



Zahlungen in
die Public Cloud
verlagern – mit
CGI All Payments

CGI

Nachhaltigkeit, Ressourcenflexibilität, reduzierte Kapazitätsplanung, optimierte Ausfallsicherheit, erhöhte Effizienz und geringere Kosten: Dies sind nur einige der vielversprechenden Vorteile einer Cloud für Banken – ganz unabhängig davon, ob es sich dabei um eine Private oder Public Cloud handelt.

Die Argumente, warum Banken ihre Rechenzentren durch Clouddienstleistungen ersetzen sollten, sind überzeugend. Im Rahmen unserer Kundenbefragung [CGI Voice of Our Clients](#) 2021 gaben dem entsprechend auch 60 % der 264 befragten Führungskräfte von Finanzinstituten an, dass sie im Laufe der nächsten zwei Jahre mindestens 21 % ihrer Anwendungen in die Cloud verlagern wollen.

Bei Datensätzen, die zu fast hundert Prozent aus personenbezogenen Informationen bestehen, wäre eine Kompromittierung mit schwerwiegenden Auswirkungen verbunden. Aus diesem Grund genießt Datensicherheit hier eine besonders hohe Priorität. Viele Banken sind der Ansicht, dass das Risiko bei Private Clouds geringer ist. Die meisten zögern, ihre Kernsysteme – oder „Kronjuwelen“, wie einer unserer Kunden sie nennt – in eine Public Cloud zu verlagern, da hier besondere Sicherheitsrisiken auftreten können.

Der Schutz wichtiger Daten und Systeme ist jedoch nicht der einzige Punkt, der Banken davon abhält, eine Public Cloud zu nutzen. Auch gesetzliche und regulatorische Anforderungen spielen eine große Rolle. Vor dem Hintergrund dieser Herausforderungen ist klar, dass die Verlagerung des Zahlungsverkehrs in die Public Cloud in einem sehr komplexen und fordernden Prozess verläuft.

Wir bei CGI unterstützen unsere Kunden seit vielen Jahren bei ähnlich gelagerten Projekten – zum Beispiel bei der sicheren Satellitensteuerung, der Bereitstellung sensibler verteidigungsrelevanter Daten, der innovativen Verarbeitung von Personalausweisen oder der Implementierung marktführender Zahlungssysteme.



Unsere neuesten Projekte in diesem Bereich finden dabei sowohl in der Private als auch in der Public Cloud statt. Um unseren Kunden bei der Bewältigung ihrer Herausforderungen zu helfen, setzten wir auf drei entscheidende Erfolgsfaktoren.



Plattform

eine bedarfsorientierte, unabhängige, multi-cloudfähige Zahlungsplattform



Erfahrung

umfassendes Know-how im Infrastruktur- und Anwendungsmanagement



Sicherheit

fortschrittliche Cloudsicherheit in Kombination mit einem soliden Risikomanagement

Jedes dieser Felder ist beherrschbar; alle drei miteinander zu verbinden, setzt eine starke Fokussierung und besonderes Engagement voraus. Durch die Kombination der Faktoren waren wir in der Lage, den Zahlungsverkehr unserer Kunden sicher und nahtlos in die Public Cloud zu verlagern.

Die richtige Plattform

Bei einer Migration in die Public Cloud besteht die große Herausforderung darin, dass die Technologie der Anwendung einen effizienten und sicheren Betrieb ermöglichen muss. Obwohl es technisch machbar ist, Mainframe-Anwendungen in die Cloud zu verlagern, wird dies selten praktiziert, da Mainframe-Anwendungen weder cloudfähig noch dazu in der Lage sind, die Vorteile der Cloud zu nutzen.

