

Wenn Compliance auf Benutzerfreundlichkeit trifft

Wie eine führende irische Geschäftsbank ihre sichere Kundenkommunikation transformierte

Technische Nachweise

Architektur

- AWS-native SaaS, durchgängig cloud-first
- Datenresidenz in Irland bzw. der EU, ausgerichtet an DORA und DSGVO
- Jährlich nach PCI DSS und SOC 2 auditiert, FSQS-registriert
- Keine Appliances, die installiert, gepatcht oder gewartet werden müssen

Kontrolle

- Sicheres Senden aus gemeinsam genutzten Postfächern mit optionalem Reply Routing
- Multi-Brand-Unterstützung über Muttergesellschaften und verbundene Geschäftseinheiten hinweg
- Gemeinsame Lizenzierung und Infrastruktur ohne doppelte Administration
- Richtliniengesteuerte Zustellung und Autorisierung über alle Kanäle hinweg

Zustellung

- Sichere Portalzustellung, PDF-, Anhangsverschlüsselung sowie TLS mit Fallback
- Self-Provisioning im Portal – keine initiale Push-E-Mail erforderlich
- Veröffentlichte URL für eingehende sichere Nachrichten
- Mehrere Authentifizierungsoptionen über alle Zustellungskanäle hinweg

Zusammenfassung

Für eine führende irische Geschäftsbank – gelistet unter den Top 1000 World Banks und anerkannt als digital ausgerichtetes Institut für Privat-, Geschäfts- und Firmenkunden – ist sichere Kommunikation keine reine Backoffice-Angelegenheit. Sie ist eine regulatorische Verpflichtung und ein Versprechen an jede Kundin und jeden Kunden.

Im Rahmen des Digital Operational Resilience Act (DORA) und der DSGVO benötigte die Bank eine Verschlüsselung, die auditierbar, resilient und souverän ist. Doch die vorhandenen integrierten Tools konnten mit den realen Workflows der Bank nicht Schritt halten. Das Ergebnis war Reibung – für Mitarbeitende, für Kundinnen und Kunden sowie für die Compliance-Teams, die verantwortlich sind, wenn sichere Kommunikation nicht ausreicht.

Durch die Partnerschaft mit Echoworx transformierte die Bank die Handhabung von Kundendokumenten in einen schlanken, sicheren und skalierbaren Prozess. Das Ergebnis war messbar und unmittelbar: eine Steigerung der Nutzung von Verschlüsselung um 63 %, ein einfacheres Kundenerlebnis und ein resilientes, cloud-natives Fundament, das darauf ausgelegt ist, selbst die anspruchsvollsten regulatorischen Anforderungen Europas zu erfüllen.

Die Herausforderung

Für eine Bank dieses Ranges ist sichere Kommunikation kein nachgelagertes Thema. Sie ist eine regulatorische Verpflichtung und ein tägliches Versprechen an jede Kundin und jeden Kunden.

Die Bank verwaltete sichere Kundendokumente über ein integriertes Verschlüsselungstool. Auf dem Papier erfüllte es grundlegende Anforderungen. In der Praxis verursachte es jedoch auf allen Ebenen Reibung – für Mitarbeitende, für Kundinnen und Kunden sowie für die Compliance-Teams, die verantwortlich sind, wenn etwas nicht den Anforderungen entspricht.

Die Hindernisse waren konkret und gravierend:

- 01 | Keine Unterstützung für gemeinsame Postfächer.**
Teambasierte Workflows, die über gemeinsame E-Mail-Adressen laufen, bilden das Rückgrat des Kundenservice-Modells der Bank und ihrer SLA-Zusagen. Das bestehende Tool konnte diese Anforderungen nicht abbilden.
- 02 | Mehrstufige manuelle Arbeitsabläufe.**
Die Absicherung eines einzelnen Kundendokuments erforderte mehrere manuelle Schritte und die Koordination zwischen Mitarbeitenden – das kostete Zeit und erschwerte die Einsatzplanung zusätzlich.
- 03 | Erzwungene Kundenregistrierung.**
Kundinnen und Kunden mussten sich bei einem verschlüsselten E-Mail-Dienst registrieren, nur um auf ihre eigenen Dokumente zuzugreifen und sie zurückzusenden – eine unnötige Hürde, die dem digital-first Anspruch der Bank widersprach.
- 04 | Operativer Mehraufwand.**
Ineffiziente Prozesse führten zu Ressourcenengpässen und zogen Teams von wertschöpfenderen Aufgaben ab.

