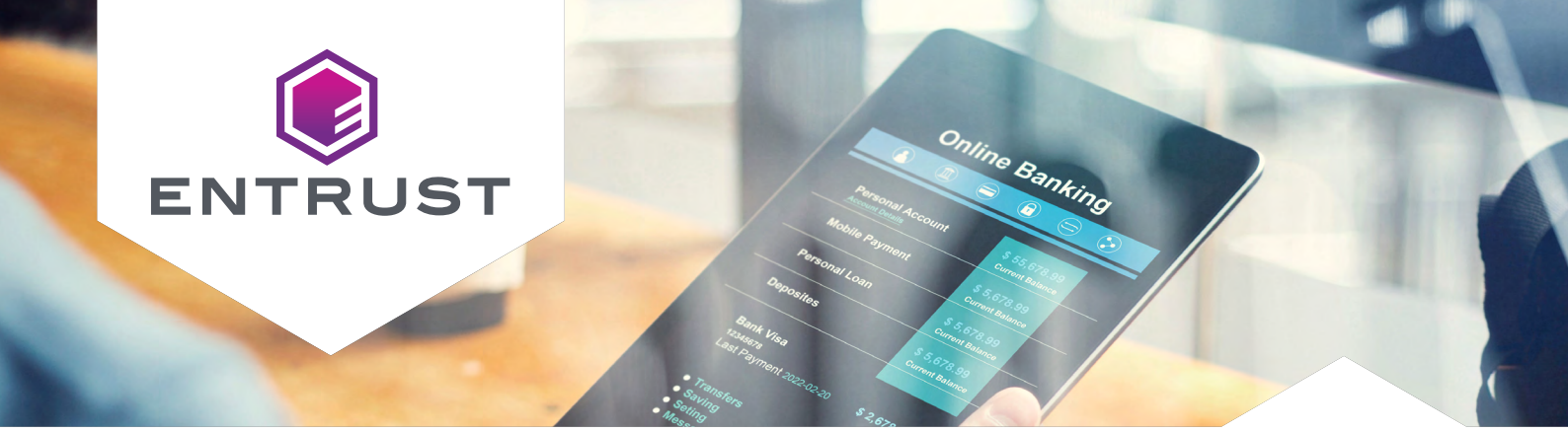


Eine der zehn größten Banken der Welt verwendet Entrust nShield HSMs, um ihren Kunden und Partnern vertrauenswürdige und zuverlässige Webdienste anzubieten

GESCHÄFTLICHE PROBLEMSTELLUNG

Alle Unternehmen mit einer kundenorientierten Online-Präsenz authentifizieren ihre Nutzer bei der Nutzung von Dienstleistungen – und für die größten Banken der Welt ist dies keine Ausnahme. Mit dem explosionsartigen Wachstum von Internet und Online-Transaktionen sind sensible Daten, die online und in der Cloud ausgetauscht werden, zunehmend zum Angriffsobjekt geworden.

Online-Dienste verwenden Anmeldemechanismen, um die Browser von Endbenutzern mit Webservern zu verbinden, und diese Verbindungen sind durch Secure Sockets Layer (SSL) geschützt, eine Technologie, die Daten im Internet verschlüsselt. Der SSL-Standard (die Technologie hinter dem Vorhängeschloss-Symbol im Browser, treffender als Transportschicht-Sicherheit oder TLS bezeichnet) ist die effektivste Schutzmaßnahme für die gesamte Internetkommunikation.

