SonicWall Email Encryption - Panoramica del flusso dei dati

Scambio sicuro di e-mail contenenti dati sensibili dei clienti o informazioni riservate.

Questo documento descrive il flusso dei dati e le misure di protezione delle informazioni personali (PII) e delle informazioni sanitarie protette (PHI) utilizzate da SonicWall Email Encryption, un servizio cloud aggiuntivo disponibile in abbonamento per le soluzioni SonicWall Email Security locali e in hosting. Nel caso descritto di seguito, un messaggio di posta elettronica proveniente da un utente SonicWall funge da esempio di client mittente. Oltre ad esaminare gli algoritmi di crittografia utilizzati dal servizio cloud e le procedure memorizzate che regolano il controllo degli accessi sul database crittografato, il testo spiega come vengono gestite le chiavi di cifratura dal servizio di crittografia nel cloud. Vengono inoltre descritte le procedure di mitigazione dei rischi e garanzia della qualità applicate da queste misure.

Per motivi di brevità abbiamo dato per scontate diverse opzioni di connessione e consegna, che tuttavia non sono l'unico modo in cui il servizio di crittografia nel cloud può gestire i dati. Questo servizio si è sviluppato nel corso di oltre 14 anni e include numerose opzioni di configurazione per soddisfare praticamente ogni possibile scenario.

Un flusso di messaggi protetto tra SonicWall Email Security e il servizio di crittografia nel cloud

SonicWall Email Encryption è un servizio ospitato sulla piattaforma cloud Amazon Web Services (AWS). Per garantire la totale sicurezza quando si lavora in questo ambiente è stato stipulato un contratto di società in affari (BAA) con Amazon.

Per l'intero ciclo di vita di un messaggio protetto, il payload del messaggio non risiede mai in forma non crittografata sul sistema. Il diagramma seguente illustra la possibile interazione tra un'appliance SonicWall Email Security e il servizio di crittografia nel cloud.

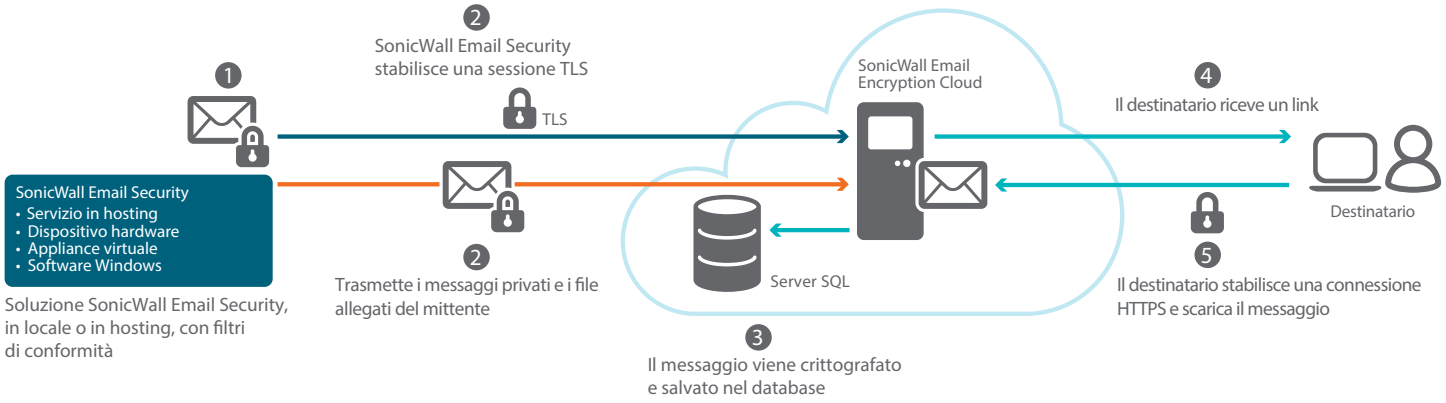

Figura 1. Flusso di messaggi tra SonicWall Email Security e il servizio di crittografia nel cloud

> "Per l'intero ciclo di vita di un messaggio protetto, il payload del messaggio non risiede mai in forma non crittografata sul sistema."

Il flusso sopra raffigurato comprende le seguenti tecnologie di crittografia:

1. Il mittente prepara e invia un messaggio contenente dati sensibili quali informazioni di carattere personale o sanitario. Il filtro di conformità SonicWall esamina ogni singolo messaggio e stabilisce se esso contiene informazioni PII o PHI da proteggere mediante la crittografia. In caso affermativo, SonicWall Email Security crea una sessione TLS protetta con il servizio di crittografia nel cloud.
2. I messaggi vengono trasmessi da SonicWall Email Security al servizio di crittografia nel cloud utilizzando la crittografia TLS. L'account del mittente, se non esiste ancora, può essere creato in modo dinamico. Il servizio elabora un'impronta digitale del messaggio al suo arrivo, la quale verrà utilizzata per valutarne l'integrità rispetto al messaggio trasmesso al destinatario.
3. I messaggi vengono cifrati dal servizio mediante crittografia AES a 256 bit e archiviati nel database in forma crittografata.
4. L'account e la casella di posta del destinatario vengono creati dinamicamente, nel caso non esistano ancora, dopodiché il destinatario riceve un'e-mail di notifica contenente un link e le istruzioni per registrarsi sul portale di crittografia nel cloud (SSL a 128 bit).
5. Con queste informazioni di registrazione il destinatario può accedere al messaggio e a tutti gli allegati tramite un server sicuro e, se lo desidera, può rispondere al mittente utilizzando la stessa interfaccia protetta. I messaggi di risposta vengono composti nel portale del servizio di crittografia nel cloud. Durante la trasmissione i messaggi vengono sempre salvati su archivi permanenti in forma crittografata.

