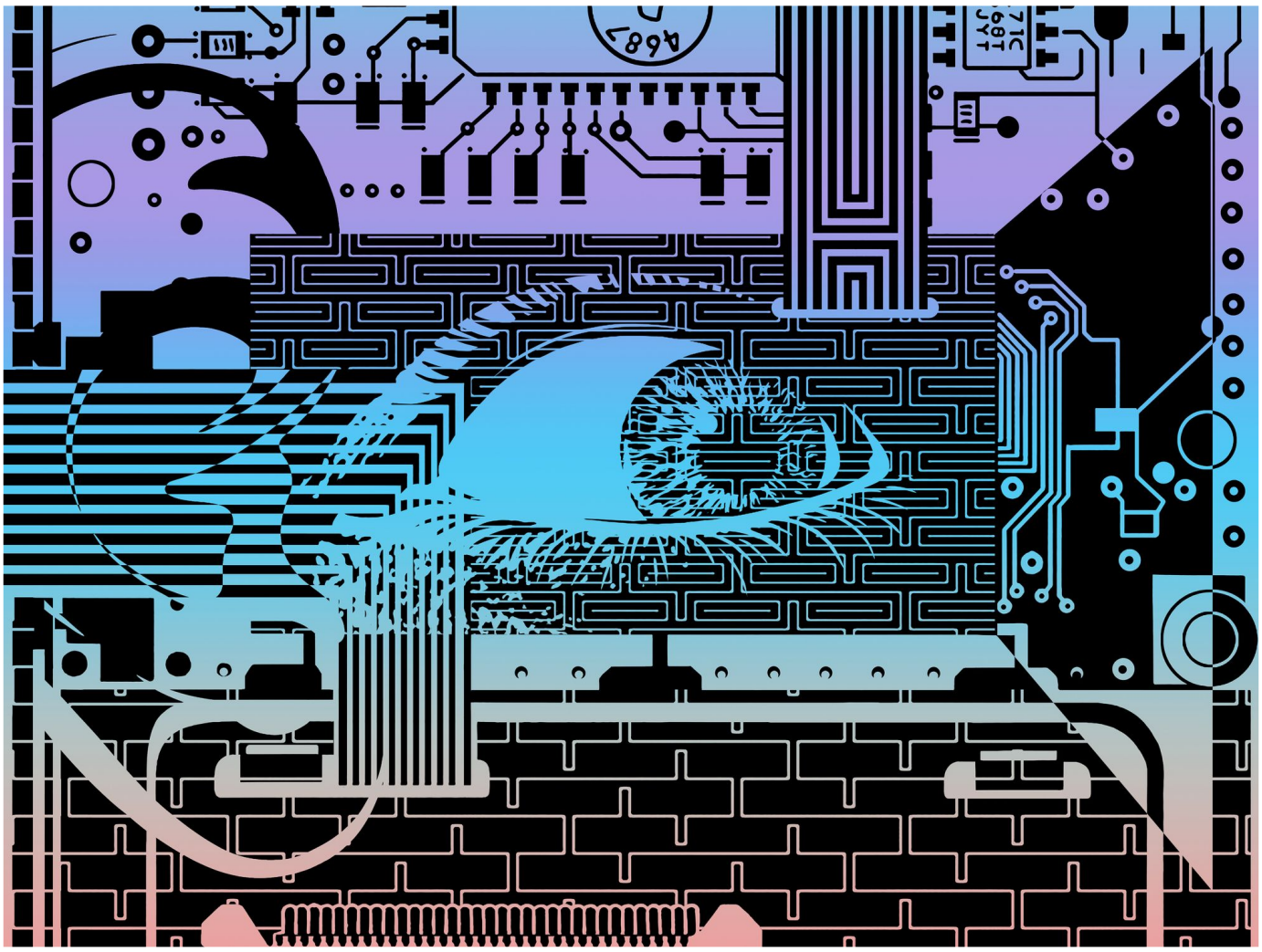

Das innerste Auge

Die Firma Omnisec wurde gegründet, um die Schweizer Bundesbehörden mit abhörsicherer Technologie zu beliefern. Nun zeigt sich: Sie tat das Gegenteil.

