KUNDENGESCHICHTE

Zwei Banken. Eine Plattform. Keine Kompromisse.

Wie ein großes deutsches Institut die Verschlüsselung über souveräne Geschäftseinheiten hinweg zentralisierte

Technische Nachweise

Bereitstellungsmodell
AWS-nativ, Multi-Region: Irland + Deutschland

Datenresidenz
Daten werden innerhalb der jeweiligen Jurisdiktion gespeichert

Schlüsselmanagement
FIPS-140-3-validiertes Schlüsselmanagement

Verwaltung des Zertifikatslebenszyklus
DigiCert-automatisierter S/MIME-Lebenszyklus

DLP-Integration
Mimecast-DLP-Integration

Verschlüsselungspunkt
Gateway-Verschlüsselung ersetzt desktopbasierte ZIP-Dateien

Standardbasierte Formate
Native PDF-, Microsoft-Office- und ZIP-Formate

Zustellung ohne Portal
Zustellung per gemeinsam genutzter Passphrase

Zusammenfassung für Führungskräfte

In der DACH-Region wird kaum etwas so genau beobachtet wie der Umgang einer Bank mit den Daten, die sie überträgt. Deutschland, Österreich und die Schweiz haben einige der strengsten und am tiefsten verankerten Sicherheitserwartungen weltweit — Erwartungen, die regulatorisch festgeschrieben, durch Governance bekräftigt und in jeder Partner- und Kundenbeziehung spürbar sind. Für ein großes deutsches Finanzinstitut war die Erfüllung dieser Anforderungen kein Projekt, sondern eine dauerhafte Verpflichtung.

Gleichzeitig lief die Verschlüsselung der Bank am falschen Ort. Ein desktopbasiertes Totemo-System übernahm die sichere ZIP-Verschlüsselung direkt am Endpunkt, sodass sensible Dateien an den Hygiene-Scans und Backup-Kontrollen vorbeigingen, die in der Region gefordert werden. Hinzu kam: Das Institut war nicht ein einziger Käufer mit einem einheitlichen Bedarf. Die Hauptbank und ihre Investment-Sparte arbeiteten als eigenständige Organisationen — jeweils mit eigener Strategie, eigenen Anforderungen an die Datenresidenz und eigener Cloud-Vision.

Die Bank wandte sich an Echoworx, um beide Probleme gleichzeitig zu lösen: die Verschlüsselung vom Desktop in die Cloud zu verlagern und zwei sehr unterschiedliche Geschäftsbereiche mit den jeweils benötigten maßgeschneiderten Umgebungen auszustatten, ohne dabei in zwei voneinander getrennte Lösungen zu zerfallen.

Das Ergebnis: eine einheitliche, standardbasierte Verschlüsselungsplattform, die fragmentierte Kontrolle wieder zentral zusammenführte, strenge Anforderungen an die Datensouveränität über separate AWS-Regionen hinweg erfüllte und es jeder Geschäftseinheit ermöglichte, nach ihren eigenen Vorgaben zu arbeiten — alles unter einem Dach.

Die Herausforderung

01 | Verschlüsselung am falschen Ort.
Der endpointbasierte Ansatz der Bank für die sichere ZIP-Verschlüsselung wirkte zunächst praktisch, barg jedoch eine grundlegende Schwachstelle. Wenn Dateien von Desktop zu Desktop verschlüsselt werden, durchlaufen sie weder die unternehmensweiten Hygiene-Scans noch die Backup-Prozesse, die im DACH-Raum aus Compliance-Sicht als unverzichtbar gelten. Jede ZIP-Datei, die den Rechner eines Mitarbeitenden verließ, ließ damit auch die Governance der Bank hinter sich. Für ein Institut unter dieser regulatorischen Beobachtung ist sichere Kommunikation, die die eigenen Kontrollen umgeht, überhaupt nicht sicher — sondern eine Lücke, die nur darauf wartet, entdeckt zu werden.

