Dropbox Business

Responsabilità condivisa: lavoriamo insieme per mantenere i tuoi dati al sicuro

Dropbox lavora con i propri clienti in possesso di Dropbox Business e Dropbox Education per mantenere al sicuro i loro dati. Adottiamo misure esaustive per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni; formare i dipendenti sulle pratiche in ambito di sicurezza e privacy; costruire una cultura in cui conquistare la fiducia dei clienti è la massima priorità e sottoporre i nostri sistemi e le nostre pratiche ad analisi e controlli rigorosi di terze parti.

Mentre Dropbox è responsabile della sicurezza di ciascun aspetto del servizio che è sotto il nostro controllo, i clienti svolgono un ruolo fondamentale nel garantire che i propri team e i propri dati siano protetti e al sicuro. In qualità di amministratore di un team Dropbox Business o Education, hai la possibilità di configurare, utilizzare e monitorare il tuo account attraverso modalità che consentono di rispondere alle esigenze della tua organizzazione in termini di sicurezza, privacy e conformità.

Abbiamo redatto questa guida per aiutarti a comprendere il lavoro svolto da Dropbox al fine di mantenere al sicuro il tuo account e per scoprire che cosa puoi fare per mantenere la visibilità e il controllo sui dati del tuo team.

Le responsabilità di Dropbox

Garanzia di sicurezza all'interno della nostra architettura

Milioni di aziende in tutto il mondo fanno affidamento su di noi per proteggere i loro file più importanti. Per guadagnare la loro fiducia, dedichiamo tutto il nostro impegno nel realizzare prodotti sicuri su cui gli amministratori come te possono contare. Ecco alcuni dei modi in cui salvaguardiamo la nostra architettura e le nostre reti.

Architettura distribuita

L'architettura di Dropbox distribuisce diversi livelli di informazioni all'interno di più servizi. Non solo consente di velocizzare la sincronizzazione rendendola più affidabile, ma contribuisce a migliorare la sicurezza. La natura dell'architettura di Dropbox prevede che l'accesso a qualsiasi servizio individuale non possa essere utilizzato per ricreare file o documenti di Paper.

Reti sicure

La rete interna di Dropbox è separata con sistemi rigorosi dalla rete Internet pubblica. Il traffico Internet da e verso la rete di produzione è controllato attentamente tramite servizi proxy dedicati, i quali, a loro volta, sono protetti da rigide regole di firewall. L'accesso all'ambiente di produzione è riservato ai soli indirizzi IP autorizzati e richiede l'autenticazione a più fattori in tutti gli endpoint.

Crittografia dei dati degli utenti

I clienti in possesso di Dropbox Business ed Education interagiscono con i nostri sistemi attraverso le nostre applicazioni, mobile, desktop e web e attraverso le API. Garantiamo la protezione dei tuoi file e documenti di Paper, in transito o inattivi, indipendentemente dal tipo di applicazione che stai utilizzando.

Dati in transito

Per proteggere i dati in transito tra le app Dropbox e i suoi server, Dropbox utilizza la tecnologia Secure Sockets Layer (SSL)/Transport Layer Security (TLS) per il trasferimento dei dati, creando un tunnel sicuro protetto da crittografia Advanced Encryption Standard (AES) a 128 bit o superiore. I file in transito tra un client Dropbox (al momento desktop, mobile, API o web) e il servizio in hosting è crittografato mediante SSL/TLS. Allo stesso modo, i dati dei documenti

di Paper in transito tra un client Paper (al momento mobile, API o web) e il servizio in hosting sono crittografati mediante SSL/TLS. Per i punti finali che controlliamo (desktop e dispositivi mobili) e i browser più recenti, utilizziamo un solido algoritmo di cifratura e supportiamo la forward secrecy perfetta e il pinning dei certificati. Inoltre, sul Web contrassegniamo tutti i cookie di autenticazione come sicuri e abilitiamo la HTTP Strict Transport Security (HSTS) con includeSubDomains attivato.

