Zentrale Open Source-Lösung

eMails im Briefumschlag

Verschlüsselung. Beim Landkreis Lüneburg wurde das Open Source-Produkt Gnu-PGP (Pretty Good Privacy) in die bestehende eMail-Infrastruktur integriert. Die Anwender können nun auf Knopfdruck verschlüsselte eMails senden und empfangen – ganz ohne Schulungen, ohne Sicherheitsverluste und ohne Lizenzkosten.

Wer nicht will, dass seine eMails für jeden lesbar durch das Web 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 alle Nachrichten offen wie eine Postkarte empfangen.

Um dennoch beides zusammen zu ermöglichen – also Verschlüsselung und Inhaltsprüfung – gibt es mehrere mögliche Lösungen: Man installiert auf jedem Desktop beide Systeme – was den Nachteil hat, dass die Mails in einer Art „Quarantäne“ entpackt werden und dann erst gescannt werden können. Ein solches System über mehrere hundert oder gar tausend Anwender-Rechner zu verteilen, kostet nicht nur Zeit und Geld, es birgt auch viele mögliche Fehlerquellen.

Eine andere Möglichkeit wählte der Landkreis Lüneburg: Dort werden die Mails sofort beim Eintritt in das Netzwerk auf einem zentralen Server entschlüsselt und gescannt und erst dann an den User weitergeleitet. Das Problem: Solche Lösungen sind meist teuer und erfordern eine komplett neue IT-Infrastruktur.

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

Die externen Mails zusätzlich zu verschlüsseln, hatte mehr Gründe als die „Pretty Good Privacy“ – der sichere elektronische Datenaustausch war besonders für den „Fachdienst Soziales“ des Landkreises interessant. Hintergrund: Sozialhilfeempfänger erhalten für einen Arztbesuch 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 bezieht, werden darüber hinaus alle Daten zwischen den Renten-, den Arbeitskassen und der Sozialhilfekasse abgeglichen.

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

Verschlüsselung gefordert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ein Handbuch herausgegeben, das das TDDSG (TelediensteDatenschutzGesetz) 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. Wer also irgendeine Form von elektronischer Verwaltung anbietet, ist zu einer Unterrichtung nach §4, Abs. 1 TDDSG verpflichtet, aus der Bürger erfährt, wie er seine persönlichen Daten für Dritte uneinsehbar an den Landkreis schicken kann. Dieses Handbuch empfiehlt für die Verschlüsselung ebenfalls PGP.

Im Landkreis Lüneburg wird der Verkehr im Intra- und Internet neben Clearswifts Mailsweeper durch eine umfangreiche Sicherheitsarchitektur mit einem mehrstufigen Virenscan überwacht. Einem Nutzer hatte der IT-Service bereits eine Verschlüsselungslösung für seine eMails zusammengestellt. Mit der Desktopversion von „Gnu-PGP“ konnte er seine Mails für fremde Augen unlesbar machen – allerdings galt das auch für Mailsweeper und die Virenscanner. Deshalb wandte sich der Leiter des Fachdienstes IT-Service, Michael Ziegeler, an Clearswift und trug sein Problem vor. Das Unternehmen hatte für das Problem zwar keine eigene Lösung parat, wusste jedoch trotzdem Rat und empfahl den IT-Dienstleister Netformat in Hannover. Die Firma könne eine auf Gnu-PGP basierende Verschlüsselung an die API-Schnittstelle (Application Programming Interface) des Mailsweepers einbauen und damit Verschlüsselung und Inhaltsprüfung zentral kombinieren.

Geringe Softwarekosten

Das Angebot an Mail-Verschlüsselungslösungen auf dem Markt ist groß. So ist aus dem einst kostenlosen PGP-Produkt inzwischen eine kommerzielle Lösung entstanden; die PGP Corporation bietet den PGP Universal Server für Firmen an. Ein PGP-Universal Server kam für den Landkreis aber aus verschiedenen Gründen nicht in Frage. Zum einen ist das US-Produkt ein teures Vergnügen: 20 000 US-Dollar hätte die Anbindung von 500 Mailadressen 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 lässt sich nicht mit dem Mailsweeper kombinieren. Die Produkte von Firmen wie Onaras und Utimaco brauchen ebenfalls eine eigene Infrastruktur und hätten damit bereits laufende Applikation in Lüneburg überflüssig gemacht. Dies ist ein bekanntes Problem des Verschlüsselungsmarktes. So stellte die Meta-Group bei einer Umfrage fest, dass 35 Prozent der Projekte zur zentralen Verschlüsselung daran scheitern, dass sich andere Sicherheitsprodukte nicht einbinden lassen. „Ich kann ja nicht meine ganze Infrastruktur wegwerfen, weil einige Anwender eMail-Verschlüsselung brauchen“, erklärt Ziegeler seine Situation. Das ist auch gar nicht nötig, selbst wenn große Firmen die Situation so darstellen sollten. Denn nach dem Gespräch mit Netformat wurde deutlich, dass die Open Source-Software Gnu-PGP, so wie Netformat sie anbietet, mit dem Mailsweeper zusammenarbeitet, ohne ihn zu behindern. Eine so angepasste PGP-Lösung passte perfekt in das Konzept der Behörde: Sie bleibt für den Anwender unsichtbar, regelt alle Abläufe zentral und sie beruht auf Open Source-Software. Der Preis belief sich inklusive Installation auf nur 3 000 Euro.

