CASE STUDY

GROSSE INDISCHE BANK IMPLEMENTIERT DATENZENTRIERTE SICHERHEIT UND ERFÜLLT PCI-DSS-ANFORDERUNGEN

Eine der größten Banken Indiens mit Hunderten von Millionen Kunden an Tausenden Standorten hat datenzentrierte Sicherheit eingeführt. Das Unternehmen arbeitet im Rahmen seiner Finanzgeschäfte und Unternehmensziele in großem Umfang mit PANs (persönlichen Kontonummern) und anderen Arten personenbezogener Daten. Ein Großteil dieser Daten ist gemäß PCI DSS als sensibel einzustufen und erfordert einen entsprechenden Schutz. Ohne angemessene Sicherheit bestand für dieses große Finanzdienstleistungsunternehmen das Risiko der Nichteinhaltung der Compliance-Anforderungen, was zahlreiche finanzielle und rechtliche Konsequenzen hätte nach sich ziehen können.

HERAUSFORDERUNGEN

Dieses Finanzdienstleistungsunternehmen hat mehr als 100 Millionen Kunden und setzt alles daran, seine Kunden bestmöglich zu bedienen. Die Herausforderung besteht jedoch darin, Trends, Muster und Erkenntnisse über die verschiedenen Kundengruppen genau zu verstehen. Die richtige Analyse von Kundendaten ist daher von entscheidender Bedeutung, wenn es darum geht, Erkenntnisse für strategische Geschäftsentscheidungen zu gewinnen. Dabei stand die Bank jedoch vor dem Problem, dass viele der für die Analyse verwendeten Daten wie beispielsweise PINs, Kundennamen und Track2-Zeichen gemäß den PCI DSS (Payment Card Industry Data Security Standards), die von der indischen Zentralbank für alle Finanzinstitute vorgeschrieben sind, als sensibel eingestuft sind.

Das Unternehmen arbeitet in verschiedenen Datenumgebungen, die in den Geltungsbereich von PCI fallen. Für das OLTP (Online Transaction Processing) setzt die Bank z. B. den beliebten Payment Switch BASE24 ein, der von ACI Worldwide bereitgestellt wird. Darüber hinaus nutzt die Bank auch die Datenreplikationslösung Golden Gate von Oracle für ihre Produktionsumgebung. Für diese Anwendungen schreibt die indische Zentralbank vor, dass Transaktionsprotokolldateien, POS-Transaktionsprotokolldateien, Host-Schnittstellenprotokolldateien, Kundenautorisierungsdateien, Host-Schnittstellenspeicher- und -weiterleitungsdateien und Geldautomatenprotokolldateien PCI-DSS-konform sein müssen. Das Hauptproblem bestand jedoch darin, dass das Unternehmen Speichersysteme verwendete, die primäre Kontonummern, Kreditkartennummern und andere Finanzinformationen mit spezifischen Bankidentifikationsdaten enthielten, wodurch die Einhaltung der gesetzlichen Compliance-Standards erschwert wurde.

„Durch die Zusammenarbeit mit comforte und die Implementierung der Datensicherheitslösung von comforte konnten wir unsere Organisation stark verbessern. Mit der Tokenisierung waren wir in der Lage, unsere Sicherheit zu optimieren und gleichzeitig die Herausforderungen der PCI Compliance zu meistern. Nun verfügt unser Unternehmen über die richtige Sicherheitstechnologie, um sensible Daten effektiv zu verwalten und unsere Sicherheitsinitiativen voranzutreiben." – Hauptgeschäftsführer einer großen indischen Bank im öffentlichen Sektor.

UNTERNEHMENSZIELE

- Erreichen der PCI-Compliance
- Schutz von Karteninhaberdaten
- Verbesserung von Sicherheitsmaßnahmen

WACHSTUM SICHERN MIT COMFORTE

Comforte verfügt über mehr als 20 Jahre Erfahrung im Bereich Datenschutz für unternehmenskritische Systeme und ist der perfekte Partner für Unternehmen, die ihr wertvollstes Gut schützen müssen: ihre Daten. Die Datensicherheitssuite SecurDPS von comforte wurde von Grund auf so konzipiert, dass sie den Anforderungen an die Datensicherheit in einer Welt gerecht wird, die von digitalen Business-Innovationen, anspruchsvollen Kunden und permanenten technologischen Herausforderungen geprägt ist. Mit unserem Fachwissen, unserer innovativen Technologie und unserem lokalen Support helfen wir Ihnen, Ihr Wachstum zu sichern.
Nehmen Sie noch heute Kontakt mit unseren comforte Experten auf, um mehr zu erfahren:
comforte.com/contact

LÖSUNGEN

Um den Herausforderungen im Umgang mit sensiblen Daten zu begegnen, benötigte diese Bank eine Datenschutzlösung mit den notwendigen Funktionalitäten, wie z. B. formatbewahrende Tokenisierung, Remote File Support, umfassendes Key Management, granulare Zugriffskontrolle und Auditing sowie nahtlose Interaktion mit Disaster-Recovery-Lösungen, um den besten Schutz der persönlichen Daten im Hinblick auf die PCI-Compliance zu gewährleisten. Das Unternehmen entschied sich daher für SecurDPS Nonstop von comforte, um dieser Herausforderung gerecht zu werden. Diese Lösung von comforte konnte transparent in die BASE24-Anwendung integriert werden, ohne dass Änderungen am Quellcode erforderlich waren. Die Implementierung wurde innerhalb von zwei Monaten ohne Unterbrechung der strategischen Abläufe abgeschlossen. Mit diesem Verfahren war comforte in der Lage, alle PANs, Kundennamen, Track2-Zeichen und anderen sensiblen Daten zu tokenisieren, was die Risiken der Nichteinhaltung von Vorschriften erheblich reduzierte. Auf diese Weise konnten alle Stakeholder, die für die datengesteuerten Prozesse und die Entscheidungsfindung verantwortlich sind, ihre Arbeit wie gewohnt fortsetzen.

VORTEILE

Mit der Einführung von SecurDPS Nonstop konnte die Bank ihr HPE Nonstop-System durch die erfolgreiche Tokenisierung sensibler Daten erheblich verbessern. Durch das Erreichen der PCI-Zertifizierung konnten Strafzahlungen in Höhe von bis zu 500.000 US-Dollar pro Vorfall sowie andere Verluste durch Betrug mit primären Kontonummern im Falle einer Kompromittierung oder eines Datenverstoßes vermieden werden. Das Unternehmen konnte das Vertrauen seiner Kunden durch den Schutz personenbezogener Daten weiter festigen und verfügt damit über eine solide Grundlage für weiteres Wachstum und Expansion. Künftig kann die Bank primäre Kontonummern, Kundennamen, Track2-Zeichen und andere sensible Datenelemente, die in den Anwendungen BASE24 und Golden Gate anfallen, angemessen schützen und gleichzeitig die Compliance-Vorgaben erfüllen.

> *Durch die Zusammenarbeit mit comforte und die Implementierung der Datensicherheitslösung von comforte konnten wir unsere Organisation stark verbessern. Mit der Tokenisierung waren wir in der Lage, unsere Sicherheit zu optimieren und gleichzeitig die Herausforderungen der PCI Compliance zu meistern. Nun verfügt unser Unternehmen über die richtige Sicherheitstechnologie, um sensible Daten effektiv zu verwalten und unsere Sicherheitsinitiativen voranzutreiben.*
>
> *Hauptgeschäftsführer einer großen indischen Bank im öffentlichen Sektor*