Per impedire attacchi man-in-the-middle, l'autenticazione dei server di front-end di Dropbox avviene attraverso certificati pubblici mantenuti dal client. Prima del trasferimento di qualsiasi file si negozia una connessione criptata, che garantisce l'arrivo dei file ai server di front-end di Dropbox.

Dati archiviati

I file di Dropbox archiviati sono criptati con Advanced Encryption Standard (AES) a 256 bit. I file sono archiviati in più data center in blocchi di file distinti. Ogni blocco è frammentato e criptato utilizzando un codice robusto. Solo i blocchi modificati tra una revisione e l'altra vengono sincronizzati. Anche i documenti di Paper archiviati vengono crittografati con lo standard AES (Advanced Encryption Standard) a 256 bit. i documenti di Paper sono archiviati in più aree di disponibilità tramite sistemi di terze parti.

Garanzia di un servizio affidabile

Un sistema di archiviazione è utile solo se è affidabile. Per questo motivo, abbiamo sviluppato diversi livelli di ridondanza per Dropbox che impediscono la perdita di dati e assicurano la loro disponibilità. Le copie ridondanti dei metadati sono distribuite su dispositivi indipendenti all'interno di un data center con almeno un modello di disponibilità N+2. Vengono eseguiti backup incrementali dei metadati con cadenza oraria e backup completi ogni tre giorni. I metadati vengono archiviati su server ospitati e gestiti da Dropbox. L'archiviazione dei blocchi di file di Dropbox utilizza sistemi che includono provider in house e di terze parti progettati per offrire una durabilità dei dati del 99,999999999%.

Nella rara eventualità di un'interruzione di servizio, gli utenti di Dropbox avranno comunque accesso alle più recenti copie sincronizzate dei propri file nella cartella locale di Dropbox presente sui computer associati. Le copie dei file sincronizzati nella cartella del client desktop/locale di Dropbox saranno accessibili da un hard disk dell'utente durante i periodi di inattività, le interruzioni di servizio o in modalità offline.

In modo simile, le copie ridondanti dei dati dei documenti di Paper sono distribuite su dispositivi indipendenti all'interno di un data center con un modello di disponibilità N+1. Vengono inoltre eseguiti con cadenza giornaliera backup completi dei dati dei documenti di Paper. L'archiviazione dei documenti di Paper di Dropbox utilizza sistemi di terze parti progettati per offrire una durabilità dei dati annuali del 99,9999999999%. Nella rara eventualità di un'interruzione di servizio, gli utenti avranno comunque accesso alle copie sincronizzate più recenti dei propri documenti di Paper in modalità "offline" nell'applicazione mobile.

Limitazione dell'accesso dei dipendenti ai sistemi backend

Diamo per scontato il fatto che quando un cliente in possesso di Dropbox Business, Enterprise o Education come te, archivia i propri file con Dropbox, si aspetta da parte nostra una gestione responsabile di questi ultimi. In quanto parte di questa responsabilità, ci assicuriamo che l'accesso dei dipendenti di Dropbox ai nostri sistemi interni venga sottoposto a rigorosi controlli. Per cominciare, l'accesso tra la nostra rete aziendale e quella di produzione è limitato a utenti selezionati. Ad esempio, l'accesso alla rete di produzione è basato sulla chiave SSH e limitato ai team di tecnici che necessitano di accedervi in quanto rientra nelle loro mansioni. La configurazione dei firewall viene sottoposta a severi controlli ed è limitata a un numero ridotto di amministratori. L'accesso ad altre risorse, compresi data center, utilità per la configurazione di server, server di produzione e utilità per lo sviluppo di codice sorgente, viene accordato dietro esplicita approvazione da parte degli opportuni responsabili. I responsabili registrano le richieste, le motivazioni e le approvazioni relative agli accessi, i quali vengono concessi da individui competenti.

Garanzia della consapevolezza dei dipendenti in ambito di sicurezza e privacy

Parte della garanzia di un servizio sicuro consiste nell'accertarsi che le persone che lavorano in Dropbox comprendano in che modo essere consapevoli della propria sicurezza e riconoscere attività sospette. A questo proposito, ai dipendenti di Dropbox viene richiesta la conoscenza delle norme di sicurezza prima ancora di ottenere l'autorizzazione ad accedere ai sistemi. Inoltre, i dipendenti partecipano a corsi di formazione obbligatori sulla sicurezza e sulla privacy per i nuovi assunti, alla certificazione annuale e a una sensibilizzazione continua su tali temi mediante e-mail informative, conferenze, presentazioni e risorse disponibili sulla nostra intranet.

