90 IN.KU

November 2023

Die Crypto AG aus Zug: CIA und BND konnten mitlesen

Im Februar 2020 bestätigte sich, was seit den 1990er Jahren vermutet worden war: Das Zuger Traditionsunternehmen Crypto AG arbeitete jahrzehntelang mit dem deutschen und amerikanischen Geheimdienst zusammen und verkaufte kompromittierte Chiffriergeräte. Die Operation trug den Namen «Rubicon» und erhielt in den Medien den Namen «Cryptoleaks». Die Enthüllung erregte weltweit Aufsehen.

Die Firma Crypto AG in Steinhausen bei Zug existierte seit den frühen 1950er Jahren, als der schwedische Unternehmer Boris Hagelin seinen Firmensitz von Schweden in die Schweiz verlegte. Er hatte beste Beziehungen zu den amerikanischen Geheimdiensten, die ihm von allem Anfang an den Weg ebneten.
Hagelin sorgte dafür, dass die US-Geheimdienste die verschlüsselten Nachrichten mitlesen konnten und produzierte fortan sichere Maschinen für die Nato-Staaten, Schweden und die Schweiz und weniger sichere für alle anderen. 1970 verkaufte Boris Hagelin seine Crypto AG an eine liechtensteinische Firma, die direkt vom US Geheimdienst CIA und dem deutschen Nachrichtendienst BND kontrolliert wurde. Damit waren diese Geheimdienste während Jahrzehnten in der Lage, Nachrichten von über 100 Staaten zu entziffern. Die Existenz der Operation «Rubicon» wurde in den Medien von Bernd Schmidbauer, Kanzleramtsminister unter Kanzler Helmut Kohl in den Jahren 1991-09, bestätigt. Sie gilt als die grösste und erfolgreichste Geheimdienstoperation seit dem Zweiten Weltkrieg.
Die Enthüllung erregte weltweit Aufsehen, sie kam aber mindestens 20 Jahre zu spät, die Forderung nach einer parlamentarischen Untersuchungskommission wurde abgelehnt und die Aufregung legte sich. Ein offizieller Untersuchungsbericht der Verwaltung kritisierte, dass der Schweizer Nachrichtendienst zwar davon wusste, aber den Bundesrat nie offiziell eingeweiht hatte.

Die Chiffriermaschine CX-52 war die erste Maschine, welche der Schwede Boris Hagelin in der Schweiz entwickelte und ab 1952 mit seiner Crypto AG verkaufte. Rechts daneben ist das kleine Taschenchiffriergerät CD-57 zu sehen, das ab 1957 in den Handel kam.

IN.KU

Die Crypto AG in Zug – erste Adresse für Schweizer Chiffriertechnik

Die Crypto AG in Zug war während Jahrzehnten eine der renommiertesten weltweit tätigen Hersteller von Verschlüsselungsgeräten und Sicherheitstechnik. Boris Hagelin gründete die Firma am 13.Mai 1952 in Zug, sie übernahm alle seine bisherigen Tätigkeiten aus Schweden. Die erste in der Schweiz verkaufte Chiffriermaschine war die CX-52. Sie war nach damaligen Standards eine der besten und sichersten Chiffriermaschinen. Anders als bei späteren Maschinen gab es keine schwächeren Versionen. Spätere Maschinen wurde in der Regel in zwei Varianten hergestellt: Die sichere Variante für die Nato, Schweden und die Schweiz, eine weniger sichere Variante für alle anderen. Bis etwa 1970 stellte man in Zug mechanische, teilweise auch elektromechanische Chiffriergeräte – Rotormaschinen und Telexgeräte – her, teilweise mit interessantem Zubehör. Dazu gehörte zum Beispiel ein Lesegerät für Telexstreifen, welche einen sicheren Zufallscode erhielten. Das Prinzip ist unter dem Namen One-Time-Pad bekannt und gilt auch heute noch als unknackbar. Ab den 1970er Jahren folgten elektronische Geräte, auch abhörsichere Telefone und Mobiltelefone gehörten später dazu.

Die Crypto AG hatte Niederlassungen in Brasilien, Malaysia, im Sultanat Oman und in den Vereinigten Arabischen Emiraten, sie hatte Kunden in über 130 Ländern weltweit.

