Zerto arbeitet mit Entrust, um die Integrität seiner Geschäftsanwendungen sicherzustellen

Zerto wurde 2010 gegründet mit der einzigartigen Vision, dass eine Disaster-Recovery-Technologie (Notfallwiederherstellung) keine Versicherungspolice, sondern ein Wettbewerbsvorteil sein sollte.

Zerto unterstützt Kunden bei der Beschleunigung der IT-Transformation, indem es die Risiken und die Komplexität der Modernisierung und der Cloud-Nutzung durch IT-Resilienz aus dem Weg räumt. Indem mehrere Legacy-Lösungen durch eine einzige IT-Resilienz-Platform™ ersetzt werden, kombiniert Zerto Notfallwiederherstellung, Backup und Cloud-Mobilität in einer einfachen, konvergenten Lösung. Die Software-Plattform von Zerto ist unternehmensweit einsetzbar und bietet kontinuierliche Verfügbarkeit für eine stets aktive Kundenerfahrung. Gleichzeitig vereinfacht sie die Mobilität von Workloads, um Anwendungen zu schützen, wiederherzustellen und frei zwischen hybriden und Multi-Clouds zu verschieben.

Zerto hat die IT-Märkte revolutioniert und aufgezeigt, was im Bereich Disaster Recovery alles möglich ist. Das Unternehmen hat sein innovatives Produkt auf der Grundlage einer Technologie für kontinuierliche Datensicherung entwickelt. In einer Welt, in der sich Unternehmen darauf verlassen müssen, dass die Technologie immer funktioniert, ist dieses Angebot zu viel mehr als nur einem Disaster-Recovery-Tool geworden.

> **„Im Vergleich zu anderen Anbietern sind die Implementierung und der Support von Entrust viel besser. Entrust nShield Solo HSMs sind einfacher zu benutzen und zu sichern. Zudem gefällt uns die grafische Benutzeroberfläche sehr gut.“**
>
> – Nadav Svirsky, Corporate IT Infrastructure Lead, Zerto

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Zerto

GESCHÄFTLICHE PROBLEMSTELLUNG

Als führender Anbieter für IT-Resilienz-Lösungen, musste Zerto sicher gehen können, dass die eigenen Geschäftssysteme nicht anfällig für Störungen sind. Dafür benötigte das Unternehmen eine verlässliche Public-Key-Infrastruktur (PKI).

Eine PKI-Infrastruktur ist ein System aus Hardware, Software, Richtlinien, Prozessen und Verfahren, die zum Erstellen, Verwalten, Verteilen, Verwenden, Speichern und Widerrufen von digitalen Zertifikaten und öffentlichen Schlüsseln erforderlich sind. PKIs helfen dabei, Personen, Geräte und Dienste zu identifizieren, sodass der kontrollierte Zugriff auf Systeme und Ressourcen, der Schutz von Daten und die Rechenschaftspflicht bei Transaktionen gewährleistet sind. Um höchste Sicherheit garantieren zu können, sind Geschäftsanwendungen der nächsten Generation verstärkt auf PKI-Technologie angewiesen, da zeitgemäße Geschäftsmodelle mehr und mehr von elektronischer Interaktion abhängig sind, die Online-Authentifizierung und die Einhaltung strenger Datensicherheitsvorschriften erfordern.

Um öffentliche Schlüssel an den zugehörigen Benutzer (Besitzer des privaten Schlüssels) zu binden, verwenden PKIs digitale Zertifikate. Digitale Zertifikate bilden die Credentials, welche die Überprüfung der Identitäten zwischen Benutzern in einer Transaktion erleichtern. Ähnlich wie ein Reisepass die Identität einer Person als Bürger eines Landes bescheinigt, stellt das digitale Zertifikat die Identität der Benutzer innerhalb des Ökosystems fest. Da digitale Zertifikate zur Verifizierung der Identität der Nutzer, an die verschlüsselte Daten geschickt werden, oder der Unterzeichner von Informationen verwendet werden, ist der Schutz der Authentizität und Integrität des Zertifikats unerlässlich, um die Vertrauenswürdigkeit des Systems aufrechtzuerhalten. Diese Vorgabe war zentral für das Geschäftsmodell von Zerto als vertrauenswürdiger Anbieter.

TECHNISCHE PROBLEMSTELLUNG

Zertifizierungsstellen (Certified Authorities/CAs) stellen die digitalen Berechtigungsnachweise aus, mit denen die Identität der Benutzer bestätigt wird. CAs untermauern die Sicherheit einer PKI und der Dienste, die sie unterstützen, und können daher im Mittelpunkt raffinierter und gezielter Angriffe stehen. Um das Risiko von Angriffen auf CAs zu verringern, sind physische und logische Kontrollen sowie Härtungsmechanismen, wie zum Beispiel Hardware-Sicherheitsmodule (HSMs), zur Notwendigkeit geworden, um die Integrität einer PKI zu gewährleisten.

Zerto verwendet eine Microsoft-Plattform, und die IT-Abteilung wusste aus der Zusammenarbeit mit Microsoft, dass die beste Methode zur Sicherung ihrer CAs die Verwendung eines HSM ist. HSMs bieten eine unabhängig zertifizierte, manipulationssichere Umgebung und sind ein integraler Bestandteil der Sicherung von sensiblen Schlüsseln und Geschäftsprozessen.

Zerto

> **Der Einsatz von Entrust nShield Solo HSMs zur Sicherung unserer CAs lässt uns ruhig schlafen. Unser Management ist der Ansicht, dass die Risikominderung die Investition wert ist.**
>
> – Nadav Svirsky, Corporate IT Infrastructure Lead, Zerto

LÖSUNG

Das IT-Team von Zerto hatte Erfahrung mit mehreren HSM-Anbietern und entschied sich für den Einsatz von Entrust nShield®Solo HSMs. Laut Nadav Svirsky, Corporate IT Infrastructure Lead, entschied sich Zerto für Entrust, weil „im Vergleich zu anderen Anbietern die Implementierung und der Support von Entrust besser sind. Entrust nShield Solo HSMs sind einfacher zu benutzen und zu sichern. Zudem gefällt uns die grafische Benutzeroberfläche sehr gut."

ERGEBNISSE

Zerto teilt seine quantifizierbaren Ergebnisse, die sich aus der Installation von Entrust nShield HSMs ergeben, zum Schutz seiner CAs nicht mit. Bezüglich der nun vorhandenen Best Practice hinsichtlich CA-Sicherheit, was das ursprüngliche Ziel des Projekts war, merkt Svirsky an: „Unsere Kunden müssen darauf vertrauen können, dass unsere Systeme sicher und vertrauenswürdig sind. Leider erkennt man den Wert von Datensicherheit oft erst dann, wenn etwas schief geht. In solchen Momenten kann man beobachten, wie der Ruf, der Umsatz und der Aktienkurs eines Unternehmens sinken. Der Einsatz von Entrust nShield Solo HSMs zur Sicherung unserer CAs lässt uns ruhig schlafen. Unser Management ist der Ansicht, dass die Risikominderung die Investition wert ist."

Zerto

LEISTUNG, ZUVERLÄSSIGKEIT UND SCHUTZ

Geschäftliche Anforderungen

- Reduzierung des Risikos interner Datensicherheitsprobleme

Technische Anforderungen

- Sichere Root-of-Trust für CA-Server zu angemessenen Kosten

Lösung

- Entrust nShield Solo HSMs

Resultat

- Risikoreduzierung
- Sicherheit für das Zerto-Management

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

Kontakt:
HSMinfo@entrust.com