datorer är kopplade till samma Dropbox-konto eller när olika Dropbox-konton delar en mapp.

Spara hårddiskutrymme

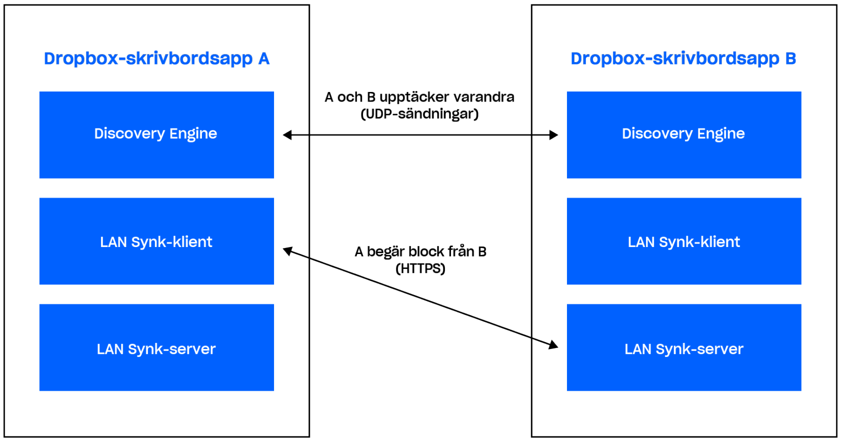
Användare kan frigöra lagringsutrymme på sina datorer genom att göra endast de filer de vill ha på sin hårddisk tillgängliga offline. Detta frigör datorutrymme genom att allt annat förvaras enbart online på dropbox.com.

LAN-synk

När denna funktion är aktiverad laddas nya och uppdaterade filer från andra datorer på samma LAN-nätverk ner, vilket sparar tid och bandbredd jämfört med att ladda ner filerna från Dropbox-servrarna.

Arkitektur

Det LAN-synksystem som körs i klienten består av tre huvudkomponenter: daemon, servern och klienten. Daemon hittar maskiner på nätverket att synka med. Detta är begränsat till maskiner som har auktoriserad åtkomst till samma personliga eller delade Dropbox-mappar. Servern hanterar begäranden från andra maskiner i nätverket och servar de begärda filblocken. Klienten begär filblock från nätverket.



Daemon

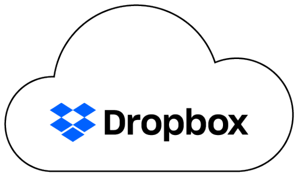
Samtliga maskiner i LAN-systemet skickar och lyssnar periodvis efter UDP-sändningspaket över port 17500 (som reserverats för LAN-synk av IANA). Paketen innehåller protokollversionen som används av den datorn, de personliga och delade Dropbox-mapparna som stöds, den TCP-port som används för att köra servern (som kan vara en annan än 17500 om den porten inte är tillgänglig) och en slumpmässig identifierare för maskinen. När ett paket upptäcks läggs maskinen till i en lista för varje personlig och delad mapp, vilket indikerar ett potentiellt mål.

Protokoll

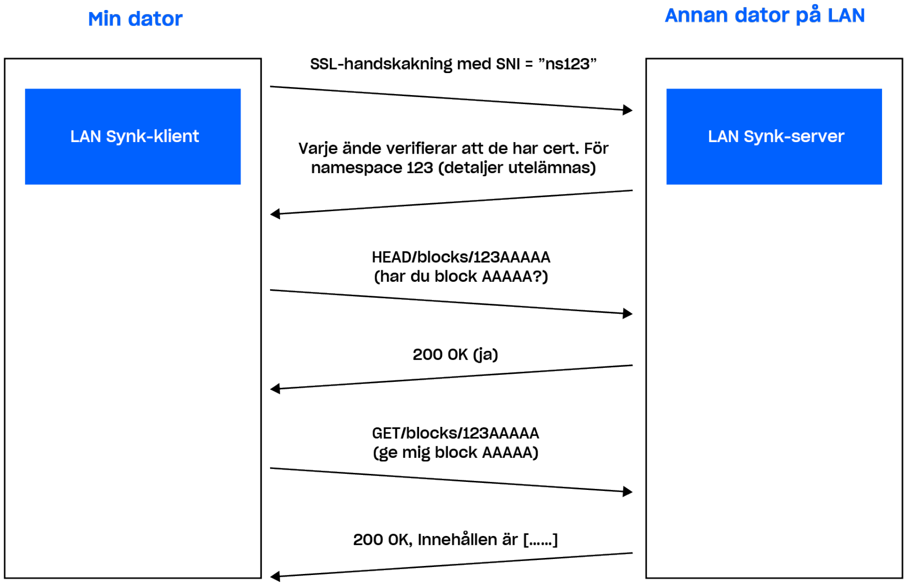
Den faktiska överföringen av filblock görs över HTTPS. Varje dator kör en HTTPS-server med slutpunkter. En klient avsöker flera peers för att se om de har blocken, men laddar endast ner blocken från en server.

I syfte att hålla din data säker ser vi till att endast klienter som är autentiserade för en viss mapp kan begära filblock. Vi ser också till att datorer inte kan utgöra sig för att vara servrar för mappar som de inte kontrollerar. För att lösa detta genererar vi SSL-nyckel-/certifikatpar för varje personlig Dropbox eller delad mapp. Dessa distribueras från Dropbox-servrar för de användardatorer som är auktoriserade för mappen. Nyckel-/certifikatparen roteras så fort medlemskapet ändras (till exempel när någon tas bort från en delad mapp). Vi kräver att båda ändarna av HTTPS-anslutningen autentiserar med samma certifikat (certifikatet för Dropbox-kontot eller den delade mappen). Detta bevisar att båda ändarna i anslutningen är auktoriserade.

När vi upprättar en anslutning meddelar vi servern vilken personlig Dropbox eller mapp som vi försöker ansluta till genom att använda SNI (Server Name Indication), så att servern använder rätt certifikat.



Dropbox distribuerar cert./nyckelpar
för namespace 123



Server/klient

Med det protokoll som beskrivs ovan behöver servern bara veta vilka block som är relevanta och var de finns.

Klienten upprätthåller en lista över peers för varje personlig Dropbox-mapp och delad mapp baserat på resultaten från daemon. När LAN-synksystemet får en begäran om att ladda ner ett filblock skickar det en begäran till ett slumpmässigt utvalt antal peers som den har upptäckt för den personliga Dropbox-mappen eller delade mappen och begär sedan blocket från den första som svarar att den har blocket.

Vi använder anslutningspooler som gör att vi kan återanvända redan upprättade anslutningar i syfte att undvika latens. Vi öppnar inte en anslutning förrän den behövs, och när den har öppnats håller vi den aktiv ifall vi behöver den på nytt. Vi begränsar också antalet anslutningar till en enskild peer.

Om ett filblock inte hittas eller kan laddas ner, eller om anslutningen visar sig vara långsam, förlitar sig systemet på Dropbox-servrarna för att hämta blocket.

Datacenter och funktionstjänstleverantörer

Dropbox företags- och produktionssystem förvaras i tredjepartsleverantörers datacenter och hos leverantörer av hanterade tjänster i olika regioner i USA. Alla SOC-rapporter gällande underleverantörernas datacenter och/eller avtalsvillkor och säkerhetsfrågeformulär till underleverantörer granskas minst en gång om året för att säkerställa tillräckliga säkerhetskontroller. Tredjepartsleverantörer av tjänster ansvarar för de fysiska, miljömässiga och operativa säkerhetskontrollerna inom ramen för Dropbox-infrastrukturen. Dropbox bär ansvaret för säkerheten rörande logik, nätverk och applikationer i den del av vår infrastruktur som är inhyst på tredjepartsdatacenter.

Vår leverantör som tillhandahåller tjänster för hantering och lagring, Amazon Web Services (AWS), ansvarar för den logiska säkerheten och nätverkssäkerheten som tillhandahålls genom deras infrastruktur. Anslutningarna skyddas genom deras brandvägg, som är konfigurerad i ett ”avvisa allt”-läge. Dropbox begränsar åtkomst till miljön till ett begränsat antal IP-adresser och medarbetare.

Infrastruktur i Tyskland, Australien, Japan och Storbritannien

Dropbox erbjuder lagring av filblock i regioner utanför USA för kvalificerade kunder. Vår infrastruktur finns på Amazon Web Services (AWS) i Tyskland, Australien, Japan och Storbritannien, och replikeras i respektive region för att garantera redundans och skydda mot dataförlust. Metadata om filer lagras på servrar som ägs av Dropbox. Paper-dokument och -förhandsvisningar lagras för närvarande i USA för alla kunder.

Verksamhetskontinuitet

Dropbox har infört ett system för att hantera verksamhetens kontinuitet (BCMS) som anger hur vi återupptar eller upprätthåller tjänsterna till användare – samt hur vi bedriver vår verksamhet som ett företag – om det sker ett avbrott i affärskritiska processer och aktiviteter. Vi bedriver en cyklisk process som utgörs av följande faser:

- ***Företagspåverkan och riskbedömning***

  Vi gör en bedömning av konsekvenser för verksamheten (BIA) minst en gång om året för att identifiera processer som är avgörande för Dropbox, bedöma den potentiella effekten av avbrott, fastställa prioriterade tidsramar för återställning samt identifiera våra kritiska beroenden och leverantörer. Vi utför också en riskbedömning som rör hela företaget minst en gång om året. Riskbedömningen hjälper oss att systematiskt identifiera, analysera och utvärdera risken för incidenter som leder till avbrott för Dropbox. Riskbedömningen och BIA tillsammans ger oss uppslag för kontinuitetsprioriteringar samt strategier för riskmininimering och återställning av planer för verksamhetens kontinuitet (BCP:er).

- ***Planer för verksamhetens kontinuitet***

  Team som har identifierats som kritiska för Dropbox kontinuitet av BIA använder denna information för att utveckla BCP:er för sina kritiska processer. Dessa planer bidrar till teamets kännedom om vem som ansvarar för att återuppta processerna i en nödsituation, vem från ett annat Dropbox-kontor eller en annan plats som kan ta över deras processer under ett avbrott och vilka kommunikationsmetoder som ska användas vid en kontinuitetshändelse. Dessa planer hjälper oss även att förbereda oss för ett avbrott genom att centralisera våra återställningsplaner och annan viktig information, som när och hur planen ska användas, kontakt- och mötesuppgifter, viktiga appar och återställningsstrategier. Dropbox kontinuitetsplaner utgör en del av vår företagsomfattande krishanteringsplan (CMP), som fastställer Dropbox team för kris- och incidenthantering.

- ***Plantestning/övningar***

  Dropbox testar utvalda delar av sina planer för verksamhetens kontinuitet minst en gång om året. Testen överensstämmer med omfattningen och målen för BCMS, grundas på lämpliga scenarier och utformas med tydliga syften. Testerna kan omfatta både bordsdiskussioner och fullskaliga simulationer av verkliga incidenter. Teamen uppdaterar och förbättrar sina planer för att hantera problem och stärka insatskapaciteten baserat på resultaten från testerna samt erfarenhet från verkliga incidenter.

- ***Granskning och godkännande av BCMS***

  Minst en gång om året granskar vår ledning BCMS som en del av granskningen av Dropbox förtroendeprogram.

Katastrofåterställning

Vi har en katastrofåterställningsplan för att hantera kraven på informationssäkerhet under större kriser eller katastrofer som påverkar driften av Dropbox Business. Dropbox-teknikteamet granskar planen varje år och testar utvalda delar minst en gång om året. Relevanta upptäckter dokumenteras och spåras tills problemet har lösts.

Vår katastrofplan (Disaster Recovery Plan, DRP) berör både hållbarhets- och tillgänglighetkatastrofer, som definieras enligt följande.

- En hållbarhetskatastrof består av en eller flera av följande faktorer:
  - En fullständig eller permanent förlust av ett huvudsakligt datacenter som lagrar metadata, eller av flera datacenter som lagrar filblock.
  - Förlorad förmåga att kommunicera eller serva data från ett datacenter som lagrar metadata, eller från flera datacenter som lagrar filinnehåll.
- En tillgänglighetskatastrof består av en eller flera av följande händelser:
  - Ett driftstopp på mer än 10 dagar.
  - Förlorad förmåga att kommunicera eller serva data från en lagringstjänst/ett datacenter som lagrar metadata, eller från flera lagringstjänster/datacenter som lagrar filblock.