Zweimal wären die Machenschaften der Firma Crypto AG beinahe aufgeflogen: Ein erstes Mal während des Jugoslawien-Krieges anfangs der 1990er Jahre. Die jugoslawische Regierung merkte, dass man ihr schwache Testgeräte geliefert hatte und drohte der Firma, den Betrug öffentlich zu machen. Ein zweites Mal kam der Verdacht auf, als der Verkaufsingenieur Hans Bühler im Jahr 1992 während 292 Tagen wegen Spionagevorwürfen von der iranischen Regierung festgehalten wurde. Der Fall erregte weltweit Aufsehen.

Das internationale Geschäft der Firma Crypto AG wurde im Jahr 2018 an den schwedischen Unternehmer Andreas Linde verkauft, das Schweizer Geschäft wurde 2023 nach einem Management Buyout zu CyOne Security AG umbenannt, diese Firma ist heute im Besitz des Schweizer Technologie- und Rüstungsunternehmens Ruag.

Nachdem die Firma Crypto AG jahrelang rein mechanische Chiffriergeräte verkauft hatte, musste sie in den 1970er Jahren auf Elektronik umstellen. Die HC-520 war die erste elektronische Chiffriermaschine und kam 1977 auf den Markt.

Boris Hagelin

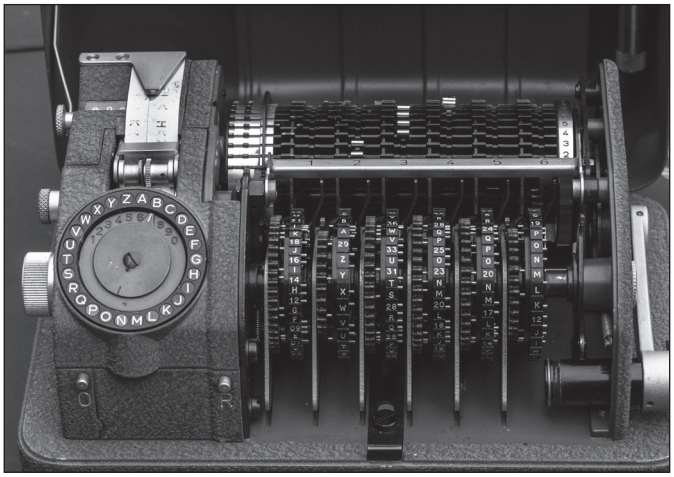
Boris Hagelin wurde 1892 im Russischen Kaiserreich (heute Aserbaidschan) geboren, sein Vater war an der Seite von Emanuel Nobel im Erdölgeschäft tätig. Hagelin besuchte Schulen in St.Petersburg und Lundsberg (Schweden) und studierte anschliessend Maschinenbau in Stockholm und arbeitete ebenfalls für die Firmen von Nobel. Zu seinen Aufgaben gehörte die Aufsicht über die 1915 gegründete AB Cryptograf von Arvid Damm, der 1921 eine erste Chiffriermaschine zum Patent anmeldete. Hagelin war überzeugt, dass er diese Maschine verbessern konnte und reichte 1928 ein erstes Patent dafür ein. In der Folge entwickelte Boris Hagelin weitere Maschinen und suchte dafür Käufer in Europa und in den USA. 1940 fuhr er mit dem letzten Schiff aus Genua in die USA und blieb dort während des ganzen Krieges. In dieser Zeit konnte er enge Beziehungen zu den US-Nachrichtendiensten und vor allem William Friedman aufbauen. Friedman (1891-1969), hatte einen ähnlichen Hintergrund wie Hagelin, war gleich alt und gilt als Doyen der US-Kryptologie. Es gelang Hagelin eine Lizenz für seine als C-38 bekannte Maschine der US-Regierung zu verkaufen, die davon 140 000 Stück herstellen liess. Sie erhielt den Namen M-209. Friedman sorgte nach dem Krieg dafür, dass Hagelin seine ersten Maschinen aus der Schweiz an verschiedene Länder verkaufen konnte. Bedingung war aber immer, dass die US-Geheimdienste in der Lage waren, die verschlüsselten Nachrichten zu lesen. Weil das neutrale Schweden die Chiffriermaschinen als Kriegsmaterial taxierten, war Hagelin 1948 in die Schweiz übersiedelt, wo er ab 1952 zunächst aus seinem Chalet an der Weinbergstrasse in Steinhausen bei Zug begann, Chiffriermaschinen zusammenzubauen und zu verkaufen. Sein erster Mitarbeiter war der Ostschweizer Oskar Stürzinger (1920-2011), der später Chefingenieur wurde. Die hier abgebildeten Maschinen stammen aus seinem Nachlass. Stürzinger war in die Geheimnisse von Boris Hagelin eingeweiht, er wird in den geheimen Papieren «Siegfried» genannt.