Nachdem Netformat dargelegt hatte, wie das Projekt zu verwirklichen sei, ging es schnell: Innerhalb von drei Tagen hatten der Lüneburger IT-Sicherheits-Administrator Stefan Domanske und ein Spezialist von Netformat die Lösung gemeinsam installiert. Als Server diente der Intel-Server, der auch schon Clearswifts Lösung beherbergte. Mit seinem 1 GB-Arbeitsspeicher und der 100 Megabit Ethernet-Verbindung versorgt er das gesamte Netzwerk.

Unsichtbarer Helfer

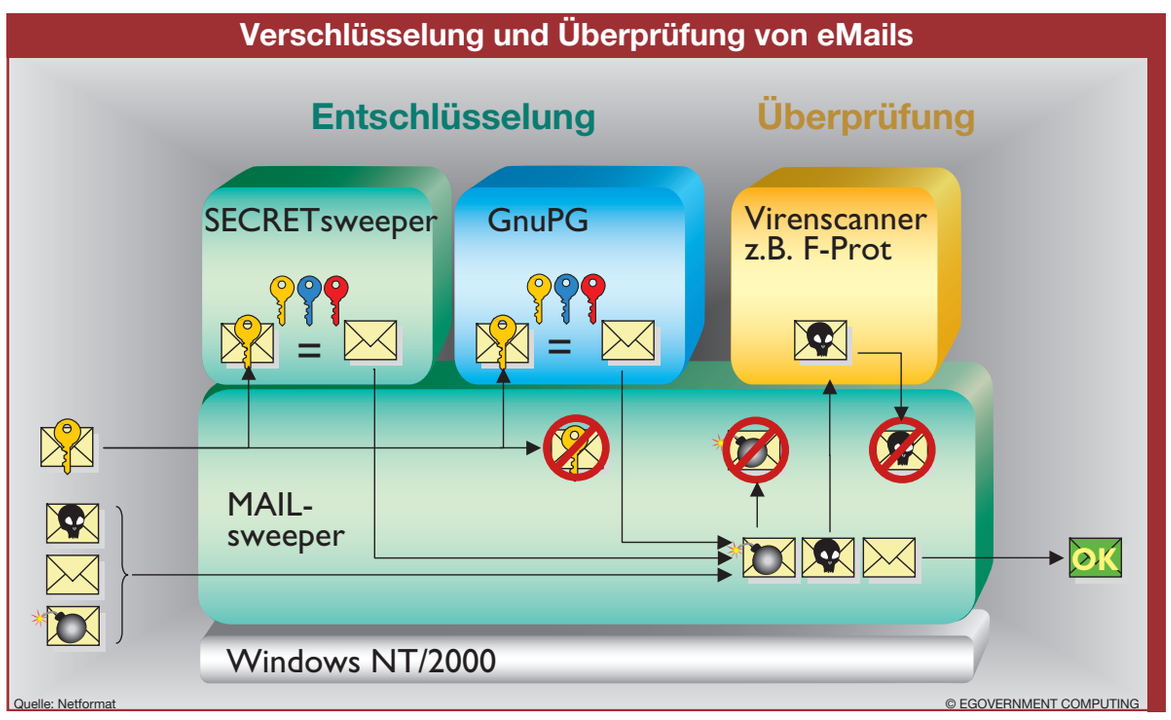
Da das System zentral läuft, war der Schulungsaufwand für die Mitarbeiter minimal: „Wir haben einen kurzen Hinweis verschickt, dass Mails jetzt verschlüsselt werden können – das war alles“, erklärt Ziegeler. Die meiste Arbeit erledigen der Server und das IT-Serviceteam.

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 dazu gehörige Mailadresse eingetippt wird, weiß der Server, dass er die Mail verschlüsseln muss. Desgleichen, wenn eine Mail von diesem Kommunikationspartner ankommt: Der Server entschlüsselt sie und leitet sie dann nach einer Inhaltsprüfung im internen Netz an den Adressaten weiter. Da der Server die gesamte Verschlüsselung vollautomatisch übernimmt, war keine Schulung für die Applikation notwendig. 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.