Vi definierar ett mål för återställningstid (RTO), som den tidslängd och servicenivå som affärsprocessen eller tjänsten måste återställas på efter en katastrof, och ett mål för återställningspunkt (RPO) som är den längsta tolererbara period som data kan förloras efter ett serviceavbrott. Vi mäter också verklig återställningstid (RTA) under testning av katastrofåterställning, vilket utförs minst årligen.

Dropbox planer för incidenthantering, verksamhetens kontinuitet och katastrofåterställning kan testas vid planerade intervaller och vid betydande organisationsmässiga eller miljömässiga förändringar.

Applikationssäkerhet

Dropbox användargränsnitt

Dropbox-tjänsten kan användas och nås via ett antal olika gränssnitt. Alla har säkerhetsinställningar och säkerhetsfunktioner som bearbetar och skyddar användardata och gör dem lätta att komma åt.

- ***WEB***

  Det här gränssnittet kan nås via alla moderna webbläsare. Användare kan ladda upp, ladda ner, visa och dela sina filer. Med webbgränssnittet kan användare också öppna befintliga lokala versioner av filer från sina datorers standardprogram.

- ***Klienten***

  Dropbox-klienten är en kraftfull synkroniseringsklient som sparar filer lokalt för åtkomst offline. Den ger användarna full åtkomst till sina Dropbox-konton och fungerar med operativsystemen Windows och Mac. Filer kan visas och delas direkt i operativsystemets filläsare.

- ***Mobil***

  Dropbox-appen är tillgänglig för iOS- och Android-enheter så att användarna har åtkomst till filerna var de än är. Med mobilappen kan användare också göra filer tillgängliga för offlineåtkomst.

- ***API***

  Dropbox-API:erna erbjuder ett flexibelt sätt att läsa och skriva till Dropbox-användarkonton, och ger åtkomst till avancerade funktioner som sökning efter och revidering och återställning av filer. API:erna kan användas för att hantera användarlivscykeln för ett Dropbox-företagskonto, utföra åtgärder för alla medlemmar i ett team och aktivera åtkomst till adminfunktioner för Dropbox Business.

Paper-användargränsnitt

Paper-tjänsten kan användas och nås via ett antal olika gränssnitt. Alla har säkerhetsinställningar och säkerhetsfunktioner som bearbetar och skyddar användardata och gör dem lätta att komma åt.

- ***WEB***

  Gränssnittet kan användas med alla moderna webbläsare. Det låter användarna skapa, visa redigera, ladda ner och dela sina Paper-dokument.

- ***Mobila enheter***

  Paper-mobilappen är tillgänglig för smarttelefoner och surfplattor med iOS och Android så att användarna har åtkomst till sina Paper-dokument var de än är. Mobilappen är byggd som en hybridapplikation bestående av inbyggd kod (iOS eller Android) som ligger runt en intern webbgranskningsserver.

- ***API***

  Dropbox-API:n som beskrivs ovan innehåller slutpunkter och datatyper för hantering av dokument och mappar i Dropbox Paper, inklusive stöd för funktionalitet som åtkomsthantering, arkiv och permanent borttagning.

Kryptering

Överföring av data

Dropbox använder Secure Sockets Layer (SSL)/Transport Layer Security (TLS) vid överföring av data för att skydda data som skickas mellan Dropbox-appar och våra servrar. Detta skapar en säker tunnel som skyddas av Advanced Encryption Standard-kryptering (AES) om 128 bitar eller högre. Fildata som skickas mellan en Dropbox-klient (för närvarande dator, mobil, API eller webb) och värdtjänsten är krypterade via SSL/TLS. På liknande vis krypteras Paper-dokumentdata som skickas mellan en Paper-klient (för närvarande dator, mobil, API eller webb) och värdtjänsten alltid via SSL/TLS. För slutpunkter som vi kontrollerar (klient och mobil) samt moderna webbläsare använder vi starka chiffer och stödjer perfect forward secrecy och certificate pinning. Vi flaggar dessutom alla autentiseringscookies på webben som säkra och aktiverar HTTP Strict Transport Security (HSTS) med includeSubDomains aktiverat.

Obs! Dropbox använder endast TLS och har upphört med användningen av SSLv3 på grund av kända sårbarheter. TLS kallas dock ofta ”SSL/TLS”, så vi använder den beteckningen här.

För att förhindra mellanhandsattacker verifieras Dropbox-frontendservrar via publika certifikat hos klienten. Innan några filer eller Paper-dokument förs över förhandlas en krypterad anslutning, vilket bidrar till att säkerställa en säker leverans till Dropbox-frontendservrarna.

Vilande data

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

Nyckelhantering

Dropbox infrastruktur för nyckelhantering är utformad med säkerhetskontroller för drift, teknik och rutiner, med mycket begränsad åtkomst till nycklar. Generering, utbyte och lagring av krypteringsnycklar distribueras för decentraliserad bearbetning.

- ***Filkrypteringsnycklar***

  Dropbox har konstruerats för att hantera användarnas filkrypteringsnycklar så att tjänsten blir mer användarvänlig, samt för att aktivera avancerade produktfunktioner och stark kryptografisk kontroll. Filkrypteringsnycklar skapas, lagras och skyddas av produktionssystemets säkerhetskontroller för infrastrukturen och säkerhetspolicyer.

- ***Interna SSH-nycklar***

  Åtkomst till produktionssystemen begränsas med hjälp av unika SSH-nyckelpar. Säkerhetspolicyer och -rutiner behöver skyddas av SSH-nycklar. Ett internt system hanterar det säkra utbytet av offentliga nycklar och privata nycklar lagras på ett säkert sätt. Interna SSH-nycklar kan inte användas för åtkomst till produktionssystem utan en separat tvåfaktorautentisering.

- ***Nyckeldistribution***

  Dropbox automatiserar hanteringen och distributionen av känsliga nycklar till enbart de system som krävs för drift.

Certifikatpinning

Dropbox tillhandahåller certifikatsnålning i moderna webbläsare som stöder HTTP Public Key Pinning-specifikationen och på våra dator- och mobilklienter. Certifikatsnålning är en extra kontroll för att säkerställa att tjänsten du ansluter till är den du förväntar dig och inte ett bedrägeri. Vi använder detta för att skydda dig mot andra metoder som skickligare hackare kan använda sig av för att försöka spionera på din aktiviteter.

Skydda autentiseringsdata

Dropbox använder mer än bara vanlig hashning för att skydda användares inloggningsuppgifter. I enlighet med bästa praxis i branschen används en slumpmässigt genererad och användarunik saltsträng för varje lösenord och vi använder iterativ hashning för att sakta ner beräkningen. Dessa förfaranden bidrar till att skydda mot nyckelsöknings-, ordliste- och regnbågsattacker. Som en extra försiktighetsåtgärd krypterar vi hashvärdena med en nyckel som lagras avskilt från databasen, vilket bidrar till att hålla lösenord säkra vid en kompromettering som endast rör databasen.

Genomsökning efter sabotageprogram

Vi har utvecklat ett automatiserat system som söker efter skadlig kod vid den tidpunkt då eventuellt innehåll delas utanför ursprungsanvändarens konto. Systemet utnyttjar både egenutvecklad teknik och standarddetekteringsmotorer i branchen, och är utformat för att hindra skadlig programvara från att spridas.

Produktsäkerhet

Med Dropbox får både IT-avdelningar och slutanvändare de funktioner för kontroll och översikt de behöver för att hantera sina verksamheter och data. Med Dropbox får du allt du behöver för att arbeta – dina verktyg, material och andra användare – allt på ett ställe. Dropbox är mer än säkert lagringsutrymme – det är ett smart, användarvänligt sätt att optimera ditt befintliga arbetsflöde.

Nedan beskrivs några av funktionerna för administratörer och slutanvändare, samt tredjepartsintegreringar som hanterar viktiga IT-processer.

Observera: Vilka funktioner som är tillgängliga varierar beroende på prenumeration. Se dropbox.com/business/plans för mer information.

Innehållskontroller

Att skydda känsliga affärstillgångar – som immateriell egendom (IP) och personlig identifierbar information (PII) – är avgörande för IT- och datasäkerhetsteam. Dropbox tillhandahåller branschledande lösningar för att hantera, övervaka och skydda ditt material, från detaljerade innehållsbehörigheter till policyer för arkiveringsskyldighet. Nedan visas de viktiga Dropbox-produkter och -funktioner som har stöd för innehållskontroll.

Detaljerade innehållsbehörigheter och delade fil- och mappbehörigheter

- ***Åtkomst till delade filer***

  En teammedlem som äger en delad fil kan inaktivera åtkomst för specifika användare och inaktivera kommentering för filen.

- ***Behörigheter för delade filer***

  En teammedlem som äger en delad mapp kan inaktivera mappåtkomst för specifika användare, ändra/visa/redigera åtkomst för specifika användare och överföra ägarskap för mappar. Beroende på teamets globala delningsåtkomst kan varje ägare av en delad mapp kanske också kontrollera om mapparna kan delas med personer utanför teamet, om andra med redigeringsåtkomst ska kunna hantera medlemskap och om länkar kan delas med personer utanför teamet.

- ***Lösenord för delade länkar***

  Alla delade länkar kan skyddas med ett lösenord som anges av ägaren. Innan fil- eller mappdata skickas används ett åtkomstkontrollager för att verifiera att rätt lösenord har angetts och att alla andra krav (som team-, grupp- eller mapp-ACL) uppfylls. I så fall lagras en säkerhetscookie i användarens webbläsare och gör att den tidigare verifieringen av lösenordet blir ihågkommen. Med delningskontroller kan administratörer också konfigurera standardlösenord, istället för att de ska vara självvalda, för att bättre kunna skydda teamens material.

- ***Utgångsdatum för delade länkar***

  Användare kan ställa in ett utgångsdatum för alla delade länkar för att tillhandahålla tillfällig åtkomst till filer eller mappar. Med delningskontroller kan administratörer också konfigurera standardgiltigheter, istället för att de ska vara självvalda, för att bättre kunna skydda teamens material.

Åtkomst till Paper-dokument och delade Paper-mappar

- ***Åtkomst till Paper-dokument och delade Paper-mappar***

  En teammedlem som äger ett Paper-dokument eller en delad Paper-mapp kan ta bort åtkomsten för specifika användare och inaktivera redigering för dokumentet.

- ***Åtkomst till Paper-dokument***

  En teammedlem som äger ett Paper-dokument kan ta bort åtkomsten för specifika användare som är uttryckligen listade i delningspanelen. Både Paper-dokumentets ägare och redigerare kan ändra visnings- och redigeringstillstånd för specifika användare samt ändra dokumentets länkningspolicy. Länkningspolicyn styr vilka användare som kan öppna dokumentet och vilka behörigheter de har. Teamadministratören kan ställa in teamöverskridande policyer för länkar och dokumentdelning.

- ***Åtkomster till Paper-mappar***

  En teammedlem som är medlem i mappen kan ändra dess delningspolicy och ta bort åtkomst för specifika användare som uttryckligen lagts till i mappen.

Fil- och mappåtgärder

- ***Teammappar för filer***

  Administratörer kan skapa teammappar som automatiskt ger grupper och andra användare rätt åtkomstnivå (visa eller redigera) för det innehåll de behöver.

- ***Detaljerade åtkomst- och delningskontroller***

  Med delningskontroller kan administratörer hantera medlemskap och åtkomst för mappar på högsta nivå eller undermappar så att användare och grupper i och utanför företaget endast har åtkomst till de mappar som de behöver.

- ***Teammappshanterare***

  Administratörer kan visa alla sina teammappar och skräddarsy inställningar för delning från en central plats för att förhindra att konfidentiellt material delas av misstag.

- ***Delade mappar för Paper-dokument***

  Administratörer kan skapa delade Paper-mappar som automatiskt ger andra användare rätt åtkomstnivå – kommentera eller redigera – för det innehåll de behöver.

- ***Fjärradering***

  När medarbetare lämnar teamet eller tappar bort en enhet kan administratörer fjärradera Dropbox-data och lokala filkopior. Filer tas bort från både datorer och mobila enheter när de kopplas upp mot internet och Dropbox körs.

