

Totemo TrustMail bei Evonik: Zusätzliches Vertrauen bei Kunden, Partnern und Lieferanten durch geschützten E-Mail Verkehr

Mit einer kostenoptimierten Gateway-Lösung schützt Evonik in der E-Mail Kommunikation seine wichtigsten Informationen, ohne dabei bei den Benutzern für zusätzlichen Aufwand zu sorgen. Benutzerfreundlichkeit und Sicherheit ergänzen sich in diesem Projekt zum Nutzen aller Beteiligten.



JOCHEN GINTZEL,
CIO EVONIK INDUSTRIES

„MIT DER TOTEMO-LÖSUNG HABEN WIR DEN E-MAIL-NUTZERN EIN EINFACH ZU HANDHABENDES VERFAHREN ZUR VERFÜGUNG GESTELLT, INFORMATIONEN MIT EXTERNEN PARTNERN SICHER AUSZUTAUSCHEN.“

Für Evonik, ein internationaler Industriekonzern aus Deutschland mit rund 40'000 Mitarbeitern und den Geschäftsfeldern Chemie, Energie und Im-

mobilien, sind E-Mails ein wichtiges Kommunikationsmedium zum Austausch von Informationen mit Kunden, Lieferanten, Behörden und anderen Partnern. Täglich werden tausende E-Mails über das Evonik E-Mail System an externe Empfänger versendet.

Die geschäftliche Herausforderung

Arijo Nazari-Azari, Projektleiter im Bereich IT Compliance & Qualitymanagement bei Evonik beschreibt die geschäftliche Begründung für das Projekt zur sicheren E-Mail Kommunikation folgendermassen:

„Neben gesetzlichen und Evonik IT-Sicherheits-Anforderungen, sensible Informationen geschützt zu übertragen, erwarten unsere Kunden und Geschäftspartner, dass wir einen sicheren E-Mail

Schriftverkehr unterstützen. In vielen Fällen ist dies sogar Voraussetzung für eine Geschäftsbeziehung.“

„Mit der Totemo-Lösung geben wir unseren Mitarbeitern das richtige Werkzeug, um die notwendige Vertraulichkeit und Integrität im Bereich der E-Mail Kommunikation sicherzustellen.“

Ziele und Erwartungen

Von Beginn an wurde eine kostenoptimierte Gateway-Lösung angestrebt. Den Benutzern sollte kein zusätzlicher Aufwand im alltäglichen Gebrauch von E-Mail entstehen und das neue System sollte in das bestehende Umfeld bei Evonik problemlos integriert werden können (Lotus Notes, Microsoft Exchange, eigene PKI Infrastruktur).

Das Fazit

Totemo konnte alle Anforderungen von Evonik erfüllen. Dazu Arijo Nazari-Azari: „Wir können heute für den definierten Benutzerkreis der Verschlüsselungslösung die notwendige Sicherheit in der E-Mail-Kommunikation gewährleisten und das mit einer kostenoptimierten Lösung. Kurz und knapp, wir konnten das Projekt in angemessener Zeit und Qualität erfolgreich durchführen.“

Totemo AG

Totemos marktführende Sicherheitslösungen umfassen Secure Messaging, Secure Managed File Transfer und Secure Mobile Messaging für Unternehmen und Behörden jeglicher

Grösse. Mit dem ganzheitlichen Ansatz zur Sicherung der unternehmensweiten Online-Kommunikation wird gewährleistet, dass sämtliche E-Mails, File Transfers, Web-Interaktionen und Transaktionen vertraulich, zuverlässig und effizient abgewickelt werden.

Zu den Kunden von Totemo zählen Organisationen und Unternehmen aus den Branchen Financial Services, Government, Application Service Provider (ASP), Outsourcing Provider, Health Care, Industrie und Professional Services. Das Schweizer Unternehmen wurde im September 2001 gegründet und ist in Küsnacht (ZH) domiziliert.

totemo ag

Cloud Computing –Chance oder Sicherheitsrisiko?



AMMAR ALKASSAR, VORSTAND DES
TELETRUST DEUTSCHLAND E.V.

Cloud Computing birgt für Unternehmen in puncto Sicherheit nicht nur Risiken,

sondern kann dazu beitragen, die eigenen Sicherheitsmaßnahmen umfassend zu optimieren. Zu diesem Ergebnis kommt die Europäische Agentur für Netz- und Informationssicherheit (ENISA) in einer kürzlich veröffentlichten Untersuchung zu diesem Thema. Gerade für den Mittelstand bieten Cloud Computing und virtualisierte Arbeitsumgebungen auch Chancen, die Sicherheit um Größenordnungen zu verbessern.

Dabei kommt dem Konzept vertrauenswürdiger Infrastrukturen („Trusted Infrastructures“) eine zentrale Rolle zu. IT-Systeme müssen dann nicht nur definierte

Sicherheitsanforderungen erfüllen. Sie müssen viel mehr technisch in der Lage sein, ihre aktuellen Sicherheitseigenschaften gegenüber anderen Systemen verlässlich nachzuweisen.

„Glauben reicht an dieser Stelle nicht mehr“, so TeleTrust-Vorstand Ammar Alkassar, „wenn Unternehmen ihre gesamten Daten externen und möglicherweise verschiedenen Dienstleistern anvertrauen, muss die technische Infrastruktur jederzeit nachweisbar gewährleisten, dass diese Daten nach den eigenen Richtlinien verarbeitet werden – völlig unabhängig wo dies gerade geschieht.“

Zukunftsweisend könnten dabei Konzepte wie Trusted Virtual Domains (TVD) werden. In TVDs werden plattformübergreifend Arbeits- und Serversysteme gruppiert und zu einer virtualisierten Sicherheitsumgebung zusammengefasst. Damit wird eine verlässliche und dennoch einfach zu handhabende Informationsflusskontrolle möglich.

Geringere Kosten und schnellere Reaktionszeiten

Durch die Einbettung in eine größere Struktur, lassen sich Kosten für Sicherheitsmaßnahmen drastisch senken. Zudem erlaubt eine zentrale Administration

schneller auf umfassende Sicherheitsprobleme wie eine DDoS-Attacke zu reagieren und ständig verfügbare Sicherheits-Spezialisten gezielt einzusetzen. Auch sicherheitskritische Patches können schneller integriert werden. Dies kann insbesondere für kleinere und mittelständige Unternehmen eine signifikante Sicherheitserhöhung zu geringeren Kosten bedeuten.

Ammar Alkassar ist Vorstandsmitglied des IT-Sicherheitsverbandes TeleTrust Deutschland und Vorstandschef des Saarbrücker Trusted Computing Spezialisten Sirrix AG.