

Wenn das Vertrauen der Mandanten nicht kompromittiert werden darf

Wie eine führende Magic-Circle-Kanzlei ihre sichere Kommunikation modernisierte — bei vollständig erhaltenen Mandantenprozessen

Technische Proof Points

Architektur

- AWS-native SaaS, durchgängig cloudorientiert
- Integration in die bestehende Mimecast-Umgebung
- Kein Rip-and-Replace des bestehenden Stacks
- Vollständige Funktionsparität mit der Legacy-PGP-Universal-Appliance

Kontrolle

- Ausgehendes S/MIME mit automatischer Schlüsselauswahl
- Optionales PGP über Keyword-Trigger in der Betreffzeile
- Signaturen auf jede ausgehende Nachricht angewendet
- LDAP-Schlüsselveröffentlichung für die unternehmensweite Nutzung
- Externe Lookups über den Global TrustPoint Aggregator

Zustellung

- Entschlüsselung eingehender S/MIME- und PGP-Nachrichten am Gateway
- Automatische Erfassung öffentlicher Schlüssel aus signierten Nachrichten
- Entfernung der Schlüssel nach der Erfassung hält Postfächer sauber
- Abgestimmt auf die eingehenden Richtlinien von Mimecast
- Portalzustellung wird für breitere Anwendungsfälle geprüft

Zusammenfassung

Für eine Kanzlei, die einige der weltweit erfolgreichsten Rechtsangelegenheiten betreut, ist sichere Kommunikation keine Support-Funktion, sondern Teil der juristischen Arbeit selbst. Ihr Ruf für Diskretion ist ebenso grundlegend wie ihre juristische Expertise — und jede verschlüsselte Nachricht muss diesem Anspruch gerecht werden.

Doch die Verschlüsselungsinfrastruktur der Kanzlei beruhte auf einer veralteten Legacy-PGP-Universal-Appliance. Sie trug zwar weiterhin die zertifikatsbasierten Workflows der anspruchsvollsten Mandanten, ließ sich jedoch immer schwerer warten und kaum noch mit einer modernen, cloudorientierten Sicherheitsstrategie vereinbaren.

Die Kanzlei entschied sich für Echoworx, um einen verifizierten Ersatz mit vollständiger Funktionsparität einzuführen: eine cloudnative Plattform, die bestehende PGP- und S/MIME-Workflows bewahrte, sich nahtlos in die sichere E-Mail-Umgebung integrierte und die strengen Anforderungen sensibler juristischer Kommunikation respektierte.

Das Ergebnis war eine moderne, standardbasierte Verschlüsselungsgrundlage, die Workflows ohne Unterbrechung weiterführte, Governance stärkte und digitales Vertrauen nachhaltig absicherte.

Die Herausforderung

01 | Ein Ruf, der keinen Raum für Kompromisse lässt

In der Spitzenklasse juristischer Beratung ist Vertrauen die eigentliche Währung — und eine einzige fehlerhaft behandelte Kommunikation kann eine über Jahre aufgebaute Mandantenbeziehung gefährden. Die wichtigsten Partner und Kontakte der Kanzlei bestanden auf spezifischen, etablierten Verschlüsselungsprozessen — präzisen PGP- und S/MIME-Abläufen mit kaum Spielraum für Abweichungen. Jede Ersatzplattform musste diese Erwartungen exakt erfüllen, denn für diese Kanzlei ist der Schutz vertraulicher Kommunikation kein Zusatzmerkmal. Er ist Teil der eigentlichen Mandatsarbeit.

02 | Legacy-Verschlüsselung, die nicht mehr mithalten konnte

Die PGP-Universal-Appliance der Kanzlei hatte ihren Zweck erfüllt, wurde jedoch zunehmend schwerer zu warten und passte immer weniger zu einem modernen, cloudorientierten Sicherheitsansatz. Als Mimecast-Kunde benötigte die Kanzlei eine Verschlüsselungsebene, die sich nahtlos in die bereits bewährte Umgebung einfügt — keine disruptive Umstellung, die ihre Mitarbeitenden dazu zwingt, ihre Arbeitsweise neu zu erlernen. Die Anforderung war klar: Alle funktionierenden Workflows erhalten, die darunterliegende Infrastruktur modernisieren.

03 | Governance über ein komplexes Netz externer Kontakte hinweg

Diese Kanzlei tauscht sensible Inhalte mit Partnern, Mandanten und externen Rechtsberatern weltweit aus — jeweils mit eigenen Schlüsseln, eigenen Verzeichnissen und eigenen Erwartungen. Diese Komplexität über eine veraltete Infrastruktur zu steuern, erzeugte Reibung und ließ Raum für Inkonsistenzen. Benötigt wurde eine einheitliche, gesteuerte und standardbasierte Grundlage, die die richtigen Schlüssel finden, den richtigen Schutz anwenden und Kontrolle über jede Nachricht nachweisen kann, die den Perimeter der Kanzlei verlässt.

