**Anwenderbericht**

# Content Security bei der NORD/LB

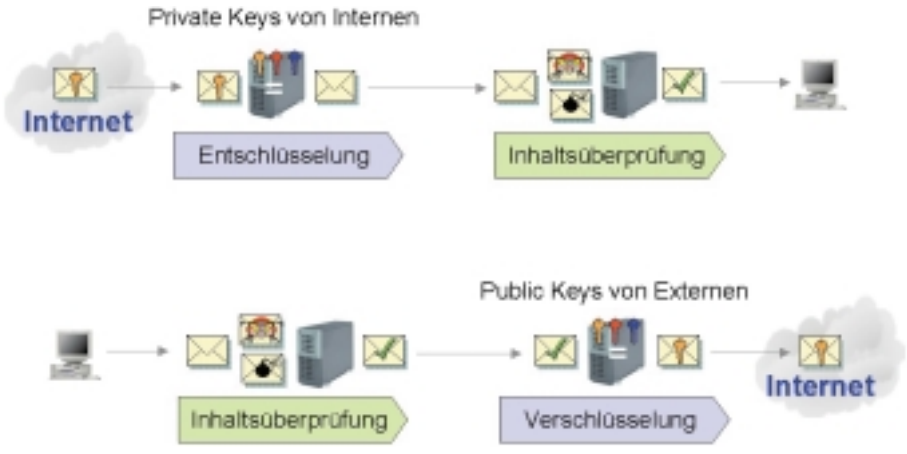
***Von Sabine Baehre, Nürnberg***

Eine zuverlässige Mail-Architektur bildet das Rückgrat eines jeden IT-Sicherheitskonzeptes. Die NORD/LB Norddeutsche Landesbank hat in Zusammenarbeit mit dem IT-Netzwerkdienstleister netFORMAT eine integrierte Lösung erarbeitet, die einen angemessenen Schutz vor den Risiken der E-Mail-Nutzung bietet.

Die NORD/LB ist eine Universalbank mit geschäftspolitischer Konzentration auf Norddeutschland sowie Nord- und Osteuropa. Als Landesbank der drei Bundesländer Niedersachsen, Sachsen-Anhalt und Mecklenburg-Vorpommern unterstützt sie die öffentliche Hand bei kommunalen Finanzierungen. Als Girozentrale übernimmt sie die Aufgaben einer Zentralbank für 87 Sparkassen in diesen drei Ländern.

Mit einem täglichen Aufkommen von 30–40 000 Nachrichten zählt das E-Mail-System zu den zentralen Anwendungen der Bank. Ein mehrstufiger Antiviren-Schutz sorgt dafür, dass keine Viren, Word-Makros oder Trojaner Schaden anrichten können. In jüngster Zeit entstand zunehmender Bedarf, E-Mails auch für den Austausch von explizit personenbezogenen und vertraulichen Daten sowie Dateien mit den Geschäftspartnern einzusetzen. Die Vorteile: ein zeitnaher Kundenservice durch schnelle und persönliche Ansprache sowie weit weniger Arbeitsaufwand und Kosten als beim klassischen Postweg.

Die technische Umsetzung in der Groupware stellte dabei kein Problem dar. Anders sah es im organisatorischen Bereich aus: Es galt gesetzliche Bestimmungen zu beachten sowie Mail-Richtlinien und passende Sicherheitsmaßnahmen festzulegen. Um ein entsprechendes Kommunikationskonzept zu erarbeiten wurde ein Projektteam unter Leitung von Rainer Siebert gebildet, dem IT-Sicherheitsmanagers der NORD/LB. Mit ins Boot holte sich Siebert den Netzwerkdienstleister netFORMAT.




*Bu*

Das Ziel war eine „zentrale Ver- und Entschlüsselung von E-Mails für vorgegebene Kommunikationsbeziehungen“ zu realisieren. Die Ver-/Entschlüsselung sollte bankseitig nicht auf den Desktops der Endbenutzer, sondern automatisiert auf dem Mail-Server der NORD/LB ablaufen. Zwar sind die meisten kryptographischen Produkte auf das Ziel Ende-zu-Ende-Sicherheit hin ausgerichtet, ihre Anwendung setzt jedoch voraus, dass jeder Endbenutzer das Konzept des Schlüsselmanagements versteht und fehlerfrei anwenden kann.

