Zentrale Verschlüsselung löst Sicherheitsproblem

Verschlüsselung trotz Virenschutz und Content Scan

Autor: ***Jürgen Schneider-Jansohn,***
Projektleiter eMail-Sicherheit bei der netFORMAT GmbH

Ohne Frage ist der Austausch von eMails die meistgenutzte Anwendung im Internet. Mittlerweile entsteht ernsthafter Bedarf, eMails auch für den Austausch von explizit personenbezogenen und vertraulichen Daten und Dateien mit den Geschäftspartnern einzusetzen. Für viele Unternehmen stellt jedoch der angemessene Einsatz von Verschlüsselungstechnik immer noch eine schwierige Herausforderung in ihrem B2B-Verkehr dar.

Einen effizienten und zugleich benutzerfreundlichen Ausweg aus der Misere bietet die zentrale eMail-Verschlüsselung. Gegenüber der bisher üblichen Methode der Client-Verschlüsselung ermöglicht eine zentralisierte Lösung in Unternehmen eMail-Verschlüsselung zu etablieren, ohne Anwender zu schulen und flächendeckend Software auf PCs installieren zu müssen. Damit auf diesem Wege aber nicht am anderen Ende die Überprüfung nach unerwünschten Inhalten oder bösartigen Programmcodes wie Viren oder Würmer kompromittiert wird, ist die Beibehaltung der eingesetzten Content-Scan-Methoden unerlässlich.

Typische Anwendungsszenarien

- Sichere Kommunikation mit / für Personalabteilungen, Steuerbüro, Zulieferer, Rechtsanwälte, ...
- Gefahrlose Nutzung von automatischen Weiterleitungen (auch an private ‚Web-Adressen')
- Anbindung von Partner-Unternehmen mit eigener SMTP-Domäne
- Überprüfung der Echtheit von signierten Sicherheitswarnmeldungen (CERT)
- Automatische Signierung ausgehender Nachrichten um „Versand unter falschem Namen" nachweisen zu können (SPAM/Viren)

Die netFORMAT Netzwerk- und Systemlösungen GmbH hat aus diesen Anforderungen heraus eine zentrale eMail-Lösung entwickelt, die das Content-Scan-Produkt „MAILsweeper for SMTP" um die Fähigkeit der Ver- und Entschlüsselung erweitert. In gleicher Art und Weise wie innerhalb des Clearswift-Produktes Virenscanner und andere Methoden angewendet werden, um Sicherheits- und Unternehmensrichtlinien durchzusetzen, wird mit Hilfe der lizenzfreien PGP-Variante GnuPG die Ver- und Entschlüsselung realisiert. Künftig wird auch der Standard S/MIME durch Verwendung von OpenSSL nutzbar sein. Diese Funktionserweiterung vereinigt Inhaltsüberprüfung und Inhaltssicherung auf einem Server, so dass es möglich ist, eine verschlüsselte eMail auf Viren hin automatisch zu überprüfen. Speziell für Unternehmen, die bereits einen MAILsweeper im Einsatz haben, ergibt sich so ein äußerst kostensparender Ansatz.

Die beiden Verschlüsselungsmethoden Inline-PGP und S/MIME-PGP werden bei eingehend eMails selbständig erkannt und angewendet. Ausgehende Methoden werden in Absprache mit dem externen Geschäftspartner beim Schlüsselaustausch vereinbart und über Zuordnung in Adresslisten aktiviert. Die Ver- und Entschlüsselung erfolgt in beide Richtungen einstufig. Das jeweilige Verfahren wird bei jeder Nachricht immer nur einmal angewendet. Enthalten eingehende ‚entschlüsselte' eMails nach dem Prozess immer noch verschlüsselte Anteile, wird die eMail abgelehnt. Die Nachricht wird isoliert, Absender und

Empfänger werden informiert. Das gleiche gilt für einen Virusfund bei ein- und ausgehenden Nachrichten. Hier kann beispielsweise zusätzlich der Administrator informiert werden, um den Inhouse-Virus zu finden.

MAILsweeper for SMTP von Clearswift analysiert den gesamten ein- und ausgehenden eMail-Verkehr am Gateway und erlaubt Unternehmen so, Verwaltungs- und Sicherheitsrichtlinien durchzusetzen, um unerwünschte eMails zu blockieren und gleichzeitig rechtliche Vorgaben einzuhalten. Die eMails werden am SMTP Gateway automatisch und benutzertransparent dem Filter, dem Monitoring und Reporting unterzogen. Verifikationen wie Überprüfung von Dateianhängen auf Viren, Vorgaben für erlaubte und nicht erlaubte Dateitypen, Größenbeschränkung von Dateianhängen, Prüfung des Mail-Inhalts sowie die Abwehr unerwünschter Daten lassen sich detailliert festlegen.

„Die Kombination von MAILsweeper mit dem Verschlüsselungsinstrument von netFORMAT bringt für die Anwender einen echten Mehrwert. Verschlüsselte Dateianhänge stellen nun nicht länger eine Illusion á la Copperfield dar“, kommentiert Frank Brandenburg, Geschäftsführer der Clearswift GmbH. *„Wo unsere Content-Scanner bisher im Trüben fischen mussten, denn was unsichtbar ist, kann schließlich nicht gescannt werden, kommt nun endlich Licht ins Dunkel.“*

Bei diesem zentralen Ansatz benutzt der Anwender sein eMail wie bisher. Er muss nichts über die implementierten Methoden wissen und auch bei der Bedienung seiner eMail Clients nichts beachten. Die einzigen Hinweise über den Zugewinn an Sicherheit wird er durch Hinweistexte bei entschlüsselten eMails oder durch Verschlüsselungs-Bestätigungen erhalten. Und auch dies ist vollständig und individuell durch die Administratoren konfigurierbar.

Die Lösung ist flexibel einsetzbar. Sie arbeitet unabhängig von der eingesetzten Groupware-Lösung und unterstützt sowohl Site-to-Site- als auch End-to-End-Verschlüsselung. Ebenso ist der dedizierte Einsatz als reines Verschlüsselungs-Gateway ohne zusätzlichen Aufwand möglich.

Die Einrichtung einer zentralen eMail-Lösung hat sich inzwischen beim Landkreis Lüneburg zu einer sinnvollen und pragmatischen Lösung entwickelt. Eingesetzt wird die netFORMAT-Lösung für den Austausch von strengvertraulichen, personenbezogenen Daten mit anderen Behörden. Stefan Domanske, EDV-Leiter beim Landkreis Lüneburg, nennt die Vorteile: “Die Mitarbeiter des Landkreises Lüneburg können sicher und unkompliziert via eMail kommunizieren, denn die Verschlüsselung findet völlig transparent und ganz ohne ihr Zutun am Gateway statt. Es gibt keinen Roll-out von Client-Software, keine Mitarbeiterschulung, und es sind keinerlei Modifikationen am Client-Rechner nötig. Lediglich der Administrator des Mail-Servers muss das korrekte Schlüsselmanagement beherrschen“.