SOPHOS

SOPHOS CENTRAL DEVICE ENCRYPTION – BRIEFING TECNICO

Panoramica

Questo documento offre una panoramica dei concetti tecnici di Sophos Central Device Encryption, inclusi il processo di crittografia, le protezioni utilizzate e come vengono gestite le chiavi. Il processo di crittografia varia a seconda che il dispositivo esegua Windows (BitLocker) o macOS (FileVault). Questo briefing non va inteso come documento sostitutivo della Guida per Amministratori di Central Device Encryption, che è disponibile su Sophos.it

Windows

Per crittografare un dispositivo Windows, occorre installare l'agent di Sophos Central Device Encryption sul computer e assegnare un criterio di crittografia in Sophos Central. Il dispositivo riceverà il criterio e avvierà il processo di crittografia.

Processo di crittografia - Windows

1. Il dispositivo riceve un criterio di crittografia da Sophos Central. Il criterio include le impostazioni necessarie per attivare la crittografia del dispositivo.
   Nota: se l'unità non è stata predisposta per BitLocker o se il TPM sul computer non è stato attivato, verrà chiesto all'utente di svolgere queste attività e riavviare il sistema. Nei sistemi più recenti, questo passaggio non è necessario.
2. Viene creata una chiave di ripristino per il dispositivo, che consiste in un ID univoco e una password di 48 cifre.
   Nota: il PIN, la password e la chiave di crittografia dell'utente non vengono mai inviati a Sophos Central. Solo la chiave di ripristino viene archiviata.
3. La chiave di ripristino viene offuscata e inviata in maniera sicura a Sophos Central tramite SSL. Sophos Central riceve la chiave di ripristino, la crittografa utilizzando una chiave ottenuta da un'appliance virtuale di gestione delle chiavi e la archivia in maniera sicura. Sophos Central invia un messaggio al dispositivo per confermare di aver ricevuto e archiviato la chiave.
4. Quando il dispositivo riceve da Sophos Central il messaggio di conferma dell'archiviazione della chiave, installa una protezione dell'accesso. Esistono quattro tipi diversi di protezione dell'accesso: TPM+PIN, TPM-only (solo TPM), Passphrase e USB key (chiave USB). Ne verrà installata solo una. La protezione che viene installata dipende da una combinazione di fattori legati al software e all'hardware. Leggi la sezione "Protezioni di BitLocker" per saperne di più.
5. Una volta completata l'installazione di una protezione dell'accesso, l'utente deve riavviare il dispositivo. Al riavvio del dispositivo, verrà chiesto all'utente di inserire il nuovo PIN o la nuova password di BitLocker, oppure di connettere la chiave USB, a seconda della protezione in uso.
   Nota: se viene utilizzato il metodo di autenticazione "TPM-only", l'utente non dovrà inserire un PIN o una password.
6. Una volta effettuata l'autenticazione nell'ambiente di preavvio ed eseguito l'accesso a Windows, avrà inizio la crittografia del disco. Gli utenti possono controllare lo stato del processo di crittografia aprendo Pannello di controllo -> Sistema e sicurezza -> Crittografia unità BitLocker. Il dispositivo riferisce a Sophos Central il proprio stato di crittografia, che è visibile nella console di Sophos Central Admin.

Protezioni di BitLocker

BitLocker prevede il concetto di "protezioni", ovvero metodi diversi per accedere (o "sbloccare") i dispositivi e i volumi crittografati.

Protezioni dell'accesso

Per il processo di avvio del dispositivo, Central Device Encryption utilizza le seguenti protezioni.

- TPM+PIN
- TPM-only
- Passphrase
- USB key

Tieni presente che Central Device Encryption abilita solo uno di questi metodi per ogni dispositivo.

Per determinare la protezione specifica da utilizzare, viene considerata una combinazione di fattori legati all'hardware e al software del dispositivo. Leggi la Guida per amministratori di Central Device Encryption per informazioni più dettagliate.

TPM+PIN

Questa protezione usa il Trusted Platform Module (TPM) più un PIN per l'autenticazione. L'utente deve inserire un PIN nell'ambiente di preavvio a ogni avvio del computer.