Boris Hagelin verkaufte seine Crypto AG im Jahr 1970 an eine Tarnfirma des amerikanischen Geheimdienstes CIA und des deutschen Bundesnachrichtendienstes BND. Diese Dienste waren fortan in der Lage Nachrichten von über 100 Ländern mitzulesen. Sie wussten von den Menschenrechtsverletzungen der Junta in Argentinien 1976 bis 1983 und von den Urhebern des Bombenanschlags auf die Diskothek La Belle in Berlin im Jahr 1986.

IN.KU

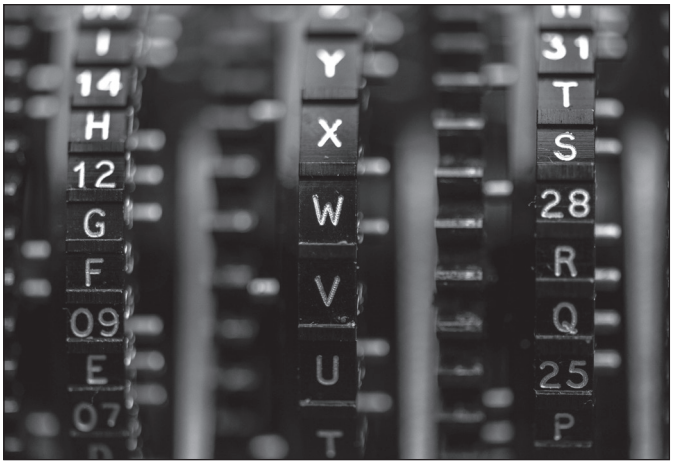
Die CX-52 – ein Museumsstück aus der Schweiz

Die CX-52 ist die wohl am häufigsten abgebildete Chiffriermaschine der Firma Crypto AG und wurde in den Diskussionen um die «Cryptoleaks» zu einer Art Symbol für den Skandal. Dies, obwohl die Maschine nach den Standards der damaligen Zeit zu den sichersten Chiffriermaschinen gehörte. Ohne Zusatzgeräte ist die Bedienung des berühmten Chiffriergerätes umständlich: Sind die Grundeinstellungen einmal gemacht, muss der zu verschlüsselnde Buchstaben an einem Rad auf der Vorderseite links angewählt werden, danach muss – ähnlich wie bei einer alten Registrierkasse – eine Kurbel auf der rechten Geräteseite betätigt werden. Danach kann der verschlüsselte Buchstabe abgelesen werden. Einzige Erleichterung bietet ein eingebauter Drucker, der den Klartext und das Chiffrat mitschreibt. Damit entfällt eine Fehlerquelle und der Verschlüsselungsvorgang ist nachvollziehbar.



Die CX-52 verfügt über sechs austauschbare Rotoren, insgesamt existierten zwölf solche Rotoren. Sie weisen folgende Teilungen auf: 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 & 47. Auf jeder Position sitzt ein kleiner Reiter, der entweder aktiv oder passiv ist. Er kann mit Hilfe eines mitgelieferten kleinen Schlüssels manipuliert werden. Die hohe Anzahl der Rotoren – die Enigma hatte ursprünglich nur drei Rotoren – erhöht die Komplexität der Chiffrierung und damit die Sicherheit. Einen entscheidenden Anteil spielt aber eine Trommel, die oberhalb der Rotoren zu finden ist und die ebenfalls mit Hilfe von Reitern programmiert werden kann. Sie regelt die Fortschaltung der Rotoren der Chiffriermaschinen und sorgt dafür, dass die Fortschaltung unregelmässig geschieht. Die regelmässige Fortschaltung der Rotoren war eine der Hauptschwächen der Enigma-Chiffriermaschine.

