Open-Source-Lösung schützt E-Mails

Mit Hilfe des Open-Source-Produkts „GNU-PGP" (Pretty Good Privacy) senden und empfangen die Mitarbeiter des Landkreises Lüneburg verschlüsselte E-Mails auf Knopfdruck.

VON STEFAN DOMANSKE*

Es gleicht der Quadratur des Kreises: Wer nicht will, dass seine E-Mails für jeden lesbar durch das Internet geschickt werden, der muss sie verschlüsseln. Dann kann er aber im eigenen Netz den so entstandenen Datensalat nicht mehr auf Viren und schädliche Inhalte prüfen bevor er zum Nutzer gelangt – denn nur der darf die Daten wieder entschlüsseln. Wer hingegen jedes Bit vor dem Eintritt ins eigene Netzwerk genau auf Schädlinge untersuchen lassen will, muss seine Nachrichten offen wie eine Postkarte durch das weltweite Netz verschicken.

Komplizierter Spagat

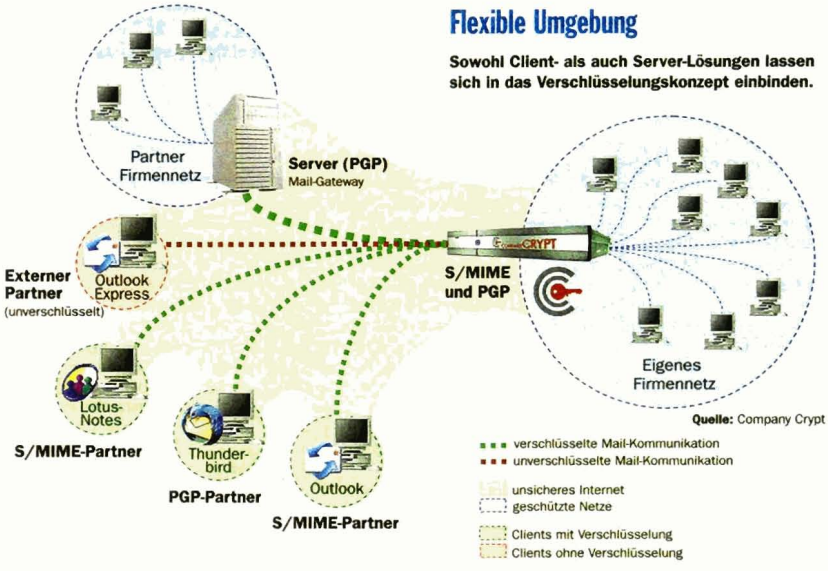
Für die schwierige Kombination gibt es mehrere mögliche Lösungen: Man entscheidet sich für Verschlüsselung oder Inhaltsprüfung und unterlässt jeweils das andere. Oder man installiert auf jedem Desktop im Unternehmen Software für beide Funktionen – was den Nachteil hat, dass E-Mails in einer Art Quarantäne entpackt und erst danach gescannt werden. Ein solches System über mehrere hundert oder gar tausend Anwender-PCs zu verteilen, kostet zudem nicht nur Zeit und Geld, es birgt auch viele Fehlerquellen.

Hier lesen Sie ...

- welche Anforderungen der Landkreis Lüneburg bei der Wahl einer E-Mail-Verschlüsselungslösung stellte;
- warum die Wahl auf die Open-Source-Lösung „GNU-PGP" fiel;
- wie die Anbindung an das bestehende Content-Filtering-System erfolgte;
- welche Pläne der Landkreis im Hinblick auf seine mobilen Mitarbeiter hat.

Beides wollte der Landkreis Lüneburg vermeiden und entschied sich daher für eine anderen Ansatz: Hierbei verschlüsselt und scannt man die Mails sofort beim Eintritt in das Netzwerk auf einem zentralen Server und schickt sie erst dann an die Anwender weiter. Das Problem: Solche Lösungen sind meist teuer und verlangen eine komplett eigene Infrastruktur.