- ***Kontoöverföring***

  När en användare tagits bort från ett team (manuellt eller via katalogtjänster) kan administratören föra över filer och ägarskap till Paper-dokument som skapats av den före detta teammedlemmen från den användarens konto till en annan teammedlem. Kontoöverföringsfunktionen kan användas när en användare tas bort eller när som helst efter att en användas konto tagits bort.

Följande funktioner är tillgängliga som tilläggsfunktioner (kontakta försäljningsavdelningen för ytterligare information).

- ***Skanna material***

  Med tillägget för avancerade team- och innehållskontroller kan Dropbox Advanced- och Enterprise-företagskunder skanna efter nytt och befintligt innehåll i Dropbox för att hitta och undvika datasårbarheter.

- ***Konfigurera och lös ut anpassade arbetsflöden***

  Med tillägget för avancerade team- och innehållskontroller kan administratörer vidta anpassbara åtgärder mot filer som bryter mot företagets policyer.

- ***Konfigurera varningar***

  Administratörer kan övervaka säkerhetsproblem i realtid och undvika datasårbarheter. Få varningar om filer som delas externt och skanningar av känsliga data.

Innehållsöversikt

Säkerhetsvarningar och aviseringar

Dropbox Enterprise-administratörer kan få aviseringar i realtid när missbruk, riskfyllda aktiviteter eller potentiella dataläckor identifieras på deras konton. Följande händelser kan övervakas:

- Massraderingar
- Massdataförflyttningar
- Känsligt innehåll som delas externt
- Skadlig kod som delas utifrån med ditt team
- Sabotageprogram som delas inifrån ditt team
- För många misslyckade inloggningsförsök
- Inloggning från ett högriskland
- Ransomwaredetektion

Dropbox tillhandahåller också möjligheten att konfigurera trösklar för varningar, justera mottagare för aviseringar och utlösa varningar när mappar med känsligt innehåll delas externt. Administratör kan också markera varningar efterhand som de granskas, blir lösta eller avvisas. Och en kontrollpanelwidget visar de övergripande insikterna och trenderna för teamvarningarna för den senaste veckan.

Sida och rapporter över extern delning

Dropbox erbjuder ytterligare översikt med en sida och rapporter över extern delning. Administratörer kan skapa en rapport från antingen insiktspanelen eller sidan över extern delning. Rapporten listar teamets alla filer och mappar som delas utanför teamet, och alla delade länkar. Sidan för extern delning är en extra sida i adminkonsolen som ger administratörer möjlighet att se och filtrera (filtyp, vem som delat, länkinställningar med mera) filerna och mapparna som delas direkt utanför teamet och delade länkar.

Delningskontroller

Delningsinställningar ger team-administratörer mer kontroll över delningen och åtkomsten till deras teams innehåll. Administratörer kan konfigurera standardgiltigheter, lösenordsbegränsningar eller båda på team-nivå. Dessa begränsningar minskar risken för dataförlust genom att man tar bort ansvaret från användarna att konfigurera begränsningar.

Hemligstämpling

Team på Dropbox Enterprise kan automatiskt få etiketter på personliga och känsliga data för att skydda dem bättre från att exponeras. Administratörer får varningar om förebyggande av dataförlust (DLP) via e-post och i adminkonsolen när filer och mappar sparades i teamets mappar med känsligt innehåll delas utanför deras team. Administratörer har möjligheten att automatiskt identifiera och klassificera data som finns sparade i delade mapar och teammedlemmars personliga mappar. Dropbox Enterprise-administratörer kan aktivera automatisk dataklassificering från adminkonsolen.

Tillägg för datastyrning

Datastyrning är en övergripande uppsättning processer, tekniker och team, som förenas för att hantera och skydda en organisations datatillgångar. Här ingår möjligheten att lagra, identifiera, upptäcka och hämta företagsdata efter behov.

Dropbox-datastyrningstillägget innehåller en uppsättning funktioner som ger organisationer möjlighet att kontrollera och säkra sina data bättre, samtidigt som riskerna och kostnaderna för att följa lagar och efterlevnadskrav minskas. För närvarande inkluderar detta tillägg fyra viktiga funktioner för team- och efterlevnadsadministratörer.

- ***Utökad versionshistorik***

  Vilken filversionshistorik du har som standard beror på vilken typ av Dropbox-konto du har. Med Dropbox Business kan du emellertid köpa utökad versionshistorik (EVH) som ett tillägg separat eller som en del av datastyrningstillägget, vilket gör det möjligt att återställa en fil som raderats eller ändrats under de senaste 10 åren.

- ***Arkiveringsskyldigheter***

  Genom att lägga arkiveringsskyldighet för en teammedlem kan team- och efterlevnadsadministratörer se och exportera allt material som har skapats eller modifierats av denna person. Medlemmar som omfattas av arkiveringsskyldighet meddelas inte om skyldigheten och behåller sina behörigheter att skapa, redigera och ta bort filer.

- ***Datalagring***

  Dataretention ger teamet och efterlevnadsadministratörerna möjlighet att hindra oavsiktlig radering av innehåll som enligt lag måste sparas under en bestämd tid. Denna funktion ger kunder möjlighet att spara data i mer än 10 år efter senaste datum för ”revision”.

- ***Datadisposition***

  Datadisposition ger team och efterlevnadsadministratörer möjlighet att ta bort data permanent vid ett speciellt datum, för att tillgodose kraven för dataretention och disposition. Administratörer kan övervaka aktivitet genom rapporter som varnar dem för kommande borttagning av filer.

Återställning och versionskontroll

Dropbox-företagskunder har möjlighet att återskapa borttagna filer och Paper-dokument, och återställa till tidigare versioner av filer och Paper-dokument. Detta garanterar att ändringar av viktiga data kan spåras och hämtas.

Datasäkerhet på mobila enheter

- ***Radera data***

  För ytterligare säkerhet kan en användare aktivera möjligheten att radera alla Dropbox-data från enheten efter tio misslyckade försök att ange åtkomstkoden.

- ***Intern lagring och offlinefiler***

  Som standard lagras inte filer internt på mobila enheter. Dropbox-mobilklienter kan spara individuella filer och mappar på enheten för offlinevisning. När en enhet avlänkas från Dropbox-kontot, antingen via mobil- eller webbgränssnittet, raderas dessa filer och mappar automatiskt från enhetens interna lagring.

- ***Paper-dokument offline***

  När en enhet avlänkas från Paper via Dropbox-kontots säkerhetssida loggas användaren ut och Paper-dokument i offlineläge raderas automatiskt från enhetens interna lagring.

Teamkontroller

Eftersom alla organisationer är olika har vi tagit fram ett antal verktyg som ger administratörer möjlighet att anpassa Dropbox Business efter teamets särskilda behov. Dropbox Business har verktyg som hjälper slutanvändare att skydda sina konton och data ytterligare. Autentisering, återställning, loggning och andra säkerhetsfunktioner nedan är tillgängliga genom olika Dropbox-användargränssnitt.

Nedan visas flera kontroll- och översiktsfunktioner som är tillgängliga via adminkonsolen för Dropbox Business.

Detaljerade innehållsbehörigheter

- ***Olika administratörsroller***

  Dropbox erbjuder nivåindelade adminroller som ger en mer effektiv teamstyrning. Kontoadministratörer kan utnämnas på en av tre åtkomstnivåer. Det finns inga begränsningar för hur många administratörer ett team kan ha och alla teammedlemmar kan ges en adminroll.

- ***TEAMADMINISTRATÖR***

  Kan ställa in säkerhets- och delningsåtkomst för hela teamet, skapa administratörer och hantera medlemmar. Teamadministratören har heltäckande administratörsåtkomst. Endast teamadministratörer kan tilldela eller ändra administratörsroller, och det måste alltid finnas minst en teamadministratör för ett Dropbox-företagskonto.

- ***Administratör för användarhantering***

  Kan utföra de flesta teamhanteringsuppgifterna, inklusive att lägga till och ta bort teammedlemmar, hantera grupper och visa ett teams aktivitetsflöde.

- ***SUPPORTADMINISTRATÖR***

  Kan hantera vanliga tjänstebegäranden från teammedlemmar, som att återställa raderade filer eller hjälpa teammedlemmar som har blivit utelåsta från tvåstegsverifieringen. Supportadministratörer kan även återställa lösenord åt personer som inte är administratörer och exportera aktivitetsloggar för specifika teammedlemmar.

- ***Faktureringsadministration***

  Kan komma åt faktureringssidor i adminkonsolen.

- ***Innehållsadministration***

  Kan skapa och hantera teamets mappar i Innehållshanteraren.

- ***Rapporteringsadministration***

  Kan skapa rapporter i adminkonsolen och har åtkomst till aktivitetssidan.

- ***Säkerhetsadministration***

  Kan hantera säkerhetsvarningar, extern delning och säkerhetsrisker.

- ***Efterlevnadsadministratör (finns bara för team med datastyrningstillägget)***

  Kan hantera datastyrningssidor (bevarande av juridiska skäl, datalagring och datadisposition) och åtkomst till Innehållshanteraren.

- ***Groups***

  Team kan skapa och hantera medlemslistor inom Dropbox och enkelt ge medlemmarna åtkomst till specifika mappar. Dropbox kan även synka Active Directory-grupper med hjälp av Active Directory Connector.

- ***Företagshanterade grupper***

  Enbart administratörer kan skapa, radera och hantera medlemskap för den här typen av grupp. Användarna kan inte göra förfrågningar om att gå med i eller lämna en företagshanterad grupp.

- ***Användarhanterade grupper***

  Administratörer kan välja om användarna ska kunna skapa och hantera sina egna grupper. Administratörer kan även när som helst ändra en användarhanterad grupp till en företagshanterad grupp för att få kontroll över den.

- ***Begränsa flera konton på datorer***

  Administratörer kan blockera teammedlemmar från att länka ett andra Dropbox-konto till datorer som är länkade till deras Dropbox-konton för arbetet.

- ***Inaktiverad användarstatus***

  Administratörer kan inaktivera en användares åtkomst till sitt konto samtidigt som användarens data och delningsrelation bevaras i syfte att hålla företagsinformation säker. Administratörer kan senare återaktivera eller radera kontot.

- ***Logga in som användare***

  Teamadministratörer kan logga in som medlemmar i sina team. Detta ger administratörerna direktåtkomst till filer, mapparna och Paper-dokument i teammedlemmarnas konton, så att de kan genomföra ändringar, dela för teammedlemmars räkning eller granska händelser på filnivå. ”Logga in som användare”-händelser registreras i teamets aktivitetslogg och administratörerna kan avgöra om medlemmarna ska meddelas om dessa händelser.

- ***Delningsåtkomster***

  Teamadministratörer har övergripande kontroll över teamets delningsåtkomst vid användning av Dropbox, däribland huruvida:

  - Teammedlemmar kan dela filer och mappar med personer utanför teamet.
  - Teammedlemmar kan redigera mappar som ägs av personer utanför teamet.
  - Delade länkar som skapats av teammedlemmar fungerar för personer utanför teamet.
  - Teammedlemmar kan skapa filinlämningar och samla in filer från teammedlemmar och/eller personer utanför teamet.
  - Personer kan visa och infoga kommentarer i filer som ägs av teamet.
  - Teammedlemmar kan dela Paper-dokument och Paper-mappar med personer utanför teamet.
  - Permanenta borttagningsbehörigheter beviljas.

Teamadministratören för ett Dropbox-företagskonto kan begränsa möjligheten att ta bort filer och Paper-dokument permanent till att endast gälla teamadministratörer.

Användarregistrering och -etablering

Metoder för användaretablering och identitetshantering

- ***E-postinbjudan***

  Det finns ett verktyg i adminkonsolen för Dropbox Business som låter administratörerna generera mejlinbjudningar manuellt.

- ***Active Directory***

  Administratörer för Dropbox Business kan automatisera konfigurering och borttagning av konton i ett befintligt Active Directory-system via vår Active Directory-koppling eller tredje parts identitetsleverantörer. När Active Directory har integrerats kan det användas för hantering av medlemskap.