Boris Hagelin entwickelte die CX-52 in der Schweiz, die ersten Exemplare wurden aber noch in einem Werk in Schweden hergestellt. Später erfolgte die Herstellung vollständig in Zug, Hagelin hatte dafür seinen Chefkonstrukteur Sture Nyberg in die Schweiz gebracht. Anders als bei späteren Maschinen hatte Boris Hagelin den US-Geheimdienst bei der Entwicklung der CX-52 nicht konsultiert. Dieser zeigte sich bei der Präsentation bestürzt. Für Änderungen war es zu spät und man verständigte sich auf die Produktion eines speziellen Manuals für bestimmte Länder. In diesem Manual empfahl man Prozeduren, die leichter zu knacken waren. Damit ist eine der prinzipiellen Schwächen von vielen mechanischen Chiffriergeräten der Crypto AG angesprochen: Wurden bei den Grundeinstellungen Fehler gemacht, so war die Verschlüsselung einfach zu knacken, der entstehende Algorithmus war unter Umständen trivial. Die Schweizer Armee sah die Crypto Geräte als «nicht miliztauglich» an. Auch Norwegen kam zum gleichen Schluss. Osteuropäische Länder konnten offenbar Nachrichten, die mit schwachen Maschinen verschlüsselt waren, mitlesen.



Die CX 52 besass 6 Rotoren mit unterschiedlichen Teilungen. Die Beschriftung der Rotoren mit Zahlen und Buchstaben diente der Ausrichtung der Grundeinstellung am Anfang des Chiffrierprozesses.

Die Spezialität der CX-52 war die unregelmässige Fortschaltung der Rotoren. Dafür war die Trommel, auch Stangenkäfig genannt, oben im Bild verantwortlich. Auf einem Papierstreifen wurden Schlüsseltext und Klartext festgehalten.

Die Eingabe des Textes erfolgte über ein Rad. War es eingestellt, wurde die Kurbel rechts betätigt und der verschlüsselte Text konnte abgelesen werden. Eine Tastatur war als Sonderzubehör erhältlich.

Trotzdem war die CX-52 ein Verkaufserfolg. Sie war in über 50 Ländern weltweit in Gebrauch und wurde von der deutschen Firma Hell in Lizenz hergestellt. Belgien nutzte sie bis in die 1990er Jahren, weil sie als komplett mechanische Maschine immun war gegen den elektromagnetischen Impuls EMP einer Nuklearexplosion. Sie wurde in verschiedenen Versionen für das Heer aber auch für zivile Stellen produziert und fand in zahlreichen Ländern Europas Verwendung.

IN.KU

Ein Chiffriergerät für die Tasche: Die CD-57

Das Chiffriergerät CD-57 gelangte ab 1957 in den Handel und wurde aufgrund seiner geringen Grösse auch als Taschenchiffriergerät bezeichnet. Das ist allerdings sehr relativ: Mit den Massen 17.7 x 8.0 x 4.0 cm und einem Gewicht von einem Kilogramm war das Gerät etwa so gross wie eine Zigarrenschachtel und alles andere als handlich. Trotzdem hatte es eine Vorrichtung, um es am Gürtel des Übermittlungs-Spezialisten zu fixieren. Das Gerät war vor allem im Kalten Krieg sehr beliebt, die Firma Crypto AG verkaufte davon mehr als 12 000 Stück. Von diesem Gerät gab es starke und schwache Versionen, die Unterschiede zeigen sich teilweise erst, wenn man das Gerät komplett demontiert hat. Die starken Geräte wurden an Nato-Länder, Schweden und die Schweiz geliefert, die schwachen Geräte gingen als CD-55 an die übrige Welt. Vergoldete Spezialversionen wurden für den damaligen Schah von Persien und den Vatikan hergestellt. Eine Spezialversion nutzte einen Code auf Lochstreifen.

