Fortune-500-Versorgungsunternehmen richtet hochverfügbare öffentliche Schlüsselinfrastruktur in geografisch weitläufiger Umgebung ein

Wie die Erfahrung von Entrust und seine hochgradig sicheren Hardware-Sicherheitsmodule (HSMs) halfen, einem der größten Versorgungsunternehmen der USA ein hohes Maß an Sicherheit anbieten zu können und gleichzeitig neue Kundendienstleistungen zu ermöglichen.

DAS ZIEL: ZUKUNFTSFIT WERDEN

Das IT-Team eines der größten Versorgungsunternehmen der USA hat sich selbst und seiner Sicherheitsinfrastruktur ein ambitioniertes Ziel gesetzt.

Das Team wollte seine Position als Marktführer behaupten und mit der kontinuierlichen Weiterentwicklung der Technologie im Energiesektor Schritt halten. Es musste sicherstellen, dass die Kunden weiterhin ihre Dienstleistungen erhielten, während gleichzeitig die Infrastruktur auf neue und anspruchsvolle Technologien wie Smart Metering und Smart Grid vorbereitet wurde. Sie wollten die hohen Sicherheitsanforderungen, die die Auditoren und das Ministerium für Innere Sicherheit der USA gestellt hatten, nicht nur erfüllen, sondern übertreffen. Und es sollten neue Dienstleistungen entstehen, die es Mitarbeitern und Kunden ermöglichen würden, Tablets und Smartphones für den Zugriff auf das Netzwerk zu verwenden.

> **„Wir wussten, dass wir eine zertifizierte Hardware-Lösung brauchten. Wir mussten sicherstellen, dass alle unserer privaten Schlüssel den höchsten verfügbaren Schutz erhielten. Zu oft haben wir von Diebstählen privater Schlüssel gehört, die ganze PKIs in Gefahr brachten. Die Bereitstellung unserer Dienstleistungen für die Öffentlichkeit steht bei uns an erster Stelle und wir mussten dafür sorgen, dass wir das höchstmögliche Maß an Sicherheit boten."**
>
> – Leitender Sicherheitsanalyst bei Fortune-500-Versorgungsunternehmen

Fortune-500-Versorgungsunternehmen

Um diese Ziele zu erreichen, plante das Sicherheitsteam des Versorgungsunternehmens, zu einer aktualisierten Version der Software und Hauptserver-Plattformen ihrer öffentlichen Schlüsselinfrastruktur (public key infrastructure, PKI) zu migrieren. Ihre bestehende PKI war nun beinahe zehn Jahre alt und hatte die Aufgabe zur Authentifizierung interner Server und Laptops bestens erfüllt. Allerdings war eine neue Lösung vonnöten, um Zertifikate für diese Mobilgeräte auszustellen und andere neue Technologien bei gleichzeitigem Erhalt eines Höchstmaßes an Sicherheit umzusetzen.

Eine neue PKI würde neue Dienstleistungen wie Code Signing und Zeitstempel ermöglichen, um die Integrität und angemessene Governance ihrer internen Softwareentwicklungsprozesse sicherzustellen. Außerdem wäre ein „Bring your own device"-Ansatz (BYOD) möglich, bei dem eine Zertifikatsregistrierung den Zugriff von mobilen Geräten und Tablets auf das Netzwerk auf kontrollierte und sichere Art und Weise gewährleisten würde.

DIE HERAUSFORDERUNG: EINE KOMPLEXE UND WEITLÄUFIGE UMGEBUNG

Die eigentliche Herausforderung dieses Projekts war die Arbeit in der einzigartigen Umgebung des Versorgungsunternehmens. Um die hohe Verfügbarkeit, Redundanz und Notfallwiederherstellungsfunktionalität zu erreichen, die erforderlich waren, musste das Team die PKI in Verbindung mit einer komplexen Server-Cluster-Infrastruktur bereitstellen, die sich an mehreren Standorten befand. Bei erfolgreicher Umsetzung könnte die Infrastruktur des Versorgungsunternehmens so die Anforderungen der nächsten zehn Jahre problemlos erfüllen können. Allerdings waren über die Konfiguration einer PKI in dieser schwierigen Umgebung wenig bekannt – manche Experten behaupteten zwar, dass es möglich war, aber es war auf jeden Fall eine Mammutaufgabe.

Aufgrund der Sicherheitsanforderungen war schnell klar, dass Hardware-Sicherheitsmodule (HSMs) zum Einsatz kommen mussten. „Wir wussten, dass wir eine zertifizierte Hardware-Lösung brauchten", berichtet der leitende Sicherheitsanalyst des Unternehmens. „Wir mussten sicherstellen, dass alle unserer privaten Schlüssel den höchsten verfügbaren Schutz erhielten. Zu oft haben wir von Diebstählen privater Schlüssel gehört, die ganze PKIs in Gefahr brachten. Die Bereitstellung unserer Dienstleistungen für die Öffentlichkeit steht bei uns an erster Stelle und wir mussten dafür sorgen, dass wir das höchstmögliche Maß an Sicherheit boten."

DIE LÖSUNG: ENTRUST NSHIELD HSMS UND FACHMÄNNISCHE BERATUNG

Um diese innovative Lösung bereitzustellen, entschied sich das Unternehmen für ein Lösungspaket von Entrust, das nShield® Connect, nShield Edge HSMs sowie das nShield Zeitstempel-Optionspaket enthielt. Aufbauend auf ihrer fundierten Erfahrung mit Entrust-Produkten und dem Wissen um die überlegene Kombination aus einem hohen Maß an Sicherheit und Benutzerfreundlichkeit, konnte das Sicherheitsteam darauf vertrauen, dass die Entrust-Lösungen die erforderliche Konfigurierbarkeit und Flexibilität bieten würden, die in dieser Umgebung vonnöten waren.

