

Sicurezza End-to-end per la posta e documenti allegati

Con un approfondimento sulla soluzione HPE SecureMail

Febbraio 2016



Un'analisi indipendente
realizzata da

Reportec

Executive Summary

L'email è una delle principali forme di comunicazione verso l'esterno e rappresenta uno dei principali vettori per i più nuovi tipi di attacco. Di conseguenza la protezione della posta elettronica va considerata una priorità critica da affrontare in modo strutturato e con soluzioni in grado di individuare e bloccare i molti e mutevoli tipi di attacco che diventano sempre più sofisticati.

Pressoché tutti i produttori di soluzioni di sicurezza informatica hanno sviluppato soluzioni per implementare un qualche tipo di protezione della posta elettronica ma le soluzioni, tra di loro, sono molto variegate e hanno specificità importanti. Inoltre, non tutti i produttori affrontano con le loro soluzioni di protezione lo stesso numero di tematiche.

HPE Security, la divisione dedicata alla sicurezza informatica all'interno della neo costituita HP Enterprise dopo la riorganizzazione del colosso statunitense, ha sviluppato un'interessante soluzione modulare denominata HP SecureMail che affronta i molteplici aspetti della protezione della posta elettronica non dimenticando di affrontare temi quali la sicurezza in ambito mobile e cloud.

Questo White paper esamina le caratteristiche e le specificità di tale soluzione.

Sommario

Executive Summary	1
Sommario	2
HPE Secure Mail	5
HPE SecureMail Mobile Edition	7
HPE SecureMail Application Edition	10
Componenti aggiuntive di HPE SecureMail	13
HPE SecureMail Cloud	14

Sicurezza End-to-end per la posta e documenti allegati

Con un approfondimento sulla soluzione HPE SecureMail

Anche se crescono nuove forme di comunicazione, come l'Instant Messaging, che dal consumer si espande nell'ambito business, la posta elettronica è innegabilmente un elemento critico nei processi aziendali. Di fatto, una pratica comune è quella di utilizzare la casella di posta elettronica come repository non solo delle corrispondenze importanti con colleghi, collaboratori, clienti e fornitori, ma anche di file e documenti che possono essere così recuperabili in qualsiasi momento, anche attraverso un dispositivo mobile.

Non è poi passato così tanto tempo da quando la posta elettronica rappresentava la killer application per la diffusione dei dispositivi mobili in azienda e lo sviluppo della Unified Communication e Collaboration non fa altro che confermarne l'utilità. Questo, però, insieme allo sviluppo della mobility non fa che fornire continui grattacapi ai responsabili dei sistemi informativi e della sicurezza in particolare.

La sicurezza dei dati sta diventando sempre più importante e oramai una priorità per i dipartimenti IT in alcuni settori economici come sanità e finanza, in particolare per quanto riguarda i dati privati dei clienti o assistiti. Non si tratta solo di regolamenti cui adeguarsi, perché piuttosto che le sanzioni per una mancata uniformità, i rischi maggiori in caso d'incidente sono i danni derivanti dalla perdita di fiducia da parte della clientela. Chi manterrebbe il conto in una banca dopo che questa non è riuscita a impedire che il vostro conto corrente venisse prosciugato? Le frodi informatiche non sempre arrivano a questi eccessi, ma ci sono molti dati, a cominciare dalle identità digitali, che sono "oro" per i cyber criminali e le imprese devono dimostrare di poter tutelare i beni e gli interessi dei propri clienti.

L'email è una delle principali forme di comunicazione verso l'esterno, cioè oltre il firewall. È quindi anche, se non adeguatamente protetta, la principale via per immettere nel sistema aziendale dei malware o, più in generale, dei kit software preposti a sferrare attacchi all'infrastruttura. Ma non basta entrare, bisogna anche uscire con i dati copiati ed è sempre l'email a rappresentare una delle vie d'uscita più vulnerabili e, come tale, utilizzata per portare le informazioni all'esterno dell'azienda.

Se guardiamo solo l'ultimo decennio, possiamo osservare come la posta elettronica sia stata utilizzata per realizzare varie tipologie di truffe o attacchi informatici. Vanno ricordati, per esempio, i "worm", cioè un particolare tipo di codice malware il cui scopo era di penetrare nel computer della vittima lasciando traccia del suo passaggio con un virus, praticamente impedendone l'uso. Per entrare utilizzava un messaggio email contenente un allegato infetto e, per diffondersi si "autoinviava" a tutti i contatti della vittima stessa. Il più famoso è "I Love You", il cui scopo era compiere il "giro del mondo" nel più breve tempo possibile.

Erano i tempi in cui gli hacker agivano per goliardia e per mettere alla prova le proprie capacità. Ma ben presto questi hanno cominciato a capire le potenzialità dei "giocattoli" che avevano per le mani e, ormai, molti hanno indossato un "cappello nero", quel "black hat" che identifica gli esperti informatici "cattivi", i quali hanno scelto di utilizzare le proprie capacità da hacker per commettere azioni illecite.

Ancora oggi evoluzioni di I Love You o semplicemente pezzi di codice che lo componevano sono utilizzati in alcune fasi degli attacchi mirati o di quelli persistenti (Advanced Persistent Threats).

