Un'impresa Fortune 500 di pubblica utilità implementa un'infrastruttura a chiave pubblica a elevata disponibilità in un ambiente distribuito geograficamente

Come le competenze e gli HSM (Hardware Security Module) di Entrust a elevata sicurezza hanno aiutato una delle principali imprese di pubblica utilità statunitensi a garantire una forte sicurezza permettendo al contempo nuovi servizi al cliente.

L'OBIETTIVO: PREPARARSI AL FUTURO

Il team informatico di una delle principali imprese di pubblica utilità statunitensi ha fissato un obiettivo ambizioso per sé e per la propria infrastruttura di sicurezza.

Erano infatti determinati a rimanere all'avanguardia della tecnologia nel settore energetico, e per farlo dovevano garantire un servizio continuo ai clienti preparando allo stesso tempo la loro infrastruttura per innovazioni nuove e impegnative come le misurazioni e le reti intelligenti. Il loro obiettivo era soddisfare e superare gli elevati requisiti di sicurezza imposti dai revisori e dalla Homeland Security. Non solo: desideravano abilitare nuovi servizi, come ad esempio la possibilità di utilizzare tablet e smartphone per accedere alla rete.

> **« Sapevamo di aver bisogno di una soluzione hardware certificata. Dopo aver sentito storie sui furti di chiavi private che avevano compromesso interi PKI, è diventato chiaro che dovevamo dotare le nostre del più alto livello di sicurezza presente sul mercato. La nostra principale priorità è quella di fornire servizi al pubblico garantendo il più alto elevato livello di protezione disponibile. »**
>
> – Analista della sicurezza di un'impresa Fortune 500 di pubblica utilità

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Impresa Fortune 500 di pubblica utilità

Per raggiungere questi obiettivi, il team di sicurezza dell'impresa doveva migrare verso una versione aggiornata di piattaforme del software PKI (infrastruttura a chiave pubblica) e del server del core. Il loro PKI esistente, ormai vecchio oltre dieci anni, era adatto per l'autenticazione di server e computer portatili interni. Ma per emettere certificati per questi dispositivi mobili e accogliere nuove tecnologie garantendo allo stesso tempo i più alti livelli di sicurezza, avevano bisogno di una soluzione completamente nuova.

Un nuovo PKI avrebbe permesso di introdurre nuovi servizi come la firma di codici e le marcature temporali per garantire l'integrità e una gestione adeguata dei processi interni di sviluppo del software, ma anche soluzioni BYOD (Bring your Own Device) per registrare certificati e permettere ai dispositivi mobili e ai tablet di accedere alla rete in modo controllato e sicuro.

LA SFIDA: UN AMBIENTE COMPLESSO E DISTRIBUITO

La sfida vera e propria di questa distribuzione consisteva nel lavoro all'interno dell'ambiente unico dell'impresa. Per ottenere gli alti livelli di disponibilità, nonché le funzionalità di ridondanza e disaster recovery di cui avevano bisogno, il team avrebbe dovuto distribuire il PK in combinazione con una complessa infrastruttura cluster di server presente in luoghi diversi. In caso di successo, l'infrastruttura aziendale sarebbe stata in grado di soddisfare facilmente le necessità del decennio a venire. Tuttavia, le informazioni sulla configurazione di un PKI in questo tipo di ambiente erano scarse: secondo alcuni esperti era un'impresa possibile, ma ardua.

Considerati i requisiti di sicurezza, il team sapeva che la soluzione avrebbe dovuto includere HSM (Hardware Security Module). "Sapevamo che avremmo avuto bisogno di una soluzione hardware certificata", spiega il principale analista della sicurezza dell'impresa. "Dopo aver sentito storie sui furti di chiavi private che avevano compromesso interi PKI, è diventato chiaro che dovevamo dotare le nostre del più alto livello di sicurezza disponibile sul mercato. La nostra principale priorità è quella di fornire servizi al pubblico garantendo il più alto elevato livello di protezione disponibile".

LA SOLUZIONE: HSM NSHIELD E IL PARERE DEGLI ESPERTI DI ENTRUST

Per distribuire questa soluzione innovativa, l'azienda ha scelto una suite di soluzioni di Entrust che includeva nShield® Connect, HSM nShield Edge e nShield Time Stamping Option Pack. Grazie all'esperienza con i prodotti di Entrust e il livello superiore di sicurezza e funzioni intuitive, il team dedicato alla sicurezza sapeva che queste soluzioni avrebbero fornito la configurabilità e la flessibilità necessarie per questo ambiente complesso.

