Anwenderbericht

Hannover Rück versichert E-Mail-Verkehr

Compliance hat bei der Hannover Rück oberste Priorität im Rahmen der Geschäftsgrundsätze. Dabei spielt auch die IT-Security eine übergeordnete Rolle. So hat sich die weltweit agierende Rückversicherungsgruppe für den Einsatz der E-Mail-Verschlüsselungslösungen Z1 SecureMail Gateway und Z1 SecureMail Messenger der Zertificon Solutions GmbH entschieden. Alle ein- und ausgehenden Nachrichten werden zentral abgesichert. Dies gewährleistet zum einen Gesetzeskonformität und zum anderen hohe Integrität bei der Zusammenarbeit mit Kunden, Partnern und Lieferanten.

Zentrale Lösung statt Einzelplatzinstallationen

Diese vernetzte Struktur erfordert ein E-Mail-Verschlüsselungssystem, das zentral den gesamten elektronischen Nachrichtenverkehr mit sämtlichen Kommunikationspartnern auf unkomplizierte Weise absichert. Bis dato griff die Hannover Rück auf Einzelplatzinstallationen von PGP Desktop zurück, die einen hohen Verwaltungsaufwand sowie Komplexität in puncto Schlüsselverwaltung etc. aufwiesen. Hinzu kamen Risiken durch die Tatsache, dass die Anwender die Verantwortung hatten, selbst zu entscheiden, in welchen Fällen verschlüsselt wird und in welchen nicht. Alternativ genutzte ZIP-Archive mit Verschlüsselung und Passwort-Schutz waren ebenfalls nur eine Kompromisslösung, da diese bei vielen Kommunikationspartnern – und auch dem Kunden selbst – auf den Mailgateways gesperrt sind. Ein üblicher Virenscanner kann die Archive nicht untersuchen und bekannte Schädlinge lassen sich daher in solchen ZIP-Archiven verschicken.

Wolfgang Lindner
Hannover Rück

PKI- und passwortbasierte E-Mail-Verschlüsselung

Der Consulting-Partner michael-wessel.de Informationstechnologie GmbH stellte die Lösungen PGP Universal Server, Utimaco SecureMail Gateway, ICC Julia MailOffice und Z1 SecureMail Gateway/Messenger vor und verglich diese.

Die Entscheidung fiel auf die Produkte der Zertificon Solutions GmbH. Z1 SecureMail Gateway agiert als SMTP-Proxy, der E-Mails automatisch verschlüsselt, entschlüsselt, signiert und Signaturen überprüft. Es arbeitet konform zu S/MIME und OpenPGP, den beiden international etablierten Standards für E-Mail-Sicherheit.

Ein wesentliches Merkmal der Z1 SecureMail Messenger Komponente ist die Möglichkeit des Versands vertraulicher Nachrichten via PDF. Die E-Mail wird hier passwortverschlüsselt. Dies funktioniert gänzlich ohne PKI (Public Key Infrastructure)-Technologie oder Zertifikate, wie sie bei herkömmlichen Lösungen erforderlich sind. Dies vereinfacht den sicheren Austausch von elektronischen Nachrichten erheblich. Ein weiterer Vorteil ist die Tatsache, dass die Lösung nicht nur zum vertraulichen Nachrichtenaustausch mit externen Kommunikationspartnern einsetzbar ist, sondern sich auch auf einfache Weise zur Absicherung des internen E-Mail-Verkehrs eignet. Da die Hannover Rück sowohl mit Kommunikationspartnern arbeitet, die die PKI-Technologie bevorzugen, als auch mit Partnern, die diese nicht präferieren oder besitzen, wurde die Entscheidung für Z1 SecureMail Gateway mit der Z1 Messenger-Komponente getroffen.

hannover re®

Die Hannover Rück-Gruppe betreibt alle Sparten der Schaden- und Personen-Rückversicherung und unterhält dabei Beziehungen mit über 5.000 Versicherungsgesellschaften in rund 150 Ländern. Ihre weltweite Infrastruktur besteht aus über 100 Tochter- und Beteiligungsgesellschaften, Niederlassungen und Repräsentanzen auf allen fünf Kontinenten mit circa 2.000 Mitarbeitern. Das Deutschland-Geschäft wird von der Tochtergesellschaft E+S Rück betrieben.

