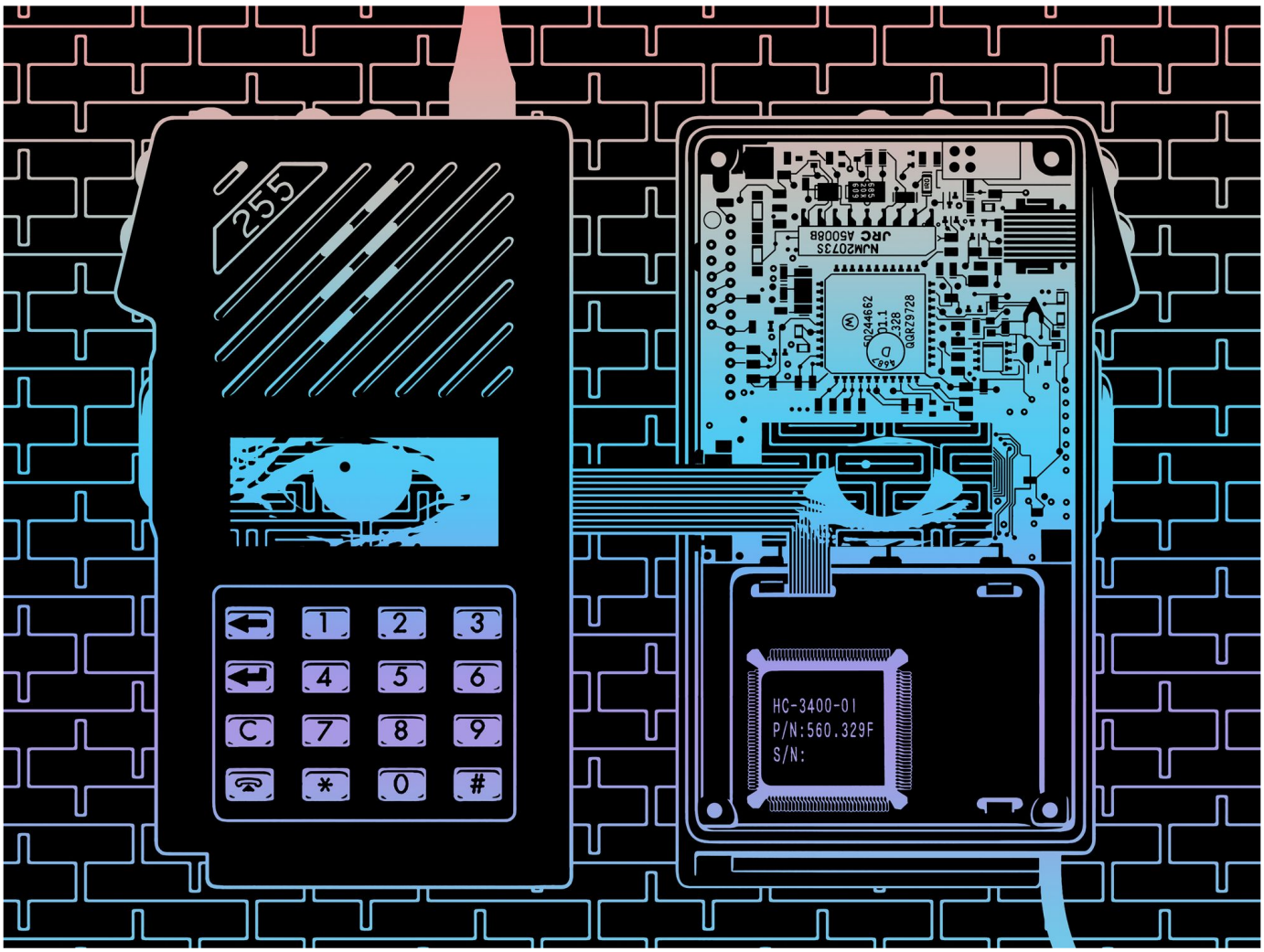

Die mysteriöse Schwesterfirma

Die Crypto AG war nicht allein im Dienst ausländischer Mächte. Erstmals lässt sich belegen, dass die CIA mithilfe der Firma Infoguard auch Schweizer Unternehmen abgehört hat.