Eine Recherche von Mehdi Atmani, Adrienne Fichter, Sylke Gruhnwald (Text) und Gregory Gilbert-Lodge (Illustration), 26.11.2020

Bern, 10. November, kurz nach 15 Uhr: Die Kamera ist auf SVP-Ständerat Werner Salzmann gerichtet. Salzmann, in grauem Anzug und mit goldenem Berner Bären im Knopfloch, liest von seinen Notizen ab: «Während ihren Abklärungen wurde der GPDel versichert, dass die von der Crypto AG bezogenen Geräte systematisch überprüft wurden und die Schweizer Behörden von diesem Lieferanten nie schwache Verschlüsselungsgeräte erhalten hätten. [...] Hingegen wurde in den Geräten eines anderen Lieferanten mangelhafte Verschlüsselungstechnik nachgewiesen.»

Salzmann ist Mitglied der parlamentarischen Geschäftsprüfungsdelegation, kurz GPDel. Er hat Journalisten zur Orientierung ins Medien-

zentrum des Bundes geladen. Das Thema: die Publikation des GPDel-Berichts zum Fall Crypto.

Im Februar hatten sich Salzmann und seine Kolleginnen der Geschäftsprüfungsdelegation an die Arbeit gemacht, um Licht in eine Angelegenheit zu bringen, von der die Öffentlichkeit gerade erst erfahren hatte: die Spionageoperationen rund um die Crypto AG, eine Schweizer Herstellerin von Verschlüsselungsgeräten. Über diese Firma hatten Geheimdienste aus den USA und Deutschland jahrelang die Kommunikation von Staaten aus aller Welt abgehört, während der Schweizer Geheimdienst davon wusste und selber davon profitierte.

An der Pressekonferenz spricht Salzmann hauptsächlich darüber, wer in der Schweizer Politik eingeweiht war und wer nicht. Dass nebst der Crypto AG noch eine weitere Firma manipulierte Verschlüsselungsgeräte verkauft hat, erwähnt er nur beiläufig. Auch den Namen der Firma sagt Salzmann nicht: «Diese Firma, welche im Bericht der GPDel nicht namentlich genannt wird, hat ihre Geschäftstätigkeit vor ein paar Jahren bereits eingestellt.»

Journalisten sind seither der Frage nachgegangen, um welche Firma es sich dabei handeln könnte. Denn die Implikationen sind gewaltig: Gemäss dem Bericht der parlamentarischen Geschäftsprüfungsdelegation geht es um einen Schweizer Hersteller, der «an den Bund und an zwei Grossfirmen unsichere Geräte geliefert hat».

Nun ist das Geheimnis gelüftet. Alfred Heer, Präsident der GPDel, hat der Republik bestätigt: Es handelt sich um die Schweizer Firma Omnisec. Am Mittwochabend hat das SRF-Nachrichtenmagazin «Rundschau» ebenfalls darüber berichtet. Omnisec soll Mitte der 2000er-Jahre mehrere Schweizer Sicherheitsbehörden mit unsicheren Faxgeräten beliefert haben. Darunter die beiden Schweizer Nachrichtendienste, den Strategischen Nachrichtendienst (SND) sowie den Dienst für Analyse und Prävention (DAP). Auch die UBS kaufte gemäss «Rundschau»-Recherchen manipulierte Geräte.

Dass ausgerechnet Omnisec Behörden und Banken in der Schweiz ausspionieren liess, überrascht. Schliesslich wurde Omnisec zu genau einem Zweck gegründet: um zu verunmöglichen, dass die Geheimdienste der USA und Deutschlands sensible Schweizer Kommunikation abhören konnten. Omnisec war als 100 Prozent schweizerisch deklariert, wurde jährlichen Checks durch den Bund unterzogen und galt seit jeher als «Sauberfirma».

