



Gabor

Handel

GBS Success Story

Zentrales E-Mail Lifecycle Management für mehr Effizienz

iQ.Suite

Das Unternehmen

Die Gabor AG ist auf Herstellung und Vertrieb von Damen- und Herrenschuhen spezialisiert. Das Rosenheimer Unternehmen steuert die Produktion von 25.000 Paar Schuhen täglich und zählt damit zu den Großen seiner Branche.

Die Herausforderung

Thomas Fischer, IT- und Netzwerkadministrator von Gabor, weiß wo der Schuh drückt. Die laufend steigende Mailflut zwang ihn zu raschem Handeln. Immer mehr Werbemails belasteten den Mailserver. Einzelne Mitarbeiter mussten gar ein Spam-Aufkommen von über 90 Prozent verkraften, was einen hohen Arbeitszeitverlust und damit Kostenfaktor für das Unternehmen darstellte. Hinzu kam die Anforderung der Vertriebspartner, statt per Briefpost generell über das Medium E-Mail zu kommunizieren. Hier galt es, vertrauliche Informationen wie zum Beispiel Angebote und Rechnungen in den elektronischen Nachrichten via Verschlüsselung vor „unliebsamen Mitlesern“ zu schützen.

„Bei der E-Mail-Verschlüsselung gingen wir bislang clientbasiert vor, was umständlich und zu aufwändig war“, erläutert Fischer. So war die Verschlüsselung an einzelnen Arbeitsplätzen admini-

Für den Vertrieb der rund 400 angebotenen Modelle je Saison arbeitet Gabor eng mit über 6.000 Händlern im In- und Ausland zusammen, mit denen sich der Schuhspezialist intensiv per E-Mail austauscht.

strator- und anwenderunfreundlich, da zu komplex und kostenintensiv, wie zum Beispiel die Schlüsselverwaltung am Client. Zudem bestand Gefahr, dass einzelne Anwender aus Versehen vertrauliche E-Mails unverschlüsselt versenden, beispielsweise beim nochmaligen Versand alter Nachrichten. Für die Spamfilterung und Verschlüsselung suchte Gabor eine Softwarelösung, die sowohl die Unternehmensrichtlinien als auch die Anforderungen von Administrator und Anwendern sowie der Vertriebspartner erfüllt.

„Für das Mehr an Sicherheit und Effizienz mit der iQ.Suite waren keine hohen Investitionen in Aufbau und Pflege einer Verschlüsselungs-Infrastruktur notwendig.“

Thomas Fischer – IT- und Netzwerkadministrator

Die Lösung

Nach Evaluierung verschiedener E-Mail-Systeme entschied sich Fischer für die modulare und regelbasierte iQ.Suite für Microsoft Exchange von GROUP Business Software. Der große Vorteil der Lösung liegt für Fischer in der Serverbasierteit. Dadurch ist gewährleistet, dass eingehende E-Mails zunächst entschlüsselt, dann auf Viren und Inhalte geprüft und anschließend archiviert und zugestellt werden, ohne Interaktion durch die Anwender. Bei ausgehenden E-Mails ist der Ablauf umgekehrt: erst die Viren- und Inhaltsprüfung am Server, dann die Archivierung und Verschlüsselung. „Mit geringem Aufwand haben wir so alle wichtigen Sicherheitschecks vollzogen, noch ehe die E-Mail überhaupt das Haus verlässt beziehungsweise den Empfänger erreicht“, sagt Fischer.

Ein weiterer Grund für den Einsatz der iQ.Suite bei Gabor war die unternehmensweite Skalierbarkeit der Lösung und die flexible Erweiterbarkeit bis hin zur Realisierung eines durchgängigen und integrierten E-Mail Lifecycle Management (ELM). Dieses umfasst neben der Verschlüsselung und Spamabwehr auch den Virenschutz, die E-Mail-Klassifizierung und -Compliance sowie E-Mail-Archivierung. „Dank der integrierten Module legen die E-Mails nur kurze Wege zurück. Außerdem fügt sich die Lösung bei bester Performance sehr gut in die vorhandene IT-Architektur ein und hält auch stärkstem Mailverkehr stand. Selbst ein umfangreicher Newsletter-Versand bremsst das System nicht aus“, kommentiert Fischer.

