

GLOBALER ZAHLUNGSDIENSTLEISTER ERREICHT EINHALTUNG VON PCI-VORSCHRIFTEN UND SCHÜTZT DIE DATEN SEINER KUNDEN DURCH TOKENISIERUNG

Dieser amerikanische multinationale Zahlungsdienstleister (PSP) unterhält eines der fortschrittlichsten und flächendeckendsten Zahlungsverarbeitungsnetzwerke der Welt. Er verwaltet sicher die privaten Daten von Milliarden von Kredit- und Debitkarten und verarbeitet Zehntausende von Zahlungstransaktionen pro Sekunde. Dieses riesige Hochgeschwindigkeitsnetz ermöglicht elektronische Geldtransfers von fast 50 Millionen Händlerstandorten, über eine Million Geldautomaten und mehr als 15.000 Finanzkunden auf allen Kontinenten der Welt, mit Ausnahme der Antarktis. Bei einem so großen Netz, das ein so immenses Transaktionsvolumen verwaltet, ist es von entscheidender Bedeutung, dass die Daten sicher und dennoch schnell zwischen Plattformen im gesamten Netz fließen können.

HERAUSFORDERUNGEN

Der Schutz der privaten Daten, die mit über einer Milliarde Karten verbunden sind, ist eine große Herausforderung. Diese Milliarden von Karten enthalten nicht nur Unternehmensdaten, sondern auch die privaten Daten von Einzelpersonen. Die Wahrscheinlichkeit ist groß, dass Sie persönlich mindestens eine dieser Karten besitzen oder benutzen.

Da es so viele Akteure gibt, ist dieses Netz ein interessantes Ziel für Cyberangriffe. Im Falle einer Datenpanne können die persönlichen und finanziellen Daten von Millionen von Menschen gefährdet sein. Ein Verstoß kann auch für das betroffene Unternehmen katastrophale Folgen haben, da die Kunden nicht mehr darauf vertrauen, dass ihre Daten ordnungsgemäß behandelt werden. Dies kann das Image eines Unternehmens auf Jahre hinaus schädigen. In einer solchen Situation kann die Bedeutung des Datenschutzes nicht hoch genug eingeschätzt werden.

Deshalb wird jede Transaktion geschützt und anhand von Hunderten von Variablen und Parametern zur Betrugserkennung überprüft. Aber selbst mit einem hochmodernen und vielschichtigen Sicherheitssystem ist es einfach nicht möglich, jede Lücke in einer komplexen Netzarchitektur mit Tausenden von Verbindungen zu Partnern in der ganzen Welt zu schließen. Die vielen Datenschutzverletzungen, die in den letzten Jahren Schlagzeilen gemacht haben, sind ein Beweis dafür.

Im Bewusstsein der Unzulänglichkeiten herkömmlicher Ansätze für die Datensicherheit verlangte dieser PSP, dass die Daten im Ruhezustand geschützt werden, um die Auswirkungen von Sicherheitsverletzungen zu minimieren. Die Lösung sollte sicherstellen, dass im Falle einer Datenschutzverletzung die kompromittierten Daten für den Angreifer unbrauchbar sind. Da das Unternehmen große Mengen an Kundendaten aus der ganzen Welt verwaltet, muss die Lösung auch Branchenstandards und Vorschriften wie GDPR und PCI DSS erfüllen. Mit der Autorisierung von Zehntausenden von Transaktionsnachrichten pro Sekunde sind die Anforderungen an eine Datenschutzlösung außergewöhnlich hoch. Erstens sind Leistung und Durchsatz geschäftskritisch und dürfen nicht beeinträchtigt werden, da sich andernfalls Verzögerungen exponentiell über das Netzwerk ausbreiten und das Transaktionsvolumen stark reduzieren könnten. Und zweitens sind die Ausfallsicherheit des Netzwerks und die Fehlertoleranz von zentraler Bedeutung, denn jede Sekunde Ausfallzeit würde bedeuten, dass Zehntausende von Transaktionen nicht autorisiert werden könnten. Schließlich muss der PSP Daten zwischen vielen verschiedenen Plattformen austauschen, was eine flexible Lösung unerlässlich macht.

Kurzum, das Unternehmen benötigte eine umfassende Lösung, die die Benutzerdaten angemessen verschlüsselt, die Netzwerkleistung nicht beeinträchtigt und den Branchenstandards entspricht.

KURZ & BÜNDIG

comforte hat es einem der weltweit größten PSPs ermöglicht, die sensiblen Daten von Milliarden von Karten zu schützen und damit die Einhaltung von Datenschutzstandards wie PCIDSS und GDPR zu erreichen.



Wir brauchen eine Lösung, die die Lücke zwischen einem Weltklasse-Produkt, das einfach nur eine gehärtete Sicherheitslösung bietet, und einem Weltklasse-Produkt, das die gesamte Palette an Sicherheits-, Anwendungstransparenz- und Betriebsfaktoren berücksichtigt, schließt. Das Gesamtpaket ist weitaus entscheidender als die bloße Bereitstellung von starker Sicherheit.