Per il dipartimento che si occupa della sicurezza informatica la sfida consiste nel riuscire a implementare un sistema per la protezione della posta elettronica che sia facile da integrare nel sistema informativo e non penalizzi i processi di business per i quali l'email è ormai vitale, ma al tempo stesso che sia conforme alle leggi nazionali e internazionali e ai regolamenti industriali.

Una soluzione che appare "definitiva" è la crittografia che renderebbe illeggibile i dati e le informazioni contenute nelle mail, soprattutto se a essere cifrati fossero tanto i messaggi quanto i file allegati. Ma non è così semplice: gli approcci tradizionali non riescono a garantire la sicurezza che ci si aspetta quando il messaggio è codificato. I sistemi legacy, come S/MIME e PGP PKI, sono complessi, spesso troppo per l'IT aziendale. Inoltre non sono compatibili con piattaforme molto diffuse, quali Gmail, Yahoo e Android. Dall'altro lato, chiavi simmetriche utilizzate da sistemi proprietari, potrebbero generare un falso senso di sicurezza, perché, al costo di una complessa gestione delle chiavi, che dovranno essere memorizzate in un database a sua volta sicuro, potrebbero portare a un grave danno in dati "persi", allorquando una chiave venisse compromessa. Anche implementare sistemi di posta proprietari personalizzati rischia di aggiungere complessità, senza aumentare affidabilità e sicurezza.

Per ridurre il rischio, la risposta non può essere rinunciare alla posta elettronica, né restringerne l'utilizzo. Eppure, anche a causa di queste problematiche molte imprese continuano a basare molti processi critici su una documentazione cartacea, che non solo rallenta il go to market e le decisioni interne, ma impone costi di gestione elevati e ostacola l'efficientamento.

In realtà c'è un rischio anche maggiore, considerando l'attuale tendenza alla digitalizzazione di molti processi. Oggi il consumatore medio è abituato a gestire la propria vita personale e familiare con strumenti quali i dispositivi mobili, dove la posta elettronica è ancora molto impiegata ma sempre più soppiantata da altre forme di comunicazione. Per un'impresa rimanere ancorata al cartaceo può significare "l'estinzione". Si pensi a quanti portali offrono servizi come la prenotazione di visite specialistiche, viaggi, soggiorni alberghieri oppure preventivi per assicurazioni, prestiti bancari, piani tariffari, senza dimenticare l'e-commerce e immaginando, invece, quanti servizi ancora da inventare sorgeranno nei prossimi anni. Si potrà restare scettici sulla dematerializzazione nella Pubblica Amministrazione, ma non si può restare fuori dalla corsa alla digitalizzazione. Neanche se le proprie attività sono "limitate" a rapporti con altre imprese, perché il fenomeno è totale.

HPE Secure Mail

Hewlett Packard Enterprise ha sviluppato una soluzione di crittografia per la posta elettronica disponibile per desktop, dispositivi mobili e cloud. Scalabile fino a milioni di utenti, rende sicure e mantiene private le informazioni personali e sensibili, come dati relativi alla salute, agli orientamenti religiosi o politici e altro, permettendo a imprese e organizzazioni di intraprendere un percorso di transizione verso la dematerializzazione e un utilizzo massiccio della documentazione elettronica.

La caratteristica generale più importante di HPE SecureMail è l'unicità della soluzione: in pratica la stessa sia per i computer desktop sia per i dispositivi sia per gli ambienti cloud. La decifrazione può essere fatta dal pc, via Web o dal device mobile, tanto da un utente interno quanto da quello esterno e comprende scansione e filtraggio della posta in ingresso e in uscita.

La soluzione può essere installata sia on premise sia su cloud pubblici o privati, come pure in ambienti ibridi, come nel caso di un servizio come Office 365 di Microsoft. In particolare, sono supportati sistemi quali Outlook, Exchange, Blackberry Enterprise Server (BES) e altri sistemi di mobile device management (MDM). Questo è possibile anche perché HPE SecureMail mantiene una completa separazione tra la crittografia e il metodo di autenticazione, lasciando libertà di scelta per quest'ultimo, compresi Active Directory, LDAP o sistemi proprietari con propri portali.

Altresì rilevante è la centralità del dato nella protezione sia del messaggio sia degli attachment, che sono memorizzati su storage interni e non di terze parti. In altre parole tutto viene cifrato e protetto, in modo che quandanche la posta venisse intercettata, il contenuto criptato non sarebbe di alcun valore.

Fondamentale è il sistema per la gestione delle chiavi per le prestazioni e la qualità del servizio. Basato sullo standard sviluppato da HPE, l'HPE Identify-Based Encryption (IBE), il sistema di cifratura non richiede che sia memorizzata o gestita alcuna chiave di cifratura.

È un aspetto cruciale, perché impedisce al malintenzionato di acquisire tali chiavi e riduce drasticamente gli oneri di un amministratore.



