Crittografia si, ma con il giusto Key Mgmt System



In un mondo sempre più interconnesso, le violazioni dei dati catturano sempre più i titoli dei giornali. La sicurezza delle informazioni sensibili è vitale ed i requisiti normativi come il Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA) e Sarbanes-Oxley (SOX) creano sfide per le aziende che giustamente guardano alla crittografia come mezzo necessario per proteggere le proprie informazioni.

Crittografia che assume un ruolo principale per ogni tipo di organizzazione e con essa diventa ancor più importante un'attenta gestione delle chiavi di crittografia senza cui i nostri dati sarebbero inutilizzabili. Non solo: con l'aumento dell' impiego della crittografia occorre far fronte ad un numero crescente di chiavi di crittografia richieste dalle applicazioni.

Pertanto una gestione ben organizzata ed efficace di queste chiavi diventa essenziale per garantire sia la disponibilità che la sicurezza delle informazioni crittografate. E' altresì necessaria una gestione centralizzata delle chiavi e dei certificati per poter eseguire le complesse attività relative alla generazione, al rinnovo, al backup e al ripristino di chiavi e certificati.

Per tutti questi motivi ci si affida spesso ad una soluzione di Key Management capace di gestire efficientemente l'intero ciclo di vita delle chiavi tramite una completa fruibilità e scalabilità tra le differenti tecnologie crittografiche, che sappia interagire con il maggior numero di tipologie di sistemi target e, soprattutto, che sappia operare in un contesto di infrastrutture globali di tipo eterogeneo, quindi

anche ambienti Cloud o Hybrid-Cloud.

Ma andiamo con ordine e cominciamo ad esaminare le caratteristiche tecniche principali che deve avere un vero sistema di Key Management.

– Innanzitutto deve essere in grado di controllare dove viene generata la chiave, come viene gestita, conservata, utilizzata e revocata, oltre alla gestione dei metadati collegati alle chiavi. Queste operazioni devono seguire un flusso logico semplice da comprendere ed inequivocabile nell'operare proprio per evitare il più possibile errori umani indotti dall'operatore.

– Poi deve garantire la protezione delle chiavi sia per la loro memorizzazione che per l'archiviazione. L'utilizzo di un unico repository centralizzato consente inoltre di realizzare facilmente il backup includendo il database delle chiavi nelle procedure di backup già presenti nei flussi operativi. Ciò facilita il recupero in caso di smarrimento di chiavi o certificati. Il tutto deve poi rispettare i criteri del NIST per la distribuzione delle chiavi verso le piattaforme target che ne richiedono l'uso.

– Deve conferire caratteristiche prestazionali e di scalabilità per superare eventuali prestazioni di picco, anche in presenza di alti volumi di chiavi utilizzate.

– Deve poter adottare protocolli universali, come KMIP o ANSI X9.24, capaci di cooperare con il più alto numero di target disponibili sul mercato.

Quindi deve fornire supporto multipiattaforma, multisito e multivendor in modo da eseguire tutte le funzioni di gestione di chiavi e certificati su diverse piattaforme, sistemi operativi e posizioni geografiche.

– Monitoraggio. La scadenza del materiale di crittografia deve essere monitorata in modo da generare avvisi in tempo utile

per avviare la sostituzione.

– Infine deve assicurare la tracciabilità delle operazioni, in modo da poter effettuare tutte le opportune verifiche attribuendo le rispettive responsabilità, con un controllo degli accessi basato su ruoli

Nella condizione ideale, tutto questo dovrebbe essere gestito e soddisfatto da un'unica entità capace di semplificare operatività, efficienza e fruibilità.

In realtà, osservando la situazione presente nelle infrastrutture IT odierne, soprattutto presso le grandi organizzazioni bancarie e/o finanziarie, notiamo una certa proliferazione di diversi sistemi di gestione delle chiavi, molte volte dedicati o specializzati per ambiente, come ambienti mainframe, ambienti distribuiti su server convenzionali e ultimamente anche ambienti Cloud.

Ed è proprio presso queste realtà che si manifesta l'esigenza di una certa agilità ed automazione tipiche dei moderni processi aziendali, in cui è richiesta una gestione più organizzata e semplificata dell'intero ciclo di vita delle chiavi di crittografia, indipendentemente dalla piattaforma target, in modo da soddisfare tutte le operazioni di crittografia quotidiane eseguite attraverso i vari cloud pubblici, data center e applicazioni on-premise.

La proliferazione di strumenti e software diversi, a volte con funzionalità complementari, proprio per cercare di fornire tutte le funzioni necessarie previste da un KMS (Key Management System) di livello bancario unificato e flessibile, rende più complessa la gestione con conseguenti oneri sia dal punto di vista puramente economico che da quello efficienziale.

Basta pensare, ad esempio, ai processi di importazione delle chiavi che in molti casi avvengono ancora manualmente. Oppure alla necessità di condivisione e trasferimento delle chiavi

tra mainframe, server convenzionali e persino servizi basati su cloud. Per non parlare poi della gestione di molteplici repository delle chiavi distribuiti sulle diverse piattaforme.

Ebbene, in questo contesto è interessante considerare soluzioni come quella proposta da IBM con Enterprise Key Management Foundation (EKMF), un sistema che centralizza su IBM zEnterprise la gestione delle chiavi di livello bancario e che fornisce aggiornamenti e distribuzione automatizzati delle stesse ad un'ampia gamma di applicazioni e sistemi, gestendone completamente il loro intero ciclo di vita sia che si tratti di chiavi simmetriche, chiavi asimmetriche e certificati digitali.

Si tratta di una soluzione con delle univocità nel suo genere che la rendono capace di supportare i complessi processi aziendali nel rispetto delle normative di sicurezza aiutando il superamento di qualsiasi tipo di audit interno ed esterno. La necessità di operare in contesti ibridi dove è fondamentale l'integrazione con i sistemi mainframe z/OS esalta le interessanti funzionalità offerte da EKMF. Funzionalità rese disponibili anche tramite API che consentono alle applicazioni, in esecuzione sia nel cloud che sui mainframe, un facile utilizzo delle chiavi di crittografia.

Nel mondo d'oggi, quando pensiamo alla protezione dei dati mediante l'adozione della crittografia, non bisogna mai sottovalutare l'importanza della scelta contestuale di un buon Key Management System proiettato su scenari evolutivi e sicuri in modo tale da preservare ed esaltare l'investimento, necessario per proteggere oggi e domani i nostri preziosi dati.

Articolo a cura di **Luigi Perrone**

https://www.ictsecuritymagazine.com/articoli/crittografia-si-ma-con-il-giusto-key-mgmt-system/