Eine Recherche von Mehdi Atmani, Adrienne Fichter, Sylke Gruhnwald (Text) und Gregory Gilbert-Lodge (Illustration), 11.11.2020

Der parlamentarische Untersuchungsbericht zur Verschlüsselungsfirma Crypto AG, der gestern veröffentlicht wurde, soll endlich Licht in die Machenschaften der 90er-Jahre bringen, in dieses Jahrzehnt der Geheimnistuerei und behördlichen Vertuschung im Schweizer Nachrichtendienstwesen. Geklärt werden soll mit diesem Bericht vor allem, wer in der Schweizer Politik und bei den Nachrichtendiensten davon wusste, dass der US-amerikanische und der deutsche Geheimdienst mit manipulierten Chiffriergeräten der Zuger Firma Crypto AG über hundert Staaten abhörten.

Ausgeblendet werden andere wichtige Akteure: Schweizer Firmen, die mit der Crypto AG verbandelt waren, ebenfalls von ausländischen Geheimdiensten kontrolliert wurden und noch heute aktiv sind. Auch sie waren grosse Nummern im Verschlüsselungsgeschäft. Und auch sie sollen von der CIA angeworben worden sein und manipulierte Geräte verkauft haben.

Wie zum Beispiel Infoguard, die Schwesterfirma der Crypto AG.

Während die Crypto AG ihre Verschlüsselungsgeräte an Regierungen lieferte, war Infoguard für Firmenkunden zuständig. Unsere Recherchen belegen erstmals, dass die Firma Anfang der 90er-Jahre vom amerikanischen Geheimdienst CIA und dem deutschen Nachrichtendienst BND damit beauftragt wurde, auch die Schweizer Privatwirtschaft abzuhören.

Geschehen ist dies überwiegend mit Sprachverschlüsselungsprodukten: Manipulierte Funkgeräte wurden an Firmenkunden, etwa Schweizer KMU, aber auch an Strafverfolgungsbehörden in der ganzen Welt verkauft.

Weder die Behörden noch die Öffentlichkeit wissen bisher, welche Firmen davon betroffen waren.

Klar ist jedoch, dass die Crypto-Affäre damit eine neue Dimension annimmt.

Zu Cryptoleaks und dieser Recherche

Anlass für unsere Recherchen waren die Cryptoleaks, eine Enthüllung über die sogenannte Operation Rubikon. Ein investigatives Journalistenteam von SRF, ZDF und «Washington Post» konnte dank eines 280-seitigen Dokuments namens Minerva beweisen, dass der deutsche Bundesnachrichtendienst (BND) und die CIA zwischen 1970 und 1993 ein Geheimbündnis hatten, um rund 100 Staaten auszuspionieren. Seit vielen Monaten forschen wir – ein dreiköpfiges Reporterinnenteam der Republik und von «Le Temps» – in der Vergangenheit des Schweizer Geheimdiensts und untersuchen mehrere Schweizer Firmen, die ebenfalls im Dienste ausländischer Mächte handelten. Wir sind dafür durch die Schweiz gereist, um mit den Quellen und Akteuren von damals zu sprechen, die heute noch leben. Eine Reise, die uns aufgrund der Pandemie digital auch nach Deutschland, Schweden, in die Niederlande, in die USA und nach Südafrika führte. Einige Quellen aus dem Umfeld des NDB und der Firmen waren im Nachgang der Cryptoleaks sehr auskunftsbereit. Andere wollten nichts mehr damit zu tun haben. Viele Quellen und Dokumente sind noch im Bundesarchiv klassifiziert oder – im Fall von Peter Regli – vernichtet worden. Dennoch ist es uns gelungen, an Kopien der unveröffentlichten Dokumente zu kommen.

