DuD
Datenschutz und Datensicherheit

Eine „PGP-Policy“ für Unternehmen

Dirk Fox

Insbesondere für kleinere Unternehmen oder Unternehmenseinheiten, die ihre E-Mail-Kommunikation schützen wollen, ist PGP[1] seit der Verfügbarkeit europäischer Lizenzen eine interessante Option.

Die von Rainer W. Gerling in DuD 12/1997 publizierte „Betriebsvereinbarung E-Mail und Internet“ schreibt in § 8 die Verschlüsselung von E-Mails vertraulichen und personenbezogenen Inhalts vor. Der vorliegende Beitrag ergänzt diese Regelung um einen Vorschlag für die technische Umsetzung unter Verwendung von PGP.

Dipl.-Inform.
Dirk Fox

ist Security Consultant der Secorvo security consulting GmbH in Karlsruhe. Schwerpunkte: Kryptologie, insbesondere digitale Signatursysteme, Public Key Infrastrukturen, Sicherheit in Rechnernetzen.
E-Mail: fox@secorvo.de

[1] Siehe Roessler, DuD 7/1998, S. 377-381.

Einleitung

Die aktuelle Version 5.53 des von Phil Zimmermann entwickelten Programms „Pretty Good Privacy“ (PGP) ist für kleine und mittlere Unternehmen ein geeignetes Hilfsmittel zum Schutz der E-Mail-Kommunikation.

Eine Reihe wichtiger Mechanismen allerdings, wie beispielsweise der Rückruf von Zertifikaten, müssen bei der Verwendung von PGP organisatorisch geregelt werden, da die Struktur des „Web of Trust“ diese nicht unterstützt.[2]

Die im folgenden vorgeschlagenen Einsatzregeln („Policy“) legen die erforderlichen organisatorischen Abläufe fest.

1 Grundsätzliches

- **Verantwortlichkeit**: Es werden ein PGP-Verantwortlicher und ein Stellvertreter bestimmt. Sie unterstehen in ihrer Funktion dem Sicherheitsbeauftragten und berichten an diesen.
- **Schulung**: Neue Mitarbeiter erhalten eine Einweisung in die Nutzung von PGP. Dazu stellt der PGP-Verantwortliche eine Dokumentation zusammen.

2 Schlüssel-Generierung

Alle Mitarbeiter erzeugen ihre PGP-Schlüssel auf ihrem eigenen Rechner selbst.

- **Schlüssellänge**: Die Schlüsselmindestlänge beträgt 768 bit; empfohlen werden 1024 bit.
- **Passphrase**: Die Passphrase sollte aus mehr als 10 nicht ausschließlich alphabetischen Zeichen bestehen und Satzzeichen oder Sonderzeichen, numerische Zeichen und Groß- und Kleinbuchstaben enthalten. Die Passphrase darf nicht aufgeschrieben werden.
- **Namensvergabe**: Die Haupt-ID wird im Format „Vorname Nachname <dienstliche Internet-E-Mail-Adresse>„ eingegeben. Weitere Namen (z. B. private E-Mail-Adresse) sind zulässig.
- Die Verwendung eines eigenen, zu einem früheren Zeitpunkt erzeugten PGP-Schlüssels ist zulässig, sofern er die oben geforderten Eigenschaften besitzt und sichergestellt ist, daß die Passphrase nur dem Schlüsselinhaber bekannt ist.
- **Gruppenschlüssel**: Für die Verschlüsselung von Nachrichten an alle Mitarbeiter einer Gruppe oder eines Projekts kann ein separater Gruppen- oder Projekt-Schlüssel (ID: „Projektname <E-Mail-Adresse des Verteilers>„) erzeugt werden. Der zugehörige geheime Entschlüsselungsschlüssel wird von den Mitarbeitern in ihren Schlüsselring aufgenommen.

[2] Zu den Grenzen von PGP bei der Schlüsselzertifizierung siehe Camphausen, DuD 7/1998, S. 382-385.