Convalida delle nostre pratiche

Per essere certi che le nostre pratiche di sicurezza funzionino al meglio, chiediamo a terze parti di assicurarne l'efficienza. Specialisti eseguono penetrazioni periodiche e test di vulnerabilità sugli ambienti aziendali e di produzione di Dropbox. Alle problematiche identificate viene data massima priorità e conseguente risoluzione da parte del nostro team di ingegneri. Inoltre, revisori esterni valutano le nostre pratiche in materia di sicurezza facendo riferimento agli standard di settore. Per aiutarti a comprendere meglio e valutare le nostre pratiche, produciamo il nostro rapporto SOC 3, e i certificati ISO 27001, 27017, 27018, e 22301 disponibili online. Puoi inoltre richiedere il nostro rapporto SOC 2, il rapporto di valutazione requisiti HIPAA, il rapporto e la valutazione BSI C5 (disponibili in inglese e tedesco) e il risultato dei test di penetrazione previo accordo di non divulgazione (sotto NDA).

Comunicazione delle problematiche al cliente

Stato del servizio

Dropbox rende disponibile un sito di terze parti che comunica ai clienti lo stato del nostro servizio a Dropbox Business ed Education. In quanto cliente attuale, puoi visitare in qualsiasi momento status.dropbox.com per visualizzare lo stato corrente del sito, oltre a interruzioni di servizio e interventi di manutenzione precedenti.

Notifica delle violazioni

Nell'eventualità di una violazione dei dati, riceverai una notifica da Dropbox, come previsto dalla legislazione applicabile. Disponiamo di politiche e procedure di reazione in caso di incidenti, incluso il processo di notifica di una violazione, che ci consente di inviare, se necessario, una notifica ai clienti interessati. In caso tu abbia siglato un accordo HIPAA o un accordo europeo sul trattamento dei dati personali, riceverai notifiche come indicato nel dettaglio nei summenzionati accordi.

Tutti gli strumenti necessari per la tua sicurezza

Il nostro obiettivo è quello di fornire a te e agli altri amministratori in possesso di Dropbox Business ed Education gli strumenti necessari per prendere decisioni responsabili e informate sulla sicurezza del tuo team. Per assisterti nella configurazione, nell'utilizzo e nel monitoraggio del tuo account in un modo in grado di soddisfare le tue esigenze, la tua Console amministratore è dotata di funzionalità di sicurezza che ti consentono di agire per conto del tuo team. Attraverso guide come questa, il nostro Whitepaper sulla sicurezza di Dropbox Business, il centro assistenza e il nostro team di supporto, forniamo informazioni per aiutarti a comprendere in che modo queste impostazioni possono aiutarti a configurare in maniera responsabile il tuo account.

Responsabilità del cliente

Scopri di più sulle nostre pratiche

Stabilire se Dropbox Business o Education sia la soluzione giusta per le esigenze della tua azienda è un processo importante. Ti invitiamo a dedicare parte del tuo tempo alla convalida delle nostre pratiche, così come faresti con qualsiasi altra applicazione. Per ottenere gli strumenti necessari, dovrai verificare le nostre pratiche di sicurezza, i nostri certificati ISO 27001, 27017, 27018 e 22301; il rapporto di garanzia SOC 3 e il questionario STAR Livello 1 e 2 CSA disponibile online. Inoltre, per aiutarti a prendere una decisione consapevole possiamo fornire accesso a documentazione aggiuntiva previa sottoscrizione di un accordo di riservatezza. Sono inclusi i nostri rapporti di audit SOC 1 e SOC 2, il rapporto sulle valutazioni C5 (disponibile in inglese e tedesco) e una mappatura delle nostre pratiche e raccomandazioni interne per i clienti che necessitano di soddisfare i requisiti previsti dalla normativa in materia di sicurezza dei dati, privacy e notifiche delle violazioni HIPAA/HITECH, nonché i riepiloghi dei nostri test di penetrazione di applicazione più recente. I nostri termini di servizio, le Norme di uso accettabile e il Contratto di collaborazione standard sono disponibili per la consultazione online e per assicurarti che Dropbox Business o Education siano la giusta soluzione per il tuo team.