Dabei handelte es sich nicht um geringfügige Unannehmlichkeiten. Für ein digital geführtes Institut mit ehrgeizigen Modernisierungszielen waren sie zugleich Compliance-Risiken und Schwachstellen im Kundenerlebnis.

Die Evaluierung

Die Bank hatte ihre Hausaufgaben gemacht. Sie ging mit einem klaren Verständnis in die Evaluierung, was konkurrierende Tools nicht leisten konnten.

Sie kam mit präzisen, konkreten Fragen – die wichtigste davon lautete: **Wie unterstützen Sie gemeinsame Postfächer?**

Darauf folgte ein rigoroser Proof of Concept. Die Bank suchte keine Versprechen. Sie wollte, dass jeder geschäftskritische Workflow demonstriert wird – unter der Maßgabe ihrer eigenen geschäftlichen, regulatorischen und regionalen Anforderungen, einschließlich Datenresidenz, Multi-Brand-Architektur sowie der Zertifizierungen, die ihre Compliance- und Security-Review-Teams voraussetzten.

Echoworx beantwortete jede Frage. Der Proof of Concept bestätigte genau das, was die Bank sehen musste: eine Plattform, die flexibel genug war, ihre konkreten Prozesse abzubilden, und ein Compliance-Fundament, das stark genug war, um ihre regulatorischen Anforderungen zu erfüllen.

Die Lösung

Echoworx stellte eine cloud-native Verschlüsselungsplattform bereit, die die operativen Herausforderungen der Bank löste und gleichzeitig regulatorische Compliance in den Mittelpunkt stellte.

„Diese Bank kam mit einer Compliance-Vorgabe und einem sehr spezifischen operativen Problem zu uns – und beides musste gemeinsam gelöst werden, nicht getrennt“, sagt Derek Christian, Engagement Manager bei Echoworx. „Die Frage nach dem gemeinsamen Postfach hat uns alles gesagt. Sie wussten genau, was sie brauchten, sie hatten bereits gesehen, was andere Tools nicht leisten konnten, und sie wollten den Nachweis – Workflow für Workflow, unter ihren eigenen regulatorischen und regionalen Anforderungen. Was wir gemeinsam aufgebaut haben, hat nicht nur ihre Compliance-Anforderungen erfüllt. Es hat ihnen auch ein Fundament gegeben, das auch dann Bestand hat, wenn sich die Verpflichtungen aus DORA und DSGVO weiterentwickeln, sowie eine Plattform, die sich kontinuierlich erweitern lässt, ohne zusätzliche Komplexität zu schaffen.“

Arbeitsabläufe, die der tatsächlichen Arbeitsweise der Bank entsprechen

Gemeinsame Postfächer und Antwort-Routing – Die kollaborativen Abläufe, die das vorherige Tool nicht unterstützen konnte, funktionieren jetzt reibungslos. Mitarbeitende senden sicher aus gemeinsamen Postfächern und leiten Antworten an eine andere Adresse als die Absenderadresse weiter. So wird echte teambasierte sichere Kommunikation ermöglicht, die den SLA-Anforderungen der Bank entspricht.

Geräteunabhängige sichere Nachrichtenerstellung – Mitarbeitende verfassen sichere Nachrichten und fügen Dateien auf jedem Gerät hinzu, ohne organisatorische Eingabeaufforderungen oder unnötige Unterbrechungen bestehender Prozesse.