Wie war es möglich, dass sich auch diese Firma an Spionageaktivitäten beteiligte? Von wem wurde sie kontrolliert? Was wussten die Schweizer Geheimdienste? Und: Warum wurde die Firma 2018 aufgelöst – also im selben Jahr, in dem die CIA auch die Crypto AG verkaufte?

Fragen wie diese haben uns seit dem Frühling beschäftigt, als die Crypto-Affäre aufflog. In der Zwischenzeit haben wir mit ehemaligen Omnisec-Mitarbeitern und mit Expertinnen gesprochen, Handelsregisterauszüge ausgewertet und Produktdokumentationen studiert. Auch ETH-Professor Ueli Maurer, der angeblich eine massgebliche Rolle bei der Entwicklung von Verschlüsselungsalgorithmen bei Omnisec-Produkten spielte, hat sich ausführlich geäussert.

Dabei sind wir auf auffällige Parallelen und Verbindungen, aber auch auf viele Widersprüche gestossen – Ereignisse, die sich selbst die innersten Zirkel bei Omnisec nicht erklären können. Sofern sie denn sprechen.

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.

Eine langjährige Fehde

Die Spurensuche reicht zurück bis Ende der 1940er-Jahre. Damals machten in der Schweiz zwei Kryptografie-Experten gemeinsame Sache: der Luzerner Edgar Gretener und der Schwede Boris Hagelin. Sie entwickelten das Telekrypto-Gerät 35. Gretener soll seinem Kollegen und Freund Hagelin sogar die Niederlassungsbewilligung vermittelt haben, schreibt der Journalist Res Strehle in seinem Buch «Operation Crypto».

Doch die beiden Männer begannen, sich zu misstrauen. «Hagelin hat den Eindruck, Gretener bürde ihm die Entwicklungskosten auf und lasse die Erträge bei sich entstehen», schreibt Strehle. Bald darauf hatte jeder seine eigene Firma: Hagelin die Crypto AG, Gretener die Gretag. Sie konkurrierten «um die gleiche Art von Geräten, um den gleichen Markt, die gleichen potenziellen Kunden», wie es ein Geheimdienstkenner ausdrückt.

Während die Crypto international gute Geschäfte machte, hatte die Gretag zuerst vor allem im Schweizer Markt die Nase vorn. Sie galt als Hauptlieferantin der hiesigen Behörden. Dies, weil der Bund während des Kalten Kriegs die technologische Entwicklung bei der Gretag vollumfänglich finanzierte und selbst zum treusten Kunden wurde, wie Recherchen der WOZ gezeigt haben. Dem Schweizer Aussenministerium wurden etwa sogenannte James-Bond-Koffer (vom Typus Gretacoder 805) verkauft, mit denen Diplomaten verschlüsselte Telexmeldungen ins Bundeshaus absetzen konnten.

Doch den Erfolg erlebte der Gretag-Gründer nicht mehr. Edgar Gretener soll schwer depressiv gewesen sein und beging im Jahr 1958 Suizid. Seine wachsende Firma wechselte in den Besitz der Basler Ciba-Geigy, der heutigen Novartis. Dort wurde sie zum Allerweltsladen mit mehreren tausend Mitarbeiterinnen und hundert verschiedenen Patenten, von Chiffriermaschinen bis zu Druckgeräten.

Zu sicher für Geheimdienste

Der US-Auslandsgeheimdienst CIA und sein deutsches Pendant, der BND, beobachteten die Erfolgsgeschichte des «Tigers» – so wurde die Gretag bei

der CIA intern genannt – derweil mit Sorge. Die beiden Geheimdienste hatten es in der Zwischenzeit geschafft, die Crypto AG vollständig unter ihre Kontrolle zu bringen, und verkauften über die Firma mit Sitz in Steinhausen im Kanton Zug fortan verschiedene Produktetypen: Befreundeten Staaten wurden einwandfreie Geräte verkauft, den anderen Staaten knackbare Geräte. Der Produktionsstandort Schweiz versprach dabei Neutralität.

