DuD
Datenschutz und Datensicherheit

PGP, zum Dritten

Neue Verschlüsselungskonzepte für „alte“ Software

Rainer W. Gerling, Stefan Kelm

Seit nunmehr rund einem Jahrzehnt gilt das Programm PGP („Pretty Good Privacy“) als der Standard für E-Mail- und Datei-Verschlüsselung, insbesondere unter Internet-Benutzern. Im vergangen Jahr wurde PGP von NAI eingestellt[1] und später vom Startup PGP Corp. wiederbelebt. Jetzt steht mit PGP Universal ein neues Produkt vor der Tür. Die neuen Konzepte werden vorgestellt und mit vorhandenen Lösungen verglichen

Dr.
Rainer W. Gerling

Datenschutzbeauftragter der Max-Planck-Gesellschaft, Lehrbeauftragter für Datensicherheit an der FH München. Studium der Physik an der Universität Dortmund. Promotion und Habilitation an der Universität Erlangen-Nürnberg.
E-Mail: rgerling@gmx.de

Stefan Kelm
Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: Public Key Infrastrukturen, digitale Signaturen, Rechner- und Netzwerksicherheit
E-Mail: kelm@secorvo.de

[1] Gerling/Kelm: PGP, quo vasisti? DuD 2002, 300-301.

1 Einleitung

Seit einiger Zeit ist PGP 8, das unter aktuellen Betriebssystemen (z.B. Windows XP und Mac OS X) funktioniert, verfügbar.[2] Aus Sicht vieler Nutzer, die ein freies (im Sinne von kostenloses) PGP erwarteten, erschien dies jedoch als ein Rückschritt: PGP 8 Freeware ist nur noch ohne Plugins für E-Mail Programme verfügbar; lediglich einige wenige Plugins von Drittanbietern (z.B. QDpgp[3] für Pegasus Mail) erlauben ein kostenloses Gespann aus E-Mail-Programm und PGP 8. Auch das von vielen Anwendern geschätzte PGPdisk ist nicht in der Freeware-Version, sondern nur noch in der kostenpflichtigen PGP Personal-Version enthalten.[4]

Den kompletten Quellcode von PGP gibt es auch in der aktuellen Version wieder zeitnah und vollständig. Und die Veröffentlichung des Quellcodes hat nicht mehr den faden Beigeschmack, nur als Hilfsmittel für das Unterlaufen der US-amerikanischen Exportvorschriften zu dienen. Jedoch erscheinen die entsprechenden Lizenzbestimmungen im Vergleich zu früheren Versionen etwas schärfer.

Die Einführung von PGP (oder grundsätzlich der E-Mail-Verschlüsselung) in Unternehmen sowie im Privatbereich blieb jedoch in der Vergangenheit weit hinter den Erwartungen zurück. Mit Argumenten wie „Ich habe ja nichts zu verbergen“ oder „Warum sollte ein Fremder meine E-Mails lesen wollen?“ werden unverschlüsselte E-Mails auch und insbesondere im kommerziellen Umfeld tagtäglich in großen Mengen verschickt. Hinzu kommt, dass viele Menschen über kein PGP-Schlüsselpaar verfügen, also gar keine verschlüsselten E-Mails senden bzw. empfangen können. Die Herausforderung an dieser Stelle ist somit die Lösung des Problems: Wie bekomme ich die Leute zum Verschlüsseln?

Weitere wesentliche Gründe, die aus heutiger Sicht gegen einen flächendeckenden Einsatz von Verschlüsselungssoftware sprechen, sind die mangelnde Sensibilisierung („Awareness“), sowie das fehlende Verständnis der Benutzer – auch versierte Anwender verstehen häufig nicht, was sie zu tun haben, um gesichert per E-Mail kommunizieren zu können, selbst wenn heute viele Standard-Anwendungen bereits über entsprechende Icons zum Signieren/Verschlüsseln verfügen.

Eine Lösung, die vor allem aus Unternehmenssicht auf der Hand liegt, ist eine vollautomatische Schlüsselgenerierung und Verschlüsselung, ohne dass der Mitarbeiter/Nutzer aktiv werden muss. Jeden PGP-Aktivisten wird es ob solcher Lösungsvorschläge wahrscheinlich schütteln; er will die Verschlüsselung selbstverständlich aktiv kontrollieren, und vor allem will er auch den Schutz seines privaten Schlüssels selbst in die Hand nehmen.