Der ideale Standort

Die Neutralität – immer wieder lobten CIA und BND diese vermeintliche Charakteristik der Schweiz. Doch genauso liebten die ausländischen Geheimdienste auch die praktisch inexistenten Schweizer Exportkontrollen.

Restriktionen für Verschlüsselungsgeräte? Kannte die Schweiz lange nicht.

Dies war einer der Hauptgründe, weshalb sich der Schwede Boris Hagelin zu Beginn des Kalten Kriegs im Kanton Zug niederlassen wollte. Während seine Heimat Chiffriergeräte als Kriegsmaterial einstufte und deren Export oft verboten hatte, wurden sie in der Schweiz als Dual-Use-Güter verbucht – als Güter für den zivilen und militärischen Gebrauch. Sie fielen nicht unter

die Exportkontrollen und konnten auch an problematische Staaten ausgeliefert werden. Und so gründete Hagelin die Crypto AG in Steinhausen, Kanton Zug, und belieferte bald Militärs und Regierungen in aller Welt mit seinen hochkomplexen kryptografischen Kommunikationsgeräten.

Dies tat er im Dienst ausländischer Geheimdienste, wie wir heute wissen: Die Crypto-Geräte hatten Hintertüren, über die CIA und BND mithören konnten.

Doch nicht nur die Crypto AG war ein Ziel der Geheimdienste. Da die Schweiz stark im Verschlüsselungsmarkt mitmischte – Neutralität ist in diesem Geschäft ein Verkaufsargument –, gerieten auch andere Firmen ins Visier.

Im «Internet Archive» sind wir auf ein interessantes Dokument gestossen – eine protokollierte Anhörung des Unterausschusses für Wirtschaftspolitik, Handel und Umwelt im US-Repräsentantenhaus von 1993. Mehrmals wird darin die Schweiz erwähnt. Aufgelistet werden auch zehn Schweizer Firmen, die damals Verschlüsselungsprodukte auf dem Markt hatten: Ascom Tech AG, Brown-Boveri, Crypto AG, ETH Zürich, Ete-Hager AG, Gretag, Incaa Datacom AG, Infoguard AG, Omnisec AG, Organa.

Besonders interessant ist Infoguard. Einerseits, weil sie die Schwesterfirma der Crypto AG war. Andererseits und vor allem, weil sie heute noch existiert. Sie beschäftigt rund 150 Mitarbeiterinnen.

Infoguard entstand 1988 als Joint Venture der Crypto AG und Ascom AG. 2001 ging die Firma vollständig in den Besitz der Crypto Group Holding über – der Besitzerin der Crypto AG. Mit Infoguard wollte sich die Crypto AG Marktanteile sichern und Zugang zur Privatwirtschaft verschaffen. Sich und – so das hartnäckige Gerücht: auch der CIA.

Infoguard war unter anderem die Antwort auf das Bedürfnis nach Privatsphäre: Nach dem Ende des Kalten Kriegs fürchteten die amerikanischen Geheimdienste, dass die Sprach- und Datenkommunikation von Firmen zunehmend mit offenen Standard-Algorithmen verschlüsselt werden könnte; Verschlüsselungen also, die Open Source sind, damit für alle überprüf- und dadurch kaum manipulierbar. Diesen Trend galt es mit verschiedenen Mitteln zu stoppen – Infoguard war eines davon.

Als im Februar 2020 die Crypto-Affäre aufflog, stand schnell der Verdacht im Raum, dass über das wenig bekannte Schwesterunternehmen Infoguard auch dem Schweizer Finanzplatz manipulierte Geräte der Crypto AG untergejubelt worden sein könnten. Medien stützten die Vermutung auf Handelsregisterauszüge, die belegten, dass Infoguard bis 2018 der Crypto Holding gehörte, die ein komplexes Geflecht im Besitz der CIA gewesen ist. Und da viele Banken und Versicherungen zu den Kunden von Infoguard gehören, liegt die Vermutung nahe.

