DuD
Datenschutz und Datensicherheit

PGP, quo vasisti?

Rainer W. Gerling, Stefan Kelm

Seit mehr als einem Jahrzehnt gilt das Programm PGP („Pretty Good Privacy“) als der Standard für E-Mail- und Datei-Verschlüsselung, insbesondere unter Internet-Benutzern. Seit der ersten Version der Software hat sich jedoch vieles verändert. Im vergangenen Jahr äußerten die beiden Autoren ihre Sorge um die Zukunft von PGP.[1] An dieser Stelle aus aktuellem Anlass ein Update, denn seit der Heise Newsticker am 4. März 2002 meldete: „Kein Käufer für PGP“, droht eines der besten Verschlüsselungsprodukte vom Markt zu verschwinden. Während die Freeware-Version von PGP (PGPi) für den privaten, nicht-kommerziellen Gebrauch offenbar verfügbar bleibt, sieht es für Geschäftskunden von Network Associates (NAI) düster aus.

Dr.
Rainer W. Gerling

Datenschutzbeauftragter der Max-Planck-Gesellschaft, Lehrbeauftragter für Datensicherheit an der FH München.
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 vadis? DuD 2001, 336-338.

1 Einleitung

Nach der Heise-Meldung[2] erläuterte NAI „in einer E-Mail an seine Geschäftkunden [...], dass alle bestehenden Support-Verträge nach wie vor eingehalten, aber nicht verlängert werden. Ferner würden sicherheitsrelevante Bugs zwar künftig noch beseitigt, die gesamte PGP-Produktreihe wird aber momentan nicht mehr weiterentwickelt.“[3]

Abb. 1: Das Softwarepaket des BMWi.

Dieser von NAI in seinem Schreiben an die PGP Kunden „Maintenance Mode“ genannte Zustand soll ein Jahr, also bis März 2003 dauern.

Danach dürfte die kommerzielle Programmversion von PGP endgültig tot sein. Erfahrene Verschwörungstheoretiker mutmaßen hinter vorgehaltener Hand, dass NAI auf Druck der US-Regierung PGP vom Markt genommen habe. Hierfür gibt es jedoch keinerlei Belege.

Die Besitzer der unlimitierten Vollversion *PGP Personal Privacy* können sich freuen: Diese Version bleibt auch weiterhin im aktuellen Zustand legal benutzbar. Auch die Freeware Version kann weiterhin für nicht-kommerzielle, private Zwecke eingesetzt werden. Alle anderen PGP Versionen müssen wahrscheinlich mit Auslaufen des Lizenz-Vertrages gelöscht werden.

[2] http://www.heise.de/newsticker/data/pab-04.03.02-000

[3] Hier zitiert Heise falsch: Im NAI-Brief (siehe http://www.dud.de) steht: „...they will continue to be developed in order to meet the security needs...“. Dabei bezieht sich „they“ auf „Other products“ (E-Business Server, Desktop Firewall, VPN Client).

Für kommerzielle Nutzer in Deutschland gibt es eine weitere Hoffnung, seit sich die Glück & Kanja GmbH aus dem Insolvenzverfahren der Biodata AG herausretten konnte: Sie bietet eine PGP-kompatible Eigenentwicklung zur E-Mail-Verschlüsselung (leider nur für Outlook und Outlook Express) an.

2 GNU Privacy

Vor dem Hintergrund dieser Entwicklung kommt die Meldung des Bundesministeriums für Wirtschaft (BMWi) gerade recht: „PGP geht – GnuPP kommt“[4]. Das Programmpaket GNU Privacy Projekt (GnuPP)[5] besteht aus GNU Privacy Guard (GnuPG)[6], dem GNU Privacy Assistant (GPA)[7] und dem Windows Privacy Tray (WinPT).[8] Alle drei Programme stellte das BMWi in der Version 1.1 auf der CeBIT 2002 vor. GnuPP ist ein vom BMWi geförderter, vollständig kompatibler OpenSource-Ersatz für PGP, dessen Version 1.0 bereits im Herbst 2001 veröffentlicht wurde. Hinzugekommen ist ein völlig neu geschriebenes und gestaltetes zweiteiliges Handbuch, mit dem auch Verschlüsselungslaien die Grundlagen der E-Mail-Verschlüsselung meistern können. Das Paket GnuPP ist als Buch mit CD-ROM verfügbar (Abb. 1).