– Projektleiter



LÖSUNG

Um die Daten seiner Kunden zu schützen und die Datenschutzanforderungen zu erfüllen, beschloss das Unternehmen, proaktiv zu handeln und nach einer bewährten Datenschutzlösung zu suchen. Man erkannte schnell, dass man die Daten im Ruhezustand schützen muß. Bevor das Unternehmen mit der Suche nach Anbietern begann, wurde bereits eine Geschäftsstrategie aufgestellt. Die Initiative begann auf höchster Unternehmensebene mit der Anweisung, eine unternehmensweite Datenschutzlösung zu finden. Die Tokenisierung erwies sich schnell als die am besten geeignete Lösung, da sie sensible Daten schützt, indem sie sie für potenzielle Angreifer unlesbar macht.

Wie bereits erwähnt, bedeutete das hohe Verarbeitungsvolumen des Netzwerks, dass die Leistung der Lösung ein Hauptaugenmerk war. Das Unternehmen führte Leistungstests zwischen konkurrierenden Tokenisierungslösungen durch und stellte fest, dass SecurDPS von comferte alle anderen Lösungen übertraf.

“*Der Kontrast zwischen dem umfassenden Gesamtpaket von comferte und der eingeschränkten, sicherheitsorientierten Lösung Ihrer Mitbewerber ist sehr groß. Wir haben die Vorteile Ihrer Lösung in Bezug auf Sicherheit und Geschwindigkeit erkannt.*

– Projektleiter

Auch die Ziele der Ausfallsicherheit und Fehlertoleranz wurden erreicht. Selbst im Falle von Online-Konfigurationsänderungen bleibt das System betriebsbereit.

Die modulare Architektur und die Kompatibilität mit Tokenisierungs-Engines von Drittanbietern ermöglichen eine transparente Integration, die nur eine geringe Spur in der IT-Landschaft hinterlässt. Ein weiterer Faktor, der eine reibungslose Implementierung ermöglichte, war die Tatsache, dass das Unternehmen eine Dokumentation aller seiner bestehenden Systeme führte. Diese Voraussicht erwies sich in jeder Phase des Projekts als sehr hilfreich, vom Entwurf der Lösung bis hin zu den Tests und schließlich der Einführung der Lösung.

VORTEILE

Das Unternehmen hat eine Lösung implementiert, die dazu beiträgt, eine seiner Kernaussagen zu erfüllen, nämlich sowohl Käufern als auch Verkäufern die Möglichkeit zu geben, Zahlungen zu senden und zu empfangen, wo und wann immer sie wollen, mit der Gewissheit, dass ihre Daten sicher sind. Die Endnutzer können weiterhin ihre Geschäfte tätigen, in dem Wissen, dass ihre Daten selbst im seltenen Fall einer Datenschutzverletzung geschützt sind.

Darüber hinaus wurde auch die Netzwerkkonnektivität nicht beeinträchtigt, sodass die Kunden die gleiche Geschwindigkeit und Zuverlässigkeit genießen können wie bisher. Damit erfüllt das Unternehmen sein Versprechen von Transaktionen "überall und jederzeit". Die Entscheidung in den Datenschutz zu investieren, wurde auch durch spezifische Anfragen von Großkunden und gesetzliche Anforderungen wie PCI DSS motiviert. Nach der Einführung erhielten diese Kunden eine Demonstration der neuen Sicherheitsmaßnahmen und waren mehr als zufrieden.

Vor der Entscheidung für einen Anbieter, hatte der Kunde bereits einen Geschäftsplan erstellt und die ungefähren Gemeinkosten für dieses System berechnet. Gemeinsam waren wir in der Lage, eine Lösung zusammenzustellen, die nicht nur alle technischen Anforderungen erfüllte, sondern auch günstiger war als erwartet. Wir sind der Meinung, dass Datensicherheit nicht die Bank sprengen sollte, und diese Lösung hat dies sowohl im wörtlichen als auch im übertragenen Sinne bewiesen.

“*Wir wissen die Unterstützung, die wir erhalten haben, sehr zu schätzen. Dank des Rollout-Managements und des Supports, der 24 Stunden am Tag für uns bereitsteht, konnten wir alle unsere Termine einhalten. Und jeder, mit dem wir gesprochen haben, verfügt über das technische Know-how, das wir erwartet haben, und ist mit unseren Hochverfügbarkeitssystemen bestens vertraut. Wir sind sehr zufrieden mit comferte.*

– Projektleiter



PROJEKTZIELE

- ▶ Einhaltung der PCI DSS und GDPR Vorschriften
- ▶ Schutz der Kundendaten
- ▶ Erfüllung der Anforderungen von Schlüsselkunden
- ▶ Verringerung der Auswirkungen von Datenschutzverletzungen
- ▶ Erhaltung der Netzwerkleistung

SCHREIBEN SIE IHRE EIGENE ERFOLGS-GESCHICHTE MIT COMFERTE

Mit mehr als 25 Jahren Erfahrung in der Datenschutz auf wirklich geschäftskritischen Systemen ist comferte der perfekte Partner für Unternehmen, die ihr wertvollstes Gut schützen wollen: Daten. comferte's Data Protection Suite, SecurDPS, wurde von Grund auf entwickelt, um die Datensicherheit in einer Welt zu gewährleisten, die von digitalen Geschäftsinnovationen, mündigen Kunden und ständigen technologischen Umwälzungen geprägt ist.

Wir sind für Ihren Erfolg da. Wir bieten Ihnen unser Fachwissen, eine innovative Technologie-Lösung und lokalen Support. Um mehr zu erfahren, sprechen Sie noch heute mit Ihrem comferte-Vertreter und besuchen Sie www.comferte.com.