- ***Samlad inloggning (SSO)***

Dropbox Business kan konfigureras för att ge teammedlemmarna åtkomst genom inloggning via en central identitetsleverantör. Vår SSO-implementering använder Security Assertion Markup Language 2.0 (SAML

2.0), vilket gör etableringen enklare och säkrare genom att en betrodd identitetsleverantör autentiserar och ger teammedlemmar åtkomst till Dropbox utan ytterligare lösenord att hantera. Dropbox har dessutom inlett ett partnerskap med ledande identitetshanteringsleverantörer så att användare kan etableras och avetableras automatiskt. Läs mer i avsnittet Dropbox Business API-integreringar nedan.

- ***API***

  API för Dropbox Business kan användas av kunder för att skapa anpassade lösningar för användaretablering och identitetshantering. Läs mer i avsnittet Dropbox Business API-integreringar nedan.

Tvåstegsverifiering

Denna starkt rekommenderade säkerhetsfunktion skapar ett extra skyddslager för en användares Dropbox-konto. När tvåstegsverifiering har aktiverats måste man alltid ange lösenord och en sexsiffrig säkerhetskod när man loggar in eller ansluter till en ny dator, telefon eller surfplatta.

- Administratörer kan välja att kräva tvåstegsverifiering för alla teammedlemmar eller bara vissa.
- Kontoadministratörer kan spåra vilka teammedlemmar som har aktiverat tvåstegsverifieringen.
- Dropbox-koder för tvåstegsverifiering kan fås via sms eller appar med TOTP-algoritmstandarden (Time-based One-Time Password).
- Om en användare inte kan få säkerhetskoder med hjälp av dessa metoder kan hon eller han använda en 16-siffrig säkerhetskod för nödfall som endast används en gång. Användaren kan också använda ett sekundärt telefonnumer för att få en reservkod via sms.
- Dropbox har också stöd för den öppna standarden FIDO Universal 2nd Factor (U2F), som ger användare möjlighet till autentisering med en USB-säkerhetsnyckel de konfigurerat istället för en sexsiffrig kod.

Företagsinstallatör

Administratörer som kräver storskalig etablering kan använda vår företagsinstallatör för Windows för att fjärrinstallera Dropbox-klienten via mekanismer för hanterad programvara och distribution.

Hanterade enheter och inloggning

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

  Dropbox integrerar med EMM-leverantörer från tredje part för att ge Dropbox-företagsadministratörer med ett Enterprise-abonnemang större kontroll över hur teammedlemmar använder Dropbox på mobila enheter. Administratörer kan begränsa användningen av mobilappen för Dropbox Enterprise-konton till endast hanterade enheter (oavsett om de tillhandahålls av företaget eller är personliga), se information om appanvändning (inklusive tillgängligt lagringsutrymme och åtkomstplatser) och fjärradera en borttappad eller stulen enhet. Observera att Paper-appen för närvarande inte kan styras med EMM.

- ***Enhetsgodkännanden***

  Med Dropbox kan Dropbox Education- och Dropbox-företagsadministratörer med Advanced- och Enterprise-abonnemang ställa in begränsningar för hur många enheter som en användare kan synka med Dropbox, och kan även välja om godkännanden ska hanteras av användarna eller administratörerna. Administratörer kan också skapa en undantagslista över användare som inte är begränsade till ett visst antal enheter. Observera att Paper-mobilappen inte omfattas av enhetsgodkännanden.

- ***Krav på tvåstegsverifiering***

  Administratörer kan välja att kräva tvåstegsverifiering för alla eller bara vissa teammedlemmar. Andra krav på multifaktorverifiering kan integreras genom teamets SSO-implementering.

- ***Lösenordskontroll***

  Administratörer för Education-, Advanced- och Enterprise-team kan kräva att medlemmarna skapar och upprätthåller starka och komplexa lösenord till sina konton. När denna funktion är aktiverad kommer teammedlemmarna att loggas ut från sina webbsessioner och tvingas skapa nya lösenord när de loggar in igen. Ett inbyggt verktyg analyserar lösenordets styrka genom att jämföra det med en databas med vanliga ord, namn, mönster och siffror. En användare som anger ett vanligt lösenord ombes komma på ett nytt som är unikt och svårare att gissa för en utomstående. Administratörer kan också återställa lösenord för hela teamet eller för enskilda användare.

- ***Domänhantering***

  Dropbox erbjuder en uppsättning verktyg som ger företag möjlighet att förenkla och påskynda processen för etablering av nya användare och kontroll av Dropbox-användningen.

  - **Domänverifiering**
    Företag kan göra anspråk på äganderätten till sina egna domäner och låsa upp resten av verktygen för domänhantering.

  - **Tvingande inbjudan**
    Administratörer kan kräva att enskilda Dropbox-användare, som har bjudits in till företagets Dropbox-team, överförs till teamet eller ändrar e-postadress i sina personliga konton.

  - **Domäninsikter**
    Administratörer kan se viktig information, till exempel hur många enskilda Dropbox-konton som använder företagets e-postadresser.

  - **Kontotillägg**
    Administratörer kan tvinga alla Dropbox-användare som använder en av företagets e-postadresser att gå med i företagets team eller ändra e-postadress i sitt personliga konto.

- ***Webbsessionskontroll***

  Administratörer kan styra hur länge teammedlemmar kan vara inloggade på dropbox.com. Administratörer kan begränsa varaktigheten för alla webbsessioner och/eller sessioner som är i vänteläge. Sessioner som når dessa gränser kommer automatiskt att loggas ut. Administratörer kan också spåra och avsluta webbsessioner för individuella användare.

- ***Appåtkomst***

  Administratörerna kan visa och återkalla tredjepartsappars åtkomst till användarkonton.

- ***Avlänkning av enheter***

  Datorer och mobila enheter som är anslutna till användarkonton kan kopplas från av administratören i adminkonsolen eller av användaren själv i det enskilda kontots säkerhetsinställningar. När du kopplar från en dator raderas autentiseringsdata och du har möjlighet att radera lokala kopior av filer nästa gång datorn ansluter till internet (se **Fjärradering** nedan). När du kopplar från en mobil enhet raderas favoritmarkerade filer, cachelagrade data och inloggningsinformation. Avlänkningen tar också bort Paper-dokument som finns i offlineläge i Paper-mobilappen. Om tvåstegsverifiering är aktiverad måste användaren återautentisera varje enhet vid återkoppling. Användarnas kontoinställningar ger dessutom möjligheten att skicka en automatisk avisering via e-post när enheter kopplas samman.

- ***Styrning av nätverk***

  Administratörer för Dropbox-företagsteam med Enterprise-abonnemang kan begränsa Dropbox-användningen på företagsnätverket till enbart Enterprise-teamkontot. Denna funktion integreras med företagets nätverkssäkerhetsleverantör för att blockera eventuell trafik utanför det sanktionerade kontot på datorer. Observera att Paper för närvarande inte hanteras genom nätverkskontroll.

Mobilsäkerhet

- ***Fingeravtrycksskanning***

  Användare kan aktivera Touch ID eller Face ID på iOS-enheter och fingeravtryckslås (när detta stöds) på Android-enheter som ett sätt att låsa upp Dropbox-mobilappen.

Åtkomstöversikt

- ***Identitetsverifiering vid teknisk support***

  Innan Dropbox-supporten utför en felsökning eller lämnar ut kontouppgifter måste kontoadministratören verifiera sin identitet genom att tillhandahålla en slumpgenererad engångskod. Denna PIN-kod är endast tillgänglig via adminkonsolen.

Användarkontoaktivitet

Varje användare kan se följande sidor i kontoinställningarna för att kunna hämta aktuell information angående den egna kontoaktiviteten.

- ***Delningssida***

  På denna sida visas de delade mapparna som för närvarande finns i användarens Dropbox, samt delade mappar som användaren kan lägga till. En användare kan avbryta delningen av mappar och filer och ange delningsbehörigheter.

- ***Filsida***

  Denna sida visar de filer som delats med användare och respektive datum då varje fil delades. Användaren har möjlighet att ta bort åtkomst till dessa filer. För att visa Paper-dokument som har delats med användaren av andra personer kan användaren gå till ”Delat med mig”-sidan i navigeringsgränssnittet för Paper-dokument.

- ***Länksida***

  Denna sida visar alla aktiva delade länkar som användaren har skapat och skapandedatumet för dem. Den visar även alla länkar som andra delar med användaren. Användaren kan inaktivera länkar eller ändra behörigheter.

- ***E-postaviseringar***

  En användare kan välja att få e-postaviseringar omedelbart när en ny enhet eller app kopplas till deras Dropbox-konto.

Åtkomst till användarkonto

- ***Kopplade enheter***

  Enhetsdelen i en användares kontosäkerhetsinställningar visar alla datorer och mobila enheter som är kopplade till användarens konto. För varje dator visas IP-adress, land och ungefärlig tid för senaste aktivitet. En användare kan koppla från valfri enhet, med möjlighet att få filer på kopplade enheter raderade nästa gång de ansluts till internet.

- ***Aktiva webbsessioner***

  Sessionsdelen visar alla webbläsare som är inloggade på en användares konto. Varje webbläsare visas IP-adress, land och inloggningstid för den senaste sessionen, samt ungefärlig tid för den senaste aktiviteten. En användare kan fjärravsluta alla sessioner via användarkontots säkerhetsinställningar.

- ***Länkade appar***

  I delen för **länkade appar** visas en lista över alla tredjepartsappar med åtkomst till en användares konto, samt vilken typ av åtkomst varje app har. En användare kan återkalla alla appars behörighet till användarens Dropbox.

Aktivitetsflöde

Dropbox Business registrerar filåtgärder i teamets aktivitetsflöde som nås från adminkonsolen. Aktivitetsflödet erbjuder flexibla filtreringsalternativ som gör att administratörer kan utföra målinriktade utredningar av konto-, fil- eller Paper-dokumentaktiviteter. De kan till exempel visa hela historiken för en fil eller ett Paper-dokument och hur användarnas interaktion ser ut, eller visa all aktivitet för teamet under en specifik tidsperiod. Aktivitetsflödet kan exporteras som en nerladdningsbar rapport i CSV-format och integreras direkt i en SIEM-produkt (Security Information and Event Management) eller något annat analysverktyg genom lösningar från tredjepartspartner. Följande innehållshändelser registreras i aktivitetsflödet:

- ***Delning för filer, mappar och länkar***

  I förekommande fall anger rapporter huruvida händelser omfattar personer utanför teamet.

  Delade filer

  - Lade till eller tog bort en teammedlem eller icke-teammedlem.
  - Ändrade åtkomstbehörigheter för en teammedlem eller icke-teammedlem.
  - Lade till eller tog bort en grupp.
  - Lade till en delad fil i användarens Dropbox.
  - Visade innehållet i en fil som delades via en fil- eller mappinbjudan.
  - Kopierade delat innehåll till användarens Dropbox.
  - Laddade ner delat innehåll.

- Kommenterade i en fil.
- Markerade en kommentar som löst eller olöst.
- Raderade en kommentar.
- Påbörjade eller avslutade prenumeration på kommentarsaviseringar.
- Gjorde anspråk på en inbjudan till en fil som ägs av teamet.
- Begärde åtkomst till en fil som ägs av teamet.
- Avbröt delningen av en fil.

Delade mappar

- Skapade en ny delad mapp.
- Lade till eller tog bort en teammedlem, icke-teammedlem eller grupp.
- Lade till en delad mapp i användarens Dropbox, eller så tog användaren bort sin egen åtkomst till en delad mapp.
- Lade till en delad mapp från en länk.
- Ändrade åtkomstbehörigheter för en teammedlem eller icke-teammedlem.
- Överförde ägarskapet av en mapp till en annan användare.
- Avbröt delningen av en mapp.
- Gjorde anspråk på medlemskapet för en delad mapp.
- Begärde åtkomst till en delad mapp.
- La till en begärande användare till en delad mapp.
- Blockerade eller avblockerade icke-teammedlemmar från att läggas till i en mapp.
- Tillät samtliga teammedlemmar att lägga till personer i en mapp eller bara ägaren.
- Ändrade gruppåtkomst till en delad mapp.

Delade länkar

- Skapade eller tog bort en länk.
- Gjorde innehållet i en länk synligt för alla med länken eller endast teammedlemmar.
- Gjorde innehållet i en länk lösenordsskyddat.
- Angav eller tog bort ett utgångsdatum för en länk.
- Visade en länk.
- Laddade ner innehållet i en länk.
- Kopierade innehållet i en länk till användarens Dropbox.
- Skapade en länk till en fil via en API-app.
- Delade en länk med en teammedlem, icke-teammedlem eller grupp.
- Blockerade eller avblockerade icke-teammedlemmar från att visa länkar till filer i en delad mapp.
- Delade ett album.