2.1 Detailkritik

Die Version 1.1 von GnuPP kann in einer deutschen und englischen Version von der Webseite des Projektes heruntergeladen werden. Die Installation verläuft (vom Autor getestet unter Windows 2000 SP2, aber prinzipiell identisch unter Windows 95, 98, ME, NT4, 2000, XP), dank eines üblichen Windows Installers genau so, wie man es unter Windows gewohnt ist.

[4] http://www.sicherheit-im-internet.de/news/news.phtml?nnid=1633

[5] http://www.gnupp.de/

[6] http://www.gnupg.org/

[7] http://www.g-n-u.de/software/gpa.html

[8] http://www.winpt.org/de/index.html

GnuPG ist ursprünglich – und damit auch unter Windows – ein Unix Tool mit Kommandozeilen Oberfläche und unüberschaubar vielen Optionen – ein Albtraum für Benutzer einer grafischen Oberfläche.

Eine grafische Bedienungsoberfläche, beschränkt auf die wesentlichen Funktionen der PGP Komponenten PGPkeys und PGPtools liefert der GNU Privacy Assistant (GPA). Da auch die Windows Anwendung mit dem Toolkit GTK+ erstellt wurde, ist sie für einen Windowsanwender jedoch gewöhnungsbedürftig. Dieses Toolkit wurde ursprünglich für die Nutzung unter X Windows entwickelt, daher will ein „Windows Look and Feel“ nicht recht aufkommen. Außerdem enthält die Programmversion etliche Fehler:

- Der Versuch aus dem GPA einen geheimen Schlüssel (Private Key) über die Zwischenablage zu exportieren, führt zu einem Absturz des Programms. Zwar ist ein Export in eine Datei möglich; diese Datei lässt sich aber nicht ohne weiteres in einen PGP-Schlüsselring importieren.
- Die Darstellung der Schlüssel ist textlastig, man vermisst die „Ampeln“ von PGP, die intuitiv einfacher zu erfassen sind.
- Sowohl WinPT als auch GPA gehen nicht konsistent mit Umlauten um. WinPT stellt die BenutzerID „Test Schlüssel“ eines aus PGP importierten Schlüssels als „Test Schl\xfc\x73sel“ dar. GPA lässt die BenutzerID sogar leer. Beide können einen eigenen, mit Umlauten in der BenutzerID erzeugten Schlüssel korrekt anzeigen. GPA zeigt aber die Umlaute aus WinPT nicht richtig an, und umgekehrt ist es genauso.
- Wenig hilfreich ist die in Abbildung 2 wiedergegebene Fehlermeldung. Da keine SchlüsselID angegeben wird, kann nicht festgestellt werden, um welchen Schlüssel es sich handelt.[9]
- Beim Import des Schlüssels von Phil Zimmermann (aus der originalen Programmversion von PGP) wird das eingefügte Foto vom Schlüssel getrennt und auch getrennt dargestellt. Ein Klick auf die Zeile mit dem Foto bringt den GPA zum Absturz.

Immerhin verläuft der Import eigener Schlüsselpaare (inklusive der privaten Schlüssel) nach vorhergehendem Export aus PGP (Version 7.0.3) bis auf die Darstellung der Umlaute problemlos.

[9] Für Experten: Ursache war ein zeitlich befristeter und abgelaufener Subkey des Schlüssels.

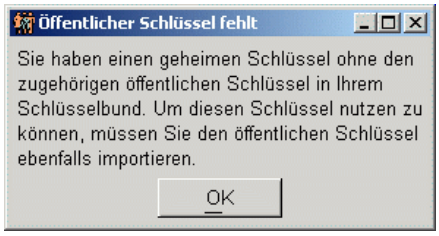

Abb. 2: Fehlermeldung des GPA.