Die Interessen eines Unternehmens oder einer Behörde jedoch sind hier völlig anders: In vielen Einrichtungen schreibt die (Security)Policy den Schutz von sensitiven Daten – insbesondere beim Transport – verbindlich vor. Hier soll ein vertraulicher E-Mail Austausch mit Kunden, Lieferanten oder Außenstellen möglich sein. Und dieses möchte das Unternehmen effektiv durchsetzen, auch wenn die Beschäftigen bezüglich dieser Maßnahmen nicht immer kooperativ sind.

Abhilfe schafft dann in der Regel nur eine serverbasierte (proxyartige) Lösung, die transparent und automatisch sämtliche E-Mails (oder solche für festgelegte Kommunikationspartner) ver- und entschlüsselt, ohne dass der Anwender aktiv werden muss. Seit einiger Zeit gibt es entsprechende Lösungen am Markt. Erstaunlicherweise kommt mit GEAM[5] die älteste Lösung aus der Open-Source Ecke. GEAM entstand im

[2] Camphausen/Kelm: Auferstanden, Verschlüsselungssoftware PGP in neuen Versionen, iX 2/2003.

[3] http://community.wow.net/grt/qdpgp.html

[4] Ebenfalls nicht enthalten ist der frühere PGPvpn-Client, dessen Rechte noch immer bei NAI liegen. Dieses Produkt ist inzwischen als „McAfeeVPN Client“ verfügbar.

[5] http://www.g10code.de/de/p-geam.html

Rahmen der GnuPG-Entwicklung. Aber auch Hersteller wie Glück & Kanja und Utimaco Safeware haben mit dem CryptoEx Business Gateway[6] bzw. dem SecurE-Mail Gateway[7] Produkte am Markt.

Am 16. September diesen Jahres stellte PGP sein neues Gateway PGP Universal[8] vor, welches – im krassen Gegensatz zu allen bisherigen PGP-Versionen – ebenfalls serverbasierte Verschlüsselungsverfahren realisiert. In Unternehmen und Behörden trifft dieses Programm schon jetzt auf ein großes Interesse.

2 Verschlüsselungs-Proxy

Proxies als „Vermittler“ einer Kommunikationsbeziehung sind in Netzwerken wie dem Internet schon lange bekannt. Relativ neu ist jedoch der Einsatz bei der E-Mail-Verschlüsselung: Auf oder neben dem E-Mailserver wird die zentrale Verschlüsselungssoftware installiert, so dass sich auf dem Arbeitsplatzrechner der E-Mail-Nutzer nichts ändert. Dies bedeutet jedoch zunächst, dass die Kommunikation zwischen dem Klienten (Arbeitsplatzrechner) und dem E-Mailserver weiterhin ungeschützt ist und daher (vor allem von internen Tätern) angegriffen werden kann. An dieser Stelle sind daher Standardverfahren der Verschlüsselung mit SSL/TLS (Siehe Kasten) unerlässlich.

Der Proxy selbst muss offensichtlich besonders vor Angriffen geschützt werden, da er zahlreiche kryptographische Schlüssel – vor allem die privaten Schlüssel der Endanwender – verwaltet. Hier sind z.B. Maßnahmen wie das „Härten“ des Betriebssystems angebracht. Ansonsten ist die Funktionalität eines solchen Proxies recht einfach, sofern die Schlüssel aller Kommunikationsteilnehmer vorhanden sind.

Solange zwei Proxies direkt miteinander kommunizieren (Abb. 1a), gibt es keine Probleme. Auch wenn ein Desktopklient eine E-Mail selbst verschlüsselt und anschließend an einen (externen) Proxy schickt (Abb. 1b), gibt es keine Probleme. Interessant ist jedoch die Frage der Integration einer verschlüsselnden Desktoplösung, wenn der entsprechende Klient (wie in Abb. 1c) „hinter“ einem lokalen Proxy steht: Je nach Art der Integration erhält der Empfänger nach der Entschlüsselung von seinem Proxy den korrekten Klartext (der erste

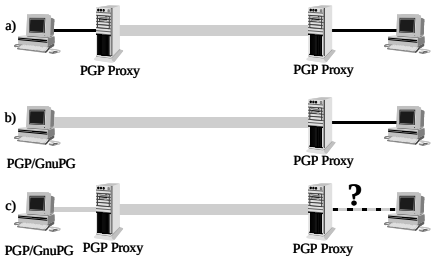

Abb. 1: Die drei verschieden Szenarien zur Kommunikation. Schwarze Linien stellen unverschlüsselte Kommunikation, graue Linien verschlüsselte Kommunikation dar.