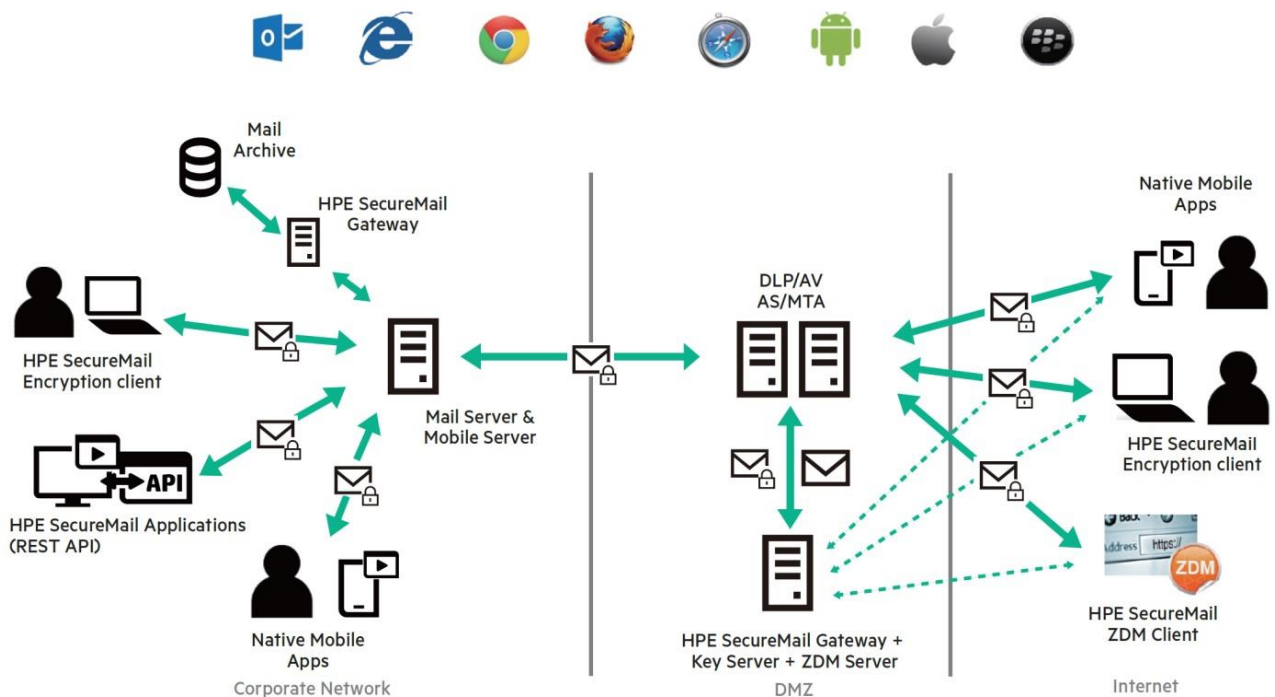
Sicurezza end-to-end per la posta e documenti allegati

Inoltre, questo permette che i messaggi possano essere inviati a qualsiasi destinatario senza che questi debba preventivamente effettuare alcun tipo di configurazione. È anche grazie a ciò che la soluzione presenta un'elevata scalabilità. Le grandi imprese possono dunque contare su ampi margini, ma non solo. La soluzione è anche integrabile nelle infrastrutture per la sicurezza della posta già in essere in azienda, quali i sistemi anti-virus, anti-spam o di content filtering, nonché quelli preposti all'archiviazione dei messaggi.

A proposito di quest'ultima operazione, va segnalato che HPE SecureMail fornisce più opzioni per un'archiviazione delle mail basata su policy con un controllo supervisionato. I messaggi vengono memorizzati come normali mail, ma, grazie alle capacità di indicizzazione, ricerca, visualizzazione, e identificazione dei dati interni alle mail stesse, HPE SecureMail semplifica le richieste durante eventuali audit, contenziosi e indagini.

Sempre grazie alle caratteristiche di HPE IBE, non occorrono le descrizioni aggiuntive delle chiavi, tipicamente richieste dai sistemi PKI e Open PGP.

Come prima accennato, HPE SecureMail supporta vari ambienti, come, per esempio Outlook, iOS, Android e BlackBerry. Sistemi diffusi, ciascuno dei quali ha una propria interfaccia e una altrettanto propria user experience. Uno dei rischi che si corrono con l'introduzione dei sistemi per la sicurezza che controllano il flusso della posta è che tale flusso venga modificato con l'introduzione di procedure che risultano ostiche agli utilizzatori. I tecnici di HPE si sono posti il problema, risolvendo, a loro modo di vedere, con un singolo "pulsante": per rendere sicura un'email, più precisamente, è sufficiente cliccare su "invio sicuro" e automaticamente il messaggio e i suoi allegati saranno crittografati. Dall'altro lato, il destinatario riceverà nella propria casella di posta in arrivo il messaggio, come una qualunque mail in "chiaro".



Schema di funzionamento di HPE SecureMail

HPE SecureMail Mobile Edition

HPE SecureMail Mobile Edition consente di leggere e inviare email codificate con HPE Security Voltage, la tecnologia che discende da Voltage Security, una tra le aziende più esperte di crittografia, che negli Stati Uniti conta tra i propri clienti sei dei primi otto gestori di sistemi per il pagamento, sette delle prime 10 banche, cui si aggiungono migliaia di aziende di medie dimensioni nel mondo, in vari settori, compresi sanità, banche e compagnie assicurative.