Configurazione delle impostazioni di condivisione e Visualizzazione delle autorizzazioni

Dropbox Business ed Education ti consentono di avere la flessibilità di configurare il tuo account per supportare le tue esigenze in termini di sicurezza, collaborazione e privacy. Gli amministratori possono esaminare e modificare queste impostazioni attraverso la Console amministratore per rispecchiare il proprio ambiente di condivisione o contesto normativo. Ad esempio, gli account possono essere configurati in modo che cartelle, link e documenti di Paper non possano essere condivisi con persone esterne al tuo team. Quando i membri del team creano cartelle condivise per file Dropbox, hanno anche la possibilità di personalizzare le impostazioni delle cartelle e scegliere il livello di accesso appropriato, che consente di apportare modifiche o di sola lettura.

Potenziamento dell'autenticazione

Pratiche di autenticazione solide consentono al tuo team di mantenere al sicuro i propri dati. Gli amministratori dovrebbero esaminare le impostazioni di autenticazione disponibili e abilitare quelle che ritengono più adatte alla protezione dei propri account. Gli account Dropbox Business ed Education includono le seguenti opzioni:

Verifica in due fasi

Gli amministratori del team possono richiedere ai membri di utilizzare una verifica in due passaggi per effettuare l'accesso ai propri account. Questa funzionalità di sicurezza fortemente consigliata aggiunge un livello di protezione ulteriore agli account Dropbox degli utenti. Una volta abilitato, sarà necessario fornire un codice di sicurezza a sei cifre o una chiave di sicurezza oltre a una password all'accesso a Dropbox o quando si effettua l'associazione a un nuovo computer, telefono o tablet.

Accesso singolo (Single sign-on, SSO)

Se la tua azienda gestisce già i criteri e l'autenticazione tramite password con un provider di identità centrale, potresti scegliere di impostare il single sign-on per il tuo team di Dropbox Business o Education. Utilizzando il tuo provider SSO esistente, i membri del tuo team non dovranno memorizzare l'ennesima password. Cosa ancora più importante, l'accesso di autenticazione a Dropbox verrà gestito utilizzando gli stessi criteri password utilizzati per gli altri servizi all'interno della tua azienda.

Verifica periodica degli accessi

L'accesso all'account del tuo team dovrebbe evolversi in base ai cambiamenti relativi alle iscrizioni al tuo team, ai ruoli interni e ai dispositivi. Sarebbe opportuno verificare con frequenza periodica che l'accesso a dispositivi e applicazioni sia garantito solo a determinate persone per far sì che le tue informazioni non finiscano nelle mani sbagliate. Modificare o rimuovere l'accesso è semplicissimo grazie alla Console amministratore.

Membri del team

È possibile aggiungere, rimuovere e verificare facilmente i membri del team dalla Console amministrazione. Per garantire che l'accesso ai dati sensibili contenuti nel tuo account Dropbox Business o Education sia fornito solo a persone selezionate, consigliamo di esaminare spesso questo elenco. Potrai quindi rimuovere l'accesso quando un utente abbandona la tua organizzazione o non necessita più dell'accesso a causa di un cambio di mansione. Analogamente, puoi modificare i ruoli dei membri del team all'interno della Console amministratore in modo che ogni account utente disponga del livello di accesso più appropriato.

Dispositivi

Tu in prima persona e i membri del tuo team dovreste verificare con frequenza periodica i dispositivi associati al tuo account e rimuovere quelli inutilizzati o non autorizzati. Il collegamento a determinati dispositivi può essere annullato sia dai membri del team che dagli amministratori. Inoltre, avete la possibilità di eliminare da remoto il contenuto Dropbox dal vostro dispositivo durante l'annullamento del collegamento. L'annullamento del collegamento e l'eliminazione dei contenuti dai dispositivi consentono di mantenere i tuoi dati al sicuro in caso di furto o smarrimento o nel caso in cui un utente decida di lasciare il tuo team.