Proxy hat „erkannt“, dass die E-Mail schon verschlüsselt war und sie daraufhin einfach an den zweiten Proxy „durchgereicht“) oder eine verschlüsselte Nachricht (der erste Proxy hat schlicht ein zweites Mal verschlüsselt), mit der er offensichtlich erst einmal nicht viel anfangen kann.

Dieses hybride Szenario, dass „hinter“ einem Verschlüsselungs-Proxy auch noch Klienten mit einer eigenen Desktop-Verschlüsselung sind, wird wohl am ehesten der Realität entsprechen. Deshalb ist eine saubere Lösung hierfür unerlässlich. Der Desktop-Klient muss sicherlich von der Existenz des Proxies wissen, um eine elegante Integration zu ermöglichen.

3 Zentrale Schlüsselerzeugung

Da viele Anwender sehr zurückhaltend bei der Generierung eigener PGP-Schlüsselpaare sind, liegt es nahe, diese Schlüsselpaare automatisch zu generieren, sobald der Anwender zum ersten Mal verschlüsselt kommunizieren will bzw. laut Security-Policy muss. PGP Universal leistet dies, wie auch andere Produkte. Unmittelbare Konsequenz dieses Verfahrens: Die privaten Schlüssel liegen nun auf dem zentralen Verschlüsselungsserver; der private Schlüssel ist damit nicht durch ein Passwort (Mantra) des Benutzers geschützt, sondern nur so sicher wie die Sicherheitsmechanismen auf dem Proxy-Server. Key Recovery[9] ist beim Zugriff auf die privaten Schlüssel kein Problem.

Um für einen Nutzer einen Schlüssel erzeugen zu können, muss die Existenz und die Identität des Nutzers vorher zweifelsfrei festgestellt werden können. Hierzu dienen in der Regel papierbasierte Registrierungsverfahren unter Einsatz von vertrauenswürdigen Instanzen (PKI). Soll demgegenüber PGP Universal einen Schlüssel automatisch generieren, muss der Benutzer elektronisch authentifiziert werden. Die einzige halbwegs „sichere“ Möglichkeit ist dabei die Verwendung einer vorhandenen digitalen Identität. Der Benutzer wird sich dazu gegen eine in der Regel in den Unternehmen bereits vorhandene Benutzerdatenbank (LDAP-Verzeichnis, Active Directory, Radius-Server oder Passwort-Datei) authentisieren müssen. Im Rahmen von PGP Universal wird hier beispielsweise die Authentisierung beim E-Mail Versand über SMTP AUTH (siehe Kasten) verwendet. Dies kann zusätzlich durch eine Transportverschlüsselung (SSL/TLS) abgesichert werden.

4 Verschlüsselung ohne Schlüssel

Ein in der Praxis sehr interessantes Problem ergibt sich immer dann, wenn der Empfänger der E-Mail keinen öffentlichen Schlüssel hat, die Policy des Unternehmens aber eine Verschlüsselung zwingend vorschreibt. Einfache Lösungen wären das Blockieren der E-Mail oder das unverschlüsselte Versenden – beides ist selbstverständlich nicht akzeptabel. Die Utimaco Lösung beispielsweise generiert in diesem Fall einen Zufallsschlüssel und verschlüsselt die E-Mail mit dem Programm PrivateCrypto.[10] Der Zufallsschlüssel wird an den Absender der E-Mail geschickt (eine mögliche Option), damit dieser ihn „out-of-band“ sicher an den vorgesehenen Empfänger kommunizieren kann. PrivateCrypto gibt es derzeit nur für Windows, was die Möglichkeiten leider einschränkt.