Portal-Selbstregistrierung und eingehende sichere Kommunikation – Kundinnen und Kunden erhalten Zugang zu sicherer Kommunikation, ohne dass zunächst eine ausgehende Initial-E-Mail erforderlich ist. Die Registrierungsbarriere ist entfallen. Als die Bank diesen Ansatz später weiter ausbauen wollte – sodass Kontakte sichere Kommunikation vollständig zu ihren eigenen Bedingungen initiieren können – ermöglichte Echoworx eingehende sichere Kommunikation über eine veröffentlichte URL, die durch eine einfache Konfiguration aktiviert wurde, ohne dass ein neuer Beschaffungsprozess erforderlich war.

Fortsetzung...

Bereitstellung mehrerer Marken über eine einzige Plattform

Die Hypothekengruppe der Bank tritt unter einer eigenen, etablierten Partnermarke auf — klar von der Muttergesellschaft abgegrenzt und zugleich eng mit ihr verbunden. Echoworx unterstützt die Bereitstellung mehrerer Marken über Geschäftsbereiche hinweg mithilfe gemeinsamer Lizenzierung und gemeinsamer Infrastruktur, sodass die Bank Administrationsaufwand nicht über mehrere Umgebungen hinweg duplizieren muss.

Ein Compliance-Fundament, das darauf ausgelegt ist, Regulierungsbehörden, Auditoren und Architektur-Gremien zu überzeugen.

Hier zeigt sich die eigentliche Tiefe der Plattform.

Echoworx wird zu 100 % auf AWS betrieben und ist unabhängig als AWS Qualified Software anerkannt — geprüft anhand des AWS Well-Architected Frameworks in den Bereichen Sicherheit, Zuverlässigkeit und operative Exzellenz. Diese Validierung ist kein Marketingprädiat. Sie ist der strukturierte, unabhängige Nachweis, den Compliance-Teams, Sicherheitsarchitekten und Procurement-Verantwortliche benötigen, bevor sie grünes Licht geben können.

Die Ergebnisse

Die Auswirkungen waren messbar, unmittelbar und nachhaltig — sowohl in Bezug auf die Compliance-Positionierung als auch auf operative Effizienz und Kundenerlebnis.

Compliance wandelte sich von einem Druckpunkt zu einem nachweisbaren, dauerhaft belastbaren Zustand.

Da jede verschlüsselte Nachricht protokolliert, jeder Policy-Trigger erfasst und jeder Zustellstatus dokumentiert wird, kann die Bank Compliance im Audit nachweisen, statt sie erst kurzfristig belegen zu müssen. Anforderungen aus DORA und DSGVO werden nicht reaktiv verwaltet — sie werden fortlaufend und systematisch erfüllt.

63 % mehr Nutzung von Verschlüsselung — getragen von Vertrauen, nicht von Vorgaben.

Die Bank setzt Verschlüsselung nach dem Prinzip der situativen Anwendung ein und überlässt es den Absendern zu entscheiden, was wann verschlüsselt wird. Die Nutzung

echoworx.com

Jede verschlüsselte Kommunikation wird über Schlüsselerzeugung, Richtlinienauslöser und Zustellstatus hinweg protokolliert. Audit Readiness ist keine kurzfristige Kraftanstrengung, sondern ein dauerhafter Zustand. DORA verlangt auditierbare Wiederherstellung, hohe Verfügbarkeit und vollständige Auditierbarkeit der Kommunikationsinfrastruktur von Drittanbietern. Die DSGVO verlangt Kontrolle über die Datenresidenz, granulären Schutz und nachweisbare digitale Souveränität. Echoworx adressiert beides — gestützt auf jährliche PCI DSS- und SOC 2-Zertifizierungen sowie dokumentierte Prozesse, die die Bank sicher und zügig durch ihre Sicherheits- und Freigabeprüfung geführt haben.