Im Kommunikationsverkehr der NORD/LB hält man dieses Modell nicht für angemessen: „Erstens muss man schon allein wegen der großen Zahl der Mitarbeiter mit einer erhöhten Fehlerwahrscheinlichkeit bei der Schlüsselhandhabung rechnen. Zweitens setzen wir im LAN- und WAN-Bereich entsprechende Mechanismen ein, die eine zusätzliche Verschlüsselung auf Ebene des Mailprotokolls nicht erforderlich machen“, begründet Siebert. Der gesicherte E-Mail-Verkehr über das Internet soll mit externen Partnern und Kunden eine Kommunikation ermöglichen, welche die gebotene Vertraulichkeit für personenbezogene Daten erfüllt. Dazu ist lediglich eine Sicherung der Verbindungsstrecke außer Haus erforderlich, vom Mail-Server des Absenders zum Mail-Server oder -Client des Empfängers. Als weiteren Grund einer zentralen Administration nennt Siebert den ansonsten schwierigen Schutz beim Virus- und Content-Scan.

Zunächst war grundsätzlich zu klären, welche Mitarbeiter die Möglichkeit erhalten sollten, verschlüsselte E-Mails zu versenden und zu empfangen. In Sachen Content Security stellte sich die Frage, wie ankommende und abgehende Internet-E-Mails geprüft werden sollten. Verifikationen wie

- Überprüfung von Dateianhängen auf Viren,
- Vorgaben für erlaubte und nicht erlaubte Dateitypen,
- Größenbeschränkung von Dateianhängen,
- Prüfung des Mail-Inhalts und
- Abwehr unerwünschter Daten

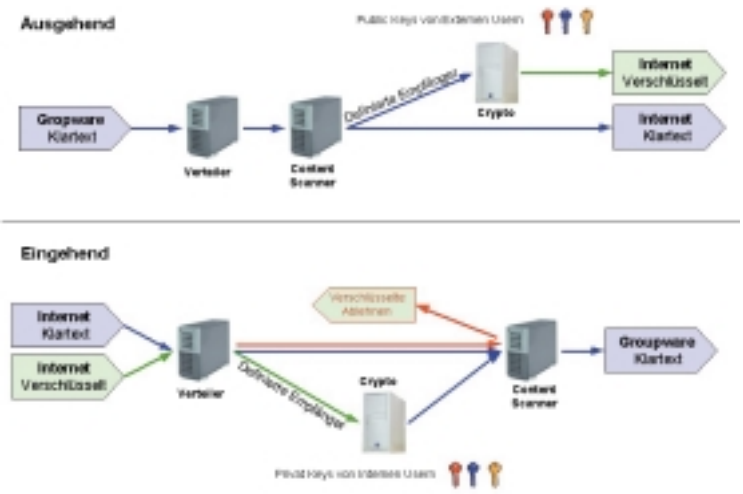
waren dabei ein absolutes Muss.

Zum Zeitpunkt des Projektbeginns Ende 2001 fand man am Markt kein System, das den projektrelevanten Anforderungen entsprach. „Deshalb erhielt netFORMAT von uns den Auftrag, eine Lösung zu entwickeln, mit der sich das Zusammenwirken von Virenscan, Content-Scan und Verschlüsselung realisieren ließ“, so Siebert im Rückblick. Vorgabe der NORD/LB war eine auf Standards basierende Lösung, um so eine Beschränkung auf bestimmte Programme, Hersteller oder Betriebssysteme zu vermeiden. „Wir wollten Unabhängigkeit vom E-Mail-System aller Beteiligten, keine Bindung an selbsterstellte Zertifikate, an eine bestimmte Groupware im Unternehmen und natürlich eine absolut zukunftssichere Lösung“, erklärt Siebert. Die Kombination von Content-Scan und Verschlüsselung war dabei sicherlich die größte Hürde.