Überzeugender wirkt das Tool WinPT. Es orientiert sich am Windows Style Guide und erscheint deshalb gewohnter. Es deckt die Funktionen der Programmteile PGPkeys, PGPtools und PGPtray aus dem originalen PGP Softwarepaket ab und ist übersichtlicher als der GPA. Es kann über den Systemtray (neben der Uhr) aufgerufen werden und ist damit leicht zugänglich. In den Funktionen für die Zwischenablage und das „aktuelle Fenster“ (auch mit Hotkeys bedienbar) steht es dem kommerziellen PGP in nichts nach. Ein Parallelbetrieb von PGP und GnuPP ist problemlos möglich, solange nicht in beiden Programmen die gleichen Hotkeys verwendet werden. Für eine Übergangszeit ist also auch ein Parallelbetrieb möglich.

2.2 E-Mail Plugins

Auf den Internet-Seiten der Initiative „Sicherheit im Internet“[10] des BMWi findet man eine GnuPP-Übersicht[11], mit einer Download-Möglichkeit für Plugins für die E-Mail Programme Microsoft Outlook und PostME.

Auf der GnuPG Webseite für Frontends[12] findet man außerdem ein Plugin für den E-Mail-Client Eudora. Eine vollständige Liste der für GnuPG verfügbaren Plugins wird man auf dieser Webseite allerdings auch zukünftig nicht finden, da der Autor von GnuPG, Werner Koch, es ablehnt, Hinweise auf „proprietäre“ Softwareprodukte aufzunehmen, deren Quellcode nicht offengelegt ist.

Außerdem gibt es eine Beta-Version von QDGPG[13] für Pegasus Mail[14]. Dieses Plugin funktioniert jedoch noch nicht ohne manuelle Nacharbeit: Hier muss das Verzeichnis mit der Datei gpg.exe (Default der deutschen Version: c:\programme\gnupp\gnupg) in den Such-Pfad aufgenommen werden.

[10] http://www.sicherheit-im-internet.de/
[11] http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=86
[12] http://www.gnupg.org/frontends.html
[13] http://community.wow.net/grt/qdgpg.html
[14] http://www.pmail.com/

Unter Windows 98/ME gibt es zudem noch Stabilitätsprobleme.

Mit enigmail[15] gibt es jetzt auch für das Browserprojekt Mozilla[16] ein Plugin zur E-Mail Verschlüsselung.

2.3 Schlüsselserver

Ein größeres Problem ist derzeit noch der Schlüsselserver. Der bislang von NAI vertriebene Server bietet sehr umfangreiche, in der Praxis wichtige Konfigurationsmöglichkeiten. Der freie PGP Public Key Server[17] von Mark Horowitz ist hingegen sehr viel einfacher: Ihm fehlen z. B. Zugriffsbeschränkungen, die benötigt werden, um interne Schlüsselserver aufzusetzen. Auch ist das Durchsetzen von Policy-Regeln damit nicht möglich. GnuPP unterstützt derzeit auch keinen LDAP-Zugriff.

2.4 Dokumentation

Die Handbücher sind sehr gut, leicht verständlich und ansprechend im Layout. Sie können als PDF-Dateien geladen werden. Viele – vor allem speziellere – Fragen bleiben jedoch offen. Profis sind daher auf die offiziellen (zur Zeit nur englischen) Dokumentationen der einzelnen Paketbestandteile angewiesen.

3 Fazit

Unter dem Strich ist das Erscheinen von GnuPG 1.1 als ein großer Fortschritt zu werten. Während es mit der originalen, kommerziellen Version von PGP schlimmer gekommen ist, als vor rund einem Jahr befürchtet, hat sich GnuPG deutlich viel versprechender entwickelt als erwartet.

Ein Wechsel von PGP nach GnuPP verursacht einen gewissen Aufwand, aber benutzbar ist GnuPP zur E-Mail-Verschlüsselung inzwischen sehr wohl.

Wer hingegen PGPdisk ersetzen muss, findet in GnuPP keine Lösung. Angeblich entwickelt die Firma Utimaco mit SafeGuard PrivateDisk ein Produkt, das vergleichbare Funktionen haben soll. Möglicherweise kann es diese Lücke füllen und wird unter ähnlicher Lizenz wie SafeGuard PrivateCrypto[18] angeboten.

[15] http://enigmail.mozdev.org/
[16] http://www.mozilla.org
[17] http://www.mit.edu/people/marc/pks/pks.html
[18] http://www.privatecrypt.de