2005/10 Dossier

https://shop.jungle.world/artikel/2005/10/alles-sehr-kryptisch

Alles sehr kryptisch

Von **claire sinn**

Eine kurze Geschichte der Verschlüsselung. Von Claire Sinn

Als Philip Zimmermann 1991 seine Software »Pretty Good Privacy« (PGP) vorstellte, war die Aufregung bei US-amerikanischen Sicherheitsbehörden groß. Dem Mathematiker und Softwareentwickler war es gelungen, mit PGP das Prinzip der asymmetrischen Verschlüsselung einem großen Anwenderkreis zugänglich zu machen. Gerade das neu aufgekommene Medium E-Mail eignete sich hervorragend, mit der Software sehr sicher zu kommunizieren.

Bereits in den achtziger Jahren hatte Zimmermann zu diesem Thema geforscht. Er konnte dabei auf wohlbekannte Algorithmen zur Verschlüsselung zurückgreifen. Neu beim Prinzip der asymmetrischen Verschlüsselung war der Umstand, dass zum Austausch der Schlüssel selbst kein sicherer Übertragungskanal mehr benötigt wurde. Im Gegensatz zur symmetrischen Verschlüsselung müssen beide Kommunikationspartner ein eigenes Schlüsselpaar erstellen, wobei zum Verschlüsseln der öffentliche Schlüssel (public key) des Empfängers zum Einsatz kommt, der die so verschlüsselte Nachricht mit seinem dazu passenden geheimen Schlüssel (secret key) entschlüsselt.

Der public key lässt keinen mathematischen Rückschluss auf den secret key zu. Bei richtiger Implementierung und Anwendung war und ist es bis heute nicht möglich, den Schlüssel mathematisch zu brechen. Nur mit einer gigantischen Rechenleistung wäre es möglich, mit aufwändigem Probieren den Schlüssel zu erraten.

Nach der Veröffentlichung sah sich Zimmermann mit einem Ermittlungsverfahren konfrontiert, das erst 1996 eingestellt wurde. Der Vorwurf lautete, das Kryptosystem PGP verletze US-amerikanische Exportbestimmungen. Zwischenzeitlich wurde der Quelltext einer Version von PGP als gedrucktes Buch legal aus den USA exportiert und anschließend von Freiwilligen in aller Welt wieder digitalisiert, um daraus eine eigene Version von PGP zu kompilieren.

Erst als Mitte der neunziger Jahre die US-amerikanische Regierung die Gesetzgebung zur Kryptografie liberalisierte, wurde die Anklage gegen Zimmermann fallen gelassen. Die immer größer werdende wirtschaftliche Bedeutung des Internet mag dabei ebenso eine Rolle gespielt haben wie die Erkenntnis, dass ein halbes Jahrzehnt der Kriminalisierung die weltweite Verbreitung von PGP nicht stoppen konnte.

So ist dann auch die Reputation Zimmermanns in der Wirtschaft sehr gut. Das Design Institute des Autobauers Chrysler spendete für PGP ebenso einen Preis wie diverse andere Unternehmen

der IT-Branche, darunter das Online-Portal infoworld, das varBusiness Magazine und das Nachrichtenportal ZDNet, dessen Motto lautet: »Where Technology Means Business«

Im Jahr 2003 schließlich wurde Zimmermann zusammen mit Whitfield Diffie, Martin Hellman und Ronald Rivest, die sich mit den bei PGP zum Einsatz kommenden grundlegenden Verschlüsselungsalgorithmen beschäftigten, und Wau Holland, einem inzwischen verstorbenen Gründer des Chaos Computer Club, in die »Wall of Fame – Pioniere der Computertechnik« des Heinz-Nixdorf-Museums aufgenommen.

Das Vertrauen, das PGP entgegengebracht wurde, beruhte nicht zuletzt auf der Verfügbarkeit des Programm-Quellcodes. Jeder, der etwas davon verstand, war in der Lage nachzuvollziehen, ob der Programmcode Fehler oder gar Hintertüren aufweist, die das Prinzip der Sicherheit aushebeln.

Doch nicht jede Version von PGP wurde mit dem dazugehörigen Quellcode ausgeliefert. 1997 startete die Free Software Foundation das Projekt GnuPG, das die Entwicklung eines grundsätzlich quellenoffenen Verschlüsselungsprogramms zum Ziel hatte. Unterstützt wurde das Projekt vom Bundesministerium des Innern (BMI) und vom Ministerium für Wirtschaft. In einem Geleitwort zur Dokumentation des Gnu Privacy Guard, der eine einfache Implementierung von GnuPG ermöglichte, sagte der damalige Wirtschaftminister Werner Müller: »Wir setzen auf ›Sicherheit durch Offenheit‹. Denn die öffentliche Diskussion über erkannte Schwachstellen hilft, Sicherheitslecks schnell zu beseitigen oder gar nicht erst entstehen zu lassen.« Die Software ermögliche es »jedem Bürger und jedem Unternehmen, seine Grundrechte auf vertrauliche Kommunikation über das Internet zu wahren und die Rechtsverbindlichkeit, Integrität und Authentizität der Kommunikation zu überprüfen«.

Die Aktivität des Wirtschaftsministeriums hat in dieser Sache mittlerweile nachgelassen. Auf der Website »**www.gnupp.de**« ist nur noch eine veraltete Version des Programms verfügbar. Die folgenden drei Seiten erklären detailliert, welche Programmpakete unter Berücksichtigung der Betriebssysteme Windows und MacOS dem heutigen Stand der Technik entsprechen.

Auch das Innenministerium hat anscheinend neue Prioritäten gesetzt. Noch im Jahr 1999 hieß es in einer Stellungnahme des Ministeriums zu den Eckpunkten der deutschen Kryptopolitik: »Zentrales Anliegen der Kabinettsentscheidung ist der verbesserte Schutz deutscher Nutzer in den weltweiten Informationsnetzen durch Einsatz sicherer kryptografischer Verfahren. Die Entscheidung stellt klar, dass in Deutschland auch künftig Verschlüsselungsverfahren und -produkte ohne Restriktion entwickelt, hergestellt, vermarktet und genutzt werden dürfen.«

Doch das BMI hat mit der Novelle der Telekommunikationsüberwachungsverordnung inzwischen Fakten geschaffen, die nur schwer mit den Zielen der vergangenen Jahre in Einklang zu bringen sind. Seit dem 1. Januar sind in Deutschland alle Betreiber von E-Mailservern, die Dienstleistungen anbieten, verpflichtet, den Ermittlungsbehörden Schnittstellen zur Überwachung des gesamten E-Mailverkehrs bereitzustellen (Jungle World, 51/04).

Ein Grund mehr, endlich neue Wege bei der E-Mailkommunikation zu beschreiten.