Wenn Kunden ihre Zahlungsinfrastruktur in die Public Cloud verlagern möchten, müssen sie zunächst die richtige Plattform finden – eine bedarfsorientierte, unabhängige, multicloud-fähige Lösung mit allen Vorteilen. Die Unabhängigkeit ist dabei ein entscheidender Faktor, wenn man die Risiken im Zusammenhang mit Cloudlösungen reduzieren möchte. Einige Dienstleister bemühen sich darum, der Herausforderung mit cloudfähigen Tools zu begegnen. Durch die Verwendung der entsprechenden Tools wird die Interoperabilität der Lösung jedoch eingeschränkt. Die Banken sind dann an eine spezifische gebunden und gehen inhärente Verpflichtungen ein (d. h. implizite Kosten für die Aktualisierung einer suboptimalen Technologie).

Im Jahr 2016 haben wir damit begonnen, unsere Zahlungsplattform CGI All Payments so umzugestalten, dass sie optimal den aufgeführten Anforderungen entspricht. Basierend auf einer Datenstruktur gemäß ISO 20022 ist die Plattform speziell auf Steuerung, Echtzeitverarbeitung und die Bereitstellung zertifizierter Netzwerk-Gateways ausgelegt. Sie unterstützt außerdem die Verarbeitung jeglicher Zahlungsarten rund um die Uhr. Dank dieser Umgestaltung erfüllt CGI All Payments alle Voraussetzungen, die ein zukunftssicherer Betrieb in der Private und der Public Cloud benötigt. So sind wir dem Markt einen Schritt voraus und unsere Kunden profitieren von einer hohen Ressourcenflexibilität, Resilienz und Verfügbarkeit sowie weiteren Vorteilen.

Da sich die Zahlungsprozesse weltweit stark verändern, handelt es sich hierbei um einen besonders wichtigen Faktor. Innerhalb der nächsten fünf Jahre muss nahezu jede Bank weltweit ISO 20022-basierte Zahlungen unterstützen, da die internationalen Infrastrukturen sukzessive dahingehend weiterentwickelt werden. Inländische, regionale und internationale Zahlungen in Echtzeit und rund um die Uhr sind in einigen Fällen bereits heute Realität. Immer mehr Banken erkennen die geschäftliche Notwendigkeit, sich auf die kommende Entwicklung vorzubereiten. Darüber hinaus hat die globale Pandemie erneut aufgezeigt, dass die Zahlungsinfrastruktur flexibler sein muss, als es mit Mainframes möglich ist. Eine sichere Remote-Implementierung und -Wartung sind dabei unverzichtbar.

Die richtige Erfahrung

Um Systeme in die Public Cloud migrieren zu können, benötigt man also zunächst einmal die richtige Plattform. Doch ebenso relevant ist die Erfahrung, die man für das sichere Implementieren in eine resiliente, selbstheilende Cloud-Umgebung benötigt. Nur eine umfassende Expertise und erprobte Prozesse – alles in Verbindung mit einem effektiven Risikomanagement – machen es möglich, Risiken, Kosten und Betriebsstörungen zu minimieren. Das richtige Know-how ist ebenso entscheidend wie die Auswahl der passenden Plattform und Zahlungslösung.

Vor der Migration in eine Public Cloud führen wir eine detaillierte Anforderungsanalyse durch (CGI Cloud Risk Assessment), um die relevanten Eckpunkte zu bestimmen (Warum? Was? Wann? Wie?). Dies erleichtert das proaktive Lösen von Problemen, erhöht die Effizienz und reduziert Risiken. Um die Phase erfolgreich abzuschließen, müssen Anforderungen, Probleme, Möglichkeiten, Machbarkeiten usw. offen und klar kommuniziert werden. Die Grundlage hierfür bildet eine vertrauensvolle Beziehung, die auf Ehrlichkeit und enger Zusammenarbeit basiert.

Darüber hinaus haben wir stabile Cloudprozesse entwickelt und in die Schulung und Zertifizierung unserer Mitarbeitenden investiert, um Banken bei der Prozessimplementierung optimal unterstützen zu können. In Schulungen zeigen wir Bankmitarbeitenden, wie die implementierte Plattform funktioniert, wie sie diese proaktiv überwachen



und Probleme angehen und beheben können. Diese Managementprozesse werden umfassend getestet und erweisen sich im Betrieb als äußerst effektiv.