Doch der Beweis, dass die CIA mit manipulierten Geräten tatsächlich Schweizer Firmen ausspioniert hat, konnte bislang nicht erbracht werden. Was also ist an diesem Gerücht dran? Haben Schweizer KMU oder vielleicht sogar Grossbanken manipulierte Geräte von Infoguard erworben?

Aus dem Wikipedia der Kryptografie

Hinweise gibt die Website Cryptomuseum.com, die von gut informierten Ingenieuren aus den Niederlanden betrieben wird – eine Art Wikipedia für Kryptografiefirmen, Produkte und Geheimdienste.

Zu Infoguard heisst es dort:

> Obwohl der kommerzielle Markt nicht als Ziel des Nachrichtendiensts galt, stellte sich die CIA auf den Standpunkt, dass er eines werden könnte, vor allem im Zusammenhang mit internationalem Terrorismus. Es wurde beschlossen, dass Infoguard kryptofähige Funkgeräte verkaufen würde, die von Radiocom hergestellt worden waren, einer Tochterfirma von Ascom, und dass diese den (lesbaren) HC-3400 Drop-in-Krypto-Chip der Crypto AG enthalten würden.

Im Klartext: Die CIA wollte via Infoguard Funkgeräte verkaufen, die mit einem «lesbaren» Verschlüsselungschip der Crypto AG versehen und damit abhörbar waren, weil die Geheimdienste Zugriff auf den Schlüssel haben.

Quelle dieser Informationen sind mehrheitlich Firmenarchive und private Informanten. Gespiesen wird Crypto Museum auch aus dem sogenannten Minerva-Dokument von CIA und BND, das die Vorgänge rund um die Crypto AG detailliert beschreibt. Es liegt bis heute nur wenigen Medien vor, in Auszügen auch dem Schweizer Fernsehen.

Auf der niederländischen Website steht darüber hinaus, an wen die manipulierten Funkgeräte verkauft werden sollten – und an wen nicht:

> CIA und BND beschlossen, dass Infoguard allen Kunden lesbare Geräte verkaufen sollte, mit Ausnahme der Schweiz, Deutschland und Schweden sowie Geschäftsbanken.

Ist damit also der Verdacht widerlegt, Schweizer Firmen seien betroffen von Abhöraktionen mit Infoguard-Geräten? Nein, wie wir herausgefunden haben. Denn wenn von der Schweiz die Rede ist, sind nur die Behörden gemeint. Um dem weiter auf die Spur zu kommen, müssen wir uns das angespannte Verhältnis zwischen CIA und BND etwas genauer anschauen.

Wer hört wen wann und wie ab?

Aus dem kürzlich veröffentlichten Buch des Journalisten Res Strehle, «Operation Crypto», wissen wir, dass die Beziehung zwischen CIA und BND nicht allzu harmonisch war. Regelmässig gab es Streit darüber, wer wann und wie abgehört werden sollte, und wem man vertrauen konnte.

Auch der Kundenkreis von Infoguard wurde offenbar zum Politikum. Dazu findet sich bei Crypto Museum ein Hinweis: Während der deutsche Geheimdienst BND darauf dränge, dass gewisse Länder wie Frankreich und die Niederlande – alles Länder des Geheimdienstverbunds Maximator-Allianz – von der Überwachungsoperation ausgenommen werden sollten, wollten die Amerikaner bedingungslos ganz Europa abhören lassen.

Der niederländische Investigativjournalist Huub Jaspers bestätigt diese Information. An der Rubikon-Konferenz im Jahr 1987 kam es nach seiner Kenntnis zum hitzigen Streit zwischen CIA und BND. Jaspers arbeitet für das Magazin «Argos» beim öffentlich-rechtlichen Radio in den Niederlanden. Rubikon ist der Deckname für die jahrzehntelange Überwachungsoperation der beiden beteiligten Geheimdienste.