Außerdem wurde das Unternehmen von einem Team aus Entrust-Beratern bei der Strukturierung der Bereitstellung unterstützt. „Das Team von Entrust war großartig", so der leitende Sicherheitsanalyst. „Man muss bedenken, dass ein derartiges Projekt noch nie durchgeführt worden war. Es gab Whitepaper, die besagten, dass es möglich sei, aber Teile der erweiterten und komplexen Technologie waren noch nie in der Praxis zum Einsatz gekommen. Entrust bot die Unternehmens-HSMs, erklärte uns, wie sie zu konfigurieren und in unserer spezifischen Umgebung einzusetzen waren, und half uns durch Schulungen, die einzelnen Puzzleteile zusammenzufügen. Die Berater waren äußerst kompetent und sehr erfahren im Bereich der PKI-Technologie. Ihr Engagement für eine erfolgreiche Abwicklung des Projekts war einzigartig."

Fortune-500-Versorgungsunternehmen

Das Ergebnis? „Unsere Entrust-Lösung hatte phänomenale Auswirkungen auf unsere Betriebsprozesse. Unsere Infrastruktur unterstützt nun zahlreiche andere Projekte, die noch ausstehend waren. Und unsere PKI leistet, wofür sie geschaffen wurde: Sie stellt nicht nur Server-Zertifikate aus, sondern ermöglicht uns die verschiedensten Dienstleistungen. Wir verlassen uns in vielerlei Hinsicht auf die PKI. Und je mehr wir davon abhängen, desto mehr ist eine Sicherheit vonnöten, die auf Hardware basiert."

ENTRUST HARDWARE

Zu den zum Einsatz gekommenen Produkten dieser Lösung gehören:

Entrust nShield Connect HSM

Dieses hochleistungsfähige, an das Netzwerk angeschlossene HSM bietet sichere kryptographische Dienste als gemeinsame Ressource für verteilte Anwendungsinstanzen und virtuelle Maschinen. nShield Connect HSMs bieten eine kostengünstige Möglichkeit, ein angemessenes Maß an physischer und logischer Kontrolle für serverbasierte Systeme zu gewährleisten. Mit nShield Connect HSMs können Unternehmen:

- mit einer leistungsfähigen Schlüsselverwaltungsarchitektur Betriebskosten minimieren,
- mit einer gemeinsamen zentralen Plattform Auslastung und Skalierbarkeit maximieren,
- kryptographischen Schutz für Netzwerkarchitekturen in traditionellen und virtualisierten Implementierungen sowie Cloud-Implementierungen bieten
- und die inhärenten Schwachstellen von softwarebasierter Kryptographie überwinden.

Entrust nShield Edge HSM

Dieses HSM mit USB-Anschluss bietet Unternehmen eine kostengünstige Möglichkeit, hochgradig sichere Kryptographie zu implementieren. Aufgrund der größeren Portabilität und USB-Konnektivität eignen sich nShield Edge HSMs besonders für Laptops und in Workstation- oder Desktop-Umgebungen. Dank ihres kompakten Designs und des integrierten Smart-Card-Lesegeräts sind sie ideal für Einsätze mit begrenztem Platzangebot oder dort, wo HSMs nur gelegentlich eingesetzt werden.

Entrust nShield Zeitstempel-Optionspaket

Diese sofort einsatzbereite, hochgradig sichere Zeitstempellösung liefert genaue Zeitangaben und erstellt sichere Zeitstempel für Aufzeichnungen, Archivierungen und die Zeitplanung anderer Ereignisse im Zusammenhang mit elektronischen Aufzeichnungen und Anwendungen. Das Entrust nShield Zeitstempel-Optionspaket schützt Zeitstempel in einer unabhängig zertifizierten, manipulationssicheren Hardware und bietet überlegene Zeitgenauigkeit und Überprüfbarkeit.

Fortune-500-Versorgungsunternehmen

VORTEILE: VERFÜGBARKEIT, SICHERHEIT UND WEITERE DIENSTLEISTUNGEN

Die Entrust-Lösung bietet verschiedene wesentliche Vorteile:

Hohe Verfügbarkeit

Der Cluster-Aufbau und die Belastbarkeit der nShield HSMs ermöglichen eine größere Redundanz mit automatisiertem Failover für eine robustere Notfallwiederherstellung und kontinuierliche Verfügbarkeit.

Mehr Sicherheit

Im Zuge der Erweiterung des Netzwerks für mehr Geräte, ermöglichen Entrust nShield HSMs dem Unternehmen stärkere Authentifizierung durch die Ausstellung von Gerätezertifikaten. Die PKI kann allen Geräten Zertifikate ausstellen – persönliche Geräte erhalten dabei nur eingeschränkten Zugang zum Netzwerk.

Verschiedene HSM-Formfaktoren

Durch die Verwendung von Entrust nShield HSMs kann das Unternehmen Hardware in geeigneter Größe für Laptops und Server kaufen und ist nicht gezwungen, unnötige Anschaffungen zu machen.

Support für Smart Metering

Im Rahmen ihrer Umsetzung einer Smart-Metering-Technologie, stellt die Lösung die Integrität und Vertraulichkeit der übertragenen Daten sicher.

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