„Wer ist der befugte Vierte?“

Geheimdienste unterwandern den Schutz von Verschlüsselungsgeräten

Die Schweiz ist ein verschwiegener Ort. Ungezählte Schwarzgeldmillionen genießen Asyl in den diskreten Bankhäusern der Republik. Hier gedeiht auch ein Gewerbe gut, das ohne Öffentlichkeit auskommt: die Fabrikation von Verschlüsselungsgeräten.

Allererste Adresse bei den Heimlichkeitswerkzeugen war über viele Jahrzehnte die Crypto AG in Zug. Sie wurde 1952 von dem legendären schwedischen Kryptologen Boris Hagelin gegründet, dessen „Hagelin-Maschinen“, Pendants zu den deutschen „Enigma“-Geräten, während des Zweiten Weltkriegs zu Hunderttausenden auf seiten der Alliierten im Einsatz waren.

E. STUDHALTER

Crypto-Firmensitz in Zug: Tief in die Trickkiste gegriffen?

„Inzwischen hat die Crypto AG“, laut Firmenprospekt, „langjährige partnerschaftliche Beziehungen zu Kunden in über 130 Ländern“ aufgebaut. Crypto liefert neben Sprachverschlüßlern auch Chiffriergeräte für Datennetze.

Doch hinter der gediegenen Fassade wurde offenbar die dreisteste Geheimdienstfinte des Jahrhunderts inszeniert: Deutsche und amerikanische Dienste stehen im Verdacht, bis Ende der achtziger Jahre Cryptos Schutzgeräte so manipuliert zu haben, daß ihre Codes im Handumdrehen zu knacken waren.

Zu den Crypto-Kunden zählen neben so ehrwürdigen Institutionen wie dem Vatikan auch Länder wie der Irak, Iran und Libyen, die ganz oben auf den Prioritätenlisten der US-Dienste stehen. Anfang der neunziger Jahre geriet die diskrete Firma in den Verdacht, ein nicht ganz sauberes Spiel zu spielen. Woher kamen zum Beispiel die „direkten präzisen und unwiderlegbaren Beweise“, auf die sich US-Präsident Reagan berufen konnte, als er das Bombardement Libyens befahl, das er als Drahtzieher des Anschlags auf die Berliner Diskothek La Belle brandmarkte? Offenbar konnten US-Dienste verschlüsselte Funksprüche zwischen Tripolis und der Ost-Berliner Botschaft mitlesen.

Hans Bühler, Verkaufsingenieur der Crypto AG, geriet zwischen die Fronten des Geheimdienstkrieges. Am 18. März 1992 wurde der ahnungslose Handelsreisende in Teheran festgenommen. Während neuneinhalb Monaten Einzelhaft in einem Militärgefängnis mußte er sich immer wieder fragen lassen, an wen er die Teheraner Codes und die Schlüssel Libyens verraten habe.

Schließlich bezahlte Crypto großmütig die geforderte Kaution von rund einer Million Mark, kündigte dem freigelassenen Bühler jedoch wenige Wochen später. Begründung: Bühlers Publizität „leider gerade auch mit und nach der Rückkehr“ schade dem Unternehmen. Doch Bühler begann unbequeme Fragen zu stellen und bekam verblüffende Antworten.

Schon die Besitzverhältnisse der Crypto AG sind verworren. Eine „Stiftung“, gegründet von Hagelin, schafft nach Angaben der Firma „beste Voraussetzungen für die Eigenständigkeit des Unternehmens“.

Doch große Teile der Aktien sind unter wechselnden Konstellationen im Besitz deutscher Eigner. Eugen Freiberger, der 1982 als Verwaltungsrat fungierte und in München residierte, verfügte damals über alle bis auf 6 der 6000 Crypto-Aktien. Josef Bauer, der 1970 in den Crypto-Verwaltungsrat gewählt wurde, gibt inzwischen an, er habe als Steuerbevollmächtigter der Münchner Treuhandgesellschaft KPMG „das Mandat für die Siemens AG wahrgenommen“. Erst als die Crypto AG nicht mehr aus den Schlagzeilen herauszuhalten war, so ein Insider, hätten sich deutsche Aktionäre von der brisanten Beteiligung getrennt.