Wir erreichen Huub Jaspers über eine sichere Telefonleitung. Er sagt: «Die Deutschen wollten auch den Niederländern und Franzosen sichere Infoguard-Geräte liefern. Die Amerikaner haben das verhindert.»

Die USA setzten sich demnach durch: Zum einen sollten also verbündete Staaten abgehört werden. Zum andern auch die Schweizer Privatwirtschaft.

Der Chip HC-3400

Ist dies dann auch tatsächlich geschehen?

Ja, bestätigen mehrere voneinander unabhängige Quellen, darunter auch Insider aus dem Umfeld der Infoguard. Zumindest hat das Unternehmen manipulierte Geräte an Firmen in Deutschland, Schweden und der Schweiz ausgeliefert. Die Quellen zitieren als Beleg aus dem Minerva-Dokument von CIA und BND. Darin heisst es zusammengefasst:

> Infoguard verkaufte nicht nur «lesbare Geräte» an kleine Schweizer Unternehmen und an feindliche Länder, sondern auch an Strafverfolgungsbehörden (Polizei) und nationale Sicherheitsbehörden befreundeter Nationen.

Bei den von Infoguard verkauften Crypto-Produkten handelte es sich um die von Crypto Museum genannten manipulierbaren Chips HC-3400.

Jaspers berichtet von seinen Recherchen über die Operation Rubikon, gestützt auf verschiedene CIA-Dokumente wie Minerva. Er bestätigt: «Ascom lieferte die Hardware, von der Crypto kamen die Algorithmen, und die Infoguard baute alles zusammen.» Damals mussten Verschlüsselungen in Chiffriergeräte direkt eingebaut werden, es existierte noch keine Software dafür. Das Verschlüsselungsmodul für die bei der Polizei beliebten Ascom-Funkgeräte lieferte also die Crypto AG. Es enthielt den für die CIA «lesbaren» Kryptochip HC-3400. Zwei solche Funkgeräte kosteten 10’000 Euro.

Die Infoguard verkaufte wie auch die Crypto AG zwei Versionen davon: zum einen die stark verschlüsselten Funkgeräte, zum anderen auch eine Serie, deren Verschlüsselungsalgorithmus insgeheim abgeschwächt wurde. «Die sichere Version, die ging an Banken, grosse kommerzielle Banken. Und an die Behörden in Schweden, Deutschland und in der Schweiz», sagt Jaspers.

Darauf konnten sich die zerstrittenen Geheimdienste CIA und BND schliesslich einigen. Sie nannten die Einigung das «4-Säulen-Abkommen».

Alle anderen Kunden erhielten eine geschwächte Version, «selbstverständlich», wie Jaspers sagt, «ohne dass sie darüber informiert wurden».

«Ja, sie sind manipuliert worden»

Verschlüsselungsgeräte mit lesbaren Chips wurden in der Schweiz also an Firmen ausgeliefert. Und auch an Schweizer Ableger ausländischer Firmen aus «feindlichen Staaten». Vermutlich ist damit zum Beispiel der Iran gemeint.

Doch was wussten die Techniker bei Infoguard, die alles zusammenbauten?

Der Entwicklungschef von Infoguard in den 80er-Jahren, der ehemalige Crypto-AG-Ingenieur Jürg Spörndli, will nichts von den manipulierbaren Geräten gewusst haben. «Zu meiner Zeit war Infoguard sauber», sagte er diesen Frühling der «Aargauer Zeitung».

Doch eine andere Quelle sagt: Spörndli sei nicht naiv gewesen und habe begriffen, dass Hintertüren eingebaut werden: «Er durfte keine eigenen Verschlüsselungsalgorithmen für Crypto-/Infoguard-Produkte entwickeln.»

Was sagt er heute dazu?

Wir haben Jürg Spörndli angerufen.