Mit seinen derzeit rund 400 Computerarbeitsplätzen erledigt der Landkreis Lüneburg die behördlichen Belange für die 172 000 Einwohner des niedersächsischen Kreises. Der Landkreis lässt seine E-Mails schon seit 2002 von einer Software auf gefährliche Inhalte untersuchen. „Mailsweeper" von Clearswift sorgt dafür, dass Viren und Würmer nicht ins Netz der Behörde gelangen. Dafür zerlegt die Software Dateianhänge, auch wenn sie als Zip-Archiv ankommen oder als Tabellenkalkulation Daten enthalten, und prüft, ob sie gefährlichen Code mitbringen. Diese Funktion sollte auf jeden Fall auch weiterhin gewährleistet sein.



Die externen Mails auch zu verschlüsseln hatte mehr Gründe als die „Pretty Good Privacy" im Namen des Open-Source-Produktes. Der sichere elektronische Datenaustausch war besonders für den „Fachdienst Soziales" interessant: Sobald ein Sozialhilfe-Empfänger zum Arzt geht, bekommt er einen Zuschuss, die Krankenhilfe. Im Rahmen dieses Verfahrens tauschen das „Deutsche Dienstleistungszentrum für das Gesundheitswesen" (DDG) und der Fachdienst regelmäßig Krankendaten aus.

Damit niemand doppelte Bezüge von den sozialen Trägern erhält, werden zudem zwischen den Rentenkassen, den Arbeitskassen und der Sozialhilfekasse die Daten abgeglichen. Sonst könnte zum Beispiel jemand in der Stadt und im Landkreis gleichzeitig Sozialhilfe beantragen, ohne dass es auffiele.

Der Fachdienst trat eines Tages an den IT-Service heran und wollte einen alten Zopf abschneiden: Um die Sozialhilfedaten mit anderen Leistungsträgern abzugleichen oder Krankendaten für die Krankenhilfe-Abrechnung zu verschicken, steckten die Mitarbeiter eine Diskette in einen Umschlag und verschickten diesen per Post – in der Annahme, die Daten seien so sicherer als per E-Mail. Dieses Verfahren kostete außer Zeit auch Geld. Die Informationen einfach per E-Mail zu versenden war gesetzlich jedoch nicht möglich, da personenbezogene Daten vor neugierigen Blicken geschützt werden müssen.

Verschlüsselung per Gesetz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ein Handbuch herausgegeben, das das TDDSG (Teledienste-Datenschutz-Gesetz) ausführt. Darin ist zweierlei geregelt: Erstens müssen personenbezogene Daten verschlüsselt werden. Zweitens hat der Bürger ein Recht auf Selbstdatenschutz. Das bedeutet, dass er die Möglichkeit haben muss, Informationen verschlüsselt an den Landkreis zu verschicken. Wie er das tun kann, muss ihm der Landkreis als Anbieter gemäß Paragraf 4, Absatz 1 TDDSG mitteilen. Das Handbuch empfiehlt für die Verschlüsselung ebenfalls PGP.

„Innerhalb von drei Tagen wurde die Lösung installiert."

Stefan Domanske, Administrator

Im Landkreis Lüneburg wacht neben Clearswifts Mailsweeper eine umfangreiche Sicherheitsarchitektur mit einem mehrstufigen Virenscan über die Sicherheit des Netzes. Einem Nutzer hatte der IT-Service bereits eine kostenfrei verfügbare Verschlüsselungslösung für seine E-Mails zusammengestellt. Mit der Desktop-Version von GNU-PGP konnte er seine Mails für fremde Augen unlesbar machen – allerdings auch für Mailsweeper und die Virenscanner.