Il servizio di crittografia nel cloud e gli algoritmi FIPS 140-2

La crittografia di questo servizio cloud si basa sull'interfaccia Microsoft CryptoAPI e utilizza le librerie convalidate FIPS 140-2 fornite da Microsoft con il sistema operativo Windows Server. Il servizio di crittografia è in grado di fornire funzioni in piena conformità allo standard FIPS 140-2 utilizzando Microsoft CryptoAPI. Per maggiori informazioni sui certificati FIPS Microsoft: https://technet.microsoft.com/en-us/library/cc750357.aspx.

Controllo degli accessi ai dati

Il servizio di crittografia nel cloud utilizza le migliori pratiche del settore per proteggere e controllare gli accessi al database. Mentre i dati inviati e ricevuti

dal servizio di crittografia sono sempre protetti da canali di crittografia forte, quelli presenti nel database vengono protetti mediante una combinazione di più misure: crittografia forte, controllo degli accessi a livello di campo e un sistema di verifica applicato al livello dei dati. Grazie a questa combinazione di misure, l'archivio dati viene definito un "database gestito".

Una delle caratteristiche di progettazione basilari del database consiste nel fatto che il livello dell'applicazione non ha accesso diretto ai record e ai campi. Questo impedisce che richieste non autorizzate possano accedere a dati non consentiti o violare l'integrità dell'archivio dati. L'unico modo per poter accedere al tracciamento e alla reportistica dei dati (e alle relative chiavi di crittografia) consiste nell'inviare una richiesta, da parte di un utente autenticato, al livello logico del sistema di sicurezza e dell'azienda. Ogni richiesta è convalidata sulla base delle autorizzazioni di accesso concesse all'utente che effettua la richiesta. Questi servizi vengono erogati a livello dei dati mediante un approccio al database noto come "Stored Procedures". L'accesso ai dati viene consentito solamente dopo che la richiesta è stata convalidata. Ciò vale sia per i mittenti che per i destinatari dei messaggi.

Un altro vantaggio di questa procedura risiede nell'efficacia della protezione contro gli attacchi SQL Injection e contro la manipolazione da parte di hacker che tentano di accedere a dati non di loro proprietà.

Gestione delle chiavi di crittografia

Il servizio di crittografia della posta elettronica nel cloud gestisce le chiavi di crittografia in automatico, sgravando gli utenti finali di questo compito. Il codice dell'applicazione del sistema genera automaticamente e archivia una chiave unica per crittografare e decrittografare ogni messaggio, nonché una per ciascun megabyte di dati dei file allegati. A titolo di esempio, un messaggio contenente un allegato da 5 MB avrà 6 chiavi uniche generate per proteggerne i dati. L'accesso alle chiavi di crittografia è limitato dalla funzione di controllo di accesso ai dati descritta nella sezione precedente, che impedisce accessi non autorizzati alle chiavi. Le chiavi archiviate vengono eliminate automaticamente appena scade il loro messaggio corrispondente, ovvero dopo 30 giorni per impostazione predefinita o anche prima, se il cliente lo desidera.

Best practice per la progettazione dell'applicazione, la codifica e la garanzia della qualità

Il servizio di crittografia nel cloud prevede un processo di controllo formale delle modifiche per garantire che venga messo in produzione solo software verificato. Le caratteristiche dei prodotti e le richieste di eliminazione dei difetti sono riesaminate da un apposito comitato (Request Review Board) composto da personale esperto di reparti come gestione e sviluppo dei prodotti, assicurazione della qualità e supporto clienti affinché se ne tenga conto nelle release programmate dei prodotti. Dopo l'approvazione, un team intersettoriale assicura che le caratteristiche di progettazione funzionale e i test di garanzia della qualità siano riconducibili a requisiti formalmente documentati.

I processi di gestione prodotti, progettazione e garanzia della qualità si svolgono in base a una metodologia prestabilita. Prima dell'implementazione vengono documentate e riesaminate le caratteristiche delle release di prodotto, la copertura dei casi di prova, e le istruzioni d'installazione. Le release vengono implementate dal team addetto alle operazioni dapprima su un server di prova in modo da testare sia la funzionalità del software che il processo d'installazione. Infine il prodotto viene autorizzato alla messa in produzione, fase in cui poi viene sottoposto a un test di approvazione interno.

Il servizio di crittografia nel cloud utilizza le migliori pratiche del settore per proteggere e controllare gli accessi al database. Mentre i dati inviati e ricevuti dal servizio di crittografia sono sempre protetti da canali di crittografia forte, quelli presenti nel database vengono protetti mediante una combinazione di più misure: crittografia forte, controllo degli accessi a livello di campo e un sistema di verifica applicato al livello dei dati. Grazie a questa combinazione di misure, l'archivio dati viene definito un "database gestito".

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com