PGP Universal schickt dem Empfänger ohne Schlüsselpaar eine URL (Web-Adresse), wo er über ein Webmail-Interface die E-Mail lesen und eventuell vorhandene Anhänge herunterladen kann. Der Zugriff auf diese Webmail-Oberfläche ist durch ein Passwort geschützt. Im einfachsten Fall erzeugt der Empfänger beim ersten Zugriff auf die Webmail-Oberfläche sein Passwort selbst. Dies setzt stets voraus, dass die E-Mail, welche die URL enthält, ohne abgehört zu werden beim Empfänger ankommt, denn diese E-Mail ist unverschlüsselt. Der anschließende Zugriff auf die Webmail-Oberfläche erfolgt SSL/TLS-verschlüsselt per https. Deutlich sicherer (aber auch organisatorisch aufwendiger) wäre die automatische Vergabe eines Initialpasswortes, das out-of-band an die Empfänger kommuniziert werden muss.

PGP bietet im Rahmen von PGP Universal ferner einen kleinen lokalen PGP-Proxy

[6] http://www.cryptoex.com/
[7] http://www.utimaco.de/
[8] http://www.pgp.com/

[9] Gerling Company Message Recovery DuD 1998, 38.

[10] http://www.privatecrypto.de/

als zusätzliche Desktopkomponente an (PGP Satellite). Dieser kann von der Webmail-Oberfläche herunter geladen und (falls dies nicht mit der Firmen-Policy des Empfängers kollidiert) installiert werden. Dieser Proxy ist derzeit nur für Windows verfügbar. Er implementiert die wesentlichen Verschlüsselungsroutinen und kann in der Funktionalität mit GPGrelay[11] verglichen werden.

Ein wesentlicher Unterschied zur „normalen“ PGP-Desktopversion ist der Umgang mit sog. „Domain Policies“ (s.u.). Der PGP Satellite „erinnert“ sich an sein Ursprungsunternehmen und setzt deren Policy weiter konsequent um, auch wenn sie beispielsweise auf dem Rechner eines anderen Unternehmens installiert wurde. Damit kann z.B. erreicht werden, dass auf eine verschlüsselte E-Mail auch verschlüsselt geantwortet werden muss.

Es bleibt abzuwarten, inwieweit die Kommunikationspartner eines Unternehmens sich die Kommunikationsverfahren aufzwingen lassen. Das hängt zu einem wesentlichen Teil auch von der Beziehung der Kommunikationspartner ab: einem Lieferanten kann man als Unternehmen eher etwas „nahe legen“ als einem Kunden. Ein zukünftig auch erhältliches PGP 9 soll in allen Lizenzversionen (Freeware, Personal, Enterprise) auch die PGP Satellite Funktionalität enthalten.

5 Domain Policies

PGP Universal hat seine Stärken in der Durchsetzung von sog. Domain Policies und der Integration in Firmenabläufe. Innerhalb dieser Domain Policies kann sehr detailliert festgelegt werden, welche Kommunikationsbeziehungen auf welche Art und Weise geschützt werden müssen. Da die Policies von den Proxies (also auch von dem PGP Satellite) realisiert werden, kann ein Unternehmen somit an zentraler Stelle Verschlüsselungsverfahren durchsetzen, ohne dass der Benutzer „mitspielen“ muss. Dies ist somit eine Stärke von PGP Universal gegenüber existierenden Open-Source Lösungen, die doch mehr von der Individualnutzung geprägt sind.

Die Domain Policy muss vor der Einführung gut überlegt werden, da an vielen „Einstellschrauben“ gedreht werden kann. Dabei muss das Sicherheitsbedürfnis gegen die Einfachheit der Nutzung abgewogen werden. Die Ausdehnung der eigenen Policy auf kleine Enklaven bei den Kommunikationspartnern (PGP Satellite) muss mit diesen abgestimmt werden, denn auch die Kommunikationspartner verfügen in der Regel über eine eigene Policy.

6 Fazit

Die PGP Corp. begibt sich mit PGP Universal eindeutig auf eine Gratwanderung. Langjährige PGP-Anwender werden von der serverbasierten Verschlüsselung zunächst einmal abgeschreckt werden – Unternehmen und Behörden jedoch suchen häufig nach genau diesen Funktionalitäten.

Am einfachsten stellt sich die Gratwanderung zwischen einfacher Benutzung und Sicherheit als ein „Schieberegler“ zwischen den Endpunkten „einfach“ und „sicher“ dar. Der Regler kann nicht gleichzeitig an beiden Enden sein. Bisher war die Meinung, dass dieser Regler bei „sicher“ stehen muss. Diese Einstellung fehlt es in der Praxis aber an breiter Akzeptanz. Jetzt wird versucht, den Regler in Abhängigkeit vom Einsatzszenario in Richtung „einfach“ zu schieben. Hierbei wird mehr oder weniger viel Sicherheit aufgegeben. Die Frage, die sich nun stellt ist, wie viel Sicherheit darf ich aufgeben, um mehr Nutzer ins Boot zu holen? Die Antwort ist stark vom jeweiligen Einsatzszenario abhängig. Der von PGP Corp. eingeschlagene Weg ist nicht grundsätzlich „dumm“ oder „schlecht“.

