comforte

CASE STUDY

PCI- UND DSGVO-DATENSCHUTZANFORDERUNGEN IM NETZWERK FÜR ZAHLUNGSVERARBEITUNG OHNE AUSFALLZEITEN ERFÜLLT

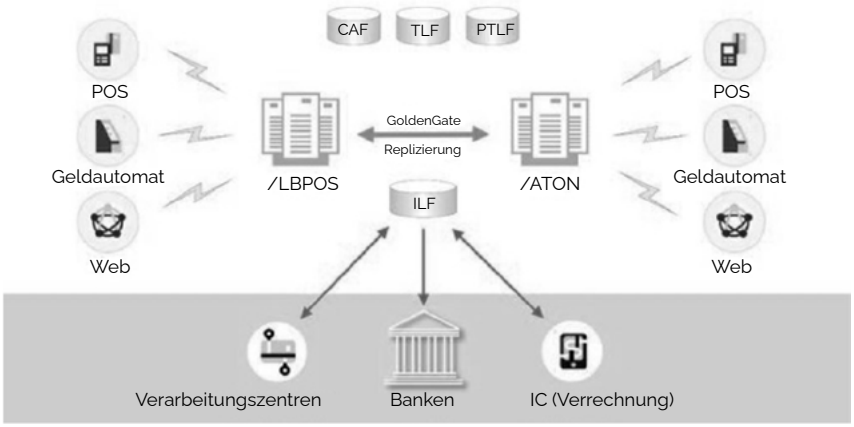
Bankart ist ein Verarbeitungszentrum für Kartenzahlungen mit Hauptsitz in Slowenien, das 23 Banken und andere Institutionen in sechs Ländern und in vier verschiedenen Währungen bedient. Bankart bietet seinen Kunden zuverlässige, sichere und kosteneffiziente Dienstleistungen für die Abwicklung von Transaktionen mit verschiedenen Bankzahlungsinstrumenten.

Mit seinem zentralen Autorisierungssystem (CAS) verarbeitet Bankart jeden Monat über 30 Millionen Geldautomaten-, POS-, Internet- und Mobil-Transaktionen auf Base24 Classic von ACI. Bankart kontrolliert und verwaltet auch die Geldautomaten- und POS-Netzwerke für die meisten der von ihm betreuten Institute. Neben der Zahlungsabwicklung und dem Netzwerkmanagement ermöglicht das CAS auch die Validierung von Karten und die Verifizierung von PINs. Sollte eine Bank aufgrund technischer Probleme nicht in der Lage sein, eine Autorisierung durchzuführen, übernimmt Bankart die Offline-Autorisierung für sie.

HERAUSFORDERUNG: PCI- UND DSGVO-KONFORMER DATENSCHUTZ

Das zentrale Autorisierungssystem von Bankart muss rund um die Uhr in Betrieb sein und wird daher auf hochverfügbaren HPE NonStop-Servern in einer Konfiguration mit zwei Standorten im aktiven Modus gehostet. Ein Teil der Daten wird auf Back-Office-Systeme repliziert, die auf Windows-Servern laufen. Beide Autorisierungsserver sind mit dem POS-Netzwerk, dem Geldautomaten-Netzwerk und den Web-Schnittstellen für Online-Transaktionen verbunden, die alle an die von Bankart bedienten Banken, andere Verarbeitungszentren und Vermittlungsstellen weitergeleitet werden. Zur Verwaltung dieser Daten müssen verschiedene Datenbanken, Dateien und Protokolle mit Karteninhaberdaten gepflegt werden.

