CASE STUDY

MERCURY PROCESSING SERVICES INTERNATIONAL SICHERT WACHSTUM MIT DSGVO- UND PCI-KONFORMEM DATENSCHUTZ

Mercury Processing Services International ist ein Dienstleister im Zahlungsverkehr mit Sitz in Kroatien und Slowenien. Das Unternehmen betreut über 5,6 Millionen Konten im Finanz- und Bankensektor in Europa, dem Nahen Osten und Afrika und verarbeitet durchschnittlich 1,5 Millionen Transaktionen pro Tag. Technologische Expertise ist der wichtigste Faktor für den Ausbau und die Vertiefung von Geschäftsbeziehungen sowie die Hauptquelle für Innovationen in der Zahlungsbranche.

HERAUSFORDERUNG: PCI- UND DSGVO-KONFORMER DATENSCHUTZ

Ausgangspunkt des Projekts war die PCI-Anforderung zum Schutz von Karteninhaberdaten. Später wurde das Projekt auf den Schutz zusätzlicher Datenelemente ausgeweitet, um die Anforderungen der DSGVO zu erfüllen.

GemäßPCI-Anforderung3.4müssenKarteninhaberdatenunlesbargemachtwerden, egal wo sie gespeichert sind. Karteninhaberdaten sind per Definition primäreKontonummern(PAN)undalleDaten,diedirektmiteinerbestimmtenPAN verknüpft werden können, wie z. B. der Name des Karteninhabers.

Die Anforderungen der DSGVO gehen noch einen Schritt weiter, da sie einen ähnlichen Schutz für personenbezogene Daten vorschreiben. Personenbezogene Daten sind wesentlich weiter gefasst als Karteninhaberdaten und werden als alle jene Daten definiert, die zu einer tatsächlichen Person zurückverfolgt werden können, einschließlich Name, Adresse, Nationalität, biometrische Daten usw.

DSGVO und PCI DSS fordern außerdem, dass sensible Daten innerhalb der Organisation und ihrer Partner nur nach dem Need-to-know-Prinzip, also bei tatsächlichem Bedarf sichtbar sein dürfen. Das bedeutet, dass sie auch innerhalb der Organisation unlesbar gemacht werden müssen, um zu verhindern, dass sie versehentlich von Insidern und Partnern eingesehen werden.

Mercury brauchte eine Lösung, die all diese Arten von Daten nicht nur im Hinblick auf die Compliance-Anforderungen richtig schützt, sondern auch, um eine weitere Schutzebene zu etablieren, mit der die Daten für potenzielle Hacker unbrauchbar werden. Hacker entwickeln ständig neue Methoden, um in Systeme einzudringen. Daher ist eine datenzentrierte Lösung das Herzstück der Datensicherheitsstrategie eines Unternehmens, damit die Daten, auf die zugegriffen wird, im Falle einer Datenschutzverletzung keinen verwertbaren Nutzen haben.

KERNMERKMALE

- Zahlungsabwickler, der täglich 1,5 Millionen Transaktionen abwickelt, erfüllt jetzt die Anforderungen an die PCI- und DSGVO-Datensicherheitsstandards, indem alle sensiblen Daten unlesbar gemacht werden.
- Effizienter Datenschutz ermöglicht Mercury die Verarbeitung noch größerer Transaktionsvolumina.
- Hochflexible und skalierbare Lösung, die schnell und einfach implementiert werden kann.

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.

LÖSUNG

Mercury entschied sich zum Schutz seiner Daten für SecurDPS von comforte, da diese Lösung die Datenschutzanforderungen erfüllte und schnell und einfach implementiert werden konnte, ohne den Geschäftsbetrieb zu unterbrechen.

Datenzentrierte Sicherheit
SecurDPS reduziert das Geschäftsrisiko, da es sensible Daten durch einen Token-Wert ersetzt, der im Falle einer Offenlegung bedeutungslos ist. Eine datenzentrierte Sicherheitsstrategie schützt die Daten an sich, sodass diese selbst dann nicht verwendet werden können, wenn alle anderen Sicherheitsmaßnahmen versagen. Damit werden auch die PCI- und DSGVO-Anforderungen erfüllt, wonach keine sensiblen Daten auf zentralen Unternehmenskomponenten gespeichert werden dürfen. Zudem sind tokenisierte Daten vor einer versehentlichen Offenlegung durch unbefugte Insider und Dritte geschützt, da der Zugriff auf sie nur mit entsprechender Autorisierung möglich ist. Dadurch werden die Abhängigkeit von Ersatzkontrollen als vorübergehende Maßnahme zum Bestehen von Sicherheitsaudits verringert und die Anforderungen von PCI und DSGVO erfüllt, wonach sensible Daten nur nach dem Need-to-know-Prinzip zugänglich sein dürfen.