HPE SecureMail Mobile Edition funziona su dispositivi iOS, Android e Blackberry, che è possibile controllare attraverso policy di utilizzo e sicurezza. La soluzione, in questo modo estende la protezione centrata sui dati di HPE Security e rende conforme alle normative per la privacy e la security la gestione dei messaggi email e loro allegati, residenti o in transito sui dispositivi. Tutto questo, spiegano in HPE, senza modificare l'utilizzabilità del dispositivo da parte dell'utente finale. Più precisamente, è stata progettata una user experience nativa che integra la sicurezza con le capacità delle app e permette di applicare le policy di sicurezza in maniera non invasiva.

Caratteristiche principali

Basata sulla scalabile e consolidata tecnologia di HPE IBE (Identity-Based Encryption), HPE SecureMail Mobile Edition utilizza appunto una crittografia IBE a chiave pubblica con gli standard IETF RFC 509, RFC 5091, RFC 5408, RFC 5409 e IEEE 1363.3.

La soluzione estende la compliance ai dispositivi mobile, con una protezione end to end di messaggi email e attachment, mitigando il rischio di violazioni alla confidenzialità dei dati.

L'utilizzo di una tecnologia completamente "push", elimina il rischio di falle nelle procedure di sicurezza, anche grazie al formato HPE IBE, unico e consistente, per i messaggi, fornendo le stesse garanzie in qualsiasi ambito di utilizzo, interno o esterno all'azienda: i dati restano protetti per tutto il tempo in cui si trovano sul dispositivo mobile.

Un sistema di Mobile Device Management (MDM) completa e migliora la sicurezza e la compliance, senza entrare in conflitto con le policy. Questo è particolarmente utile in ambienti BYOD (Bring Your Own Device), laddove fosse necessario integrare soluzioni MDM, perché consente di operare il controllo a livello di dispositivo e di data center, proteggendo messaggi e allegati ovunque si trovino, anche quando sono in "mano" a clienti, partner e fornitori.

Principali funzionalità per gli utenti di dispositivi mobili	
Integrazione con le app e le funzionalità dei dispositivi	Le app di HPE SecureMail mobile convivono con le applicazioni per la posta già presenti sui dispositivi mobili, senza bisogno di creare apposite cartelle di posta in arrivo speciali né imponendo l'uso di un servizio webmail aggiuntivo. Anche la visualizzazione dei file attach avviene con le usuali applicazioni. Anche la lista dei contatti rimane la stessa sempre utilizzata.
Una User Experience nativa	L'interfaccia e la user experience si adatta a ciascuna delle piattaforme mobile supportate, preservando la familiarità con il dispositivo utilizzato da ognuno. Le app HPE SecureMail sono state disegnate per i diversi ambienti, in modo da sfruttarne le tecnologie native, come il multitasking, la rotazione dello schermo e permettere gli abituali approcci di utilizzo delle funzionalità. Per spedire un messaggio sicuro basterà attivare con un "tap" del polpastrello la funzione "Send Secure", invio sicuro.
Sistema di posta elettronica standard	Le email vengono gestite con il sistema di posta già in uso, sul quale comparirà il bottone "invio sicuro", ma per il resto sarà quello standard, comprese le piattaforme Web, quali Gmail, Hotmail o Yahoo Mail.
Accesso con le credenziali già in uso	Per l'autenticazione si possono utilizzare le credenziali aziendali già in uso, oppure si potrà scegliere di impiegare il servizio HPE Voltage per l'emissione di credenziali. L'accesso da remoto è consentito via LDAP, senza necessità di instaurare una VPN (Virtual Private Network).
Comunicare in maniera sicura con più imprese	Un'applicazione HPE SecureMail mobile può interfacciarsi con qualsiasi impresa disponga di HPE Security Voltage. La stessa app può essere utilizzata da mittenti e destinatari per più identità e account mail.
App Store standard	HPE SecureMail Mobile edition è disponibile sugli usuali app store (Apple Store, Google Play e Blackberry AppWorld. La configurazione è semplice e immediata.