Doch den Datenverkehr, der über Gretag-Geräte abgewickelt wurde, konnten die Geheimdienste nicht knacken. «Die Geheimdienste konnten Ende der 1970er-Jahre nicht mehr als 7 Prozent der verschlüsselten Kommunikation von Gretag-Geräten abfangen und entschlüsseln», steht im Firmeneintrag auf Cryptomuseum.com, einer Art Wikipedia für Kryptografiefirmen und Geheimdienstgeschichte, die sich unter anderem auf interne Firmenarchive stützt.

Mit anderen Worten: Gretag blieb während des gesamten Kalten Kriegs *unreadable,* wie es im Geheimdienstjargon heisst: nicht lesbar.

Dies geht auch aus weiteren Dokumenten hervor, die uns vorliegen. Darin steht: «Die grösste Gefährdung ging von einer Schweizer Firma aus, der Gretag in Regensdorf (Schweiz).» Und vier Sätze später: «Die Gretag war tatsächlich zu dieser Zeit die einzige ernst zu nehmende Konkurrenz.» In den Dokumenten beschreibt ein BND-Mitarbeiter, wie gegen die Schweizer Firma deshalb Verleumdungskampagnen gestartet wurden.

Dass Gretag-Geräte lange «unknackbar» waren, belegen auch Dokumente des Nachrichtendiensts im Bundesarchiv. Darin finden sich deutliche Hinweise, dass die Chiffriergeräte nicht von westlichen Diensten «gelesen werden konnten». Denn noch Ende der 1980er-Jahre versuchte der BND, den Verkauf von Gretag-Maschinen an die DDR zu unterbinden, und intervenierte dabei direkt in Bern, wie Geheimdiensthistoriker Adrian Hänni bestätigt.

Die Geburtsstunde von Omnisec

Dem Chemiekonzern Ciba-Geigy wurde diese Spionagewelt zunehmend unheimlich. Und als die Beratungsfirma McKinsey ihr eine neue Strategie vorschlug – «zurück zum Kerngeschäft» – leitete sie den Verkauf ihrer Elektroniksparte ein. Der Plan war, zuerst die militärische Einheit von Gretag loszuwerden, mitsamt ihren erfolgreichen Chiffriermaschinen.

Dabei schaltete sich allerdings das Bundesamt für Rüstung ein. Seine Bedingung: Hochsensible Chiffriergeräte durften nicht an beliebige Käuferinnen aus dem Ausland verkauft werden. Der Bund begründete dies mit der gefährdeten «Staatssicherheit». Ein neuer Eigentümer müsse aus der Schweiz stammen und mit Schweizer Kapital finanziert sein. Auch das Personal müsse unverdächtig sein, keinen Migrationshintergrund haben.

100 Prozent Swissness war also gefordert. Gewährleisten konnte dies die Argonium SA, ein Genfer Hightechkonsortium. Hier fand das Problemkind der Ciba-Geigy im April 1987 eine neue Heimat. Mit neuem Namen: Omnisec.

Einfluss aus dem Ausland

Doch schon bald bildeten sich Verbindungen ins Ausland. Die Argonium war selbst nur einen Monat zuvor gegründet worden – von Anwalt Urs Ingold, der für den militärischen Nachrichtendienst, Untergruppe

Nachrichtendienst und Abwehr, gearbeitet haben soll. Er war der erste Eigentümer von Omnisec und taucht auch in den Minerva-Dokumenten der CIA auf.

Anzeichen für ausländische Einflussnahme finden sich im Handelsregister. Bis ins Jahr 2000 wurden insgesamt 20 Millionen Franken an Aktienkapital von der Briefkastenfirma Torcross Holding N. V. mit Sitz auf der Insel Curaçao in die Omnisec eingeschossen. Die Dokumente dazu unterzeichnet hat ein US-amerikanischer Anwalt: Donald G. Glascoff. Er arbeitete damals für die New Yorker Anwaltskanzlei Cadwalader, Wickersham & Taft. Ihr werden laut der WOZ «exzellente Verbindungen zu US-Geheimdiensten» nachgesagt.