Die Lösung

Die Kanzlei entschied sich nach einer vollständigen Proof-of-Concept-Evaluierung für Echoworx — einer Evaluierung, in der jeder Workflow geprüft wurde und die durchgängig zu einem eindeutigen positiven Ergebnis führte. Ausschlaggebend für die Entscheidung war vor allem eines: Echoworx konnte die Fähigkeiten der Legacy-Appliance vollständig abbilden und sie zugleich auf eine resiliente, cloudnative Grundlage überführen — und das bei nahtloser Integration in die bestehende sichere E-Mail-Umgebung der Kanzlei.

„Diese Kanzlei kam mit einer sehr klaren Anforderung auf uns zu: Jeder PGP- und S/MIME-Workflow, auf den ihre wichtigsten Mandanten angewiesen sind, musste ohne Kompromisse erhalten bleiben“, erklärt ein Engagement Lead von Echoworx. „Wir haben im Proof of Concept jeden Anwendungsfall verifiziert, jeden einzelnen sauber migriert und alles in die sichere E-Mail-Umgebung integriert, der die Kanzlei bereits vertraut. Genau so sieht in der Praxis eine echte Like-for-Like-Migration aus — und genau das ist die Grundlage dafür, dass sich die Beziehung weiterentwickeln kann.“

PGP- und S/MIME-Funktionsparität — präzise fortgeführt

Im Zentrum der Migration stand der exakte Ersatz der zertifikatsbasierten Verschlüsselung der Kanzlei. Ausgehende Nachrichten nutzen nun S/MIME mit automatischer Schlüsselauswahl auf Basis der verfügbaren Empfängerschlüssel; optional kann PGP über ein Keyword in der Betreffzeile ausgelöst werden. So konnten die Personen, die auf sichere Kommunikation angewiesen sind, exakt die Schritte beibehalten, die sie bereits kannten. Nichts musste neu erlernt, nichts neu abgestimmt werden. Die Workflows, die die Mandanten der Kanzlei erwarten, liefen ohne Unterbrechung weiter — verändert hat sich nur die zugrunde liegende Plattform.

Signaturen auf jeder ausgehenden Nachricht — Vertrauen sichtbar gemacht

Weil S/MIME und PGP im Zentrum der Kommunikationspraxis dieser Kanzlei stehen, wird die gesamte ausgehende E-Mail über Echoworx geleitet, um jede Nachricht zu signieren. Diese Signatur ist mehr als ein technisches Detail — sie ist ein Echtheitsnachweis in jedem einzelnen Austausch. Sie gibt Empfängern die Sicherheit, dass eine Nachricht tatsächlich von der Kanzlei stammt und unverändert angekommen ist. Für eine Institution, deren Name erhebliches Gewicht trägt, wird diese nachweisbare Authentizität zu greifbarem digitalem Vertrauen.

Eingehende Entschlüsselung und sauberes, müheloses Schlüsselmanagement

Echoworx übernimmt die Entschlüsselung eingehender S/MIME- und PGP-Nachrichten am Gateway und arbeitet dabei im Einklang mit den E-Mail-Sicherheitsrichtlinien der Kanzlei, damit jede eingehende Nachricht lesbar und zugleich geschützt bleibt. Die Plattform erfasst außerdem öffentliche Schlüssel aus signierten Nachrichten automatisch und entfernt diese nach der Erfassung, sodass sie niemals in Postfächern erscheinen oder bei Endnutzern Verwirrung stiften. Alles geschieht unsichtbar am Gateway und hält die Nutzererfahrung für die Menschen, die täglich darauf angewiesen sind, klar und reibungslos.

Raum für Wachstum — im eigenen Tempo der Kanzlei

Mit der zertifikatsbasierten Verschlüsselung nun auf einer modernen Grundlage prüft die Kanzlei Echoworx Portal Delivery als zusätzlichen Kanal — als pragmatische Möglichkeit, sichere Kommunikation auf breitere Anwendungsfälle auszuweiten und eine natürliche Akzeptanz über Teams und Standorte hinweg aufzubauen. Die Infrastruktur steht; die Kanzlei kann die nächsten Schritte zu ihren eigenen Bedingungen und in ihrem eigenen Tempo gehen.

Fortsetzung...

Globale Schlüsselerkennung über vertrauenswürdige Verzeichnisse

Sicherheit beginnt bei der Registrierung. Echoworx setzte für jeden neuen Empfänger eine automatisierte, sichere Benutzerverifizierung durch: Ein systemgenerierter Code, der außerhalb des eigentlichen Kanals per Telefon oder SMS übermittelt wird, verknüpft die Portalregistrierung direkt mit den eigenen Identitätsprüfungsstandards der Bank. Ab diesem Punkt können Nutzer ihre Zugangsdaten selbst verwalten. Doch am Tag der Migration Tausende bereits vertrauenswürdiger Kontakte zu übernehmen, durfte nicht bedeuten, dass gleichzeitig Tausende Verifizierungshürden entstehen. Deshalb nutzte die Bank ihre bestehende Plattform für den Versand von Willkommensnachrichten, und Echoworx ermöglichte für diese bestehenden, bereits verifizierten Nutzer eine kontrollierte und bewusst eingeräumte Ausnahme. Für alle neuen Nutzer ab diesem Zeitpunkt gilt der vollständige, fest definierte Verifizierungsstandard. Hohe Sicherheit dort, wo sie zählt — reibungsloses Onboarding dort, wo es sinnvoll war.