Principali funzionalità per l'IT aziendale	
Gestione centralizzata basata su security policy granulari 1	Protezione e conformità alle normative e regolamenti vengono semplificate grazie a una soluzione di enforcement semplice che riduce il rischio di violazioni dei dati.
Gestione centralizzata basata su security policy granulari 2	La soluzione fornisce un esauriente e consistente sistema di policy control su messaggi di posta elettronica e attachment. Per esempio, a livello di messaggio e attachment è possibile definire se un utente può leggere il contenuto, rispondere al solo mittente o a tutti i destinatari, inoltrare la mail o modificarla. È anche possibile agire a livello di dominio, definendo a quali account di posta l'utente può inviare email sicure.
Implementazione e scalabilità globale	HPE SecureMail Mobile Edition impiega la gestione delle chiavi di HPE Security Voltage, che non richiede di gestire certificati o attributi aggiuntivi per ogni coppia di chiavi, riducendo notevolmente gli oneri amministrativi. A differenza di altre soluzioni, inoltre, non impone l'utilizzo di caselle di posta elettronica Web dedicate, anche qui evitando necessità di gestione aggiuntive. La distribuzione delle app HPE SecureMail Mobile Edition è quindi semplice e senza limiti di scalabilità.
Integrazione con le soluzioni di sicurezza e i server di posta	HPE SecureMail Mobile Edition si integra facilmente con i sistemi aziendali di sicurezza, per esempio per l'autenticazione e la Data Loss Prevention (DLP) o i sistemi di pulizia e gestione della posta elettronica, comprese le funzioni di ricerca e archiviazione e quelle gestite attraverso Mobile Device Management.
Integrazione nativa con la suite HPE SecureMail Suite	Gli utenti possono operare indifferentemente con le soluzioni HPE SecureMail per desktop, gateway, applicazioni business e dispositivi mobili..
Supporto per BlackBerry Enterprise Server Push	La versione della app HPE Security Voltage per BlackBerry può essere distribuita ai dispositivi aziendali BlackBerry attraverso la piattaforma push BlackBerry Enterprise Server (BES), senza operazioni aggiuntive. Gli utilizzatori possono anche utilizzare il software BlackBerry per desktop e l'application loader, seguendo le procedure cui sono abituati per installare le applicazioni nel loro dispositivo BlackBerry

HPE SecureMail Application Edition

La protezione centralizzata dei dati fornita di HPE SecureMail può essere estesa ai dati strutturati e destrutturati presenti nei messaggi e gli attachment che vengono inviati, ricevuti e gestiti direttamente da applicazioni di business, portali o siti Web destinati a raccogliere o contenere informazioni riservate. Basti pensare ai dati di registrazione di un abbonato a qualsiasi servizio o ai form da compilare online per richiedere una visita medica o un preventivo per un'assicurazione. È il mondo delle applicazioni in cloud cui gli utenti di tutto il mondo si stanno abituando e verso il quale va estesa la protezione dei dati.

Questa estensione è attuata grazie ad HPE SecureMail Application Edition, che abilita una maggiore penetrazione in azienda dei processi di business automatizzati, proteggendo i dati che vengono gestiti direttamente dalle applicazioni, rendendo sicura la posta elettronica end to end interna e proveniente dal cloud.

Sempre più applicazioni generano, memorizzano e utilizzano email nel flusso legato ai processi di business. Email che contengono dati sensibili, come quelle che si scambiano gli individui, e che richiedono analoga protezione. Non a caso ci sono specifiche regolamentazioni che toccano questi temi (come HIPAA, HITECH, PCI e SOX). Ma ci sono anche comunicazioni interne che partono in automatico dalle applicazioni, per esempio, quando viene approvato un piano o confermato lo stanziamento di un budget per un progetto, l'applicativo manda agli interessati una comunicazione via mail contenente informazioni strategiche per l'azienda. Informazioni che è preferibile evitare possano essere diffuse all'esterno per errore.

Caratteristiche principali

- HPE SecureMail Application Edition protegge i messaggi di posta elettronica salvaguardando la riservatezza di fatture, estratti conto, approvazioni e altri messaggi parte di flussi di lavoro, sistemi di CRM o altre applicazioni, che possono contenere dati sensibili, comprese, per esempio, credenziali di accesso e altro ancora.
- La protezione è basata sul dato, per cui questo viene protetto continuamente ovunque "vada".
- La soluzione è compatibile con qualunque client, sia esso desktop, mobile o Web, e con tutti gli attuali browser disponibili per pc o dispositivo mobile.
- L'implementazione è anche facilitata da un'integrazione che non richiede alcuna modifica all'architettura di gestione della posta elettronica, né un re-instradamento delle email né l'utilizzo di SDK (Software Development Kit).
- Basata su HPE SecureMail, la soluzione è consolidata, sicura, scalabile e gestibile con bassi costi operativi.

Un'unica soluzione

Finora è stato necessario adottare approcci basati su un'applicazione esterna della crittografia o utilizzanti, al massimo, dei gateway TLS (Transport Layer Security) o SMTP (Simple Message Transport Protocol) sui quali

installare, non sempre facilmente, un sistema di cifratura e decifratura). Ciò non è più sufficiente, perché lascia "scoperto" il messaggio che viaggia internamente all'infrastruttura aziendale o che viene spedito da un'applicazione, tipicamente saltando i gateway. Analogamente, con questa architettura i dati contenuti nei messaggi sono vulnerabili finché questi non superano il gateway di uscita, cioè fintanto che restano sulle applicazioni, sui pc o sul server di posta. In pratica, le email sono a rischio finché non viene criptata e dopo che viene decifrata.

Sono situazioni di rischio che permangono anche finché si resta all'interno della propria rete, figuriamoci quando l'applicativo deve scambiare messaggi con l'esterno, magari un cliente o un fornitore. Evidentemente simili architetture non sono end to end, come è stata invece progettata HPE SecureMail.

HPE SecureMail Application Edition protegge i dati contenuti nel messaggio non appena questo viene spedito dall'applicazione, prima che passi dal backbone di posta, e per tutto il percorso fino alla destinazione. Un'architettura che assicura la compatibilità con tutte le normative su ricordate.