## Zwei Welten

Auf Basis der Anforderungen wurden die am Markt befindlichen Produkte beziehungsweise Standards getestet. Bei der Verschlüsselungstechnik entschied man sich für beide verbreiteten Methoden: PGP und S/MIME. Während PGP dem Anwender ermöglicht, seine Schlüssel selbst zu generieren, benötigt S/MIME zwar immer eine Zertifizierungsinstanz, ist aber in vielen E-Mail-Clients (z. B. Netscape Communicator und Microsoft Outlook) integriert. „Zudem verfügen beide Systeme über bewährte Verschlüsselungsalgorithmen“, so Jürgen Schneider-Jansohn, Systemspezialist Netzwerksicherheit bei netFORMAT. Als Content-Scanner wurde das Produkt Clearswift MAILsweeper ausgewählt, für das seine Flexibilität in der Zusammenarbeit mit verschiedenen Virenscannern, die breite Palette an Filtermöglichkeiten, Ausbaufähigkeit und Stabilität sprachen.

Die PGP-Ver- und Entschlüsselung leistet die Software „PGP eBusiness Server“ von Network Associates (NAI). Diese Applikation entspricht der Kommandozeilenvariante des für private Zwecke frei verfügbaren PGP. Die Verwendung von PGP für kommerzielle Zwecke erfordert jedoch den Erwerb einer Lizenz. Eine Integration in die bestehenden Infrastruktur-Server hätte nach PGP-Produktpolitik eine Lizenzierung jedes Systems zur Folge gehabt, sodass hier zwangsläufig hohe Kosten entstanden wären. Um diesen Nachteil zu umgehen, wurde ein separates Hardwaresystem aufgebaut, auf das der betroffene E-Mail-Verkehr zur Ver- und Entschlüsselung umgeleitet wird. Zur weiteren Kostenreduzierung laufen bei netFORMAT Untersuchungen, den PGP-eBusiness-Server durch die auch für kommerzielle Zwecke kostenfreie OpenPGP-Software GNU Privacy Guard (GNUPG) zu ersetzen.



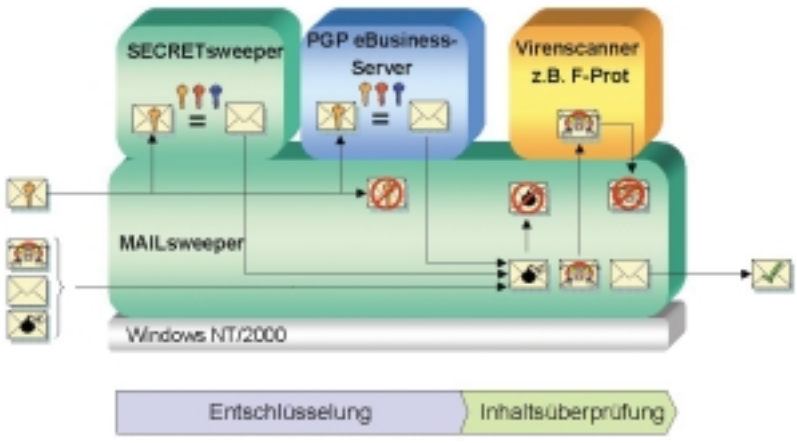

*Bu*

Um das bereits erwähnte Problem zwischen Content-Scan und Verschlüsselung zu lösen, wurde das Mail-Routing modifiziert: Für ausgehende Mails erfolgt die Verschlüsselung nach dem Content-Scan, eingehende Mails werden vor dem Content-Scan entschlüsselt. Dazu wurde der MAILsweeper über das Plug-in SECRETsweeper um S/MIME-Funktionen erweitert. Diese Implementierung gestaltete sich relativ einfach, da sie vom Hersteller als solche vorgesehen ist. Wesentlich schwieriger hingegen sah es bei der Umsetzung der PGP-Funktionen aus. Damit das Content-Security-System bei eingehenden E-Mails automatisch die verwendete Verschlüsselungsmethode erkennt und entsprechend reagiert, mussten die Fähigkeit des MAILsweepers und die Fähigkeit des PGP-eBusiness-Servers miteinander kombiniert werden, was detaillierte Kenntnisse über interne Abläufe und Schnittstellen des MAILsweepers, den Aufbau von SMTP-Nachrichten und Erfahrung im Umgang mit PGP erforderte.