Die Produktion von HC-3400-Chips habe nach seinem Weggang bei Infoguard im Jahr 1990 begonnen. Er selbst sei vorher bei der Crypto AG an der Entwicklung des Vorgängermodells beteiligt gewesen. Auch hier sei bereits ein schwacher Algorithmus zum Einsatz gekommen. Über die HC-3400-Chips sagt Spörndli: «Die wurden damals bei der Sprachverschlüsselung eingesetzt. Ob die sauber waren? Da will ich meine Hand nicht ins Feuer legen.»

Ein halbes Jahr nachdem die Crypto-Affäre aufflog, rudert der ehemalige Technische Direktor der Infoguard also zurück. Und räumt ein: «Ja, die von Infoguard hergestellten und verkauften Geräte mit integrierten Chips der Crypto sind vermutlich manipuliert worden. Von der Firmenpolitik her und von dem, was wir in den letzten Wochen und Monaten gelernt haben, ist das gut möglich.»

Bei allen Crypto-Produkten und -Komponenten habe er sich stets mit dem Chefkryptologen der Crypto AG, Kjell-Ove Widman, abstimmen müssen, sagt Spörndli. Nur Widman habe durchgeblickt. Der Schwede war von 1980 bis 1994 bei der Crypto AG tätig. Er soll wegen seiner Loyalität gegenüber den Vereinigten Staaten angeworben worden sein. Widman habe während des Falklandkriegs 1982 auch Argentinien die abhörbaren Kommunikationsgeräte HC-500 der Crypto AG verkauft. Auf Anfrage wollte Widman dazu keine Stellung nehmen.

Dass die Infoguard-Geräte manipuliert waren, stützt eine kürzlich veröffentlichte Enthüllung des niederländischen Magazins «Argos» und Huub Jaspers: Darin heisst es, dass mehr als 600 geschwächte SE-660-Funkgeräte mit denselben Chips an die niederländischen Behörden Ende der Neunzigerjahre und in den Nullerjahren verkauft wurden – an einen «befreundeten Staat».

«In den Niederlanden ist dies nun ein kleiner Skandal», sagt Crypto-Museum-Redaktor Paul Reuvers, «da dieses Equipment von Sonderermittlungsteams der Polizei, von SWAT-Teams, zum VIP-Schutz, von der Niederländischen Bank, dem Schutz der Königsfamilie und so weiter verwendet wurde.»

Brisant ist auch: Gemäss dem Beitrag waren dieselben Funkgeräte – «made by Infoguard» – mit eingebauter Hintertür auch beim UN-Kriegsverbrechertribunal zum Bürgerkrieg in Jugoslawien in Den Haag im Einsatz.

An den genauen Kundenkreis der Infoguard möge er sich nicht mehr so genau erinnern, sagt Spörndli: «Die KMU waren unwichtig, doch Banken waren gute Kunden, ebenso Unternehmen aus der Rohstoffbranche und Unternehmen, die mit Erdöl handelten.» Genutzt wurden diese Mobilfunkgeräte beispielsweise für Verkaufsgespräche und für den Austausch von Interna auf Managementebene. Damit wollten sich Firmen vor Wirtschafts- und Industriespionage schützen.

Wir fragen uns nun: Wer war von Überwachung betroffen? Kantonalbanken? Andere Finanzdienstleister? Globale Rohstofffirmen?

Hier bricht unsere Spur ab.

Die neue Infoguard

Das ist insofern nicht weiter erstaunlich, als aus Infoguard mittlerweile ein neues Unternehmen geworden ist. Das Geschäft der ersten Infoguard-Ära Anfang der 90er-Jahre verlief harzig und entsprach offenbar nicht den Vorstellungen der Geheimdienstchefs.