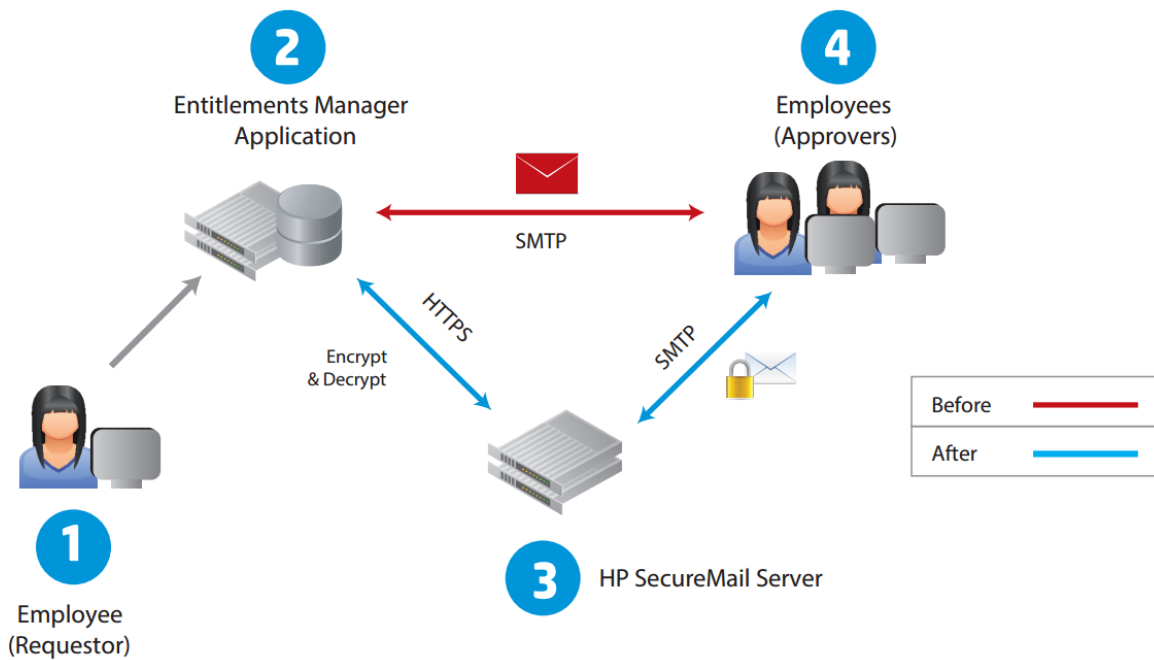
L'integrazione con le applicazioni

HPE SecureMail Application Edition fornisce due modalità per lo scambio sicuro dei messaggi tra le applicazioni: via servizio Web di tipo REST oppure tramite protocollo SMTP.

La prima possibilità si basa su un servizio REST semplice ed efficace, che consente l'interazione tra le applicazioni e HPE Identity-Based Encryption (IBE) attraverso HTTPS. Ciò avviene tramite un'interfaccia API che attiva la cifratura o la decifratura dei dati. Questa soluzione attua una protezione centrata sui dati, che sono quindi al sicuro sia durante la trasmissione sia nel momento in cui sono fermi e senza richiedere alcun intervento sul sistema di posta.

In alternativa si può utilizzare un gateway SMTP messo a disposizione da HPE SecureMail Application Edition, cui le applicazioni indirizzano i messaggi, che vengono così criptati o decriptati dal gateway stesso. In questo caso l'applicazione non viene modificata, perché non deve preoccuparsi della cifratura, però non si ha protezione end to end, come nel caso del Web service. In entrambi i casi, comunque, si minimizzano gli interventi necessari, la complessità e, in ultima analisi, i costi di amministrazione. L'API per l'integrazione via Web Service viene richiamata dall'applicazione attraverso qualsiasi linguaggio di programmazione, o quasi, tramite meccanismi standard ormai integrati nella grande maggioranza delle applicazioni.

L'utilizzo del gateway SMTP è consigliato, invece, per quelle applicazioni che non possono essere modificate o che già utilizzano il protocollo SMTP. A queste il gateway HPE SecureMail garantisce la protezione della mail dentro e fuori l'applicazione.



Un flusso di lavoro con un processo di approvazione basato su email che utilizza HPE SecureMail Application Edition

L'architettura di HPE SecureMail

HPE SecureMail Application Edition sfrutta l'infrastruttura di HPE SecureMail, che utilizza la consolidata tecnologia di crittografia di HPE Security Voltage, progettata per garantire elevata scalabilità a livello globale e semplicità di gestione. Altrettanto semplice è l'interfaccia utente che ricalca la familiarità dei client di posta elettronica.

Come accennato più volte e così com'è per il resto della suite HPE SecureMail, l'integrazione è quasi trasparente e si adatta all'ambiente preesistente per fornire una soluzione end to end, con il minor impatto possibile sui processi di business e sulle IT operation. I componenti server possono essere installati su una singola appliance, opportunamente "irrobustita" in termini di sicurezza ICT, oppure distribuiti per rispondere a eventuali esigenze di scalabilità e disponibilità.