Wolfgang Lindner, Verantwortlicher für IT-Network-Management der Hannover Rück, erklärt:
„Letztlich überzeugten uns das Preis-Leistungs-Verhältnis sowie die konstruktive Zusammenarbeit mit dem Hersteller; notwendige Fixes wurden schnell zur Verfügung gestellt und die Entwicklung war für Anpassungswünsche empfänglich. Das System ist sehr flexibel und leistungsfähig – und dabei nicht überladen mit unnötigen Funktionen.“

Sicherer Versand ohne Aufwand

Die Installation und Inbetriebnahme erfolgten ohne Betriebsunterbrechungen – ebenso sämtliche Updates/Upgrades seither. Die Einführungsphase erstreckte sich aus organisatorischen Gründen über mehrere Monate. Betriebsbereit und konfiguriert waren die Lösungen innerhalb weniger Tage. Weltweit ca. 2.000 User in der Unternehmensgruppe profitieren nun von sicherem E-Mail-Transfer.
Die Entscheidung für Zertificon fiel auf Grund der Produktfeatures, die eine hohe Flexibilität gewährleisten. Die offene Plattform ermöglicht Berechtigungsverwaltung für beliebig viele Administratoren.

Sie bietet außerdem flexible Policies sowie granulare Konfiguration der Security-Parameter je Policy bzw. Kommunikationspartner. Auch die Mandantenfähigkeit ist hinsichtlich der zahlreichen Domains und Tochter-/Schwester-Gesellschaften ein entscheidendes Kriterium. Sie bietet die Möglichkeit der disjunkten, kundenorientierten Datenhaltung, Präsentation (GUI) und Konfiguration (Customizing). Jeder Kunde kann demnach nur seine Daten einsehen und verändern.

Die E-Mail-Sicherheit ist zentral kontrollierbar, und die Anwender sind von der Komplexität sowie dem Aufwand befreit, sich mit der Thematik auseinandersetzen zu müssen.

Die User benötigen keinerlei spezielle Kenntnisse mehr und können sich somit ohne Ablenkung ihren eigentlichen Aufgaben widmen. Zudem konnte der Versand von sensiblen Informationen (z.B. Versicherungs- oder Abrechnungsdaten), der zuvor per CD-Versand oder Briefpost erfolgte, auf E-Mail umgestellt werden. Medienbrüche werden somit vermieden und Reaktionszeiten erhöht.

Anwenderfreundliche Compliance

Lindner resümiert: *„Im Rahmen von globalen Sicherheitsprojekten definierte Anforderungen an den sicheren Informationsaustausch konnten nun erfüllt werden, ohne dass das Medium E-Mail an Attraktivität für die Anwender verlor – die Handhabung ist transparent und für interne Benutzer wie gewohnt.“*

Zukunftsausblick

Die Ausweitung des Services – inklusive Customizing des entsprechenden Messenger-Frontends etc. – auf eine große Konzern-Schwester ist angedacht; ebenso die Option, Kommunikationspartnern Z1 SecureMail Stations zur Verfügung zu stellen, um sichere E-Mail-Verbindungen herzustellen.
Die server-basierende Station bezieht im Unterschied zum Gateway die öffentlichen Schlüssel der Kommunikationspartner von einem zentralen Provider wie zum Beispiel Z1 Global TrustPoint, der Beschaffung, Gültigkeitsprüfung und Verwaltung externer Zertifikate erbringt. Entsprechend ist diese Variante einfach zu administrieren und schlank beim Ressourcenbedarf.

Verwaltungsgebäude Hannover