Je nach Quelle übernahm Beat «Bert» Bettschart Omnisec schon kurz nach der Gründung oder erst nach dem Tod des vorherigen Inhabers Urs Ingold-. Bettschart blieb bis zu seinem Tod im Jahr 2002 Eigentümer, die letzten drei Jahre auch Verwaltungsratspräsident. Bettschart hatte ein eigenes Büro, besuchte Kunden – und lebte gleichzeitig mit seiner Frau und sechs Kindern in den USA. Hauptberuflich war er für Rockwell tätig, einen Konzern, der ursprünglich in der Rüstungs- und Raumfahrtbranche tätig war und heute zu Boeing gehört.

Während der militärische Teil sowie die Sprachverschlüsselungsgeräte an Omnisec gingen, blieb der zivile Teil von Gretag – dazu gehören etwa Patente für den Gretacoder, ein Chiffriergerät, das Banken benutzen – vorerst bei Ciba-Geigy. Später wurde auch dieser Unternehmensteil verkauft, und zwar an den amerikanischen Telekomkonzern AT&T. Omnisec war aber weiterhin befugt, Gretacoder-Geräte an Behördenkunden weltweit zu verkaufen.

Die Swissness, die Omnisec hätte auszeichnen sollen, war damit von Beginn an löchrig. Erstaunlicherweise schien dies weder beim Bund noch am Firmenstandort im zürcherischen Dällikon jemandem aufzufallen.

Lukrative Swissness-Fassade

Im Sommer treffen wir einen ehemaligen Mitarbeiter der Firma. Während wir draussen an der Sonne sitzen, greift der Mann, der anonym bleiben möchte, immer wieder in seine Aktentasche und holt durchsichtige Plastikmappen mit Firmenunterlagen hervor. Dazwischen zündet er sich eine Zigarette an.

Wir fragen ihn: Was machte die Omnisec besser?

Seine Antwort: Die Firma war 100 Prozent schweizerisch. Wir alle waren Schweizer. Deshalb wurde uns vertraut.

Tatsächlich setzte die Omnisec in ihrem Marketing voll auf den Schweiz-Faktor. Mitarbeitende, Verwaltungsräte, Eigentümer: Alle waren aus der Schweiz. Auf der Firmenwebsite: ein Foto des Matterhorns. Dazu der Verkaufsslogan: *Keep Your Secrets Secret* – halte deine Geheimnisse geheim.

Die Verflechtungen zum Schweizer Staat und zum Rüstungswesen blieben weiterhin eng: Hans-Jörg Bärtschi, der die Firma 2004 kaufte und bis 2015 Verwaltungsratspräsident war, ist Präsident der Rüstungskommission, einem ausserparlamentarischen Organ, das das Verteidigungsdepartement berät.

Für die Swissness des Personals sorgten regelmässige Checks: «Selbst die Putzfrau musste sich einer Genehmigung unterziehen», sagt Jürg Lindecker, Firmenchef bei der Omnisec von 1995 bis 2001. Die Generalstabsabteilung führte Kontrollen durch, ob alle Geheimhaltungsregeln eingehalten wurden. Ein Journalist der «NZZ am Sonntag» beschrieb Omnisec 2014 in einem Firmenporträt als «ein typisch schweizerisches KMU mit 55 Mitarbeitern».

Die Swissness verkaufte sich ausserordentlich gut. Von der Gretag hatte die Omnisec einen soliden Behördenkundenstamm aus der ganzen Welt geerbt. Ihr Hauptgeschäft waren Sprach-, Fax- und Datenverschlüsselungen an Regierungen, Armeen und Geheimdienste, «die das Mitlesen der Sprach- und Datenkommunikation verhindern sollen». Die Firma gewann Kunden aus der ganzen Welt. Dazu zählten Regierungen von Brasilien, Chile, Indonesien, Venezuela, Libyen und Nigeria und vielen Erdölstaaten. «Wir hatten Kunden, die unabhängig sein wollten von den Grossmächten», sagt Lindecker.