Dies halten auch die Crypto-Museum-Fachleute fest: «Es lief nicht so wie erwartet, und Infoguard wurde alles andere als ein Gewinnbringer.» Der Plan, die Schweizer Wirtschaft flächendeckend auszuhorchen, ging kommerziell nicht auf. Der Betrieb wurde in den frühen 90er-Jahren quasi eingestellt. Infoguard blieb als leere Hülle im Handelsregister eingetragen.

Doch ab 2001 gab es einen neuen Anlauf. Gemäss der «Aargauer Zeitung» pumpte die Holding Crypto Group in den folgenden zwei Jahren 9,1 Millionen Franken in Form eines Darlehens in die Infoguard. Auch die wiederbelebte Firma verkaufte offenbar zunächst Crypto-AG-Produkte.

Dass sie auf die Technik ihrer Schwesterfirma zurückgriff, liegt nahe. Sie hatte keine eigene Entwicklungsabteilung, sondern war lange die erweiterte Verkaufsabteilung von Crypto AG, sagt ein ehemaliger Verkaufsmanager von Infoguard. «Die Firma war opportunistisch und hat die Crypto-Geräte an Infoguard-Kunden verkauft.»

Die zweite Ära war von grösserem Erfolg gekrönt: Sie lieferte etwa Fax-Verschlüsselungsgeräte an Schweizer Banken wie die Credit Suisse oder UBS. Und Verschlüsselungsboxen für das sogenannte L2-Layer-Ethernet, den Verkaufsschlager von Infoguard in den Nullerjahren. Solche Boxen verschlüsseln auf der Ebene der Hardware den Datenfluss zwischen Geräten. Sie werden etwa bei der Kommunikation zwischen Bern und den Botschaften im Ausland eingesetzt, oder zwischen Niederlassungen von Banken.

Auch Swisscom kaufte bei Infoguard solche Boxen ein. Infoguard lieferte zudem in den Nahen Osten, wie wir von einem früheren Manager erfuhren.

Seit die Crypto-Affäre aufgeflogen ist, wird gemutmasst, ob auch diese Geräte manipuliert waren. «Holten sich Infoguard-Kunden gleichzeitig die CIA ins Haus?», fragte beispielsweise das Magazin «Inside IT» im Frühling.

Bislang gibt es dafür keine Belege.

Der Verdacht scheint ehemaligen Infoguard-Mitarbeitern weit hergeholt. Bei den L2-Layers habe man auf eine Open-Source-Standardverschlüsselung gesetzt, sagen sie. «Die Bankkunden sagten uns immer: Diese proprietären Schlüssel der Crypto AG wollen wir nicht», so ein ehemaliger Consultant.

Und auch ein Sprecher von Infoguard entgegnet: «Verschiedene Kunden haben diese Verschlüsselungslösungen durch externe Stellen überprüfen lassen und als absolut sicher eingestuft.» Dass die CIA auch in den Nullerjahren Infoguard-Securityexperten angewiesen hätte, solche Hintertüren in die Boxen einzubauen, lässt sich nicht erhärten.

Beim Schnaps erfuhr man mehr

Trotzdem halten sich rund um Infoguard Spekulationen. Ein Grund dafür ist die personelle Verflechtung zwischen den beiden Schwesterfirmen:

– FDP-Alt-Nationalrat Georg Stucky, der im Minerva-Dokument als Mitwisser namentlich genannt wird, war Verwaltungsratspräsident von Infoguard – und sass von 1992 bis 2016 im Verwaltungsrat der Crypto AG. Stucky ist im August 2020 verstorben.
– Auch FDP-Alt-Ständerat Rolf Schweiger war von 2014 bis 2019 im Verwaltungsrat der Crypto AG und gleichzeitig in jenem von Infoguard.
– Der langjährige Geschäftsführer der Crypto AG, Giuliano Otth, war auch Verwaltungsrat bei Infoguard.
– Auch im Management gab es Verbindungen. «Alle in der Geschäftsleitung bei Infoguard waren Crypto-Kinder», so ein früherer Marketingmitarbeiter.