Filinlämningar

- Skapade, ändrade, stängde eller raderade en filinlämning.
- Lade till användare till en filinlämning.
- Lade till eller tog bort en filinlämningsdeadline.
- Ändrade en filinlämningsmapp.
- Tog emot filer via en filinlämning.
- Tog emot filer via mejl till Dropbox.

Enskilda fil- och mapphändelser

- Lade till en fil i Dropbox
- Skapade en mapp.
- Visade i fil.
- Redigerade en fil.
- Laddade ner en fil.
- Kopierade en fil eller mapp.
- Flyttade en fil eller mapp.
- Gav en fil eller mapp ett nytt namn.
- Ändrade tillbaka en fil till en tidigare version.
- Rullade tillbaka ändringar i filer.
- Återskapade en raderad fil.
- Raderade en fil eller mapp.
- Raderade en fil eller mapp permanent.

Lyckade och misslyckade inloggningsförsök.

- Lyckat eller misslyckat inloggningsförsök.
- Misslyckat inloggningsförsök eller fel via samlad inloggning (SSO).
- Misslyckat inloggningsförsök eller inloggningsfel via EMM.
- Loggade ut.
- Ändring av IP-adress för webbsession.

Lösenord

Ändringar av lösenord eller inställningar för tvåstegsverifiering. Administratörer har inte tillgång till användares lösenord.

- Ändrade eller återställde lösenord.
- Aktiverad, återställd eller inaktiverad tvåstegsverifiering.

- Konfigurerade eller ändrade tvåstegsverifiering för användning av SMS eller mobilapp.
- Lade till, redigerade eller tog bort säkerhetstelefon för tvåstegsverifiering.
- Lade till eller tog bort säkerhetsnyckel för tvåstegsverifiering.

Medlemskap

Tillägg eller borttagning av personer i teamet.

- Bjöd in en teammedlem.
- Gick med i teamet.
- Tog bort en teammedlem.
- Stängde av eller upphävde avstängning av en teammedlem.
- Återställde en borttagen teammedlem.
- Begärde att få gå med i teamet baserat på kontodomän.
- Godkände eller avböjde en begäran om att gå med i teamet baserat på kontodomän.
- Skickade domäninbjudningar till befintliga domänkonton.
- Användare gick med i teamet som svar på kontotillägg.
- Användare lämnade domän som svar på kontotillägg.
- Blockerade eller avblockerade teammedlemmar från att föreslå nya medlemmar.
- Föreslog en ny teammedlem.

Appar

Koppla tredjepartsappar till Dropbox-konton.

- Godkände eller tog bort en applikation.
- Godkände eller tog bort en teamapplikation.

Enheter

Koppla datorer eller mobila enheter till Dropbox-konton.

- Länkade eller kopplade från en enhet.
- Använde fjärradering och raderade alla filer eller misslyckades med att radera vissa filer.
- Ändring av IP-adress för skrivbordsdatorer eller mobila enheter.

Administratörsåtgärder

Ändring av inställningar i administratörskonsolen, till exempel behörighet till delade mappar.

- ***Autentisering och samlad inloggning (SSO)***
  - Återställde teammedlems lösenord.

  - Återställde alla teammedlemmars lösenord.
  - Blockerade eller avblockerade teammedlemmar från att inaktivera tvåstegsverifiering.
  - Aktiverade eller inaktiverade SSO.
  - Gjorde inloggning via SSO obligatorisk.
  - Ändrade eller tog bort SSO-URL.
  - Uppdaterade SSO-certifikat.
  - Ändrade SSO-identitetsläge.

- ***Medlemskap***
  - Blockerade eller avblockerade användare från att begära anslutning till teamet baserat på kontodomän.
  - Ställde in begäranden för teammedlemskap på att automatiskt godkännas eller kräva manuellt administratörsgodkännande.

- ***Hantering av medlemskonto***
  - Ändrade en teammedlems namn.
  - Ändrade en teammedlems e-postadress.
  - Tilldelade eller tog bort administratörsstatus, eller ändrade administratörsrollen.
  - Loggade in eller ut som teammedlem.
  - Överförde eller raderade innehållet i en borttagen medlems konto.
  - Raderade innehållet i en borttagen medlems konto permanent.

- ***Globala delningsinställningar***
  - Blockerade eller avblockerade teammedlemmar från att lägga till delade mappar ägda av icke-teammedlemmar.
  - Blockerade eller avblockerade teammedlemmar från att dela mappar med icke-teammedlemmar.
  - Aktiverade varningar som visas för användare innan de delar mappar med icke-teammedlemmar.
  - Blockerade eller avblockerade icke-teammedlemmar från att se delade länkar.
  - Ställde in delade länkar på att endast visas för teamet som standard.
  - Blockerade eller avblockerade personer från att lämna kommentarer i filer.
  - Blockerade eller avblockerade teammedlemmar från att skapa filinlämningar.
  - Lade till, ändrade eller tog bort en logo för delade mappsidor.
  - Blockerade eller avblockerade teammedlemmar från att dela Paper-dokument och Paper-mappar med personer som inte är medlemmar i teamet.

- ***Teammappshantering för filer***
  - Skapade en teammapp.
  - Bytte namn på en teammapp.
  - Arkiverade en teammapp eller återställde den från arkivering.
  - Raderade en teammapp permanent.
  - Nedgraderade en teammapp till en delad mapp.

- ***Domänhantering***
  - Försökte verifiera eller verifierade en domän eller tog bort en domän.
  - Dropbox Support verifierade eller tog bort en domän.
  - Aktiverade eller inaktiverade sändningen av domäninbjudningar.
  - Slog på eller av ”Bjud in nya användare automatiskt”.
  - Ändrade läge för kontotillägg.
  - Dropbox Support beviljade eller drog tillbaka kontotillägg.
- ***Enterprise Mobility Management (EMM)***
  - Aktiverade EMM för testläge (valfritt) eller distributionsläge (krav).
  - Uppdaterade EMM-token.
  - Lade till eller tog bort teammedlemmar från listan över EMM-undantagna användare.
  - Inaktiverade EMM.
  - Skapade en rapport med EMM-undantagslista.
  - Skapade en användningsrapport för EMM-mobilapp.
- ***Ändringar av andra teaminställningar***
  - Slog samman team.
  - Uppgraderade teamet till Dropbox Business eller nedgraderade det till ett gratisteam.
  - Ändrade teamnamnet.
  - Skapade en teamaktivitetsrapport.
  - Blockerade eller avblockerade teammedlemmar från att ha fler än ett konto kopplat till en dator.
  - Tillät alla medlemmar eller endast administratörer att skapa grupper.
  - Blockerade eller avblockerade teammedlemmar från att radera filer permanent.
  - Inledde eller avslutade en Dropbox Support-session för en återförsäljare.

Grupper

Information om skapande, borttagning och medlemskap i grupper.

- Skapade, döpte om, flyttade eller raderade en grupp.
- Lade till eller tog bort en medlem.
- Ändrade en gruppmedlems åtkomsttyp.
- Ändrade grupp till teamhanterad eller adminhanterad.
- Ändrade externt ID för en grupp.

Paper-aktivitetslogg

Administratörer kan välja en typ av Paper-aktivitet i aktivitetsflödet eller hämta en fullständig aktivitetsrapport. Paper-händelser registreras för:

- Paper aktiverat eller inaktiverat.
- Paper-dokument skapades, redigerades, exporterades, arkiverades, tog bort permanent eller återställdes.
- Paper-dokument kommenterades, och kommentaren markerades som löst.
- Paper-dokument delades med teammedlemmar och andra personer, och delning avslutades.
- Åtkomst till Paper-dokument begärd av teammedlemmar och andra personer.
- Teammedlemmar och andra personer taggades i Paper-dokument.
- Paper-dokument visades av teammedlemmar och andra personer.
- Paper-dokument följdes.
- Paper-dokuments medlemsbehörigheter förändrades (redigera, kommentera eller skrivskyddat).
- Extern delningspolicy för Paper-dokument ändrades.
- Paper-mappar skapades, arkiverades eller togs bort permanent.
- Paper-dokument lades till i eller togs bort från en mapp.
- Paper-mapp fick nytt namn.
- Paper-dokument och Paper-mappar flyttades.

Dropbox Passwords

Dropbox Passwords erbjuder ett säkert och enkelt sätt att lagra, synkronisera och fylla i användarnamn, lösenord och kredit- och betalkort på olika enheter så att du kan skydda dina autentiseringsuppgifter online. Dropbox Passwords skyddar dina känsliga användarnamn, lösenord, lösenord och kredit- och betalkortsuppgifter med nollkunskapskryptering i molnet och på dina enheter. Våra produkter är byggda för daglig användning med inbyggd säkerhet.

Nollkunskapskryptering

Dropbox Passwords lagrar dina krypterade data i molnet men nycklarna för att dekryptera dessa data lagras bara på dina enheter. **Dropbox har aldrig tillgång till dem.** Dessa nycklar är långa, slumpmässiga och genereras på din enhet. De lämnar aldrig din enhet förutom om du bestämmer dig för att parkoppla eller registrera en ny enhet. Denna överföring använder kryptering med öppen nyckel för att både kryptografiskt signera och skydda nycklarna under överföringen så att du kan vara säker på att ingen annan kan dekryptera dem, samtidigt som du kan verifiera att de är giltiga. Den här egenskapen kallas ofta nollkunskapskryptering eftersom krypterade data är värdelösa för alla som inte har nycklarna, inklusive Dropbox. Det betyder att **bara kommer åt din information** och i det osannolika fallet att Dropbox skulle hackas är din information fortfarande säker. Krypterade data separeras från synliga Dropbox-mappar och kan inte nås med Dropbox-klienter eller API:er.

Krypteringsdetaljer

Dropbox krypterar dina data med XChaCha20-Poly1305 i kombinerat läge för implicit autentisering. Våra webbläsartillägg och mobilapplikationer använder alla krypteringsimplementeringar som stöds av libsodium, vilket är en granskad och allmänt distribuerad NaCl-gaffel.

Varje krypteringsåtgärd genererar en slumpmässig 192-bitarsnonce, som lagras med den krypterade nyttolasten för senare dekryptering. Till skillnad från AES-GCM stöder XChaCha20-Poly1305 slumpmässiga nonces. Vid dekryptering läses 192-bitarsnoncen från nyttolasten och används för att dekryptera den krypterade nyttolasten. Eventuell efterföljande kryptering genererar en slumpmässig 192-bitarsnonce oberoende av föregående nonce. Dropbox Passwords genererar slumpmässiga tal med libsodium, som naturligt går tillbaka till en kryptografiskt säker slumptalsgenerator på var och en av plattformarna vi har stöd för.

Nycklar och återställningsord

Vi genererar en 256-bitars symmetrisk nyckel (krypteringsnyckeln) från 128 bitarsentropi (användarnyckeln) via Blake2-hashing. Denna krypteringsnyckel blir alltid kvar på ägarens enheter och stannar när så är möjligt i den säkraste lagring vi har tillgång till på dessa enheter. På iPhones lagrar vi till exempel krypteringsnyckeln i iOS Keychain.

Vi använder 128-bitarsentropi som vår källa eftersom denna erbjuder tillräcklig säkerhet samtidigt som den bara kräver 12 återställningsord med BIP-39-standarden för säkerhetskopiering. BIP-39 ger ett användarvänligt sätt att representera stora slumpmässiga nycklar genom att dessa nycklar omvandlas till en lista med 12 ord. Varje 128-bitarsnyckel har en korresponderande ordlista och varje lista med 12 ord identifierar unikt 128 bitar. Den enda nackdelen är att de 12 orden faktiskt motsvarar 132 bitar, så de extra fyra bitarna används som en kontrollsumma för att identifiera fel. Återställningsorden ger användaren möjlighet att återställa sin krypteringsnyckel enheten tappas bort eller blir stulen. Vi rekommenderar att de skrivs ut och förvaras på en säker plats. Det kan också vara en bra idé att ge dem till en betrodd vän eller familjemedlem eller lagra dem på en USB-enhet.