TPM-only

La protezione TPM-only sfrutta il chip TPM senza richiedere alcuna autenticazione tramite PIN. L'utente non deve inserire alcun codice nell'ambiente di preavvio.

Nota: se è abilitata l'opzione "Richiedi autenticazione all'avvio" del criterio di Central Device Encryption, la protezione TPM-only non verrà utilizzata.

Passphrase

La protezione Passphrase utilizza come autenticazione solo una passphrase ed è idonea per i computer che non hanno un TPM. L'utente deve inserire una passphrase nell'ambiente di preavvio a ogni avvio del computer. La protezione Passphrase richiede Windows 8 o versione successiva.

USB key

La protezione USB key richiede una chiave memorizzata su un dispositivo USB. In questo scenario, la chiave USB deve essere connessa al dispositivo a ogni riavvio.

Nota: la protezione USB key viene utilizzata da Central Device Encryption solo sui computer Windows 7.

Altre protezioni

Sophos CDE utilizza anche le protezioni di BitLocker indicate di seguito.

Chiave di ripristino

Prima di avviare la crittografia sul computer, Windows crea una chiave di ripristino. La chiave di ripristino consiste in un ID univoco e una password di 48 cifre. La chiave di ripristino viene archiviata in maniera sicura in Sophos Central e permette agli utenti di accedere di nuovo al computer se dovessero dimenticare il PIN o la password di BitLocker. L'amministratore fornisce all'utente la password di 48 cifre, che deve essere inserita nella pagina di preautenticazione di BitLocker.

Una volta visualizzata la password di una chiave di ripristino in Sophos Central, viene considerata scaduta, visto che è stata resa pubblica. Alla successiva sincronizzazione con Sophos Central, il dispositivo apprenderà che la chiave è scaduta, ne genererà una nuova e invierà la nuova chiave di ripristino a Sophos Central. Di conseguenza, dopo il primo accesso successivo, la chiave di ripristino utilizzata non sarà più valida.

Nota: Sophos Central non elimina le chiavi di ripristino scadute. Le chiavi di ripristino che sono state aggiornate possono essere individuate cercando per ID volume.

Sblocco automatico

Per tutti i volumi di dati fissi viene installata una protezione Sblocco automatico. Questo significa che, dopo che un utente effettua l'accesso a un dispositivo, i volumi di dati (non il volume del sistema operativo) risultano accessibili senza ulteriore interazione da parte dell'utente.

Nota: i volumi di dati fissi non verranno crittografati se il criterio di Central Device Encryption "Cifra solo volume di avvio" è abilitato

Nota: i volumi di dati rimovibili (ad es. le chiavi USB) non verranno crittografati da Central Device Encryption

macOS

Per crittografare un dispositivo macOS, occorre installare l'agent di Sophos Central Device Encryption sul computer e assegnare un criterio di crittografia in Sophos Central. Il dispositivo riceverà il criterio e avvierà il processo di crittografia.

Processo di crittografia - macOS

1. Il dispositivo riceve un criterio di crittografia da Sophos Central. Il criterio include le impostazioni necessarie per attivare la crittografia del dispositivo.
2. All'utente viene chiesto di avviare la crittografia sul dispositivo o di posticiparla a una data futura.
   Nota: la chiave di ripristino (detta anche chiave di recupero) di FileVault non può essere inviata a Sophos Central prima dell'avvio della crittografia del disco. Durante il processo di crittografia, assicurati che il dispositivo abbia una connessione Internet, per permettere l'invio della chiave di ripristino a Sophos Central.
3. La crittografia si esegue in background e l'utente riceve una notifica una volta completato il processo. La chiave di ripristino del dispositivo viene offuscata e inviata in maniera sicura a Sophos Central, tramite SSL. Sophos Central riceve la chiave di ripristino, la crittografa utilizzando una chiave ottenuta da un'appliance virtuale di gestione delle chiavi e la archivia in maniera sicura.
   Nota: la password dell'utente non viene mai inviata a Sophos Central. Solo la chiave di ripristino viene archiviata.