> **Angesichts des zunehmenden Internet-Verkehrs und der zahlreichen SSL-basierten Malware-Angriffe, wie z.B. Heartbleed, musste diese führende Bank ihre Kapazitäten zur sicheren Überprüfung des SSL-Verkehrs erweitern und verbessern, um sicherzustellen, dass keine versteckten Viren oder andere Malware ihre Systeme infizieren kann.**

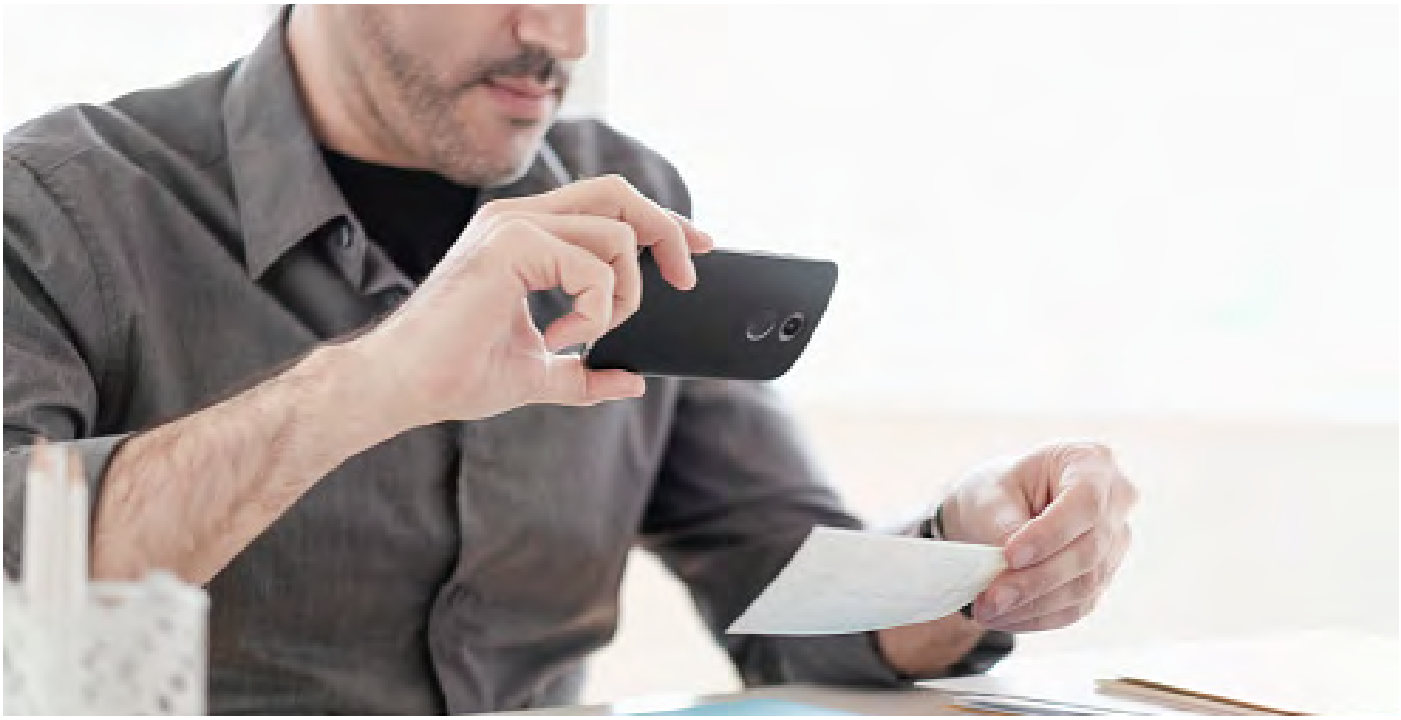
Führende Weltbank

Unternehmen, die ihren Nutzern vertrauenswürdige und zuverlässige Webdienste anbieten wollen, müssen die Vertraulichkeit, Integrität und Verfügbarkeit der durch den Dienst verarbeiteten Daten sicherstellen. Angesichts des zunehmenden Internet-Verkehrs und der zahlreichen SSL-basierten Malware-Angriffe, wie z.B. Heartbleed, musste diese führende Bank ihre Kapazitäten zur sicheren Überprüfung des SSL-Verkehrs erweitern und verbessern, um sicherzustellen, dass keine versteckten Viren oder andere Malware ihre Systeme infizieren können. Konkret konzentrierte sich dieses Projekt auf die Untersuchung des von den Partnern, Tochtergesellschaften und Mitarbeitern der Bank erzeugten Verkehrs.