Die CD-57 funktionierte nach denselben Prinzipien wie ältere Geräte und vor allem wie die CX-52. Das Gerät verfügte ebenfalls über sechs austauschbare Rotoren mit manipulierbaren Noppen. Die Bedienung erfolgte analog wie bei der CX-52: der zu verschlüsselnde Buchstaben wurde am Ring eingestellt, danach musste mit etwas Kraft ein Hebel gedrückt werden und anschliessend konnte an der Vorderseite der Maschine der verschlüsselte Buchstabe abgelesen werden. Anders als bei der CX-52 gab es keinen Drucker, womit natürlich auch eine Fehlerquelle gegeben war. Wie bei der grösseren CX-52 war die Veränderung der Grundeinstellungen eine aufwendige Sache. Das missfiel den Kunden teilweise. Für sie lieferte man komplett eingestellte Sätze von Rotoren, was natürlich gegen jegliches Geheimhaltungsprinzip verstiess.

Die Geräte waren äusserst robust und in einigen Ländern bis Ende des 20. Jahrhunderts im Einsatz.

Die CD-57 verwendete analog zur CX-52 sechs Rotoren mit unterschiedlichen Teilungen. Auch hier erfolgte die Eingabe des Textes über ein Rad an der Aussenseite des Gerätes.

Weitere Literatur

Es gibt eine umfangreiche Literatur und zahlreiche Internetseiten zur Firma Crypto AG und ihren Produkten.

- Silvan Frik: Boris Hagelin and Crypto AG: Pioneers of Encryption. In: Karl de Leeuw and Jan Bergstra (Hrsg.): The History of Information Security – A Comprehensive Handbook. Elsevier Amsterdam 2007. S. 479-486. ISBN 978-0-444-51608-4
- Res Strehle: Operation Crypto. Echtzeit, Zürich 2020, ISBN 978-3-906807-19-5
- Res Strehle: Verschlüsselt – Der Fall Hans Bühler. Werd-Verlag, Zürich 1994. Neuauflage 2020, ISBN 978-3-03922-044-1

Internetadressen

Eine umfangreiche und häufig aktualisierte Website zum Thema:
https://cryptomuseum.com/crypto/
Der Fall Crypto und das Schweizer Parlament:
https://www.parlament.ch/de/organe/delegationen/geschaefts-pruefungsdelegation/fall-crypto-ag

Impressum

Autor Dominik Landwehr (*1958) hat als Journalist und Kulturexperte gearbeitet. 2007 hat er an der Universität Basel eine Dissertation zum Thema «Mythos Enigma» vorgelegt. Seit 2019 ist er als freier Autor und Berater tätig.

Fotos Dominik Landwehr.
Das Bild von Hagelin stammt aus Wikipedia.

Gestaltung Andreas Fahrni, Schaffhausen

Gedruckt bei Drucksprint GmbH, Wängi TG

SGTI

Schweizerische Gesellschaft für Technikgeschichte und Industriekultur

Geschäftsstelle
Marktgasse 37
8400 Winterthur
Tel: 052 202 02 27
(Di./Do./Fr. erreichbar)

Präsident:
Markus Meier, Aarau

Geschäftsführung:
Hanna Gervasi

Die SGTI bietet zum jährlichen Mitgliederbeitrag von Fr. 70.–

- Vorträge, Exkursionen, Reisen, Tagungen, Ausstellungen
- jährlich 4 Zeitschriften «industriekultur», 3 IN.KU-Bulletins und weitere industriekulturelle Publikationen.
- Online-Inventar Industriekultur Schweiz www.industriekultur.ch

Weitere Unterlagen über unsere Aktivitäten erhalten Sie über die Postadresse oder per Mail.

ASHT

Association suisse d'histoire de la technique et du patrimoine industriel

Président:
Markus Meier, Aarau

Gestion:
Hanna Gervasi

- L'ASHT organise des conférences, excursions, symposiums, expositions, voyages du patrimoine industriel.
- Les membres reçoivent le bulletin IN.KU et la revue «industriekultur» et d'autres publications.
- Inventaire en ligne du patrimoine industriel de la Suisse

Cotisation annuelle: Fr. 70.–

Sur demande (Adresse postale/mail) nous vous envoyons très volontiers toute documentation concernant l'ASHT.

Mail: info@sgti.ch
www.sgti.ch
www.asht.ch
www.industriekultur.ch