MailEssentials AI

ONE-PAGER

Für Banken & Kreditgenossenschaften

Eine Überweisung wird ausgelöst. Das Gateway muss sie abfangen, bevor das Geld überwiesen ist.

Die KI schreibt die Richtlinie. Sie sieht Ihre E-Mails niemals.

Das E-Mail-Sicherheitsgateway

Ein Business Email Compromise (eine betrügerische Überweisungsanfrage, die so wirkt, als stamme sie von Ihrem eigenen CFO) kommt über denselben Kanal wie jede legitime E-Mail und ist so aufbereitet, dass sie standardmäßige Authentifizierungsprüfungen besteht. Der Fang muss am Gateway erfolgen – automatisch, bei jeder E-Mail. GFI MailEssentials AI stoppt das mit drei unabhängigen, gleichzeitig wirkenden Ebenen:

Content Filtering

Scannt Schlüsselwort-, Anhangs- und Musterregeln, in denen die von der KI erstellte Richtlinie angewendet wird.

3 Antiviren-Engines

Enthält standardmäßig Avira und BitDefender; Sophos ist optional als Zusatzmodul verfügbar. Jede Engine führt eigenständige Scans durch.

15 Anti-Spam-Filter

Blockiert Phishing und Social Engineering mit einer Erkennungsrate von >99 %.

Was die KI hinzufügt: sie erstellt die Richtlinie, die Engine setzt sie durch

Das manuelle Erstellen eines DLP-Regelsatzes für eine Rechtsordnung dauert schätzungsweise 40 Stunden. GFI MailEssentials AI liefert dasselbe Ergebnis in etwa 5 Minuten.

Cloud 1 — Beschreiben

Ein geführter Chat erfasst das Profil Ihres Unternehmens, die zuständigen Rechtsordnungen, Datentypen und geltenden Vorschriften.

Cloud 2 — Generieren

Die KI entwirft einen vollständigen Regelsatz (Bedingungen, Aktionen, Priorität), der als XML exportiert wird.

On-prem 3 — Bereitstellen

Importieren Sie das überprüfte XML in Advanced Content Filtering. Nichts läuft, bevor Sie es importiert haben.

On-prem 4 — Überwachen

Eingesetzte Regeln scannen lokal jede eingehende, ausgehende und interne Nachricht.

Cloud 5 — Neu generieren

Vor dem Ablauf (ca. 90 Tage) prüfen und innerhalb weniger Minuten erneut ausführen. Das Ergebnis fließt zurück in Beschreiben.

Die einzigen Daten, die in die Cloud gesendet werden, sind Ihr Organisationsprofil: Ihre Rechtsordnungen, Datentypen und Vorschriften. Keine E-Mail, kein Anhang und kein Empfänger verlassen jemals Ihre Infrastruktur. Jede generierte Regel steht Ihnen zur Prüfung, bevor etwas ausgeführt wird. Nichts wird bereitgestellt, bis Sie es importiert haben.

Wie das in der Praxis aussieht

Admin beschreibt:

„Wir sind ein Finanzdienstleistungsunternehmen in Deutschland und im Vereinigten Königreich. Verhindern Sie das Abfließen von Kreditkarten- und personenbezogenen Finanzdaten – außer an die von uns genehmigte Domain unseres Prozessors. Kennzeichnen Sie nationale Ausweisnummern. Einhaltung von PCI-DSS, DSGVO, SOX und FINRA.“

— Regel generiert, importiert und am Gateway durchgesetzt.

Compliance-Fit: globaler Basisstandard

Globaler Basisstandard Scans, Durchsetzung und E-Mail-Inhalte verlassen niemals Ihre Infrastruktur, und jede von der KI generierte Regel wird vor dem Live-Gang überprüft – das unterstützt die bei Bankaufsichtsbehörden weltweit üblichen Erwartungen an die Datenresidenz.	Einhaltung
Mensch-in-der-Schleife Über den Basisstandard hinaus benennen Sie die konkreten Verpflichtungen Ihrer Institution. Der KI-Assistent erstellt aus dieser Beschreibung einen Regelsatz, der den Vorschriften zugeordnet ist. Ihr Team prüft jede Regel vor der Bereitstellung. Nichts läuft, bis Sie es genehmigen.	Fähigkeit

Bereit, loszulegen?

Fordern Sie eine kostenlose Testversion an unter gfi.ai oder kontaktieren Sie den Vertrieb: sales@gfi.com.

Copyright © GFI USA, LLC. Alle Rechte vorbehalten.