Mit diesem Problem wandte sich Michael Ziegeler, Leiter des Fachdienstes IT-Service, daher an den Anbieter. Die Firma selbst hatte zwar keine Lösung im Haus, wusste jedoch jemanden, der helfen konnte: der IT-Dienstleister Netformat in Hannover. Der sei in der Lage, eine auf GNU-PGP basierende Verschlüsselung an das API (Application Programming Interface) des Mailsweeper einzubauen und damit Verschlüsselung und Inhaltsprüfung zentral zu kombinieren.

Geringe Softwarekosten

Das Angebot an Mail-Verschlüsselungslösungen ist groß. Aus dem kostenlosen PGP-Produkt ist inzwischen eine kommerzielle Lösung entstanden, die PGP Corp. bietet für Firmen den „PGP Universal Server" an. Dieser kam für den Landkreis aus verschiedenen Gründen aber nicht in Frage. Einer davon war das Geld: 20 000 Dollar hätte die Anbindung von 500 Mail-Adressen gekostet.

„Außerdem ist das mehr eine Entwicklungsumgebung", erzählt Ziegeler, „da hätten wir erst viel anpassen müssen." Zudem lässt sich in die PGP-Lösung nur ein Virenscanner einbauen, die genauere Inhaltsprüfung von Mailsweeper wäre weggefallen. RSA-Security bringt ebenfalls einen eigenen RSA-Server mit und ließe sich nicht an den Mailsweeper anhängen. Auch die Produkte von Firmen wie Onaras und Utimaco brauchen eine eigene Infrastruktur und hätten damit die bereits laufende Applikation in Lüneburg überflüssig gemacht.

Entscheidung für Open-Source

Derartige Probleme sind im Umfeld von Verschlüsselungslösungen alles andere als neu: Die Meta Group (inzwischen von Gartner gekauft) stellte bei einer Umfrage fest, dass 35 Prozent der Projekte für zentrale Verschlüsselung daran scheitern, dass sich andere Sicherheitsprodukte nicht einbinden lassen. „Ich kann ja nicht meine ganze Infrastruktur wegwerfen, weil einige Anwender E-Mail-Verschlüsselung brauchen", erklärt Ziegeler seine Situation.

Das ist auch gar nicht nötig, selbst wenn große Firmen die Situation so darstellen sollten. Nach dem Gespräch mit Netformat wurde in Lüneburg deutlich, dass sich die Open-Source-Software Gnu-PGP, so wie Netformat sie anbietet, an den Mailsweeper anschmiegen würde, ohne ihn zu behindern. Eine so angepasste PGP-Lösung passte perfekt in das Konzept der Behörde: Sie war für den Anwender unsichtbar, sie würde alles zentral regeln, und sie beruhte auf Open-Source-Software – der Preis belief sich damit inklusive Installation auf gerade einmal 3000 Euro.

„Der Schulungsaufwand für die Anwender war minimal."

Michael Ziegeler,
Leiter Fachdienst IT-Services

Nachdem Netformat der Behörde erklärt hatte, wie das Pro-

Mehr zum Thema

www.computerwoche.de/go/

155040: Unternehmen müssen E-Mails schützen; (P)
***78546:** Phil Zimmermann: „Das traditionelle PKI-Konzept hat versagt";
***77786:** Sicheres Lotus Notes.

jekt zu verwirklichen sei, ging es schnell: Innerhalb von drei Tagen hatten der Autor dieses Textes und ein Spezialist von Netformat die Lösung gemeinsam installiert. Als Server diente der Intel-Rechner, der auch schon Clearswifts Lösung beherbergte. Mit seinen 1 GB Arbeitsspeicher und der 100-Megabit-Ethernet-Verbindung versorgt er das gesamte Netzwerk.

Unsichtbarer Helfer

Da das System zentral läuft, war der Schulungsaufwand für die Mitarbeiter minimal: „Wir haben einen kurzen Hinweis verschickt, dass Mails jetzt verschlüsselt werden können, das war alles", erzählt Ziegeler. Den größten Teil der Arbeit erledigen der Server und das IT-Service-Team.