TECHNISCHE PROBLEMSTELLUNG

Die Zunahme von verschlüsseltem Datenverkehr in heutigen Netzwerken kann SSL auch zu einem Angriffsvektor machen, da sich gefährlicher Code hier verstecken und unentdeckt bleiben kann. Die SSL-Inspektion wird verwendet, um potenziell gefährliche Elemente herauszufiltern, die sich in verschlüsselten Inhalten verstecken. Dabei wird der Website-Verkehr abgefangen, entschlüsselt und inspiziert und für seinen endgültigen Bestimmungsort wieder verschlüsselt.

Hardware-Sicherheitsmodule (HSMs) bieten eine zusätzliche Schutzebene für die steigende Anzahl von SSL-Schlüsseln, die infolge des Entschlüsselungs- und Wiederverschlüsselungsprozesses verwendet werden. Das Entschlüsseln, Inspizieren und erneute Verschlüsseln des Datenverkehrs zwecks Überprüfung und Weiterleitung an einen Webserver (wo er wieder entschlüsselt wird) bedeutet, dass die für diesen Prozess erforderlichen Schlüssel häufiger abgerufen werden. In der Regel sind nicht alle verwendeten Schlüssel gleich – weshalb ein höherer Schutzbedarf besteht.



Führende Weltbank

HSMs bieten eine Root of Trust, die sicherstellt, dass alle kritischen Verbindungen nicht nur geschützt sind, sondern auch vertrauenswürdig sind. Laut dem Sicherheitsarchitekten der Bank ist es möglich, den Internet-Verkehrsfluss ohne ein Hardware-Sicherheitsmodul (HSM) zu kontrollieren, was aber sehr gefährlich ist.

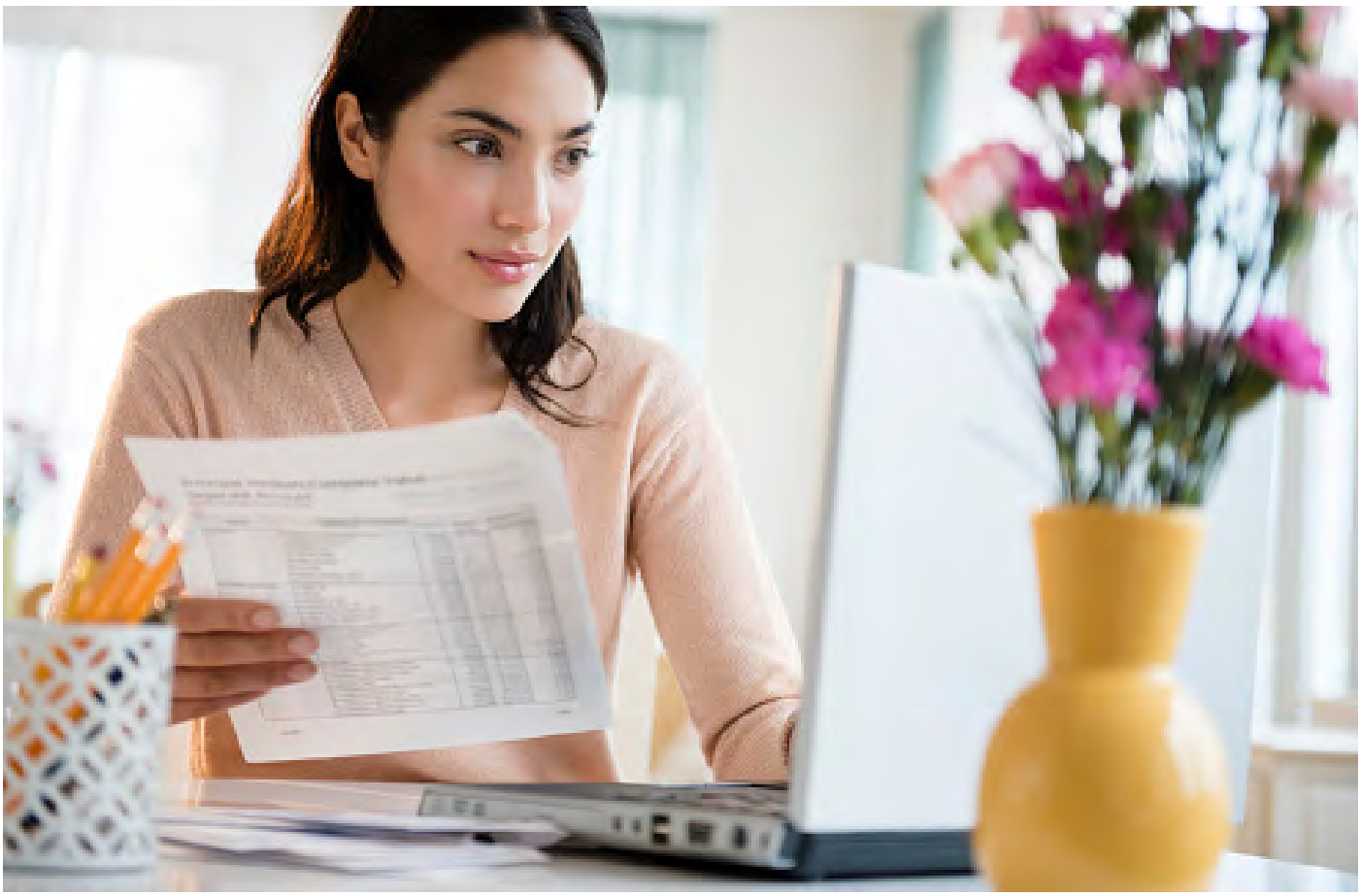
Man muss die Technologie schützen, die den Webverkehr entschlüsselt, und das bedeutet, dass die Entschlüsselungsschlüssel geschützt und gesichert werden müssen. Genau das tun die HSMs.