02 | Eine manuelle Gewohnheit, die nicht zu einer modernen Bank passte.
Die Mitarbeitenden erledigten den Prozess von Hand: Dateien wurden zu ZIP-Paketen gebündelt, Passwörter gesetzt und diese Passwörter einzeln weitergegeben. So verbreitet dieses Muster auch heute noch ist — selbst in großen Organisationen —, es verließ sich darauf, dass Menschen jeden einzelnen Schritt fehlerfrei ausführen, und darauf, dass die IT die Desktop-Verschlüsselungssoftware im gesamten Unternehmen am Laufen hält. Die eigentliche Arbeit floss damit in die Aufrechterhaltung eines Workflows, statt den Weg der Bank in die Cloud voranzubringen.

03 | Ein Institut, zwei sehr unterschiedliche Anforderungen.
Die eigentliche Komplexität reichte weit über ein einzelnes Tool hinaus. Innerhalb derselben Bank hatten unterschiedliche Stakeholder und Geschäftsbereiche unterschiedliche Wege eingeschlagen. Die Hauptbank wollte eine Verschlüsselungslösung, die sauber in bestehende DLP- und Hygiene-Prozesse eingebunden ist und externen Kontakten eine möglichst mühelose Nutzung bietet. Ihre Investment-Sparte — der Bereich Finanzdienstleistungen — verfolgte dagegen ein völlig anderes Modell: cloud-first, cloud-only, auf S/MIME ausgerichtet und an strikte Datenresidenz innerhalb Deutschlands gebunden. Beide Einheiten hatten aus ihrer jeweiligen Perspektive gute Gründe. Die Herausforderung bestand darin, beiden gerecht zu werden, ohne die Kontrolle über die Verschlüsselung wieder in genau jene Silos aufzuspalten, aus denen die Bank herauswollte.

Die Lösung

Die Bank entschied sich genau deshalb für Echoworx, weil die Plattform zwei Strategien gleichzeitig tragen konnte — Sicherheit standardisieren und zugleich die Souveränität jeder Geschäftseinheit respektieren. Zusammengehalten wurde der gesamte Ansatz durch die Breite der Zustellungsoptionen: Dieselbe Plattform bot genügend Verschlüsselungsmethoden, um die Altsysteme beider Bereiche zu ersetzen — jeweils zu ihren eigenen Bedingungen.

„Zwei Geschäftseinheiten, zwei sehr unterschiedliche Vorstellungen — die eine wollte gemeinsam genutzte Passphrasen und ZIP-Verschlüsselung, die andere S/MIME über ihr eigenes DigiCert", erklärt Derek Christian, Engagement Manager bei Echoworx. „Unsere Aufgabe war es, beiden Anforderungen gerecht zu werden, die Daten jeder Einheit in ihrer jeweiligen Region zu halten und die fragmentierte Verschlüsselung wieder unter einem Dach zusammenzuführen — ohne dass eines der Teams seine bestehende Arbeitsweise aufgeben musste."

Digitale Souveränität entlang regionaler Grenzen.

Datenresidenz in der DACH-Region ist kein bloßes Häkchen auf einer Liste — sie ist eine Vorgabe, und sie kann sich von einer Geschäftseinheit zur nächsten unterscheiden. Echoworx begegnete dieser Anforderung mit AWS-Bereitstellungen, die gezielt auf einzelne Regionen abgestimmt sind. Die Hauptbank arbeitete aus einer AWS-Region in Irland, die ihren Anforderungen entsprach, während die Investment-Sparte, deren Daten innerhalb Deutschlands verbleiben mussten, in einer separaten Region in Deutschland betrieben wurde. Durch die Nutzung von AWS-Regionen und Availability Zones zur Verankerung jeder Umgebung stellte die Plattform sicher, dass die Daten jeder Einheit genau dort blieben, wo ihre Governance es verlangte. Souveränität bedeutete in der Praxis: Jede Einheit behielt die Kontrolle über ihre eigenen Daten — in ihrer eigenen Jurisdiktion.

Standardbasierte Verschlüsselung, vertraut für alle, die sie empfangen.