Bundesrat mit Omnisec-Handys

Omnisec profitierte zudem von mehreren Geheimdienstskandalen. Da wäre zum Beispiel die Bühler-Affäre von 1993, die weltweit Kundinnen von Crypto AG zu Omnisec überlaufen liess: Ein Verkäufer der Crypto AG war damals im Iran festgehalten worden, weil die dortige Regierung den Verdacht geschöpft hatte, ihr würden manipulierte Chiffriergeräte verkauft. Das habe viele Länder aufgeschreckt, berichtet ein ehemaliger Omnisec-Verkaufsmanager: «Die Leute kauften unsere Produkte nicht deshalb, weil sie günstiger waren, sondern weil sie nicht von der Crypto AG stammten.» Der damalige Chef der Crypto AG habe sich daraufhin bei der Omnisec mit den Worten beschwert: «Ihr seid gemeine Hunde.»

Und da waren die Leaks von Edward Snowden, der 2013 das wohl grösste Überwachungsprogramm des US-Geheimdiensts NSA offenlegte. Die Empörung darüber liess die Nachfrage nach Hochsicherheits-Hardware «Made in Switzerland» nochmals ansteigen, schrieb die «Weltwoche».

Schweizer Behörden und die Armee zählten in den Nullerjahren zu den treusten Omnisec-Kunden. 2013 wurden gemäss Medienberichten auch abhörsichere Mobiltelefone an den Bundesrat geliefert. Dafür wurde ein handelsübliches Samsung-Handy aufgerüstet zu einem Modell namens Mira. Zehn dieser Smartphones inklusive Server kosteten 77'000 Franken, wie die «NZZ am Sonntag» 2014 schrieb.

War die ganze Swissness bei Omnisec – das Matterhorn, die Personalchecks, die Nähe zur Armee – am Ende bloss eine perfekte Tarnung? Sind die Schweizer Behörden ihrer «eigenen» Kryptofirma auf den Leim gegangen?

Lauter Erinnerungslücken

Die Ergebnisse der SRF-Recherchen sind happig. Gemäss der «Rundschau» hat die Omnisec mehreren Schweizer Behörden, darunter den beiden Geheimdiensten – dem Strategischen Nachrichtendienst SND sowie dem Dienst für Analyse und Prävention DAP – Faxgeräte der Modellreihe OC 500 verkauft, die manipuliert waren.

Ob es sich um eine schwache Verschlüsselung handelte, die von ausländischen Geheimdiensten geknackt werden konnte, oder von eingebau-

ten Hintertüren herrührt, ist bisher nicht bekannt. Auch an zwei Grossunternehmen hat die Omnisec solche Faxgeräte geliefert, darunter die UBS. Wer der andere betroffene Kunde war, ist unbekannt.

Dies fand der Bund Mitte der 2000er-Jahre selbst heraus. Kryptografen aus einer interdepartementalen Arbeitsgruppe waren Unregelmässigkeiten bei den betreffenden Geräten aufgefallen. Daraufhin wurde die Sache untersucht, und das Eidgenössische Verteidigungsdepartement traf, wie im Bericht der parlamentarischen Geschäftsprüfungsdelegation zur Crypto-Affäre nachzulesen ist, «die notwendigen Vorkehrungen, um diese Lücken zu beheben». Welche Vorkehrungen das sind, ist unklar.

Einer, der über die Vorgänge eigentlich Bescheid wissen müsste, ist Alt-Bundesrat Samuel Schmid. Er hatte als Vorsteher des Verteidigungsdepartements von 2002 bis 2008 – also in der fraglichen Zeitspanne – seine monatlichen Gespräche mit den Direktoren des Nachrichtendiensts SND handschriftlich festgehalten. Zwei seiner Notizhefte konnten, wie aus dem GPDel-Bericht hervorgeht, kurioserweise in der Bibliothek am Guisanplatz in Bern gefunden werden.