2019 wurden wir der erste Global Transformation Partner im Rahmen des Scaled Agile Framework (SAFe). Dieser Entwicklungs- und Bereitstellungsansatz hat uns dabei geholfen, unsere Markteinführungszeiten zu verringern und gleichzeitig die Qualität zu verbessern. Unsere agilen Teams nutzen bei der Codeentwicklung unterschiedliche Umgebungen (z. B. Nicht-Produktion, Test, Vorproduktion, Produktion). Dadurch muss pro Release weniger Code geschrieben werden und Tests laufen schneller und effektiver. Mithilfe automatisierter Testverfahren können die Teams außerdem sicherstellen, dass notwendige Veränderungen keine negativen Auswirkungen auf bereits implementierten Code haben.

Die Anwendungen werden in einer bedarfsorientierten Umgebung implementiert, um die Vorteile der Public Cloud und des automatisierten Patching oder die Selbstheilungsfunktion von Kubernetes optimal zu nutzen. Dank der Datenverarbeitung rund um die Uhr und einer hohen Systemverfügbarkeit werden konventionelle Lösungen um ein Vielfaches übertroffen. Die Cloudresilienz reduziert die Wahrscheinlichkeit von Systemausfällen; die Prozessautomatisierung trägt dazu bei, die Wiederherstellungszeit bei Geolokalisierungsfehlern auf unter 30 Minuten zu senken.

Dieser Ansatz basiert auf jahrzehntelanger Erfahrung in der Bereitstellung von Application Managed Services (AMS) für Kunden auf der ganzen Welt. Unser Mitarbeiter erfüllen die erforderlichen Sicherheitsfreigaben und arbeiten nach dem „Least-Access“-Prinzip auf der Grundlage von transparent gestalteten Service Level Agreements. So setzen sie solide, aber einfache Steuerungsprozesse und ein äußerst effektives Änderungsmanagement um und gewährleisten eine hohe Effizienz, geringe Kosten und exzellente Qualität. Alle unsere Dienstleistungen werden gut und prüffähig dokumentiert und erfüllen so eine der Hauptvoraussetzungen der Bankenaufsicht im Hinblick auf externe Dienstleistungsvereinbarungen von Finanzinstituten.



Die richtige Sicherheit

Sicherheit ist ein wichtiges Thema für jede Zahlungsinfrastruktur, da es sich hierbei um Daten handelt, die im Falle einer Sicherheitsverletzung die Wirtschaft eines gesamten Landes bzw. einer Region lahmlegen könnten. Wenn personenbezogene Daten zusammen mit Zahlungsdaten in eine Public Cloud übertragen werden, müssen die Prozesse einer noch genaueren Prüfung standhalten. Wie bei allen neuen Technologien gilt: Wenn die tatsächlichen und subjektiv wahrgenommenen Risiken auf institutioneller Ebene nicht vollständig verstanden werden, ist dies nicht nur für die Aufsichtsbehörden ein Grund zur Sorge. Auch die Sicherheitsverantwortlichen innerhalb der Bank sehen darin ein erhebliches Risiko – trotz der offensichtlichen Vorteile und Steuerungsmöglichkeiten, von denen sie profitieren.

Die großen Anbieter von Public-Cloud-Lösungen – wie Microsoft Azure, Amazon AWS und Google Cloud Platform – haben bereits erheblich in die Sicherheit investiert. Die Härtung einer Umgebung fällt jedoch in den Verantwortungsbereich des für die Implementierung zuständigen Unternehmens. Es müssen Cloudsicherheitskontrollen festgelegt und korrekt angewandt werden,



um eine hohe Sicherheit zu gewährleisten und das Entstehen von Schwachstellen zu verhindern. Sicherheitskontrollen wie NIST 800 und das SWIFT Customer Security Controls Framework sind grundlegende Voraussetzungen für sichere Zahlungssysteme. Das Wissen, auf was es bei der Anwendung dieser Ansätze ankommt, ist daher essenziell.