Echoworx sicherte Dateien in den Formaten, die externe Kontakte bereits kennen und denen sie vertrauen — PDF, Microsoft Office und ZIP. Nichts Proprietäres stand zwischen der Bank und ihren Partnern, sodass Empfänger weiterhin in den Abläufen arbeiten konnten, die sie bereits gewohnt waren. Für ein Institut, dessen Ruf auf reibungslosen und vertrauenswürdigen Austausch angewiesen ist, war standardbasiert keine technische Randnotiz. Es war der entscheidende Punkt.

Verschlüsselung zurück an das Gateway verlagert.

Die wichtigste Veränderung bestand darin, die Verschlüsselung vom Desktop an das Cloud-Gateway zu verlagern. Dort wurde sie direkt in genau jene Abläufe eingebunden, an denen sie zuvor vorbeigelaufen war — DLP, Hygiene-Scans und Backup —, sodass nun jede sichere Nachricht die Kontrollen durchläuft, die sie steuern sollen. Für die Investment-Sparte setzte sich diese Disziplin durch die langjährige Partnerschaft von Echoworx mit Mimecast für DLP fort und brachte eine cloud-first Sicherheitsarchitektur mit einer cloud-first Strategie in Einklang. Die Lücke wurde nicht durch zusätzliche Aufsicht geschlossen, sondern dadurch, dass die Verschlüsselung wieder dorthin zurückgebracht wurde, wo Aufsicht bereits verankert war.

Ein maßgeschneiderter Weg für die Hauptbank.

Die Hauptbank wollte Mitarbeitenden die Wahl des passenden Schutzes pro Nachricht ermöglichen. Dafür stellte Echoworx ein individuell entwickeltes Microsoft-365-Add-in mit zwei Optionen bereit: reine Anhangsverschlüsselung oder vollständige Nachrichtenverschlüsselung als passwortgeschützte PDF. Durch gemeinsam genutzte Passphrasen, die außerhalb des Kanals übermittelt wurden, war zudem eine portal-lose Zustellung möglich — genau das, was externe Partner oft bevorzugen. So konnten Empfänger geschützte Nachrichten direkt im Posteingang öffnen, ganz ohne Registrierung und ohne ein neues Passwort verwalten zu müssen.

Fortsetzung...

Ein maßgeschneiderter Weg für die Investment-Sparte.

Die Investment-Sparte hatte andere Anforderungen — und Echoworx erfüllte sie. Im Mittelpunkt stand S/MIME über das divisionseigene DigiCert-Abonnement. Echoworx automatisierte den gesamten Zertifikatslebenszyklus: Schlüsselerzeugung, Zertifikatsverwaltung, Signaturprüfung und das Signieren ausgehender Nachrichten. So blieb die volle funktionale Gleichwertigkeit zur bisherigen Totemo-Umgebung erhalten, und die Migration fühlte sich wie eine nahtlose Fortsetzung an. Fehlte einem Empfänger ein Schlüssel, griff automatisch ein sicheres Portal als Fallback ein, sodass keine Nachricht ungeschützt blieb. Und während die Hauptbank auf Wahlfreiheit setzte, entschied sich die Investment-Sparte für Einfachheit: ein Ein-Klick-Add-in — verschlüsseln oder nicht —, während das Routing im Hintergrund gesteuert wurde.

Die Ergebnisse

Verschlüsselung zurück unter Kontrolle.

Durch die Verlagerung der sicheren ZIP- und Anhangsverschlüsselung vom Desktop an das Cloud-Gateway durchläuft nun jede Nachricht die Hygiene-Scans und DLP-Kontrollen, die die DACH-Compliance verlangt — und schließt damit eine Lücke, die der endpointbasierte Ansatz weit offengelassen hatte.

Souveränität gewahrt — Einheit für Einheit.

Separate AWS-Bereitstellungen in Irland und Deutschland hielten die Daten jeder Geschäftseinheit innerhalb der jeweils geforderten Jurisdiktion und erfüllten so strenge Anforderungen an die Datenresidenz, ohne die Regeln der einen Division der anderen aufzuzwingen.