Enhetsregistrering

När en användare loggar in på Dropbox Passwords på en ny enhet måste enheten slutföra en säker registreringsprocedur för att få åtkomst till användarens Passwords-data. Den här proceduren hjälper till att säkerställa att en användares hemliga nyckel och Passwords-data endast blir tillgängliga från användarens registrerade enheter. Detta hjälper också till att säkerställa att en användare bara kan registrera ytterligare enheter om hen har tillgång till en befintlig registrerad enhet eller återställningsorden. Enhetsregistreringsproceduren sker på följande vis.

En ny registrerad enhet genererar slumpmässigt ett offentlig/privat 256-bitarsnyckelpar och laddar upp den offentliga nyckeln till Dropbox-servern. Sedan inträffar antingen scenario **A**, **B** eller **C**.

A: Om användaren inte tidigare har registrerat en enhet genererar registreringsenheten slumpmässigt en 128-bitars hemlig användarnyckel. Både användarnyckeln och enhetsnyckelparet lagras på en säker OS-specifik plats i enlighet med beskrivningen i följande nyckellagringsavsnitt. Enheten initierar användarens Passwords-data, krypterar dem och laddar upp den krypterade nyttolasten till Dropbox-servern.

B: Om användaren har minst en tidigare registrerad enhet skickas en begäran om godkännande av registrering till var och en av dessa enheter. Anmälningsenhetens publika nyckel är kopplad till begäran. Användaren måste sedan godkänna begäran på en av sina registrerade enheter. Om den godkänns krypterar den registrerade enheten användarnyckeln med sin privata nyckel och registreringsenhetens publika nyckel via X25519 ECDH med XSalsa20-Poly1305. Den registrerade enheten laddar upp den krypterade användarnyckeln till Dropbox-servern för att skicka till den registrerande enheten. Den registrerande enheten hämtar och dekrypterar användarnyckeln med sin privata nyckel och den registrerade enhetens offentliga nyckel. Den registrerande enheten hämtar sedan krypterade Passwords-nyttolastdata, och dekrypterar dem med användarnyckeln.

C: Om användaren tidigare har registrerat en enhet men inte längre kan komma åt dem kan hen ange sina 12 återställningsord för att lokalt rekonstruera användarnyckeln. Den registrerande enheten hämtar sedan krypterade Passwords-nyttolastdata, och dekrypterar dem med användarnyckeln.

Nyckellagring

Webbläsartillägg

I webbläsare lagras användarnyckeln i webbläsartilläggets lokala lagringsområde. Lokala lagringsvärden för webbläsartillägg är endast tillgängliga från tillägget. Eventuell kod som körs på webbplatser som användaren besöker kan inte läsa från webbläsartilläggets lokala lagringsområde. Dessutom tillåter webbläsartillägg inte körning av kod som inte ingår i det signerade tilläggspaketet, vilket eliminerar risken för en XSS-sårbarhet som skulle kunna komma åt lokala lagringsvärden.

En angripare med obegränsad åtkomst till användarens enhet kan komma åt användarnyckeln genom att läsa den lokala lagringsfilen på disken. Exempel på sådana hot är om en angripare har fysisk åtkomst till enheten eller en angripare kör skadlig skadlig kod på enheten. För att skydda mot dessa scenarier kan användaren konfigurera en lösenfras för den lokal enheten.

När en lösenfras konfigureras krypteras användarnyckeln i vila i webbläsartilläggets lokala lagring. Krypteringsnyckeln härleds från lösenfrasen genom Argon2-lösenordshashing, och krypteringsmetoden som används är XChaCha20-poly1305. Varje gång webbläsartillägget startas om måste användaren ange sin lösenfras för att dekryptera användarnyckeln och låsa upp sina data. Följaktligen kan en angripare utan lösenfrasen inte dekryptera användarnyckeln som finns lagrad i den lokala lagringsfilen på disken.

iOS

Med iOS lagras användarnyckeln i iOS Keychain som är en krypterad databasfil på disken. Den här filen krypteras med en hemlig nyckel som lagras i Secure Enclave-hårdvarumodulen med hjälp av AES256-GCM som krypteringsmetod. Endast den signerade iOS-appen Dropbox Passwords kan komma åt de objekt den har lagrat i nyckelringen. Detta förhindrar att annan kod som körs på användarens enhet kan komma åt användarnyckeln.

Android

Med Android lagras användarnyckeln i ett EncryptedSharedPreferences-objekt, som är en krypterad inställningsfil på disken. Den här filen krypteras med en huvudnyckel som lagras i den säkra Android Keystore-hårdvaran med AES256-GCM som krypteringsmetod. Endast den signerade Android-appen Dropbox Passwords kan komma åt huvudnyckeln som används för att dekryptera inställningsfilen.

Lokal autentisering

Dropbox Passwords tillhandahåller valfria lokala autentiseringsåtgärder för att ytterligare begränsa åtkomsten till användarens lösenordsdata på den fysiska enheten. För mobilapplikationer kan den lokala OS-autentiseringsgesten återanvändas (till exempel ett lösenord med kompletterande biometrisk autentisering). För webbläsartillägg kan en valfri lösenfras konfigureras. Dessa mekanismer ger ett ytterligare lager applikationssäkerhet när användarens enhets-OS är upplåst. Detta gör det möjligt för användaren att skydda sina lösenordsdata när en annan användare har tillgång till enheten, till exempel en familjemedlem eller kollega.

Förslag för lösenordsstyrka

Dropbox byggde zxcvbn-verktyget med öppen källkod som används av flera lösenordshanterare för att uppskatta lösenordsstyrkan. Verktyget jämför lösenord mot en databas med 30 000 vanliga lösenord, namn och efternamn i enlighet med amerikanska folkräkningsdata, populära engelska ord från Wikipedia och amerikansk tv och filmer, och andra vanliga mönster som datum, upprepningar (aaa), sekvenser (abcd), tangentbordsmönster (qwertyuiop) och Leet (1337). Om lösenordet som en användare försöker ange är vanligt uppmanar verktyget hen att mata in något mer unikt och svårtgissat. Inställningen **Mycket stark** hjälper gör det möjligt att säkerställa högsta nivå av kontosäkerhet för användare.

Integritet och transparens för datasäkerhet

Personer och organisationer litar på Dropbox för sitt viktigaste arbete varje dag, och det är vårt ansvar att skydda denna information och hålla den privat.

Integritetspolicy

Vår integritetspolicy finns på dropbox.com/privacy. Dropbox integritetspolicy, företagsavtal, servicevillkor och policy för godkänd användning ger information om följande villkor:

- Vilken typ av information vi samlar in och varför.
- Med vem eller vilka vi kan dela information.

- Hur vi skyddar dessa uppgifter och hur länge vi behåller dem.
- Var vi förvarar och vart vi skickar dina uppgifter.
- Detta händer om policyn ändras eller om du har frågor.

Insyn

Dropbox har åtagit sig att redovisa antalet förfrågningar om användaruppgifter som vi får från brottsbekämpande myndigheter, samt att öppet redovisa hur vi hanterar dessa uppgifter. Vi detaljgranskar alla dataförfrågningar för att säkerställa att de efterlever lagen och vi har åtagit oss att meddela användare (i den utsträckning lagen tillåter det) när deras konton blir aktuella i polisiära förfrågningar.

Dessa ansträngningar understryker vårt engagemang för att skydda våra användares sekretess och deras data. För detta ändamål har vi en insynsrapport och vi har upprättat en uppsättning principer för statliga förfrågningar. Följande principer styr vårt agerande när vi mottar, granskar och svarar på statliga förfrågningar angående våra användares data:

- ***Var öppen***

  Vi anser att onlinetjänster ska få publicera antalet och typerna av myndighetsförfrågningar som tas emot, och meddela individer när information om dem har begärts ut. Denna typ av öppenhet ger makt åt användaren eftersom hen på ett bättre sätt kan förstå förekomster och mönster i fråga om myndighetsmissbruk. Vi kommer att fortsätta att publicera detaljerad information om dessa förfrågningar och förespråka rätten att tillhandahålla mer av denna viktiga information.

- ***Kämpa mot alltför omfattande förfrågningar***

  Myndigheternas dataförfrågningar bör begränsas till specifika människor och legitima undersökningar. Vi kommer att stå upp mot schablonmässiga eller alltför omfattande förfrågningar.

- ***Skydda alla användare***

  Att ha lagar som ger människor olika skydd beroende på var de bor eller vilket land de är medborgare i är föråldrat och avspeglar inte onlinetjänsternas globala natur. Vi kommer att fortsätta kämpa för en reformering av dessa lagar.

- ***Tillhandahålla betrodda tjänster***

  Myndigheter ska aldrig kunna installera bakdörrar i onlinetjänster eller äventyra infrastruktur för att få tag i användardata. Vi kommer att fortsätta skydda våra system och verka för att förändra lagar för att tydliggöra att den här typen av aktivitet är olaglig.

Vår insynsrapport finns på dropbox.com/transparency.

Sekretesscertifieringar, intyg och regelefterlevnad

Varje dag anförtror personer och organisationer Dropbox med sina viktigaste arbetsfiler. Därför är det vårt ansvar att skydda filerna och hålla dem privata. Vårt engagemang för din sekretess ligger till grund för varje beslut vi fattar.

ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud och ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management.

Dropbox Business var en av de första stora leverantörerna av molntjänster som nådde en certifiering med ISO/IEC 27018 och ISO/IEC 27701.

ISO/IEC 27018 är en global standard för sekretess och dataskydd i molnet och publicerades i augusti 2014 för att specifikt hantera användarsekretess och dataskydd.

ISO/IEC 27701 är den första certifierbara globala standarden för hantering av sekretessinformation och publicerades 2019 för att tillhandahålla en ram för att utvidga systemet för informationssäkerhetshantering (ISMS) från ISO/IEC 27001 till ett system för hantering av sekretessinformation (PIMS) genom att inkludera datasekretessfrågor.

Standarden innehåller många krav angående hur Dropbox ska och inte ska använda din organisations information:

- ***Din organisation kontrollerar era data***

  Vi använder bara den personliga information ni ger oss för att erbjuda de tjänster ni registrerat er för. Ni kan lägga till, ändra eller ta bort data från Paper-dokument och Dropbox närhelst ni behöver.

- ***Vi är transparenta med avseende på era data***

  Vi är transparenta angående var era data förvaras på våra servrar. Vi låter er också veta vilka våra betrodda partner är. Vi berättar vad som händer när ni avslutar ett konto eller tar bort en fil eller ett Paper-dokument. Slutligen berättar vi om några av dessa saker förändras.

- ***Era data är säkra och skyddade***

  ISO/IEC 27018 och ISO/IEC 27701 utformades som förbättringar och tillägg till ISO/IEC 27001, en av världens mest accepterade informationssäkerhetsstandarder. Vi fick förnyad ISO/IEC 27001-certifiering i oktober 2021.

- ***Våra rutiner granskas regelbundet***

  Som en del av vår efterlevnad av ISO/IEC 27018, ISO/IEC 27701 och ISO/IEC 27001 genomgår vi årliga granskningar av en oberoende tredje part för att upprätthålla dessa certifieringar. Du kan om alla våra ISO-certifikat här.

Dataöverföringar

När Dropbox för över data från Europeiska unionen, Europeiska ekonomiska samarbetsområdet, Storbritannien och Schweiz, förlitar vi oss på en rad olika rättsliga mekanismer, som till exempel avtal med våra kunder och dotterbolag, standardavtalsklausuler och Europeiska kommissionens lämplighetsbeslut om vissa länder, i tillämpliga fall.

Dropbox följer Privacy Shield-ramverken mellan EU–USA och Schweiz–USA som formuleras av det amerikanska handelsdepartementet angående insamling, användning och lagring av personuppgifter som överförs från EU, Europeiska ekonomiska samarbetsområdet, Storbritannien, Schweiz till USA, även om

Dropbox inte förlitar sig på Privacy Shield-ramverken mellan EU–USA och Schweiz–USA som rättslig grund för överföring av personuppgifter. Dropbox har försäkrat handelsdepartementet att företaget följer Privacy Shield-principerna med avseende på sådana uppgifter. Du kan också läsa mer om Privacy Shield på https://www.privacyshield.gov.