Auf Wunsch von Vertriebspartnern im In- und Ausland führte Fischer die E-Mail-Verschlüsselung bei Gabor ein. Bestimmte Informationen wie Kalkulationen und Rechnungen sollten nur den Empfängern der Nachrichten zugänglich und vor Einsichtnahme geschützt sein. Mit dem Modul iQ.Suite Crypt Pro für die serverbasierte Ver- und Entschlüsselung ließ sich die Anforderung schnell in den Griff bekommen. Unternehmensweite Verschlüsselungsrichtlinien lassen sich zentral und flexibel konfigurieren. Fischer musste lediglich einen Schlüssel für jedes verwendete Kryptographieverfahren zentral am Server ablegen. Dadurch wird den Mail-Empfängern der öffentliche Schlüssel auf einfache Weise bereitgestellt, und die Kommunikationspartner

können die E-Mails samt Anhang verschlüsselt austauschen. Für noch mehr Sicherheit werden die E-Mails außerdem signiert, um Authentizität und Integrität der Nachrichten sicherzustellen.

Um verschlüsselte E-Mails auf Virenbefall zu prüfen, lassen sich mit der iQ.Suite eingehende E-Mails zuerst am Server entschlüsseln und anschließend bezüglich Malware analysieren. Hierbei werden durch einen ersten Virenscan etwaige falsche Schlüssel enttarnt. Erst dann werden die E-Mails entschlüsselt, und ein zweiter Virenscan sorgt vor der Zustellung für „saubere“ Eingangspost.

Am Anti-Spam Modul iQ.Suite Wall überzeugte Fischer die einheitliche Managementkonsole für die einfache Bearbeitung der unerwünschten Nachrichten, die treffsichere Inhaltsanalyse von E-Mails und die Sammelbenachrichtigungs-Funktion. Darüber erhalten Anwender regelmäßig Nachricht über neu gefilterte E-Mails im Spam-Verdacht, die sie sich auf Wunsch an ihre Mailbox weiterleiten können. Zur Verringerung des Aufwands hat der Administrator seinerseits die Möglichkeit, eingehende E-Mails Black- und Whitelists mit erlaubten und unerlaubten Absenderadressen zuzuordnen. So sind beispielsweise gewünschte und unerwünschte Newsletter leicht zu unterscheiden.

Die Wirkung des Spamfilters lässt sich durch die Inhaltsanalyse von E-Mails maßgeblich erhöhen. Die in iQ.Suite Wall integrierte CORE-Technologie (Content Recognition Engine) analysiert die Betreffzeile und den gesamten Inhalt von E-Mails samt Anhängen gemäß Unternehmensrichtlinien und erreicht Spam-Erkennungsraten von über 98 Prozent. Irrtümlich gefilterte E-Mails (False Positives) sind bei der Filterung nahezu auszuschließen.

Die Umsetzung

„Die automatisierte Inhaltsprüfung der Nachrichten und Anhänge mittels Spamfilter zeigte rasch ihre Wirkung, so wurde das Ziel, die E-Mail-Kommunikation auf das geschäftlich Notwendige zu begrenzen schnell erreicht. Die Kombination von Verschlüsselung und Inhaltsanalyse gewährleistet Datensicherheit und -integrität sowie die Einhaltung gesetzlicher Vorschriften zum

Datenschutz. Zudem sind wir damit vor Wirtschaftsspionage per E-Mail geschützt“, erklärt Fischer. Die Verschlüsselung der Nachrichten läuft automatisiert serverbasiert im Hintergrund ab – zur Zufriedenheit der in- und ausländischen Handelspartner und Gabor-Anwender. Nach wenigen Stunden war die Installation und Erstkonfiguration der iQ.Suite abgeschlossen.

Die Zukunft

„Um die bestehende E-Mail-Infrastruktur abzurunden, planen wir einen weiteren Virensch scanner einzuführen, der über iQ.Suite angesprochen wird. Außerdem wollen wir neben den vertrauenswürdigen E-Mails auch die dazu gehörigen Rechnungen digital signieren“, sagt Fischer, der ein positives Resümee zieht: „Für das Mehr an Sicherheit und Effizienz mit der iQ.Suite waren

keine hohen Investitionen in Aufbau und Pflege einer Verschlüsselungs-Infrastruktur notwendig, die Softwareverteilung und Anwenderschulung entfielen sogar ganz. Der kombinierte Verschlüsselungs- und Spam-/Virenschutz gewährleistet sichere und integrierte E-Mail Geschäftsprozesse, einen besseren Kundenservice und höhere Produktivität.“