Einige der wechselnden Crypto-Geschäftsführer waren vorher bei Siemens beschäftigt. Gerüchte, hinter dem Engagement habe sich der bundesdeutsche Geheimdienst BND verborgen, bestritt Crypto stets vehement.

Doch umgekehrt schien traditionell dem deutschen Dienst merkwürdig viel am Wohlergehen der Schweizer Firma zu liegen. So beriet eine geheime BND-Diskussionsrunde im Oktober 1970, „wie die Schweizer Firma Grättner enger an die Crypto AG herangeführt, bzw. fusioniert werden kann“. Außerdem überlege der Dienst, wie „die schwedische Firma Ericsson möglicherweise über Siemens zur Aufgabe ihres Chiffriergeschäfts gebracht werden kann“.

Die Geheimen haben offenbar großes Interesse, den Handel mit Verschlüsselungstechnik in geordnete Bahnen zu lenken. Ernst Polzer*, ein ehemaliger Angestellter der Crypto AG, berichtet, er habe seine Entwicklungen mit den „Leuten von Bad Godesberg“ abstimmen müssen. Dort saß die „Zentralstelle für das Chiffrierwesen“ des BND, und dieses Amt habe Crypto die Verfahren vorgeschrieben, nach denen die Codes erzeugt wurden.

Auch Mitglieder des amerikanischen Geheimdienstes National Security Agency (NSA) gingen bei der Crypto AG ein und aus. Das Memorandum eines geheimen Arbeitstreffens der Cryp-

* Name von der Redaktion geändert.

to AG im August 1975 anläßlich der Demonstration eines neuen Chiffriergerät-Prototypen nennt als Teilnehmer die NSA-Kryptologin Nora Mackebee.

Bob Newman, ein Ingenieur des Chipherstellers Motorola, mit dem Crypto in den siebziger Jahren bei der Entwicklung einer neuen Generation von elektronischen Verschlüsselungsmaschinen kooperierte, kennt Mackebee gut. Ihm wurde die Frau als „Beraterin“ vorgestellt.

„Die Leute kannten sich gut aus in Zug und haben den Motorola-Leuten Reisetips für den Besuch bei der Crypto AG gegeben“, berichtet Newman. Auch Polzer erinnert sich an die amerikanische „Aufpasserin“, die nachdrücklich die Verwendung bestimmter Verschlüsselungsverfahren forderte.

Je nach Einsatzgebiet seien die Manipulationen an den Schutzgeräten mehr oder weniger subtil gewesen, berichtet Polzer. Manchen Abnehmern sei schlicht abgemagerte Codetechnik verkauft worden, nach dem Motto „für diesen Kunden genügt das, der braucht nicht so was Gutes“.

In heikleren Fällen hätten die Spezialisten tief in die kryptologische Trickkiste gegriffen: Die so präparierten Maschinen hätten dem verschlüsselten Text „Hilfsinformationen“ beigefügt, mit denen all jene, die Bescheid wußten, den ursprünglichen Schlüssel rekonstruieren konnten. Das Ergebnis war stets dasselbe: Was für den gutgläubigen Benutzer der Crypto-Maschinen wie ein undurchdringlicher Geheimcode aussah, war für die eingeweihten Lauscher mit kaum mehr als einer Fingerübung wieder lesbar zu machen.

Die Crypto AG bezeichnet solche Berichte empört als „altes Hörensagen“ und „reine Erfindung“. Doch ein Prozeß, den die Firma gegen ihren Ex-Angestellten Bühler anstrengte, weil dieser geäußert hatte, an dem Verdacht seiner iranischen Vernehmer sei möglicherweise etwas dran gewesen, fand im November letzten Jahres ein überraschendes Ende.

Noch vor der Verhandlung, in der womöglich peinliche Details ans Licht gekommen wären, stimmte die Firma einem außergerichtlichen Vergleich zu. Seitdem schweigt Bühler eisern zu dem Fall. „Der hat wohl finanziell ausgesorgt“, vermutet ein Szenekenner.