Bisher arbeiten zehn Nutzer mit dem neuen Verschlüsselungssystem. Weitere sollen folgen: „Wir prüfen, welche Fachapplikationen dafür noch geeignet sind. Es gibt viele Stellen, die Daten zusammenstellen und verschicken“, so Ziegeler. Auch hier könnte man komfortabler mit PGP arbeiten, statt Datenträger per Post zu versenden.

Netformat arbeitet gerade daran, die Lösung auch für das Verschlüsselungsverfahren „S / MIME“ zu erweitern. „Wir planen, noch in der zweiten Jahreshälfte diese alternative Verschlüsselungstechnik zur Verfügung zu stellen. Jedoch fragen nach unserer Erfahrung 80 Prozent der Kunden PGP nach“, so Birk Zscheppank, Geschäftsstellenleiter der Netformat-Niederlassung in Hannover.

Für die Zukunft plant der 17 Mann starke IT-Service in Lüneburg, die Lösung auch auf tragbare Geräte zu erweitern. Wer mit seinem PDA Mails abruft und verschickt, könnte ebenfalls verschlüsseln, ohne zusätzliche Software installieren zu müssen, da PGP ja erst am Mailserver zum Einsatz kommt. Zwischen Server und PDA wäre die Mail dann über eine SSL-Verbindung verschlüsselt und somit vor einem unbefugten Zugriff sicher. Derzeit läuft eine solche Lösung im Testbetrieb.



ZENTRAL. Eingehende Nachrichten werden auf dem Mailserver zunächst entschlüsselt und dann überprüft

ÜBERSICHT

VORTEILE DER LÖSUNG IM ÜBERBLICK:

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

Interview

„Ein kostengünstiges Angebot, das zu uns passt“

Nachgefragt. eGovernment Computing sprach mit Michael Ziegeler, Leiter IT-Service beim Landkreis Lüneburg, über die Verschlüsselungslösung Gnu-PGP (Pretty Good Privacy).

eGovCom: Warum haben Sie sich für eine zentrale Verschlüsselungslösung entschieden?
Ziegeler: Aus drei Gründen: Wir brauchten eine zentrale Verschlüsselung, damit sie für den Anwender problemlos im Hintergrund abläuft. Unser Konzept ist es, alles zentral anzubieten, damit die Mitarbeiter möglichst wenig zusätzliche Arbeit haben. Deshalb besteht unser Netz zu 95 Prozent aus Thin Clients, die auf zentrale Presentation Server zugreifen. Zudem erforderte das keine Schulung und produziert weniger Fehler als eine eigene Installation auf jedem einzelnen Desktop.

eGovCom: Es gibt für Verschlüsselungslösungen große Firmen mit großen Namen. Wie kam es, dass der Landkreis Lüneburg die Dienste von Netformat und ein Open Source-Produkt nutzt?
Ziegeler: Der IT-Service musste feststellen, dass die meisten Anbieter eine komplett eigene Infrastruktur – also eigene Server – mitbringen. Wir haben aber vorher schon mit Clearswift zusammengearbeitet und hatten den Mailsweeper bereits im Haus. Netformat hingegen konnte uns passend zu unserer Inhaltsprüfung eine maßgeschneiderte Lösung bauen. Es war zudem ein sehr kostengünstiges Angebot, das außerdem ausgezeichnet zu unserem zentralen Konzept passte.

MICHAEL ZIEGELER, Leiter IT-Systeme beim Landkreis Lüneburg, ist zufrieden mit der Open Source-Verschlüsselungslösung

eGovCom: Konnten Sie mit der neuen Verschlüsselung ihre Ziele erreichen?
Ziegler: Ja, wir sind jetzt effektiver: Ohne Mehraufwand können die Mitarbeiter ihre Mails nun verschlüsselt verschicken – und sind damit gesetzeskonform. Der Vorgang für den Nutzer ist der Gleiche geblieben. Und das ist natürlich komfortabler und langfristig auch günstiger, als eine Diskette in einen Umschlag zu stecken, wie wir das früher gemacht haben.

eGovCom: Wie zufrieden sind Sie im täglichen Umgang mit der Verschlüsselungslösung?
Ziegeler: Wir sind sehr zufrieden, denn sie passt genau in unser Konzept, möglichst alle Dienstleistungen zentral anzubieten. Die Benutzer akzeptieren die Lösung und freuen sich über die einfache Handhabung – und den Administratoren geht es genauso.
Wir prüfen bereits, welche Fachapplikationen dafür noch geeignet sein könnten. Es gibt im Landkreis viele Abteilungen, die ihre Daten sammeln und derzeit noch auf Datenträgern verschicken. Vielleicht könnte man auch in diesen Fällen mit unserer zentralen eMail-Verschlüsselung arbeiten.

Das Interview führte Nico Litzel

DER AUTOR

STEFAN DOMANSKE

ist Administrator IT und Sicherheit beim Landkreis Lüneburg