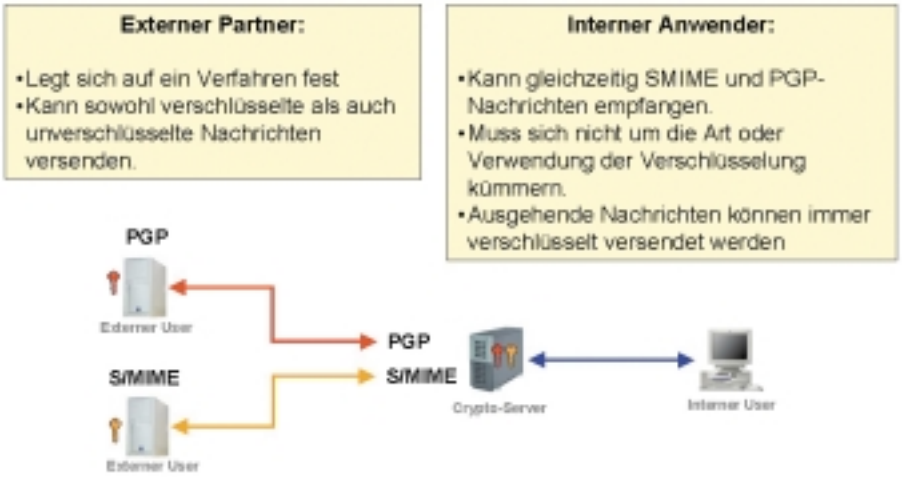
## Externe Tests

Um eine eventuell fehlerbehaftete Lösung im Produktivbetrieb zu vermeiden, wurde die Lösung zunächst intensiv bei netFORMAT getestet. „Wir mussten ganz sicher sein, dass nicht irgendwo ‘Schlupflöcher’ existierten. Ein Test bei der NORD/LB wäre ein viel zu hohes Risiko gewesen“, erklärt Schneider-Jansohn. Die Integration der neuen Sicherheitslösung gestaltete sich anschließend problemlos. Seit Ende Mai 2002 werden aus- und eingehende E-Mails für definierte Kommunikationsbeziehungen automatisch ver- beziehungsweise entschlüsselt.

Für die Mitarbeiter der NORD/LB wurden zwei Schlüsselpaare für S/MIME und (Open)PGP erzeugt. Der externe Partner wählt sine präferierte Verschlüsselungsmethode, das System erkennt dies beim Eingang




*Bu*




*Bu*

und entschlüsselt den Inhalt, sofern der „passende“ Schlüssel vorliegt. Empfänger und Absender erhalten jeweils eine Bestätigung, dass die Nachricht (de)chiffriert wurde. Für jede verschlüsselte Übertragung muss naturgemäß der öffentliche Schlüssel jedes einzelnen Empfängers vorliegen.

Die Ver- und Entschlüsselung erfolgt in beide Richtungen einstufig: Enthalten eingehende E-Mails nach dem Entschlüsselungsprozess immer noch verschlüsselte Anteile, so wird die E-Mail bei der Inhaltsprüfung abgelehnt, isoliert und Absender sowie Empfänger werden informiert. Das gleiche gilt bei einem Virusfund. Hier wird zusätzlich der Administrator informiert, um den Virus „inhouse“ zu finden. Bei übergroßen Datenmengen wird die Nachricht geparkt, der Absender informiert und die Nachricht später weitergeleitet.

## Rück- und Ausblick

Über die Erfahrungen mit der neuen Sicherheitslösung äußert man sich bei der NORD/LB sehr positiv. Siebert: „Wir haben hier eine reine SMTP-basierete Lösung, die eine automatische Ver-/Entschlüsselung mit jeder bestehenden E-Mail-Software ermöglicht. Es waren keinerlei Modifikationen am Client-Rechner der NORD/LB nötig. Lediglich der Administrator des Mail-Servers muss das korrekte Schlüsselmanagement beherrschen“. Für die Mitarbeiter der NORD/LB läuft alles unbemerkt im Hintergrund und vollständig automatisiert ab, angefangen beim Erzeugen der Schlüssel, dem Hinterlegen der Adresse und dem Schlüsselaustausch. Des Weiteren ist die Lösung so ausgelegt, dass sowohl selbsterstellte als auch Zertifikate von Zertifizierungsintanzen eingesetzt werden können. Sollte sich in der Zukunft eine Tendenz zu einer Public Key Infrastructure (PKI) entwickeln, besitzt die jetzige Lösung alle Vorraussetzungen für eine erfolgreiche Integration. ◆

Sabine Baehre betreut die PR der netFORMAT GmbH (www.netformat.de)