Archiviazione delle chiavi

Sophos Central archivia le chiavi di ripristino dei dispositivi, qualora l'utente dimenticasse il PIN o la password oppure non riuscisse più ad accedere al proprio dispositivo. Durante il processo di crittografia, un dispositivo genera una nuova chiave di ripristino e la invia tramite SSL a Sophos Central. Sophos Central riceve la chiave di ripristino, la crittografa utilizzando una chiave ottenuta da un'appliance virtuale di gestione delle chiavi e la archivia in maniera sicura.

È importante tenere presente che Sophos Central non raccoglie mai dati relativi al PIN o alla password di un utente. Viene memorizzata solo la chiave di ripristino.

Processo di ripristino

Il processo di ripristino permette agli utenti che hanno dimenticato le credenziali di accesso di poter accedere di nuovo al proprio dispositivo. Il ripristino può essere effettuato con l'aiuto di un amministratore oppure dal Sophos Self Service Portal.

Ripristino con l'assistenza di un amministratore

Gli amministratori possono trovare la chiave di ripristino di un dispositivo specifico nella console di Sophos Central Admin. Sono disponibili due metodi per individuare la chiave di ripristino:

1. Recupero della chiave di ripristino direttamente dalla console di Sophos Central. Questa opzione è particolarmente utile quando l'amministratore conosce il nome utente o il nome del computer. Dalla pagina Dispositivi o Computer in Sophos Central, basta individuare il computer interessato e aprire la sezione Device Encryption. Cliccando su "Recupera chiave di ripristino", viene visualizzata la Chiave di ripristino, ovvero una password di 48 cifre che l'utente può inserire nell'ambiente di preavvio di BitLocker per ottenere di nuovo accesso al suo dispositivo.
2. Ricerca di una chiave di ripristino utilizzando un ID chiave di ripristino o un ID volume. Questo metodo serve a cercare manualmente una chiave di ripristino specifica. L'ID della chiave di ripristino viene visualizzato agli utenti nella schermata di autenticazione in fase di preavvio e la ricerca di questo ID permette a un amministratore di individuare la password di ripristino associata. Anche la ricerca in base all'ID volume può essere utile, se l'amministratore ha un elenco di dettagli del disco e ha bisogno di trovare la chiave di ripristino. Poiché le chiavi di ripristino non vengono mai eliminate da Sophos Central, per trovare una chiave di ripristino che potrebbe essere stata aggiornata basterà eseguire una ricerca manuale.
   Nota: una volta che un amministratore visualizza una chiave di ripristino, il dispositivo client riceverà il comando di creare una nuova chiave di ripristino e di condividerla con Sophos Central. Se il computer è off-line, genererà una nuova chiave di ripristino una volta tornato on-line.

Ripristino self-help per gli utenti

Il Self Service Portal di Sophos Central (https://www.sophos.com/ssp) è un portale disponibile per gli utenti che li aiuta a recuperare le chiavi di ripristino senza dover contattare gli amministratori IT o la helpdesk. È necessario configurare gli utenti in Sophos Central in modo che abbiano accesso al Self Service Portal. Vedi la Guida in linea di Sophos Central per saperne di più.

Una volta effettuato l'accesso al Self Service Portal di Sophos Central, l'utente troverà un elenco dei suoi dispositivi nella scheda "Device Encryption". Cliccando sul pulsante "Recupera" nella colonna Chiave di ripristino, verrà fornita la chiave di ripristino.

Condivisione sicura dei file

La funzionalità Condivisione sicura dei file permette agli utenti di crittografare i file di dimensioni massime di 50 MB e di condividerli con colleghi o destinatari esterni. Quando crittografa un file, l'utente deve specificare una password e il destinatario avrà bisogno di questa password per accedere al file. I file vengono crittografati con codifica AES a 256 bit.

Nota: attualmente la Condivisione sicura dei file è disponibile solo su Windows

Scopri di più su Device Encryption e su Sophos Endpoint Protection

2023-05-23 IT-WP (NP)

SOPHOS