Die Lösung ist für den Nutzer nicht sichtbar. Er muss sich nur ein einziges Mal von seinem Gegenüber einen PGP-Schlüssel an eine zentrale Adresse schicken lassen und per Telefon dessen Echtheit überprüfen. Sobald daraufhin die dazugehörige Mail-Adresse eingetippt wird, weiß der Server, dass er die Mail verschlüsseln muss. Genauso läuft es, wenn eine Nachricht von diesem Kommunikationspartner ankommt: Der Server entschlüsselt sie und leitet sie

Den eigenen öffentlichen Schlüssel kann man anderen Teilnehmern per E-Mail zukommen lassen.

FOTO: DATENSCHUTZZENTRUM SCHLESWIG-HOLSTEIN

dann nach einer Inhaltsprüfung im internen Netz an den Adressaten weiter.

Die Schlüssel werden zentral auf dem Mailsweeper-Server verwaltet – auch damit hat der Nutzer nichts zu tun. Die Administratoren haben die Kommunikationspartner in Gruppen eingeteilt, je nachdem ob sie ausschließlich verschlüsseln oder auch mit Signaturen und Zertifikaten ihre Mails digital unterschreiben. Die für die Zertifikate notwendige Ausgabestelle (Certificate Authority) hatte der IT-Service bereits im Haus.

Zufriedene Anwender

Bisher arbeiten zehn Nutzer mit dem neuen Verschlüsselungssystem. „Auch der eine Anwender, der das vorher auf seinem Rechner selbst gemacht hatte, freut sich über die einfache neue Handhabung", beschreibt Ziegeler die Erfahrungen. In Zukunft soll die Zahl der Nutzer steigen: „Wir prüfen derzeit, welche Fachapplikationen dafür noch geeignet sind. Es gibt viele Stellen, die Daten zusammenstellen und verschicken", und hier könne man eventuell komfortabler mit PGP operieren als mit Datenträgern.

Verschlüsselung bald für PDAs

Netformat arbeitet gerade daran, die Lösung auch für das Verschlüsselungsverfahren „S/Mime" zu erweitern. Im Entwicklungslabor funktioniert das bereits. „Wir planen, unseren Kunden noch in der zweiten Jahreshälfte diese alternative Verschlüsselungstechnik zur Verfügung zu stellen. Jedoch fragen nach unserer Erfahrung 80 Prozent der Kunden PGP nach", erzählt Birk Zscheppank, Geschäftsstellenleiter von Netformats Niederlassung in Hannover.

Für die Zukunft plant der 17 Mann starke IT-Service in Lüneburg, die Lösung auf tragbare Geräte zu erweitern. Wer mit seinem PDA Mails abruft und verschickt, könnte ebenfalls verschlüsseln, ohne eine zusätzliche Software zu installieren, da PGP ja erst am Mail-Server zum Einsatz kommt. Zwischen Server und PDA wäre die Mail dann über die SSL-Verbindung verschlüsselt und damit sicher. Derzeit testet die IT-Abteilung eine solche Lösung mit dem Treo-Smartphone. Das gleiche Konzept ist darüber hinaus für Telearbeit und Web-Portale einsetzbar. *(ave)* ◆

Vorteile

- Zentrale E-Mail-Verschlüsselung und zentrale Schlüsselverwaltung;
- Anpassung an vorhandene Infrastruktur möglich;
- IT-Dienstleister Netformat begleitet durch alle Projektphasen;
- Lösung innerhalb von drei Tagen lauffähig;
- keine zusätzliche Hardware nötig;
- geringe Kosten durch den Einsatz von Open-Source-Software;
- Support und Wartung durch Netformat;
- kein Schulungsaufwand, Lösung läuft für den Nutzer unsichtbar auf dem zentralen Rechner.

***STEFAN DOMANSKE**
ist Administrator beim Landkreis Lüneburg.