Klagomål och dispyter relaterade till vår efterlevnad av Privacy Shield undersöks och löses genom JAMS, en oberoende tredje part. För mer information, läs vår sekretesspolicy (dropbox.com/privacy).

EU:s allmänna dataskyddsförordningen (GDPR)

Den allmänna dataskyddsförordningen (GDPR) är en EU-förordning från 2018 som fastställer ett nytt omfattande ramverk för hantering och skydd av personuppgifter.

Dropbox värnar om säkerheten och skyddet av våra användares data i enlighet med lagliga krav och bästa praxis som ständigt beaktas. I linje med vårt engagemang för våra användare har vi arbetat hårt för att se till att Dropbox efterlever kraven i GDPR, inklusive att utse ett dataskyddsombud, att förändra vårt integritetsprogram för att säkerställa att användare kan utöva sina rättigheter i egenskap av registrerade personer, att dokumentera våra databearbetningsaktiviteter och att stärka våra interna processer i händelse av en säkerhetsöverträdelse. Vi gör hela tiden justeringar för att se till att vår process och praxis uppfyller eller överskrider specifika krav i de nya reglerna, i takt med att vi kontinuerligt får ytterligare vägledning från dataskyddsmyndigheter.

EU:s uppförandekod för molntjänster

EU:s uppförandekod för molntjänster (EU Cloud Code of Conduct) är ett frivilligt instrument som gör det möjligt för en molntjänstleverantör som Dropbox att uppvisa vårt engagemang för GDPR-efterlevnad. Dropbox Business, som består av Standard-, Advanced-, Enterprise- och Education-abonnemang för team, har förklarats följa EU:s uppförandekod för molntjänster och fått efterlevnadsmärket ”Nivå 2”, vilket innebär att dessa tjänster har implementerat tekniska, organisatoriska och avtalsmässiga åtgärder i linje med kraven i koden. Mer information om EU:s uppförandekod för molntjänster och Dropbox efterlevnad av koden finns på kodens officiella webbplats.

För mer information om vår policy och vårt arbete med sekretess ska du läsa Dropbox-informationssammanställningen om sekretess och dataskydd.

Efterlevnad

Det finns många olika regelverksrelaterade och branschspecifika krav för säkerhet och sekretess som din organisation kan behöva efterleva. Vårt sätt är att kombinera de mest erkända standarderna med efterlevnadsåtgärder riktade mot de specifika behoven för våra kunders företag eller branscher.

ISO

Internationella standardiseringsorganisationen (ISO) har utvecklat en serie standarder i världsklass för säkerhet i fråga om information och samhället. De finns till för att hjälpa organisationer att ta fram tillförlitliga och innovativa produkter och tjänster. Dropbox har certifierat datacenter, system, applikationer, personal och processer genom en serie revisioner utförda av det oberoende och fristående företaget EY CertifyPoint i Nederländerna. Det upprätthåller sina ISO-ackrediteringar från Raad voor Accreditatie (det nederländska ackrediteringsrådet).

ISO/IEC 27001 (informationssäkerhet)

ISO/IEC 27001 är erkänt som världens främsta standard för informationssäkerhet (ISMS). Standarden utnyttjar också bästa praxis som beskrivs i ISO/IEC 27002. Eftersom vi vill behålla ditt förtroende bedriver vi hela tiden en ingående hantering av våra fysiska, tekniska och juridiska kontroller på Dropbox.

Visa ISO/IEC 27001-certifikatet för Dropbox Business och Dropbox Education.

ISO/IEC 27017 (molnsäkerhet)

ISO/IEC 27017 är en internationell standard för molnsäkerhet. Den ger riktlinjer för säkerhetskontroller i fråga om tillhandahållande och användning av molntjänster. I vår guide om delat ansvar förklaras flera av kraven för säkerhet, sekretess och efterlevnad som Dropbox och våra kunder kan lösa tillsammans.

Visa ISO/IEC 27017-certifikatet för Dropbox Business och Dropbox Education

ISO/IEC 27018 (molnsekretess och dataskydd)

ISO/IEC 27018 är en internationell standard för sekretess och dataskydd som gäller för molntjänstleverantörer som Dropbox som hanterar personuppgifter å sina kunders vägnar. Den blir en utgångspunkt för våra kunder vad gäller vanliga krav eller frågor beträffande föreskrifter och kontrakt.

Visa ISO/IEC 27018-certifikatet för Dropbox Business och Dropbox Education.

ISO/IEC 22301 (Verksamhetens kontinuitet)

ISO/IEC 22301 är en internationell standard för kontinuitetsplanering som hjälper organisationer att minska risken för störande händelser och hantera dem på ett lämpligt sätt med minsta möjliga skada om de skulle inträffa. Dropbox-systemet för verksamhetskontinuitet (BCMS) är en del av vår övergripande strategi för riskhantering för att skydda människor och verksamheter under kriser.

Visa ISO/IEC 22301-certifikatet för Dropbox Business och Dropbox Education.

ISO/IEC 27701 (hantering av sekretessinformation)

ISO 27701 är en internationell standard för hantering av sekretessinformation. Standarden ger ett ramverk för att förbättra och utöka systemet för informationssäkerhetshantering under ISO 27001 till ett system för hantering av sekretessinformation (PIMS). Dropbox Business och Dropbox Education har fått ett denna certifiering som personuppgiftsbiträde.

Visa ISO 27701-certifikatet för Dropbox Business och Dropbox Education.

SOC

SOC-rapporterna (Service Organization Controls), kända som SOC 1, SOC 2 och SOC 3 är ramverk som är framtagna av AICPA (American Institute of Certified Public Accountants) för att rapportera om interna kontroller som implementeras i en organisation. Dropbox har certifierat sina system, applikationer, medarbetare och processer i en serie revisioner med hjälp av den oberoende och utomstående revisionsfirman Ernst & Young LLP.

SOC 3 för säkerhet, konfidentialitet, integritet, tillgänglighet och sekretess

SOC 3-rapporten täcker alla fem principerna för betrodda tjänster: säkerhet, konfidentialitet, integritet, tillgänglighet och sekretess (TSP, avsnitt 100). Dropbox rapport om allmän användning är en administrativ sammanfattning av SOC 2-rapporten och innehåller den oberoende, utomstående granskarens omdöme om hur våra kontroller är utformade och fungerar.

Visa SOC 3-kontrollen för Dropbox Business och Dropbox Education.

SOC 2 för säkerhet, konfidentialitet, integritet, tillgänglighet och sekretess

SOC 2-rapporten ger kunderna en detaljerad nivå av kontrollbaserad försäkran eftersom den täcker alla fem principerna för betrodda tjänster: säkerhet, tillgänglighet, bearbetningsintegritet, konfidentialitet och sekretess (TSP, avsnitt 100). SOC 2-rapporten innehåller en detaljerad beskrivning av Dropbox-processerna och mer än 100 kontroller som vi använder för att skydda dina resurser. Utöver omdömet från vår oberoende, utomstående granskare om hur våra kontroller är utformade och fungerar innehåller rapporten granskarens testmetoder och resultaten för varje kontroll. Vår SOC 2-rapport (som ibland kallas SOC 2+) omfattar också en reviderad mappning av våra kontroller för ISO-standarderna som nämns ovan vilket ger våra kunder ytterligare transparens. SOC 2-kontrollen för Dropbox Business och Dropbox Education finns tillgänglig på begäran.

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

SOC 1-rapporten erbjuder särskilda försäkringar för kunder som bedömer att Dropbox Business eller Dropbox Education är ett nyckelelement i sina interna kontroller över program för ekonomisk rapportering (ICFR). Dessa särskilda försäkringar används främst för att kunderna ska efterleva Sarbanes-Oxley (SOX). Den oberoende utomstående granskningen utförs i enlighet med förklaringen i Standards for Attestation Engagements nr 18 (SSAE 18) och International Standard on Assurance Engagements nr 3402 (ISAE 3402). Dessa standarder har ersatt de tidigare standarderna Statement on Standards for Attestation Engagement No. 16 (SSAE16) och Statement on Auditing Standards nr 70 (SAS 70). SOC 1-kontrollen för Dropbox Business och Dropbox Education finns tillgänglig på begäran.

CSA

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

CSA STAR är ett kostnadsfritt, offentligt register som erbjuder ett program för säkerhetsförsäkran i fråga om molntjänster. Det hjälper användare att bedöma säkerhetstillståndet hos molnleverantörer som de använder eller överväger att börja använda.

Dropbox Business och Dropbox Education har fått både CSA STAR Level 2-certifiering och Level 2-bekräftelse. CSA STAR nivå 2 kräver en oberoende tredjepartsutvärdering av våra säkerhetskontroller som genomförts av EY CertifyPoint (för certifiering) och Ernst & Young LLP (för attestering) utifrån kraven i ISO/IEC 27001, SOC 2 Trust Service Criteria samt CSA Cloud Controls Matrix (CCM) v4.0.2.

Visa vårt certifiering och bekräftelse för CSA STAR Level 2 på CSA-webbplatsen.

HIPAA/HITECH

Dropbox undertecknar Business Associate Agreements (BaaS) med Dropbox-företags- eller Dropbox Education-kunder som behöver dem för att efterleva HIPAA (Health Insurance Portability and Accountability Act) och Health Information Technology for Economic and Clinical Health Act (HITECH). SeDropbox och HIPAA/HITECH för mer information.

Dropbox erbjuder en tredjparts försäkransrapport som utvärderar våra kontroller för säkerhet, sekretess och intrångsavisering under HIPAA/HITECH, samt en kartläggning över våra interna processer och rekommendationer för kunder som vill uppfylla säkerhets- och sekretesskraven enligt HIPAA/HITECH med Dropbox Business eller Dropbox Education.

Kunder som vill begära ut dessa dokument eller få mer information om köp av Dropbox Business eller Dropbox Education kan kontakta vårt försäljningsteam. Om du är teamadministratör för Dropbox Business eller Dropbox Education kan du skriva under ett BAA elektroniskt från sidan Konto i adminkonsolen.

Observera att möjligheten att underteckna ett elektroniskt BAA via adminkonsolen endast finns för USAbaserade kunder.

NIST 800-171

Amerikanska National Institute of Standards and Technology (NIST) främjar och underhåller standarder och riktlinjer för att skydda informationssystem. NIST Special Publication (SP) 800171 Revision 2(R2) ger riktlinjer för att skydda Controlled Unclassified Information (CUI) i icke-federala informationssystem och hos organisationer. Varje enhet som hanterar eller lagrar amerikansk statlig CUI, såsom forskningsinstitutioner och utbildningssektorn, bör följa NIST SP 800-171 R2. Dropboxs CUI-system, processer och kontroller validerades av en oberoende tredjepartsrevisor, Ernst & Young LLP.

NIST SP 800-171 R2-rapporten för Dropbox Business och Dropbox Education finns tillgänglig på begäran via vårt säljteam eller (för befintliga Dropbox-företagskunder) supporten.

Observera att Dropbox Paper inte ingår i NIST SP 800-171 R2-rapportens omfattning.

FERPA och COPPA (studenter och barn)

Med Dropbox Business och Dropbox Education kan kunderna använda tjänsterna i enlighet med de leverantörskyldigheter som stipuleras i den FERPA-lagen (Family Education Rights and Privacy Act). Utbildningsinstitutioner med elever under 13 års ålder kan också använda Dropbox Business och Dropbox Education i enlighet med COPPA (Children’s Online Privacy Protection Act), förutsatt att de godkänner specifika avtalsenliga villkor som kräver föräldrarnas medgivande för användningen av våra tjänster.

FDA 21 CFR Part 11

Title 21 i Code of Federal Regulations (CFR) reglerar livsmedel och läkemedel i USA för Food and Drug Administration (FDA), Drug Enforcement Administration och Office of National Drug Control Policy. Del 11 i Title 21 anger kriterierna enligt vilka FDA anser att elektroniska register och signaturer är tillförlitliga, pålitliga och i allmänhet likvärdiga med pappersregister och handskrivna signaturer som utförs på papper.

Se vår informationssammanställning om Dropbox och FDA 21 CFR Part 11 och hjälpcenterartikel för mer information om hur Dropbox kan underlätta ert efterlevnadsarbete med 21 CFR Part 11.