Eine regionale Bereitstellung im Einklang mit irischen Anforderungen und der DSGVO stellt sicher, dass die Daten der Bank genau dort verbleiben, wo sie verbleiben müssen — nicht als Annahme, sondern als nachweisbare Tatsache, gestützt auf AWS-native Infrastruktur, die in der EMEA-Region einschließlich Irland validiert ist.

wuchs organisch. Einsatz, Volumen und Zahl aktiver Absender stiegen innerhalb kurzer Zeit deutlich an und entwickelten sich weiter positiv. Diese Dynamik zeigt, was passiert, wenn die zugrunde liegende Plattform resilient, compliance-konform und im Arbeitsalltag tatsächlich vertrauenswürdig ist.

Operative Reibungsverluste beseitigt.

Manuelle Schritte wurden entfernt, die Abstimmung zwischen Mitarbeitenden vereinfacht und die Registrierungsbarriere für Kundinnen und Kunden vollständig aufgehoben. Teams gewannen Zeit und Kapazität zurück, die zuvor durch Workarounds gebunden waren — und konnten diese Ressourcen wieder für wertschöpfendere Aufgaben einsetzen.

Fortsetzung...

Nahtloses, markengerechtes Kundenerlebnis.

Kundinnen und Kunden erhielten eine sichere und reibungslose Möglichkeit, sensible Dokumente auszutauschen – ohne unnötige Registrierung und ohne ungewohnte Nutzererfahrung. Verschlüsselte Kommunikation wirkt nun wie eine natürliche, vertrauenswürdige Erweiterung des Serviceangebots der Bank.

Eine Plattform, die mit dem Unternehmen wächst.

Da die Bank die vollständige Echoworx-Plattform lizenziert hat, wird jede neue Anforderung per Konfiguration aktiviert – nicht durch neue Vertragsverhandlungen. Die Zusammenarbeit entwickelt sich kontinuierlich weiter, und die sichere Kommunikation bleibt agil genug, um mit der Geschwindigkeit des Geschäfts Schritt zu halten.

Das Gesamtbild

Diese Bank hatte sich vorgenommen, ein Tool zu ersetzen, das mit ihren Anforderungen nicht mehr Schritt halten konnte. Was sie stattdessen aufgebaut hat, ist weit belastbarer: eine cloud-native, an DORA und DSGVO ausgerichtete Plattform für sichere Kommunikation, die operative Reibungsverluste beseitigt, Compliance in einen dauerhaft belastbaren Zustand überführt und verschlüsselte Kommunikation zu etwas macht, das Mitarbeitende und Kundinnen und Kunden tatsächlich nutzen möchten.

Das ist die eigentliche Lehre aus diesem Beispiel. Für ein digital geführtes Institut besteht die größte Herausforderung der Modernisierung nur selten darin, etwas Neues hinzuzufügen – sondern vielmehr darin, Defizite zu beseitigen, ohne Bewährtes zu stören, und dabei jeden Schritt gegenüber Regulierungsbehörden und Auditoren nachweisen zu können. Indem sich die Bank für einen Partner entschieden hat, der ihre operativen Anforderungen präzise erfüllen, einer umfassenden Compliance-Prüfung standhalten und sich ohne Neuverhandlung weiterentwickeln konnte, verwandelte sie ein schmerzhaftes Tooling-Problem in ein resilientes, zukunftssicheres Fundament.

Echoworx macht genau das möglich: systematisch compliance-konform, resilient im großen Maßstab und darauf ausgelegt, gemeinsam mit den Institutionen zu wachsen, die darauf angewiesen sind.

Ist Ihre sichere Kommunikation bereit für das, was als Nächstes kommt?

Wenn integrierte Verschlüsselung Ihre Compliance-Positionierung ausbremst, Reibung für Mitarbeitende und Kundinnen und Kunden erzeugt oder zwischen Ihrem Institut und dem nächsten Modernisierungsschritt steht, gibt es einen besseren Weg nach vorn.

Sprechen Sie noch heute mit einem Experten von Echoworx.