3 Schlüssel-Aufbewahrung

- **Schlüsselringe**: Jeder Mitarbeiter verwaltet seine Schlüsselringe selbst und speichert diese auf seinem Arbeitsplatzrechner. Der Schlüsselring mit geheimen Schlüsseln (Datei „secring.skr“) kann auch auf einer Diskette gespeichert werden; bei Nichtbenutzung sollte die Diskette vor fremdem Zugriff geschützt hinterlegt oder mitgeführt werden.
- **Datensicherung**: Mitarbeiter müssen von den geheimen Schlüsseln (Datei „secring.skr“) eine persönliche Diskettenkopie erstellen und an geeigneter Stelle vor fremdem Zugriff geschützt aufbewahren.

4 Schlüssel-Authentisierung

- **Selbstsignatur**: Alle Mitarbeiter signieren ihre eigenen öffentlichen Schlüssel, mindestens bezüglich der Haupt-ID.
- Öffentliche Schlüssel der Mitarbeiter gelten als authentisch, wenn sie vom Sicherheitsbeauftragten signiert sind und

weder dessen Unterschrift noch der gesamte Schlüssel zurückgerufen ist.
- Vor dem Signieren eines fremden öffentlichen Schlüssels ist gemeinsam mit dem Schlüsselinhaber mindestens der Fingerprint zu vergleichen (über einen authentischen Kanal, z. B. persönlich oder telefonisch).
- Vor dem Signieren des öffentlichen Schlüssels eines Mitarbeiters durch den Sicherheitsbeauftragten verpflichtet sich der Mitarbeiter, bei Ausscheiden aus dem Unternehmen alle IDs mit einer E-Mail-Adresse des Unternehmens aus seinem öffentlichen Schlüssel zu löschen (und damit auch alle Signaturen unter diesen IDs) und für einen Rückruf seines öffentlichen Schlüssels mit diesen IDs von allen Schlüsselservern zu sorgen, auf denen er sein Schlüssel publiziert hat.
- Wird der Schlüssel des Sicherheitsbeauftragten zurückgerufen, müssen alle öffentlichen Schlüssel der Mitarbeiter mit dem neuen Schlüssel des Sicherheitsbeauftragten signiert werden.

5 Schlüssel-Verteilung

- Jeder Mitarbeiter exportiert seinen öffentlichen Schlüssel im ASCII-Format in eine Datei (Dateiname: „Vorname Nachname.asc“) und gibt diese an den PGP-Verantwortlichen weiter.
- Öffentliche Schlüssel sollen möglichst nach jeder Änderung (z. B. zusätzliche Signatur von Kollegen oder Ergänzung durch eine neue ID) vom Mitarbeiter exportiert und an den PGP-Verantwortlichen weitergegeben werden.
- **Schlüsselverzeichnis**: Der PGP-Verantwortliche verwaltet ein Firmen-Schlüsselverzeichnis mit den signierten öffentlichen Schlüsseln aller Mitarbeiter auf einem allen Mitarbeitern zugänglichen Server. Öffentliche Schlüssel werden dort als einzelne Dateien schreibgeschützt gespeichert.
- Neue Mitarbeiter nehmen alle öffentlichen Schlüssel aus diesem Verzeichnis in ihren Schlüsselring auf. Alle Mitarbeiter gleichen ihren Schlüsselring regelmäßig mit diesem Verzeichnis ab.
- Mitarbeiter können ihre öffentlichen Schlüssel auf PGP-Key-Servern[3] veröffentlichen.
- Die Mitarbeiter sollen den Fingerprint ihres öffentlichen Schlüssels in ihre E-Mail-Signatur aufnehmen.
- Kunden, die vertraulich und authentisch mit Mitarbeitern kommunizieren wollen, können die öffentlichen Schlüssel der Mitarbeiter entweder direkt vom Mitarbeiter per E-Mail oder von einem PGP-Key-Server beziehen.