PCI DSS

Dropbox efterlever kraven som handlare för Payment Card Industry Data Security Standard (PCI DSS). Dropbox Business, Dropbox Education och Dropbox Paper är emellertid inte avsedda att behandla eller lagra kreditkorttransaktioner. PCI Attestation of Compliance (AoC) för vår handlarstatus finns tillgänglig på begäran.

Mer information om Dropbox-företags och Dropbox Education-efterlevnad finns på dropbox.com/business/trust/compliance.

Appar för Dropbox

DBX-plattformen består av ett stabilt ekosystem med utvecklare som bygger på vårt flexibla Application Programming Interface (API). Fler än 750 000 utvecklare har byggt applikationer och tjänster för produktivitet, samarbete, säkerhet, administration med mera.

Förbyggda komponenter

Väljaren, Spararen och Inbäddaren är färdiga webb- och mobilkomponenter som gör det lätt att komma åt Dropbox i tredjepartsappar och -webbplatser med bara några få rader kod.

- Chooser gör det möjligt att välja filer från Dropbox.
- Saver låter användarna spara filer direkt i Dropbox.
- Embedder låter användarna visa filer och mappar från Dropbox.

Auktoriseringen för dessa komponenter görs helt via Dropbox. Appar beviljas åtkomst till filer valda genom delade länkar från Dropbox eller kortlivade nerladdningslänkar. Dessa färdiga komponenter kan användas oberoende eller i samband med API:t, som beskrivs nedan.

Dropbox Business API-integreringar

Det offentliga Dropbox API:t ger tredjepartsutvecklare möjlighet att komma åt och interagera med Dropbox från deras appar. Det omfattar interaktioner med filer och metadata, delning och teamfunktioner.

Auktorisering

Dropbox använder OAuth, ett protokoll som är branschstandard för auktorisering, så att användarna kan ge appar olika typer av kontoåtkomst utan att avslöja sina kontouppgifter. Vi stöder OAuth 2.0 för auktorisering av API-förfrågningar. Förfrågningar verifieras genom Dropbox-webbplatsen eller mobilappen. Dropbox stöder OAuth bästa praxis, inklusive kortlivade åtkomsttokens och PKCE för distribuerade appar.

Användarbehörigheter

Appar som använder Dropbox-API:t kan byggas med följande nivå av åtkomst till innehållet i slutanvändarens Dropbox:

- ***Appmapp.***

  En dedikerad mapp som döps efter appen skapas i appmappen för en användares Dropbox. Appen får endast läs- och skrivåtkomst till mappen i fråga och användare kan tillhandahålla innehåll för appen genom att flytta filer till mappen. Dessutom kan appen begära åtkomst till filer/mappar via Väljaren eller Spararen.

- ***Hela Dropbox.***

  Appen får full åtkomst till alla filer och mappar i en användares Dropbox och kan även begära åtkomst till filer/mappar via Chooser eller Saver.

Program kan också begära specifika omfattningar som begränsar deras beteenden genom åtkomst till undergrupper av API-slutpunkter. Till exempel kan programmen begränsas till skrivskyddad åtkomst till filer – eller möjligheten att ladda upp innehåll, men inte att skapa delningar.

Teamåtkomst

Dropbox-företagsadministratörer kan ge applikationer behörighet till administrationsfunktioner som finns i teamets adminkonsol. Vilka åtgärder teamets länkade appar kan utföra begränsas genom omfattningar, som anger vilka teaminställningar appen kan läsa eller hantera.

Vanliga kombinationer av omfattningar inkluderar:

- ***Teaminformation***

  Skrivskyddad information om teamet och användning på hög nivå.

- ***Teamrevision***

  Skrivskyddad åtkomst till teaminfo och den detaljerade händelseloggen.

- ***Teammedlemmars filåtkomst***

  Möjligheten att utföra åtgärder för teamanvändares räkning, till exempel hantera deras filer och mappar.

- *Hantering av teammedlemmar*
  Lägga till och ta bort medlemmar till och från teamet.

Webbkrokar

Webbkrokar är ett sätt för webbappar att skaffa sig realtidsmeddelanden om förändringar i en användares Dropbox. När en URI registrerats för att ta emot webbkrokar skickas en HTTP-begäran till denna URI varje gång en förändring för någon av appanvändarna registrerats. Med Dropbox Business API kan webbkrokar också användas för att generera meddelanden om ändringar i teammedlemskapet. Många säkerhetsappar använder webbkrokar för att hjälpa administratörer spåra och hantera teamaktiviteter.

Tillägg

Appar kan registrera tilläggs-URI: er, så att åtgärder kan visas i menyerna ”Dela” och ”Öppna” i Dropbox-gränssnittet. Tilläggen gör att användare kan starta anpassade arbetsflöden från tredje part direkt från en fil i en Dropbox-yta. När en åtgärd utlöses omdirigerar Dropbox användare till den angivna URI:n och skickar en filidentifierare som kan användas med API:t för att utföra alla filoperationer. En app måste auktoriseras innan ett registrerat tillägg syns för användaren. Vi kan främja en utvald uppsättning tilläggsintegreringar i menyerna ”Dela” och ”Öppna”, även om dessa appar inte har tillgång till material innan användaren auktoriserar det.

Riktlinjer för Dropbox-utvecklare

Vi tillhandahåller ett antal riktlinjer och förfaranden för att hjälpa utvecklare att skapa API-appar som respekterar och skyddar användarnas sekretess samtidigt som de förbättrar deras Dropbox-upplevelse.

- *Appnycklar*
  För varje enskild app som en utvecklare kodar måste en unik appnyckel för Dropbox användas. Och om en app tillhandahåller tjänster eller programvaror som bäddar in DBX-plattformen så att andra utvecklare kan använda den, måste varje utvecklare även registrera en egen appnyckel för Dropbox.

- *Appåtkomst*
  Utvecklare informeras om att en app ska använda en så låg privilegierad åtkomst som möjligt. När en utvecklare skickar in en app för godkännande av produktionsstatus granskar vi den för att säkerställa att appen inte begär onödigt bred åtkomst baserad på den funktion den erbjuder.

- *Granskningsprocess för appar*

  - **Utvecklingsstatus**
    När en app för Dropbox-API skapas får den utvecklingsstatus. Appen fungerar på samma sätt som andra appar med produktionsstatus, förutom att den endast kan anslutas till upp till 500 Dropbox-användare. När en app ansluter till 50 Dropbox-användare har utvecklaren två veckor på sig att ansöka om och få ett godkännande om produktionsstatus innan appens möjlighet att ansluta till fler Dropbox-användare fryses.

  - **Produktionsstatus och godkännande**
    För att godkännas för produktionsstatus måste alla API-appar följa våra varumärkesutvecklingsriktlinjer för utvecklare, samt de allmänna villkoren som beskriver otillåtna sätt att använda DBX-plattformen. Dessa otillåtna sätt inkluderar följande: att främja överträdelser av immateriella rättigheter eller brott mot upphovsrätten, att skapa fildelningsnätverk, samt att ladda ner innehåll olagligt. Utvecklare uppmanas först att ange ytterligare information om appens funktionalitet och hur den använder Dropbox API innan de skickar in appen för granskning. När appen godkänts för produktionsstatus kan ett obegränsat antal användare ansluta till appen.

Teamappsadministration

I teamadministrationskonsolen kan administratörer av Dropbox-företagsteam hantera de länkade apparna och integreringarna för sitt team.

API-partnerskap

Dropbox har arbetat nära företagets teknikpartner för att göra det möjligt för dem att utveckla integreringar med sina populära programvarupaket. Dessa partnerföretag bygger applikationer med Dropbox-API:er och har ett nära samarbete med Dropbox-arkitekter för att följa bästa praxis för säkerhet och användarupplevelse. Dessa inkluderar en mängd produktivitetsappar för slutanvändare, samt säkerhets- och hanteringsverktyg som:

- ***Säkerhetsinformation och händelsehantering (SIEM) och analys***

  Anslut Dropbox-företagskontot till SIEM och analysverktyg för att övervaka och utvärdera användarnas delning, inloggningsförsök, administrativa åtgärder med mera. Få åtkomst till och hantera medarbetarnas aktivitetsloggar och säkerhetsrelevanta data genom ert centrala logghanteringsverktyg.

- ***Dataförlustskydd (DLP)***

  Skanna filernas metadata och innehåll automatiskt för att utlösa meddelanden, rapportering och åtgärder när viktiga ändringar har gjorts i ditt Dropbox-företagskonto. Tillämpa företagets regler vid driftsättningen av Dropbox Business och få hjälp att följa efterlevnadskraven.

- ***eDiscovery och arkiveringsskyldighet***

  Hantera på rättstvister, skiljedomar och regelmässiga utredningar med data från ert Dropbox-företagskonto. Sök efter och samla relevant elektroniskt lagrad information och spara era data genom eDiscovery-processen, vilket sparar företaget tid och pengar.

- ***Digitalt kopieringsskydd (DRM)***

  Lägg till innehållsskydd från tredjepart för känsliga eller upphovsrättsskyddade data som lagras på medarbetarnas konton. Få åtkomst till kraftfulla DRM-funktioner, inklusive kryptering på klientsidan, vattenstämplar, revisionsspårning, återkallande av åtkomst och blockering av användare/enheter.

- ***Dataöverflyttning och säkerhetskopiering på plats***

  För över data till Dropbox från befintliga servrar eller andra molnbaserade lösningar och spara tid, pengar och arbete. Automatisera säkerhetskopieringar från ert Dropbox-företagskonto till lokala servrar.

- ***Autentisering och samlad inloggning (SSO)***

  Automatisera etableringen och borttagningen av användare och påskynda processen för att registrera nya användare. Effektivisera hanteringen och öka säkerheten genom att integrera Dropbox Business med ett befintligt identitetssystem.

- ***Anpassade arbetsflöden***

  Skapa interna appar som integrerar Dropbox med befintliga företagsprocesser för att förbättra interna arbetsflöden.

På sidan Dropbox-appintegreringar finns en lista över dessa teknikpartnerföretag. Slutanvändare kan ta del av utvalda första- och tredjepartsappar och -integreringar i App Center.

Dropbox-integreringar

Vi har också samarbetat med några av våra främsta teknikpartner för att skapa integreringar som marknadsförs på Dropbox-ytor. Dessa djupare integreringar utvecklas av Dropbox och partnern i samarbete. Här ingår:

Dropbox-tillägg

Med de här integreringarna kan du använda olika typer av apptillägg för att utföra åtgärder sömlöst, som att publicera en video, lägga till filer i e-post och chatt, skicka en fil för e-signatur och mycket mer, direkt från Dropbox. Dessa applikationer byggs av partnern, medan Dropbox gör det lättare att upptäcka utvalda tilläggspartner via menyn ”Öppna med” och ”Dela med”.

Slack, Zoom och Trello

Dessa integreringar byggs av Dropbox som första part, så att användare kan starta Slack-konversationer, starta möten och skapa uppgifter från Dropbox. Slutanvändare autentiseras för dessa verktyg via OAuth.

Microsoft Office för mobila enheter och webben

Med våra integrationer med Microsoft Office kan användare öppna Word-, Excel- och PowerPoint-filer som har sparats i deras Dropbox, utföra ändringar i Offices mobilappar eller webbappar och spara dessa ändringar direkt i Dropbox. Användare blir ombedda att ge åtkomst vid första försöket att öppna en Dropbox-fil i respektive Office-mobilapp eller -webbapp. Därefter kommer dessa länkningar att bibehållas.

Adobe Acrobat och Acrobat Reader

Våra integrationer med skrivbords- och mobilversionerna (Android och iOS) av dessa appar ger användare möjlighet att visa, redigera och dela PDF-filer som lagras i deras Dropbox-konton. Användare ombeds bevilja åtkomst vid första försöket att öppna en Dropbox-fil i varje app. Ändringar i PDF-filer sparas automatiskt i Dropbox.

Sammanfattning

Dropbox Business erbjuder användarvänliga verktyg så att team kan samarbeta effektivt, samtidigt som tjänsten tillhandahåller de säkerhetsåtgärder och efterlevnadscertifikat som verksamheter kräver. Vårt tillvägagångssätt består av flera skikt och kombinerar en robust backend-infrastruktur tillsammans med anpassningsbara policyer. Detta ger företag en kraftfull lösning som kan skräddarsys efter deras specifika behov. Om du vill ha mer information om Dropbox Business kan du kontakta oss på: sales@dropbox.com.