Die Ergebnisse

Die Migration erfüllte ihr zentrales Versprechen: Jeder Workflow, auf den die Mandanten der Kanzlei angewiesen waren, wurde nahtlos fortgeführt — nun gesteuert, modernisiert und auf langfristige Beständigkeit ausgelegt.

Vollständige Workflow-Kontinuität — bestätigt.

Jede Fähigkeit der zertifikatsbasierten Verschlüsselung — ausgehendes S/MIME mit automatischer Auswahl, optionales PGP per Keyword-Trigger, eingehende Entschlüsselung und Key Harvesting — wurde ohne jeden Bruch in die Cloud überführt, sodass keine Mandantenbeziehung den Übergang spürte.

Reputation geschützt — Austausch für Austausch.

Die Signierung aller ausgehenden E-Mails verleiht jeder Kommunikation nachweisbare Authentizität und stärkt damit das Vertrauen, das sich die Kanzlei über Jahrzehnte erarbeitet hat.

Mandantenprozesse ohne Ausnahme gewahrt.

Die exakten PGP- und S/MIME-Schritte, auf die sich die anspruchsvollsten Partner der Kanzlei verlassen, blieben unverändert, sodass selbst hochrangige Beziehungen ohne Unterbrechung fortgeführt werden konnten.

Nahtlose Integration in den bestehenden Stack.

Echoworx arbeitet direkt mit den E-Mail-Sicherheitsrichtlinien der Kanzlei zusammen und stärkt die sichere Kommunikationsebene, ohne die bereits genutzte Umgebung zu beeinträchtigen.

Globale Reichweite — präzise gesteuert.

Die Integration mit externen Verzeichnissen — einschließlich des Global TrustPoint Aggregators — ermöglicht es der Kanzlei, weltweit die richtigen Schlüssel zu finden und das Schlüsselmanagement am Gateway zugleich automatisiert und sauber zu halten.

Eine Plattform mit Raum für Ausbau.

Da Portal Delivery derzeit evaluiert wird, verfügt die Kanzlei über einen klaren, reibungsarmen Weg, sichere Kommunikation nach eigenem Zeitplan auf neue Anwendungsfälle auszuweiten.

Das Gesamtbild

Diese Kanzlei kam zu Echoworx, um eine veraltete Appliance zu ersetzen. Was sie stattdessen gewann, war etwas deutlich Dauerhafteres: eine cloudnative Verschlüsselungsgrundlage, in der jeder bewährte Workflow den Übergang unversehrt überstand — und eine Plattform, die gemeinsam mit einer Praxis skalieren kann, die sich an der äußersten Grenze internationaler juristischer Komplexität bewegt, wo Mandate beispiellos sind, Mandanten weltweit agieren und die Fehlertoleranz bei null liegt.

Die eigentliche Erkenntnis reicht tiefer als Technologie. Für eine Kanzlei, deren Ansehen darauf beruht, genau die Mandate zu führen, bei denen nichts schiefgehen darf — grenzüberschreitende Transaktionen, internationale Streitigkeiten, regulatorische Mandate mit Präcedenzwirkung — ist Diskretion kein Grundsatz. Sie ist gelebte Praxis. Das härteste Kriterium für eine erfolgreiche Modernisierung ist nicht, was hinzugefügt wurde, sondern was zu keinem Zeitpunkt gefährdet werden durfte. Durch die Entscheidung für eine Plattform, die ihre Legacy-Fähigkeiten präzise nachbilden, die exakten Prozesse ihrer anspruchsvollsten Mandanten respektieren und sich nahtlos in die bereits in den globalen Standorten eingesetzten Werkzeuge integrieren konnte, vollzog die Kanzlei eine der sensibelsten denkbaren Migrationen — ohne eine einzige Einbuße bei der Kontinuität. Exakte Parität war nicht das Ziel. Sie war die nicht verhandelbare Voraussetzung. Erreicht wurde etwas noch Selteneres: ein vollständiger Übergang, den die Mandanten der Kanzlei nie bemerken mussten.

Echoworx macht genau das möglich: sicher by design, resilient im großen Maßstab und konsequent ausgerichtet auf die Workflows, die die Menschen, die sich darauf verlassen, bereits kennen.

Is your secure communication ready for what's next?

If a legacy encryption appliance is straining to keep pace with a modern, cloud-first practice — or standing between your firm and the trusted processes your clients insist on — there is a way to move forward without leaving anything behind.

[Talk to an Echoworx expert today.](#)