Zentrales Autorisierungssystem (CAS) von Bankart



KERNMERKMALE

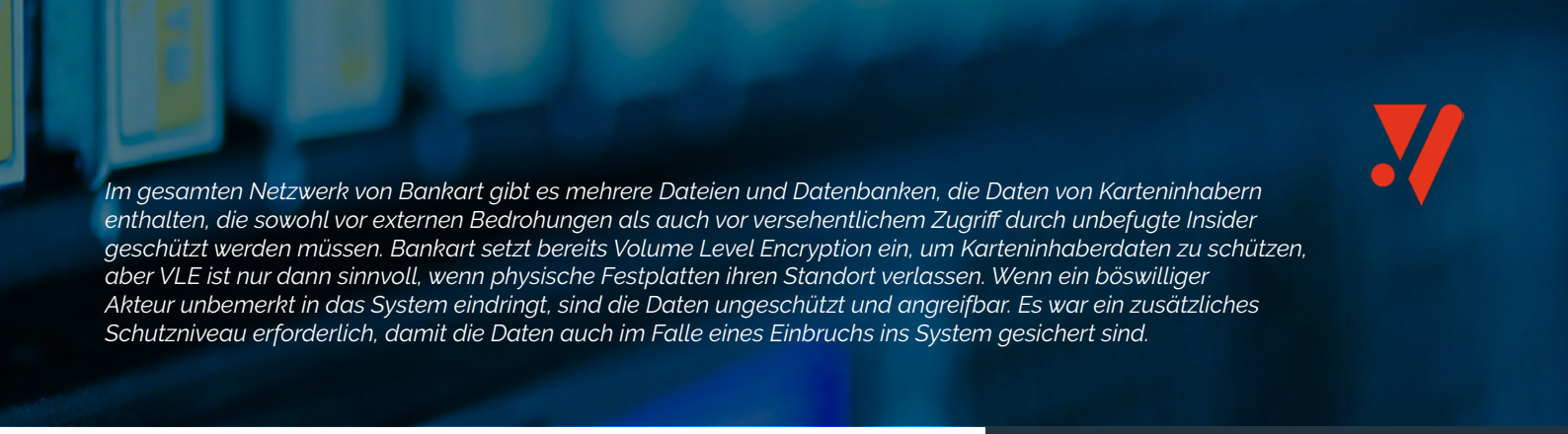
- Zahlungsverkehrsabwickler mit über 30 Millionen Transaktionen pro Monat.
- Erfüllt jetzt die PCI- und DSGVO-Anforderungen.
- Hochflexible und skalierbare Lösung, die schnell und einfach implementiert werden kann.

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



Im gesamten Netzwerk von Bankart gibt es mehrere Dateien und Datenbanken, die Daten von Karteninhabern enthalten, die sowohl vor externen Bedrohungen als auch vor versehentlichem Zugriff durch unbefugte Insider geschützt werden müssen. Bankart setzt bereits Volume Level Encryption ein, um Karteninhaberdaten zu schützen, aber VLE ist nur dann sinnvoll, wenn physische Festplatten ihren Standort verlassen. Wenn ein böswilliger Akteur unbemerkt in das System eindringt, sind die Daten ungeschützt und angreifbar. Es war ein zusätzliches Schutzniveau erforderlich, damit die Daten auch im Falle eines Einbruchs ins System gesichert sind.

ANFORDERUNGEN

Angesichts der komplexen Netzwerkkonfiguration und des hohen Dienstleistungsniveaus, das die Kunden erwarten, hatte Bankart sehr hohe Anforderungen an die Lösung, mit der die vom Unternehmen verwalteten Daten der Karteninhaber geschützt werden sollen:

- **Hohe Verfügbarkeit** – Integrierbar in ein Live-System ohne Ausfallzeiten und 24/7 verfügbar
- **Hochgradig konfigurierbar** – Vielfältige Systemkompatibilität auf Datei- und Datensatzebene
- **Einfache Integration** – Wenige oder keine Änderungen an Anwendungen oder Quellcode
- **Skalierbarkeit** – Erweiterbarkeit der Lösung auf andere Systeme innerhalb des Unternehmens sollte möglich sein
- **PCI- und DSGVO-Compliance** – Unlesbarmachen der Karteninhaberdaten, egal wo sie gespeichert sind

LÖSUNG

Bankart hat sich für SecurDPS von comforte entschieden, weil die Lösung alle oben genannten Anforderungen und noch mehr erfüllt. Die Lösung ließ sich in der komplexen IT-Umgebung von Bankart einfach und ohne Änderungen am Quellcode oder Ausfallzeiten implementieren. Sie bietet einen angemessenen Schutz der Karteninhaberdaten in Einklang mit den PCI- und DSGVO-Anforderungen. Außerdem handelt es sich um eine skalierbare, unternehmensweite Lösung, die später auf andere Systeme im Unternehmen erweitert werden kann.

Datenzentrierte Sicherheit

SecurDPS reduziert das Geschäftsrisiko, da es vertrauliche 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.

Datenschutz ohne Hindernisse

Bankart verarbeitet durchschnittlich 1,4 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 weniger Monate realisiert werden, sondern auch ohne Beeinträchtigung der Service Level.

> *Die gesamte Implementierung wurde im laufenden Betrieb durchgeführt, ohne dass die Partner oder Kunden von Bankart einen Unterschied in den Service Levels bemerkten.*
>
> *– Michael Deissner, CEO bei comforte*

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 Bankart 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 Bankart sich optimal auf dem schnell wachsenden Markt behaupten und seine Abwicklungsdienste mehr Kunden als je zuvor anbieten. Mit SecurDPS ist Bankart zudem in der Lage, kosteneffizienter zu arbeiten, da die Verschlüsselung auf Volumenebene überflüssig wird.

Dank der erfolgreichen Implementierung von SecurDPS konnten alle Projektanforderungen erfüllt werden und Bankart plant, die Lösung auf andere Systeme im Unternehmen auszuweiten.