Zwar geben all diese Leute an, nichts von den Abhöraktionen der Crypto AG gewusst zu haben. Es habe kulturelle Unterschiede zwischen den beiden Schwesterfirmen gegeben, wird erzählt. Das Personal bei Infoguard habe die Crypto-Mitarbeitenden als eher verschlossen und konservativ erlebt.

Ein ehemaliger Verkaufsmanager von Infoguard sagt, man habe eigentlich enger mit der Crypto zusammenarbeiten und von Synergien profitieren wollen. Doch die Zusammenarbeit sei mühsam gewesen. Die Crypto AG sei nicht daran interessiert gewesen, ihrer Partnerin kommerzielle Kunden «zuzuschanzen». Man erfuhr lediglich ein wenig, wenn Alkohol floss: am Weihnachtsessen, im Zuger Pickwick Pub oder den gemeinsamen «Kafifüürli» bei Kaffee und Schnaps im Winter auf dem Firmengelände.

Dass es keinen Austausch zwischen Verwaltungsrat und Management gegeben habe über die Abhörabsichten, halten ehemalige Infoguard-Mitarbeiter für unglaubwürdig: «Die Verwaltungsräte hatten ihre Dinners und Mittagessen und tagten in den Crypto-Gebäuden», sagt einer von ihnen.

Doch harte Beweise für die Spionage fehlen für die Periode von 2001 bis 2018.

Der neuen Firma kommt dies gelegen. Sie will sich vom «Geheimdienstruch» lösen. Denn mit der CIA hat die Infoguard heute nichts mehr am Hut: 2018 löste der Geheimdienst die Crypto Holding auf. Sie verkaufte die beiden Schwesterfirmen Crypto AG und Infoguard. Letztere ging in Besitz des Managements über und wurde so zu einem unabhängigen Unternehmen.

Wie gross ist das Ausmass?

Damit sind wir in der Gegenwart angelangt. Und fassen kurz zusammen: Dass die Firma der CIA auch in ihrem zweiten Leben zu Spionagezwecken diente, lässt sich nicht belegen. Dass Infoguard in der ersten Phase ihrer Existenz – also zwischen 1988 und 1992 – für Geheimdienstaktionen benutzt wurde, ist dagegen so gut wie sicher.

Und auch, dass Schweizer Unternehmen abgehört wurden.

Trotzdem bleiben viele Fragen offen:

– Wer waren die Infoguard-Kundinnen zu Beginn der 90er-Jahre, diese «kleinen Schweizer Unternehmen», die manipulierte Geräte kauften?
– Waren auch Kantonalbanken oder Privatbanken von den Abhörungen betroffen? Gehörten auch sie zu «kleinen Schweizer Unternehmen»?
– Welche ausländischen Firmen mit Schweiz-Ableger waren betroffen?

Stand heute ist die Crypto-Affäre vor allem ein aussenpolitisches Fiasko. Länder, die der etablierten Schweizer Firma vertrauten, wurden abgehört.

Durch die Untersuchung der Geschäftsprüfungsdelegation des Parlaments haben wir erste Einblicke erhalten, wer in Bundesbern involviert war.

Doch um das ganze Ausmass der ausländischen Geheimdienstaktivitäten in der Schweiz auszuleuchten, wäre es angezeigt, auch die Geschäfte von Infoguard aufzuarbeiten. Von ihnen scheint die Schweiz selber viel stärker betroffen als von jenen ihrer Schwesterfirma, der Crypto AG.

Zum Autorinnenteam

Mehdi Atmani arbeitet als freier Journalist. Für seine Videoserie «La Suisse sous couverture» auf RTS erhielt er beim Swiss Press Award die Auszeichnung «Journalist of the Year». Sylke Gruhnwald ist freie Journalistin und hat zuletzt für das dokumentarische Theaterstück «Whistleblowerin Elektra» recherchiert. Adrienne Fichter ist Redaktorin der Republik.