6 Schlüssel-Rückruf

- Der Rückruf eines öffentlichen Schlüssels wird entweder vom Schlüsselinhaber selbst vorgenommen und dies persönlich dem PGP-Verantwortlichen mitgeteilt oder vom PGP-Verantwortlichen im Auftrag des Sicherheitsbeauftragten eingeleitet.
- Gibt es Anhaltspunkte dafür, daß die Passphrase des Mitarbeiters bekannt geworden ist, muß der Schlüssel vom Schlüsselinhaber zurückgerufen werden.
- Der Schlüsselrückruf ist vom Mitarbeiter auch an PGP-Key-Server zu versenden, auf denen er seinen öffentlichen Schlüssel eingetragen hat. Der Fingerprint des Schlüssels ist aus der E-Mail-Signatur zu löschen.
- Hat ein Mitarbeiter seine Passphrase vergessen, muß der Schlüssel durch den Sicherheitsbeauftragten zurückgerufen werden. Dazu ruft dieser seine digitale Signatur unter diesem Schlüssel zurück.
- Scheidet ein Mitarbeiter aus, wird er vom PGP-Verantwortlichen zur Streichung aller IDs mit einer Firmen-E-Mail-Adresse aus seinem öffentlichen Schlüssel aufgefordert. Der Schlüssel-Eintrag auf PGP-Key-Servern ist entsprechend zu korrigieren.
- Im Falle des Ausscheidens eines Mitarbeiters oder eines Schlüsselrückrufs nimmt der PGP-Verantwortliche dessen öffentlichen Schlüssel aus dem Schlüsselverzeichnis und gibt den Rückruf umgehend (z. B. durch E-Mail) allen Mitarbeitern bekannt.
- Zurückgerufene Schlüssel werden von den Mitarbeitern aus ihren Schlüsselringen entfernt.
- Zurückgerufene Schlüssel von (nicht ausgeschiedenen) Mitarbeitern müssen schnellstmöglich durch neue Schlüssel ersetzt werden.
- Scheidet ein Mitarbeiter aus oder gibt es Anhaltspunkte dafür, daß die Passphrase eines Gruppen- oder Projekt-Schlüssels kompromittiert ist, werden alle betroffenen Gruppen- oder Projekt-Schlüssel vom Sicherheitsbeauftragten zurückgerufen und jeweils ein neuer Gruppen- bzw. Projekt-Schlüssel erzeugt.

7 Verschlüsselung

- Sämtliche vertraulichen und personenbezogenen Daten müssen sowohl intern als auch in der E-Mail-Kommunikation mit Kunden verschlüsselt ausgetauscht werden.
- Vor Nutzung des öffentlichen Schlüssels eines Kunden muß der Fingerprint über einen getrennten, möglichst vertrauenswürdigen Kanal (z. B. Telefon) bezogen und verglichen werden.
- Die gesamte interne E-Mail-Kommunikation soll verschlüsselt erfolgen.

8 Schlüssel-Recovery

- Verschlüsselt versendete Dateien und Nachrichten müssen, sofern sie nicht im Klartext archiviert sind, auch mit dem Schlüssel des Senders verschlüsselt werden (Einstellung PGP: Preferences/General: „always encrypt to default key“), damit sie auch dem Sender noch zugänglich sind.
- Dateien und wichtige E-Mails werden in Projektverzeichnissen unverschlüsselt archiviert (der Zugriffsschutz erfolgt über Paßworte und die Autorisierungsmechanismen des Betriebssystems).
- Eine Hinterlegung von geheimen Schlüsseln findet nicht statt.

9 Digitale Signaturen

- Die Passphrase soll für jede Signatur neu eingegeben werden (nur kurzzeitige Speicherung durch die Software).
- In der internen E-Mail-Kommunikation sollen Nachrichten und Anhänge immer digital signiert werden. Die Signatur soll vom Empfänger vor dem Lesen der Nachricht geprüft werden.
- Für die E-Mail-Kommunikation mit Kunden wird die Verwendung digitaler Signaturen empfohlen.

Dank

Für hilfreiche Kritik und Kommentare danke ich Fritz Bauspieß, Klaus Becker und Holger Mack.

[3] http://www.pgp.net/pgpnet/wwwkeys. html