Applicazioni di terze parti

È disponibile un robusto ecosistema di applicazioni di terze parti che puoi collegare al tuo account Dropbox Business o Education per ottenere maggiori funzionalità. Le integrazioni che forniscono servizi come SIEM, DLP e gestione dell'identità possono essere strumenti efficaci utili a rafforzare le tue pratiche di sicurezza esistenti. Mentre queste applicazioni e integrazioni di terze parti possono rappresentare un completamento significativo al tuo account, è importante ricordare che non fanno parte dei nostri servizi inclusi. Di conseguenza, a questi ultimi non si applicano i Termini di utilizzo o il contratto commerciale di Dropbox, incluso il contratto di società in affari o il contratto sul trattamento dei dati personali che probabilmente avrai già sottoscritto con Dropbox. Le applicazioni potrebbero richiedere diversi livelli di accesso alle tue informazioni a seconda della rispettiva offerta di servizio. In qualità di amministratore, puoi collegare o rimuovere applicazioni del team, le cui modifiche si applicano all'intero account, e rimuovere singole applicazioni che i membri del team potrebbero aver aggiunto al proprio account. È possibile verificare e modificare le applicazioni di terze parti e il relativo accesso attraverso la console amministratore.

Monitoraggio di attività insolite

In qualità di amministratore del team, puoi visualizzare ed esportare rapporti che descrivono gli eventi, la condivisione, l'autenticazione del tuo team e le attività dell'amministratore. Gli amministratori dovrebbero verificare con frequenza periodica questi rapporti di attività per rilevare eventuali attività insolite e contribuire a garantire la sicurezza del tuo team. Inoltre, per potenziare le tue capacità puoi prendere in considerazione l'utilizzo di un SIEM o di un'altra integrazione di monitoraggio di terze parti.

Stabilire le esigenze di crittografia

Dropbox archivia per impostazione predefinita una copia locale dei tuoi file sul tuo computer per accertarsi di mettere a tua disposizione i file necessari. Le copie locali dei tuoi file sono coperte dalla stessa protezione prevista per tutti gli altri file all'interno del tuo computer. Per garantire la loro sicurezza, consigliamo di abilitare, quando possibile, la crittografia del disco sui tuoi dispositivi e richiedere una password robusta e unica per accedere al tuo laptop, al tuo telefono, ai tuoi tablet o a qualsiasi dispositivo che fornisce l'accesso al tuo account Dropbox. L'utilizzo di password robuste e sicure sui tuoi dispositivi proteggerà anche l'accesso ai documenti di Paper.

Dropbox protegge i file caricati sul tuo account dividendo automaticamente questi file in blocchi discreti e crittografando ciascun blocco utilizzando Advanced Encryption Standard (AES) a 256 bit. Allo stesso modo Dropbox protegge i documenti di Paper crittografandoli in archiviazione permanente utilizzando Advanced Encryption Standard (AES) a 256 bit. Dropbox gestisce le chiavi di crittografia per conto dei nostri clienti per garantire la facilità di questo processo agli utenti e per abilitare determinate funzionalità.

I membri in possesso di Dropbox Business ed Education possono scegliere anche di crittografare autonomamente i file prima di caricarli su Dropbox o attraverso un'integrazione di terze parti. Tuttavia, gli utenti che decidono di crittografare i dati prima di caricarli su Dropbox sono responsabili della gestione delle relative chiavi di crittografia. La decisione di crittografare i dati prima di caricarli su Dropbox potrebbe inoltre ridurre l'efficacia di alcune funzionalità.

I clienti interessati a ottenere maggiori informazioni sull'approccio di Dropbox al tema della sicurezza sono invitati a leggere il whitepaper sulla sicurezza, disponibile sul nostro sito Web: dropbox.com/business/trust. Per saperne di più su Dropbox Business o Education e per richiedere i rapporti di audit di terze parti dietro sottoscrizione di un accordo di riservatezza, contatta sales@dropbox.com.