Außerdem ist es entscheidend, die richtigen Sicherheitstools zu nutzen, die automatisch alle Ebenen scannen, den Quellcode analysieren, nach bekannten Schwachstellen von Drittprodukten suchen und das Konfigurieren der Laufzeitumgebung validieren. Auch dies reduziert Risiken, die mit der Einführung neuer Schwachstellen durch Codeänderungen, Umgebungskonfigurationen und Drittsoftware einhergehen.

Einige Sicherheitskontrollen sind dabei sehr kostspielig in der Umsetzung und Verwaltung, tragen aber nur geringfügig zur Risikoreduzierung bei. Unser Sicherheitsansatz bietet eine gute Balance zwischen Sicherheitsrisiken, dem Einfluss von Sicherheitskontrollen auf die Produktivität und den für die Verwaltung anfallenden Kosten.

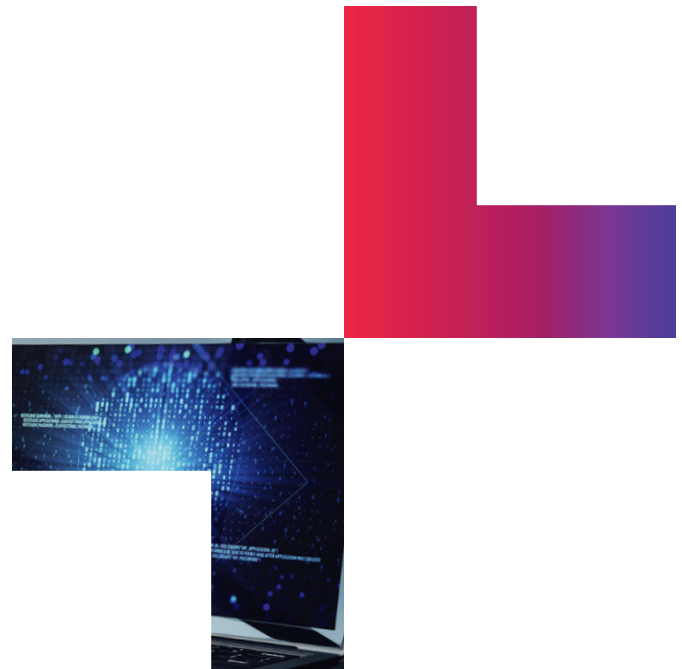
Mithilfe des Angriffsbaum-Modells (Attack Tree Modeling) lassen sich mögliche Bedrohungen und Angriffsvektoren ermitteln: eine weitere Voraussetzung für die Sicherheit von Public Clouds. Durch die Verwendung des Angriffsbaum-Modells kann den folgenden Sicherheitsbedenken bei Banken begegnet werden:

Größere Angriffsfläche, um Zahlungen zu fälschen oder Kundendaten auszuspähen: Diese Art von Angriffen kann nicht nur von Mitarbeitenden ausgeführt werden, die Zugang zu den Zahlungsverwaltungssystemen einer Bank haben, sondern bis zu einem gewissen Grad auch vom Cloud-Dienstleister der Bank. Zu den wichtigsten Sicherheitstools, um einen solchen Angriff zu verhindern, zählen:

- Multi-Faktor-Authentifizierung für alle Zugangsarten (z. B. Benutzer, Administrator)
- Verschlüsselung für den Schutz von Zahlungsdaten auf mehreren Ebenen (z. B. Data-at-rest-Verschlüsselung, Verschlüsselung während der Übertragung, digitale Signaturen)
- Trennung der Mitarbeiterverantwortlichkeiten
- Nutzung kontinuierlich überprüfter, privater Containerverzeichnisse und eingeschränkter Internetzugang von Laufzeitumgebungen

Größere Angriffsfläche, um die Serviceverfügbarkeit einzuschränken: Die bedeutendsten Sicherheitskontrollen in diesem Bereich sind Netzwerksperren, Schutz vor DDoS-Attacken, Drosselung und Zugangsbeschränkungen (auf wichtige Benutzer). Der Zugang kann durch ein privates virtuelles Netzwerk und/oder ein Site-to-Site-VPN für alle Standorte (z. B. Clouddienstleister und Bank) innerhalb einer hybriden Cloudumgebung eingeschränkt werden. Weitere Möglichkeiten für die Zugangsbeschränkung sind Jump Server, Verwaltungsserver oder die Einrichtung einer Virtual Desktop Infrastructure (VDI), in der die Installation von Software blockiert ist.