„In der Branche weiß doch jeder, wie das läuft“, meint Bühlers Ex-Kollege Polzer. „Natürlich schützen solche Geräte davor, daß unbefugte Dritte mithören, wie es im Prospekt steht. Die interessante Frage ist aber doch: Wer ist der befugte Vierte?“

G. MATHIESON / MAI

Horchposten der NSA: Angriff auf strategische Knotenpunkte des Geldverkehrs

schung und Betrug gestohlen“, urteilte Richter George Bason vier Jahre später in einem Prozeß gegen Hamiltons einstige Auftraggeber. Die juristischen Auseinandersetzungen um Schadensersatz dauern bis heute an.

Warum stiehlt eine Bundesbehörde Software? Offenbar hatten Hamiltons ehemalige Kollegen von der NSA ein Auge auf das Superprogramm geworfen und Bedarf im Namen der nationalen Sicherheit angemeldet. Mehrere Zeugen bestätigten vor einem Inslaw-Untersuchungsausschuß, daß Promis nach dem Raubzug bei Hamilton in der Geheimdienstszene auftauchte. Dort versahen es Programmierer mit geheimen Zugängen, sogenannten Trap Doors, durch die

Durch geheime Zugänge vorbei an den Burgwächtern

NSA-Schattenmänner jederzeit unbemerkt in Promis-Datenbanken eindringen konnten.

Die NSA habe gezinkte Promis-Versionen in den folgenden Jahren an Behörden in aller Welt verteilt, so die Informanten. Offenbar paßte der Inslaw-Coup auch Reagans Finanzdatenjägern exakt ins Konzept: Im Herbst 1983, nachdem Inslaw außer Gefecht gesetzt war, tauchte Promis plötzlich in der Washingtoner Weltbankzentrale auf. Das bezeugt Stephen McCallum, der seinerzeit bei der Servicefirma Control Data beschäftigt war. Die Firma war damit beauftragt, ein damals frisch eingerichtetes System von Vax-Rechnern zu warten.

Auf diesen Rechnern wurde gerade Promis installiert, und zwar, so McCallum, „als Kernstück eines Nachrichtensystems, das Daten sammelte und an die Mitgliedsbanken weiterverteilte“.

Den Nachrichtenknoten unterhielt die Weltbankabteilung für Entwicklung und Wiederaufbau – ein lohnendes Ziel für Reagans Sonderermittler, die den Verdacht hegten, korrupte Politiker in Drittweltstaaten würden Hilfsgelder auf private Konten umleiten.

Eine Unterwanderung der Weltbank-Datenzentrale könnte der gelungene Auftakt für den Einbruch in die Datenschätze der Geldwelt gewesen sein. William Casey, seinerzeit CIA-Chef und Gebieter über alle US-Geheimdienste, rühmte sich später, einer seiner größten Erfolge sei „die Penetration des internationalen Bankensystems“ gewesen.

Soviel elektronische Raffinesse ist jedoch nur selten erforderlich. Die meisten Informationen liegen offen auf den Datenstraßen herum. Wer heute eine elektronische Nachricht durch eines der großen Online-Systeme oder Internet verschickt, kann fast sicher sein, daß die NSA bei Interesse einen Blick darauf wirft.

Die Wege der Datenpakete im Internet sind unergründlich. Die Vermittlungsrechner im Netz, sogenannte Router, wählen nicht nach Art des Telefonnetzes eine direkte Verbindung zwischen Sender und Empfänger, sondern suchen für jedes eingehende Datenpaket die aktuell am wenigsten verstopfte oder die für den Betreiber billigste Reiseroute für den Sprung zum nächsten Netzknoten. Nach diesem Prinzip ist es durchaus nicht ungewöhnlich, daß Nachrichten von Krefeld nach Winsen über New York reisen.

Wayne Madsen, Koautor einer aktualisierten Version des NSA-Klassikers „The Puzzle Palace“, glaubt, daß sich die Lauscher längst Abzweigungen zu den Hauptstraßen des Internet gebaut haben. Die großen Knotenpunkte mit Namen wie „Fix East“ oder „Mae West“, die immense Datenströme kanalisieren, seien