> *Der Markt für den digitalen Zahlungsverkehr wächst ständig und damit auch die Notwendigkeit, die Datensicherheit immer stärker zu berücksichtigen. Mercury hat es sich zur Aufgabe gemacht, der Entwicklung immer einen Schritt voraus zu sein. Daher haben wir eine weitere Sicherheitsebene geschaffen, um die Daten unserer Kunden zu schützen. Damit können wir unserer Aufgabe, zuverlässige Dienstleistungen sicher und verlässlich zu erbringen, noch besser gerecht werden.*
>
> *– Jasna Fumagalli, Compliance, Security and Risk Management Director bei MPSI*

Datenschutz ohne Hindernisse
Mercury verarbeitet durchschnittlich 1,5 Millionen Transaktionen pro Tag und suchte daher nach einer Lösung, die ohne Unterbrechung des Geschäftsbetriebs oder Beeinträchtigung der Service-Levels implementiert werden konnte. Die Tokenisierung sorgt für Datenschutz ohne die Leistungseinbußen einer klassischen Verschlüsselung, da das Format und der Nutzen der geschützten Daten erhalten bleiben, sodass Geschäftsanwendungen und Analysen mit Token und nicht mit sensiblen Daten im Klartext arbeiten können.

SecurDPS ist zudem äußerst flexibel und skalierbar und konnte daher ohne Änderungen am Quellcode implementiert werden. Dadurch konnte die Lösung nicht nur innerhalb von ein paar Wochen statt Monaten implementiert werden, sondern die Umsetzung erfolgte auch ohne Beeinträchtigung der Service Level.

> *Wir waren mit der Bereitschaft von comforte, auf unterschiedlichste Wünsche und Anforderungen von uns einzugehen, sehr zufrieden. Mit Engagement und großer Sorgfalt hat das comforte Team entscheidend zum Erfolg dieses Projekts beigetragen.*
>
> *– Giovanni Cetrangolo, Head of Strategic Projects and Innovation bei Mercury Processing Services International*

PROJEKTZIELE

- Erfüllung der wichtigsten Datensicherheitsstandards nach DSGVO und PCI DSS
- Verringerung des Risikos und der potenziellen Auswirkungen von Datenschutzverletzungen
- Schutz sensibler Daten für eine sichere Datenübertragung zwischen Insidern und Partnern
- Beibehaltung der Service

VORTEILE

Die Vorteile dieses Projekts gehen über die Erfüllung der PCI- und DSGVO-Anforderungen zum Datenschutz hinaus. Im unwahrscheinlichen Fall einer Datenschutzverletzung sind alle sensiblen Daten unlesbar und damit für die Hacker unbrauchbar. Dadurch werden die Konsequenzen möglicher Sicherheitsverletzungen erheblich reduziert.

Die Tokenisierung von Daten trägt außerdem dazu bei, das Wachstum von Mercury zu sichern, da es für das Unternehmen nun wesentlich einfacher ist, Daten mit Partnern und Kunden auszutauschen und sensible Daten gleichzeitig zu schützen. Das Unternehmen ist nicht mehr auf Ersatzkontrollen angewiesen und kann seine Geschäfte deutlich schneller abwickeln. Damit kann Mercury sich optimal auf dem schnell wachsenden Markt behaupten und seine Abwicklungsdienste mehr Kunden als je zuvor anbieten.

> *Comforte ist stolz auf seine langjährige Erfolgsbilanz bei der Bereitstellung von robusten und zuverlässigen Datensicherheitslösungen für Finanzdienstleister. Wir freuen uns sehr, Mercury dabei zu unterstützen, die Sicherheit der Daten und letztlich das Wachstum zu sichern.*
>
> *- Michael Deissner, CEO bei comforte*