Zwei Strategien, eine Plattform.

Die Hauptbank und ihre Investment-Sparte betrieben jeweils das Verschlüsselungsmodell, das zu ihnen passte — portal-lose Zustellung per gemeinsam genutzter Passphrase auf der einen Seite, automatisiertes S/MIME auf der anderen — während das Institut gleichzeitig die zentralisierte, standardbasierte Kontrolle über beide zurückgewann.

Ein S/MIME-Lebenszyklus ohne manuellen Aufwand.

Die DigiCert-Integration automatisierte für die Investment-Sparte die Schlüsselerzeugung, das Erfassen von Zertifikaten und die Signaturprüfung, ersetzte damit die manuelle Schlüsselverwaltung und bewahrte zugleich die vollständige funktionale Gleichwertigkeit mit der zuvor eingesetzten Lösung.

Mühelos für die Menschen auf Empfängerseite.

Gemeinsam genutzte Passphrasen ermöglichten es den externen Kontakten der Hauptbank, sichere Nachrichten direkt im Posteingang zu öffnen — ohne Portal, ohne Registrierung — während standardbasierte Formate dafür sorgten, dass alle Empfänger in den Werkzeugen arbeiten konnten, denen sie bereits vertrauen.

Nichts blieb ungeschützt.

Ein automatisches Portal-Fallback gewährleistete die sichere Zustellung auch dann, wenn einem Empfänger kein Schlüssel vorlag, sodass ein fehlendes Zertifikat nie zu einem Sicherheitsrisiko wurde.

Migration im Takt jeder Einheit.

Beide Divisionen konnten sich von Totemo lösen, ohne die Gewohnheiten und Fähigkeiten aufzugeben, auf die ihre Mitarbeitenden angewiesen waren — funktionale Gleichwertigkeit für die Investment-Sparte, Flexibilität bei der Wahl der Methode für die Hauptbank.

Das große Ganze

Dieses Institut startete mit einem Platzierungsproblem — einer Verschlüsselung, die dort lief, wo Governance sie nicht erreichen konnte. Was daraus entstand, war jedoch etwas deutlich Dauerhafteres: eine zentralisierte, standardbasierte Grundlage, die die Unterschiede zwischen den Geschäftseinheiten nicht beseitigt, sondern bewusst respektiert.

Genau diese Unterscheidung bildet den Kern der Geschichte. In einer großen, regulierten Organisation ist der schwierigste Teil der Modernisierung selten die Technologie selbst — sondern der Umgang mit tatsächlich unterschiedlichen Anforderungen, ohne in einen Flickenteppich voneinander getrennter Werkzeuge zu zerfallen. Indem sich die Bank für eine Plattform entschied, die breit genug aufgestellt ist, um einer Sparte S/MIME und einer anderen eine portal-lose Verschlüsselung mit gemeinsam genutzter Passphrase zu bieten — und das jeweils in den erforderlichen Regionen —, verwandelte sie diese Komplexität in einen Vorteil. Dezentrale Kontrolle wurde zu zentraler Governance, ohne dass eine einzige Einheit die Autonomie verlor, die sie benötigte.

Echoworx macht genau das für Organisationen jeder Struktur möglich: vereinheitlicht dort, wo es darauf ankommt, souverän dort, wo es zählt, und durchgängig standardbasiert.

Bereit, Ihre Verschlüsselung zu vereinheitlichen, ohne dabei das einzuebnen, was Ihre Geschäftseinheiten voneinander unterscheidet?
Wenn desktopgebundene Verschlüsselung an Ihren Kontrollen vorbeiläuft oder unterschiedliche Divisionen Ihre Sicherheitsstrategie in verschiedene Richtungen ziehen, gibt es einen Weg, Governance zu zentralisieren und gleichzeitig den Anforderungen jeder einzelnen Einheit gerecht zu werden.
Sprechen Sie noch heute mit einem Echoworx-Experten.