La soluzione funziona anche senza alcun tipo di client, ma può altresì essere implementata in combinazione con client per desktop o dispositivi mobili.

Alla base la tecnologia IBE che consente di ottimizzare i costi amministrativi della crittografia anche del 60 o 80% secondo stime di HPE, soprattutto perché viene eliminata la necessità di gestire le chiavi, che vengono generate on demand. Quest'ultimo aspetto è ancora più importante sul fronte della sicurezza, in quanto annulla il rischio di perdere l'accesso ai dati e semplifica applicazioni di disaster recovery e di ricerca.

HPE SecureMail dispone di ampie funzioni per l'amministrazione, fornendo robusti sistemi per la gestione centralizzata, il logging e la reportistica. S'integra con i principali sistemi di autenticazione, aggiornamento e archiviazione.

Componenti aggiuntive di HPE SecureMail

L'architettura di HPE SecureMail si completa con una serie di componenti aggiuntive, compresi i client per i diversi dispositivi desktop o mobile o per le applicazioni. A queste, già illustrate in precedenza, si uniscono alcune componenti specifiche.

Invio diretto sicuro di documenti sensibili via mail

HPE SecureMail Statements Edition permette di spedire documentazione generata automaticamente dal sistema gestionale, quali per esempio fatture, estratti conto e altri attestati in formato elettronico, permettendo notevoli risparmi solo di stampa.

Indicizzazione e ricerca dei messaggi per Symantec Enterprise Vault

HPE SecureMail Archive Connector decifra automaticamente tutti i messaggi email quando devono essere archiviati con Symantec Enterprise Vault, permettendo di semplificare l'indicizzazione e la ricerca basata su testo. Questo senza bisogno di agire sul sistema di archiviazione, né di creare chiavi aggiuntive, come nel caso di alcune soluzioni alternative. Si ottiene, così, di poter mantenere la sicurezza dei dati e, al tempo stesso, di poterli utilizzare per vari scopi, dalla raccolta all'elaborazione, dalla revisione all'analisi.

eDiscovery Process

HPE SecureMail eDiscovery Accelerator fornisce una funzione per la decriptazione, controllata tramite policy, delle mail in una cartella di posta, facilitando l'indicizzazione e la ricerca dei messaggi. Con alcune soluzioni presenti sul mercato, c'è il rischio di non trovare un determinato messaggio perché cifrato, ma, soprattutto, si potrebbe determinare una difformità ad alcune normative. Con HPE SecureMail eDiscovery tutti i contenuti della posta criptata sono a disposizione di un supervisore autorizzato. Questo consente anche a un amministratore di implementare un eventuale workflow contemplando tutti i dati, anche quelli nei messaggi cifrati, pur mantenendo alto il livello di sicurezza.

Spedire e ricevere file di grandi dimensioni via mail

Quante volte si finisce con l'utilizzare servizi cloud consumer per trasferire file di grandi dimensioni? Uno dei problemi in azienda sono proprio le policy che impediscono ai server di posta di inviare file troppo pesanti.

HPE SecureMail Large Attachment Delivery consente di inviare e ricevere file con attachment di ogni dimensione. Mittente e destinatario non devono preoccuparsi di nulla: di fatto, quando il destinatario riceve il messaggio e cerca di aprire l'attachment, in realtà attiva un download. Questo evita i rischi legati a servizi gratuiti che non garantiscono la riservatezza delle informazioni. Inoltre, evitano le molte chiamate all'help desk, da parte di utenti alle prese con file di grandi dimensioni che non riescono a ricevere o spedire.

Crittografia di file e documenti

HPE SecureFile, applicando gli stessi principi fin qui espressi per messaggi e attachment, consente all'utilizzatore di codificare facilmente documenti e informazioni confidenziali (per esempio attraverso un

semplice bottone che si aggiunge nel menu di Microsoft Office o nelle opzioni accessibili tramite il tasto destro del mouse), garantendo però l'accesso al file tramite l'applicazione, in base a precise politiche di controllo.

Tra le caratteristiche di questo componente aggiuntivo di HPE SecureMail, la stretta integrazione con ambienti Microsoft quali Microsoft Windows, Active Directory, Exchange, e Office. Inoltre, l'integrazione con la rubrica di Outlook o Exchange, permette di gestire i permessi e definire chi può avere accesso al file criptato, chi può anche modificarlo e chi, per esempio, può anche estendere i privilegi a qualche altro utente.

Chiave hardware

HPE SecureMail supporta l'uso degli Hardware Security Module (HSM) di Thales nShield Connect. Con questi moduli cambia la configurazione di HPE Identity-Based Encryption (IBE), che genera le chiavi di sicurezza e quelle dell'utente all'interno del modulo di sicurezza blindato, cioè progettato per resistere alle manomissioni. Anche i diversi "distretti" di crittografia che è possibile definire vengono protetti nei moduli HSM.

Un ulteriore elemento di hardenizzazione è rappresentato dal supporto per Operator Card Set (OCS), che fornisce ulteriori livelli di sicurezza laddove si ipotizzino scenari incerti o remoti.