Il team ha anche fatto affidamento sulle competenze dei consulenti nel team di servizi professionali Entrust per strutturare l'implementazione. "Il team Entrust è stato fantastico", commenta l'analista della sicurezza. "Questa soluzione non è mai stata implementata prima d'ora. Esistevano white paper secondo cui era possibile farlo, ma alcune tecnologie più avanzate e complesse non erano mai state davvero implementate. Entrust ha fornito gli HSM aziendali, ci ha insegnato a configurarli e utilizzarli correttamente nel nostro ambiente tramite sessioni di formazione. I loro consulenti erano estremamente competenti ed esperti nella tecnologia PKI, e la loro dedizione per garantire il successo del progetto è stato ineguagliabile".

Impresa Fortune 500 di pubblica utilità

I risultati? "La soluzione di Entrust ha avuto un fortissimo impatto sulle nostre operazioni. L'infrastruttura può ora supportare una serie di altri progetti in sospeso, e il nostro PKI sta operando come previsto: non soltanto emette certificati server, ma permette una vasta gamma di altri servizi. Ci basiamo sul PKI per tantissime operazioni, il che rende la sicurezza basata sul hardware un requisito di fondamentale importanza."

HARDWARE ENTRUST

I prodotti implementati in questa soluzione includono:

HSM nShield Connect di Entrust

Questo HSM ad alte prestazioni collegato alla rete fornisce dei servizi di crittografia affidabili come risorsa condivisa per le istanze delle applicazioni distribuite e le macchine virtuali. Gli HSM nShield Connect offrono un modo economico per garantire livelli adeguati di controllo fisico e logico per i sistemi basati su server. Grazie agli HSM nShield Connect, le organizzazioni possono:

- Ridurre al minimo i costi operativi con una potente architettura di gestione delle chiavi
- Massimizzare l'utilizzo e la scalabilità con una piattaforma centralizzata condivisa
- Fornire una protezione crittografica per l'architettura di rete nelle implementazioni tradizionali, virtualizzate e nel cloud
- Superare le vulnerabilità intrinseche della crittografia basata su software

HSM Edge nShield di Entrust

Questo HSM collegato via USB offre alle organizzazioni un modo economico per implementare una crittografia ad alta garanzia. Gli HSM nShield Edge sono particolarmente adatti per i computer portatili e in ambienti di lavoro o desktop grazie alla facile portabilità e alla connettività USB. Inoltre, il design compatto e il lettore di smart card integrato li rende perfetti per l'implementazione in uno spazio limitato o dove vengono utilizzati solo occasionalmente.

Pacchetto di marcatura temporale nShield Time Stamping Option Pack di Entrust

Questa soluzione chiavi in mano di marcatura temporale a elevata affidabilità mantengono l'ora esatta e creano marcature temporali sicure per registrare il tempo di creazione, di archiviazione o di altri eventi associati alle registrazioni o alle applicazioni elettroniche. nShield Time Stamping Option Pack di Entrust protegge le operazioni di marcatura temporale in un hardware certificato indipendentemente e a prova di manomissione, garantendo un'accuratezza temporale e una verificabilità superiori.

Impresa Fortune 500 di pubblica utilità

VANTAGGI: DISPONIBILITÀ, SICUREZZA E MAGGIORI SERVIZI

La soluzione di Entrust offre numerosi vantaggi critici:

Elevata disponibilità

La configurazione in modalità cluster e la resilienza dell'HSM nShield permettono una maggiore ridondanza, compreso un failover automatico per garantire una disaster recovery più solida e una disponibilità continua.

Maggiore sicurezza

Con l'apertura della rete aziendale a nuovi dispositivi, gli HSM nShield di Entrust permettono un'autenticazione più solida grazie all'emissione di certificati per i dispositivi. Il PKI può emettere certificati a tutti i dispositivi, mentre a quelli personali verrebbe garantito un accesso alla rete limitato.

HSM in vari fattori di forma

L'utilizzo di HSM nShield di Entrust permette all'impresa di acquistare hardware di dimensioni adeguate per i propri computer e server, senza essere obbligata a procurarsi tecnologie non necessarie.

Supporto alle misurazioni intelligenti.

Con la distribuzione di una nuova tecnologia di misurazione intelligente da parte dell'impresa, la soluzione garantirà l'integrità e la riservatezza dei dati trasmessi.

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Scopri di più su
entrust.com/HSM

ENTRUST

Per contattarci:
HSMinfo@entrust.com