Wir stehen am Anfang einer neuen und innovativen Entwicklung. Die Lösungsvorschläge müssen diskutiert werden. Dabei geschieht sicherlich ein Reifungsprozess, der zu besseren Produkten führen wird. Zum jetzigen Zeitpunkt lässt sich über PGP Universal aus der Praxis leider noch nicht berichten. Es wird wichtig sein, die Funktionalität, aber auch die Standardkonformität sowie die Sicherheit der neuen Lösung genau zu untersuchen. Insbesondere die Domain Policies bilden aufgrund der zentralen Realisierung immer auch einen „single point of attack“. Konzeptionell klingt die neue Lösung durchaus interessant – die Praxis wird jedoch eine Reihe von zu klärenden Fragen aufwerfen.

Wir glauben, dass die endgültige Lösung eine Hybridlösung sein muss und wird. In vielen Unternehmensbereichen ist eine Proxy-Lösung anwendbar. Aber es wird immer auch Mitarbeiter geben, die eine Verschlüsselung am Endgerät benötigen. Beispiele dafür sind die Geschäftsleitung, der Datenschutzbeauftragte, der Betriebsarzt, der Betriebsrat und betriebsinterne Beratungsstellen. Die Art der transparenten Integration der klassischen Desktop-Lösungen wie PGP und GnuPG in die Proxy-Lösung wird mitentscheidend für den Erfolg sein.

Für eine Individualkommunikation zwischen Privatpersonen wird der virtuelle Briefumschlag jedoch immer mit reinen Desktoplösungen hergestellt werden.

Ein letzter Punkt: Bei einer serverbasierten Verschlüsselungslösung wird ein Überwachen immer einfacher sein, als bei einer Desktop-basierten Lösung. Auch hier wird zu diskutieren sein, wie dies gestaltet wird, oder wie es im Sinne datenschutzfreundlicher Technologien gestaltet werden kann.

Sicherer E-Mailserver

Die Kommunikation zwischen E-Mailklient und E-Mailserver erfolgt in der Regel unverschlüsselt und ungeschützt. Dies führt dazu, dass bei der E-Mailabholung mit POP3 oder IMAP das Passwort immer im Klartext übertragen wird.

Allerdings sind Lösungen bekannt: Die Kommunikation kann z.B. mittels SSL/TLS verschlüsselt werden. Hierzu wird bei der E-Mailabholung nicht mehr POP3 (Port 110) bzw. IMAP (Port 143)) benutzt, sondern POP3S (Port 995) bzw. IMAPS (Port 993). Dies ist vergleichbar mit den Protokollen HTTP (Port 80) und HTTPS (Port 443).

Beim eigentlichen Mailversand über SMTP wird in der Regel Port 25 beibehalten und über das Kommando STARTTLS die verschlüsselte Kommunikation aktiviert.

In professionellen Umgebungen ist die verschlüsselte Kommunikation zum E-Mailserver unerlässlich.

Um den rechtmäßigen Versand von E-Mail sicherzustellen, muss der Benutzer vorher authentisiert werden. Viele Betreiber einer E-Mailservers behelfen sich mit dem nicht wirklich sicheren Verfahren „SMTP after POP“. Dabei muss die E-Mail zuerst abgeholt und Benutzername und Passwort präsentiert werden; dann kann für kurze Zeit von diesem Klienten E-Mail verschickt werden.

Sauberer ist die Verwendung von SMTP AUTH[12]. Hierbei werden Benutzername und Passwort im Rahmen des SMTP Protokolls übertragen. Damit ist der Anwender auch beim E-Mailversand eindeutig identifiziert. Gängige E-Mail Programme unterstützen heute die verschlüsselten Varianten der Protokolle und Authentisierung.

[11] http://sites.inka.de/tesla/gpgrelay.html

[12] J. Myers, SMTP Service Extension for Authentication, RFC 2554, März 1999.