HPE SecureMail Cloud

Cifrare messaggi di posta dal computer in ufficio o da uno smartphone, distribuendoli attraverso portali, drive USB o altri sistemi di storage diventa facile con HPE SecureMail Cloud, che non richiede sforzi aggiuntivi da parte del destinatario.

Questo grazie a una soluzione cloud erogata in modalità Software as a Service (SaaS) che consente di proteggere email, file e documenti senza investire in infrastrutture on premise.

Caratteristiche principali

Cifrare email, file e documenti con la tecnologia di HPE SecureMail accessibile via cloud.

- I mittenti devono semplicemente "premere" il bottone invio sicuro sul sistema di posta, da pc o device mobile, mentre il destinatario non vede modificata la propria experience e non deve far altro che aprire il messaggio.
- I documenti crittografati sono a quel punto sicuri e distribuibili senza timore tramite portali, chiavette USB e vari storage di rete, senza bisogno di capire la crittografia.
- Un modulo software disponibile per il download permette l'accesso da un pc Windows per la crittografia dei documenti di Office.
- La soluzione è utilizzabile anche via smartphone, senza bisogno di definire uno nuovo account di posta né di definire un'apposita cartella di posta per i messaggi crittografati.

Le due edizioni

HPE SecureMail Cloud è disponibile in due versioni:

- **Standard Edition:** Una soluzione SaaS progettata per professionisti che hanno bisogno di una semplice ed efficace soluzione per la crittografia di messaggi e documenti, conforme alle leggi sulla privacy.
- **Enterprise Edition:** Una soluzione ibrida pensate per imprese di ogni dimensione che hanno bisogno di una customer experience personalizzata, con , per esempio, supporto multilingua, versione con il proprio brand e integrazione con le proprie infrastrutture di comunicazione, sicurezza, protezione degli endpoint, archiviazione, ricerca.

La versione Enterprise dispone di alcune caratteristiche esclusive, non comprese in quella standard, che consentono di aggiungere le funzionalità previste nella versione per l'on premise.

Personalizzazione dei district e federazione. Le organizzazioni che vogliono basare la crittografia su un loro "distretto", magari pensando di poter in futuro integrare on premise nel proprio data center la soluzione HPE SecureMail, possono attivare appunto l'opzione "district", quindi accedendo a una soluzione in cloud mono tenant, mentre normalmente è multi tenant. Il passaggio successivo è quello della federazione, che consente di interoperare facilmente con dei partner, anch'essi utilizzatori di HPE SecureMail.

Possibilità di personalizzare i colori e aggiungere il proprio logo nei messaggi email. È anche possibile personalizzare le email con messaggi di testo o, per esempio, le istruzioni per come aprire il messaggio.

Supporto multilingua, per aziende distribuite in più nazioni o per fornire istruzioni a destinatari internazionali o, ancora, per rispondere a esigenze di compliance.

Personalizzazione delle configurazioni e delle policy, per definire regole su, per esempio, come devono essere aperte le email, quali opzioni di risposta concedere, quali credenziali per l'autenticazione chiedere al destinatario. Per le personalizzazioni è disponibile un supporto da parte di HPE.

Integrazione con Active Directory locali o con LDAP, per consentire di utilizzare le propri directory interne per l'autenticazione. In questo caso, però, è necessario installare un HPE SecureMail anche on premise.

Integrazione con soluzioni di data loss prevention, magari già presenti in azienda e che fanno parte dal sistema di sicurezza e compliance. Sistemi di terze parti possono essere integrate utilizzando il sistema di scansione dei contenuti di HPE SecureMail e installando on premise una HPE SecureMail Gateway Appliance, che permette di utilizzare le policy definite nella soluzione DLP per crittografare i contenuti in cloud.

HPE SecureMail Cloud può automatizzare processi di accounting, come le fatturazioni, integrando le funzioni già disponibili on premise, quando occorre e attivando le sole licenze necessarie. Molto spesso, infatti, si tratta di operazioni periodiche. Per questo l'opzione sarà attivata periodicamente con un modello pay per use. Disponibili in cloud su richiesta anche il plug-in per Symantec Enterprise Vault e il modulo eDiscovery.



REPORTEC opera dal 2002 nel settore dell'editoria specializzata sull'ICT professionale, realizzando e pubblicando riviste, report, survey, e-magazine, libri. Pubblica le riviste cartacee Direction, Partners e gli e-magazine Cloud & Business, Solutions, Security & Business, PartnersFlip. Ha siglato un accordo con Tom's Hardware Italia per la gestione dei tre canali B2B IT Pro, Manager e Resellers accessibili all'interno del dominio tomshw.it. Reportec è Media e Content Conference Partner di IDC Italia.

Sicurezza End-to-end per la posta e documenti allegati. Con un approfondimento sulla soluzione HPE SecureMail

© Reportec S.r.l. - Febbraio 2016 - Tutti i diritti riservati

Reportec S.r.l. via Marco Aurelio, 8 - 20127 Milano - Tel: (+39) 02 36580441 Fax: (+39) 02 36580444

www.reportec.it

Tutti i marchi citati in questo documento sono registrati e di proprietà delle relative società.