Unser Sicherheitsansatz ist es, quasi die richtige Rakete mit dem richtigen Brennstoff und den richtigen Sicherheitskontrollen zu kombinieren, um den Erfolg des Projekts zu gewährleisten. Mit dieser Philosophie legen wir in jedem einzelnen Projektschritt den Fokus auf Sicherheit – nicht ausschließlich vor dem Go-Live. Sicherheit ist fest



in unserem gesamten Prozess verankert und wird nicht erst zum Schluss und nur oberflächlich berücksichtigt. So reduzieren wir die Wahrscheinlichkeit, eine Schwachstelle zu übersehen oder versehentlich eine zu erzeugen.

Wir sind uns außerdem bewusst, dass Sicherheit nicht nur Technologien, sondern auch Prozesse und Menschen umfasst. Oft sind Menschen der Schwachpunkt in Sicherheitsfragen. Die Umsetzung eines umfassenden Sicherheitsansatzes mit bewährten Prozessen hilft dabei, das Sicherheitsbewusstsein der Benutzerinnen und Benutzer zu schärfen. Dadurch werden mögliche Angriffsvektoren verringert.

Zudem stellt die Einführung einer restriktiven Rechtevergabe ein effektives Werkzeug gegen interne und externe Sicherheitsbedrohungen dar. Eine Sicherheitsüberprüfung aller Mitarbeitenden verstärkt den Schutz vor Schwachstellen und ist eine gute Ergänzung zu den anderen Sicherheitsmaßnahmen.

Wir bringen alles unter einen Hut!

Unsere Kunden arbeiten bereits „live“ mit den Systemen und wickeln ihre Zahlungsprozesse über unsere behördlich genehmigte Public-Cloud-Lösung ab. Somit ist es uns gelungen, alle essenziellen Faktoren für den Projekterfolg zu kombinieren. In enger Zusammenarbeit mit unseren Kunden haben wir komplexe Probleme gelöst und ebnen für zukunftsorientierte Banken den Weg zu mehr Nachhaltigkeit, geringeren Kosten und einer effektiveren Ressourcennutzung. Damit entsprechen wir ganz ihren Anforderungen.

Für den Erfolg unserer Kunden verbinden wir die richtigen Komponenten mit unserer Expertise und vermeiden dabei potenzielle Risiken. Darüber hinaus lässt sich der von uns entwickelte Prozess gut reproduzieren. Wir rechnen damit, dass sich die Implementierung von Zahlungsinfrastrukturen in der Public Cloud in etwa einem Jahr als Standardverfahren durchsetzen wird.

Jetzt ist also genau der richtige Moment, mit uns zusammenzuarbeiten und so von den Vorteilen einer Public oder Private Cloud zu profitieren. Denn wir unterstützen unsere Kunden dabei, das Beste aus der von ihnen gewählten Cloud-Lösung herauszuholen. Auf www.cgi.com/de oder über info.de@cgi.com gibt es mehr zu diesem Thema zu erfahren.

Möchten Sie gemeinsam mit uns eine Strategie für Ihre Cloudmigration entwickeln? Wir freuen uns drauf!







Über CGI

Insights you can act on

Wir sind ein globaler Dienstleister für IT- und Geschäftsprozesse, verfügen über 78.000 Mitarbeitende weltweit und bieten seit 1976 strategische IT- und Business Beratung, Systemintegration, Managed IT, Business Process Services und Intellectual Property auf Top-Niveau. Unsere Teams richten sich konsequent an den Geschäftsstrategien unserer Kunden aus – dadurch finden wir optimale Lösungen entlang der gesamten Wertschöpfungskette und helfen Ihnen so, den ROI zu steigern.

Für weitere Informationen kontaktieren Sie uns unter info.de@cgi.com oder besuchen Sie uns auf www.cgi.com/de

