Gli HSM nShield di Entrust consentono a uno dei 10 istituti bancari leader a livello mondiale di offrire servizi Web sicuri e affidabili a partner e clienti

LA SFIDA COMMERCIALE

Tutte le aziende con una presenza online orientata ai clienti provvedono all'autenticazione degli utenti che utilizzano i loro servizi. Le principali banche del mondo non fanno eccezione. Con il rapido sviluppo di Internet e l'aumento massiccio delle transazioni online, i dati sensibili scambiati in rete e nel cloud sono diventati l'oggetto di attacchi mirati sempre più frequenti.

I servizi online si servono di meccanismi di accesso per connettere i browser degli utenti finali ai server Web. Queste connessioni sono protette dalla tecnologia SSL (Secure Socket Layer) che cifra i dati su Internet. Indicato più propriamente con il termine TLS (Transport Layer Security), lo standard SSL costituisce la forma di protezione effettiva di tutte le comunicazioni via Internet e, non a caso, è rappresentato dal simbolo del lucchetto che appare nei browser.

> **L'aumento costante del traffico Internet e la proliferazione degli attacchi malware basati su SSL, tra cui il recente Heartbleed, hanno spinto questo importante istituto bancario a migliorare la propria capacità di ispezionare il traffico SSL in maniera sicura, per assicurare l'assenza di virus e altri malware nascosti che potrebbero infettare i sistemi.**

Banca leader a livello mondiale

Per offrire servizi Web sicuri e affidabili agli utenti, le aziende devono garantire la riservatezza, l'integrità e la disponibilità dei dati elaborati. L'aumento costante del traffico Internet e la proliferazione degli attacchi malware basati su SSL, tra cui il recente Heartbleed, hanno spinto un importante istituto bancario a migliorare la propria capacità di ispezionare il traffico SSL in maniera sicura, per assicurare l'assenza di virus e altri malware nascosti che potrebbero infettare i sistemi. Nello specifico, il progetto mira a esaminare il traffico generato dai partner, dalle società controllate e dai dipendenti della banca.

LA SFIDA TECNICA

Con l'aumento della quantità di traffico cifrato attraverso le reti, il protocollo SSL rischia di diventare un veicolo di attacchi, dato che il codice malevolo potrebbe non essere rilevato. Utilizzata per filtrare elementi potenzialmente dannosi nascosti all'interno dei contenuti crittografati, l'ispezione del traffico SSL intercetta, decifra e ispeziona il traffico di un sito Web, per poi cifrarlo nuovamente affinché raggiunga la destinazione finale.

Gli hardware security module (HSM) offrono un livello di sicurezza aggiuntivo per il numero crescente di chiavi SSL utilizzate nel processo. Decifrare, ispezionare e crittografare di nuovo il traffico, affinché venga esaminato e possa giungere al server Web (dove verrà decifrato un'altra volta), implica una maggiore frequenza di recupero delle chiavi necessarie. In generale, le varie chiavi utilizzate non corrispondono tra di loro, per cui è necessario un livello superiore di protezione.

Gli HSM stabiliscono una root of trust, assicurando che tutte le connessioni essenziali siano protette e affidabili. Secondo il Security Architect dell'istituto, ispezionare il flusso del traffico Internet senza un hardware security module (HSM) è possibile, ma molto rischioso.

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Banca leader a livello mondiale

Il ruolo di questi dispositivi è proteggere le chiavi di decrittazione, un'operazione necessaria per garantire la sicurezza della tecnologia che decodifica il traffico Web.

LA SOLUZIONE

La banca ha implementato gli HSM nShield Connect di Entrust in una configurazione "active/active" all'interno di due data center distanti circa 10 chilometri l'uno dall'altro. Gli HSM soddisfano i requisiti di sicurezza odierni di 45 server proxy, offrendo inoltre la flessibilità necessaria per le esigenze di crescita futura.

I RISULTATI

Si prevede che gli HSM nShield di Entrust raggiungano una capacità almeno cinque volte superiore a quella del sistema legacy, consentendo all'organizzazione di continuare a ispezionare il traffico Internet per individuare codice potenzialmente malevolo anche in caso di ampliamento del sistema.

Da oltre 10 anni, questa banca leader a livello mondiale collabora con Entrust, che ha scelto come fornitore di HSM in virtù della sua lunga esperienza con la tecnologia e la capacità di rispondere alle problematiche di sicurezza. Inoltre, il personale dei servizi professionali Entrust è stato coinvolto nell'installazione degli HSM e ha provveduto alla formazione dei dipendenti della banca sul loro uso.

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Banca leader a livello mondiale

Obiettivi commerciali

- Servizi Web sicuri e affidabili per gli utenti

Obiettivi tecnici

- Monitoraggio del crescente traffico Internet interno e sicurezza della tecnologia di controllo
- Protezione della complessa infrastruttura IT dell'organizzazione

La soluzione

- HSM nShield Connect di Entrust in una configurazione "active/active" per gestire e proteggere le chiavi SSL

Il risultato

- Sicurezza certificata in conformità allo standard FIPS 140-2 di livello 3 e ai Common Criteria EAL4+
- Capacità cinque volte superiore rispetto al sistema legacy
- Scalabilità semplice per le esigenze future

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