LÖSUNG

Die Bank führte Entrust nShield Connect HSMs in einer doppelten „aktiv-aktiven" Konfiguration in zwei Datenzentren ein, die etwa 10 Kilometer voneinander entfernt waren. Die HSMs erfüllen die Sicherheitsanforderungen von 45 Proxy-Servern und bieten viel Kapazität für Wachstum.

ERGEBNISSE

Die HSMs von Entrust nShield werden voraussichtlich mindestens die fünffache Kapazität des bisherigen Systems erreichen. Dadurch kann das Unternehmen den Internetverkehr auf möglichen versteckten schädlichen Code untersuchen und die Sicherheit gewährleisten, wenn das System wächst.



Führende Weltbank

Geschäftliche Anforderungen

- Bereitstellung vertrauenswürdiger und zuverlässiger Webdienste für Benutzer

Technische Anforderungen

- Überwachung des zunehmenden internen Internet-Verkehrs und Schutz der Überwachungstechnologie
- Schutz der übergreifenden IT-Infrastruktur des Unternehmens

Lösung

- Entrust nShield Connect HSMs, die "aktiv-aktiv" verwendet werden für die Verwaltung und zum Schutz von SSL-Schlüsseln

Resultat

- Zertifizierte Sicherheit nach FIPS 140-2 Stufe 3 und Common Criteria EAL4+
- Fünffache Kapazität im Vergleich zum Legacy-System
- Einfache Skalierbarkeit für zukünftige Bedürfnisse

Diese weltweit führende Bank arbeitet seit mehr als zehn Jahren mit Entrust zusammen. Sie wählte Entrust als ihren HSM-Anbieter, da Entrust über umfangreiche Erfahrungen mit der Technologie und der Lösung von Sicherheitsfragen verfügt. Zudem wurde mit dem Professional Services Team von Entrust gearbeitet, um die HSMs zu installieren und die Bankmitarbeiter in ihrer Anwendung zu schulen.

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com