Doch als wir den Alt-Bundesrat kontaktieren, um mehr über die damaligen Vorkommnisse zu erfahren, kann er sich an nichts mehr erinnern. «Ich kann Ihnen diese Frage nicht beantworten», sagt er. «Das ist 15, 17 Jahre her.»

Wie und warum Omnisec sich unbemerkt von den Schweizer Behörden in eine Tarnfirma eines ausländischen Geheimdiensts verwandelt hatte, bleibt damit weiter im Dunkeln.

Aufklärung könnten die ehemaligen Führungspersönlichkeiten der Firma leisten. Doch auch sie blocken ab. So etwa Hans-Jörg Bärtschi: Der Luzerner Finanzspezialist und Präsident der Rüstungskommission war von 2004 bis 2015 alleiniger Besitzer der Omnisec. «Das ist schon lange her», sagt er, als wir ihn auf die Passagen im GPDel-Bericht ansprechen. «Ich kann zur Omnisec nichts sagen.» Wem Bärtschi die Firma abgekauft hat und mit wessen Geld – eigenes oder geliehenes –, ist bis heute unbekannt, obwohl diese Information für die Schweiz von nationalem Interesse war.

Und auch der ehemalige Firmenchef Jürg Lindecker, der bereitwillig über vieles Auskunft gibt, stellt in Abrede, dass Omnisec in Verbindung mit ausländischen Geheimdiensten stand. «Wir waren das sicherste System», sagt er. «Es konnte nicht gebrochen werden.» Lindecker leitete die Firma bis 2001. «Was nach mir passiert ist, weiss ich nicht», sagt er. Eines sei jedoch klar gewesen: «Mein Nachfolger musste die Kosten senken.»

Viele Medien insinuierten, dass die Liquidierung der mittlerweile «amerikanischen» Gretag – der neue Besitzer war die Firma SafeNet, gegründet von zwei ehemaligen NSA-Ingenieuren – im Jahr 2004 dazu führte, dass Omnisec alle beliebten Gretacoder-Patente erbte und damit auch ins Visier der CIA geriet.

Unsere Recherchen konnten diese Hypothese jedoch nicht erhärten.

Das bizarre Ende

Sicher ist, dass die Omnisec trotz dieser Vorfälle gut unterwegs war. Ihre Produktepalette war breit: Sie richtete VPN-Schutzschilder für privaten Datenverkehr übers Internet ein, stellte abhörsichere Mobiltelefone her sowie Faxgeräte und sogenannte L2-Boxen, die Datenverkehr verschlüsseln.

Dabei wurden wie bei der Crypto AG stets Verschlüsselungsalgorithmen angewendet, welche die Firma selbst entwickelt hatte. Das bedeutet: Die Verschlüsselung war Geschäftsgeheimnis.

Vor diesem Hintergrund mutet es befremdlich an, was mit der Omnisec Mitte der 2010er-Jahre passierte. Die seltsamen Manöver begannen im Jahr 2015: Am 25. Juni dieses Jahres trafen sich Hans-Jörg Bärtschi, Besitzer, und Clemens Kammer, Firmenchef seit 2009, um 9 Uhr im Zürcher Hotel Engelmatt für eine ausserordentliche Generalversammlung.

«Traktandum: Verkauf der Unternehmensgruppe», heisst es im Protokoll. Kammers Firma, die Clemar Capital Management AG aus Zug, kaufte Omnisec. «Schluss der Sitzung: 9.30 Uhr.» Zwei Jahre später, Mitte Juni 2017, übernahm Omnisec die Argonium, ihre Mutterfirma. Clemens Kammer unterzeichnete den Fusionsvertrag für die Omnisec und die Argonium als Mitglied des jeweiligen Verwaltungsrats.

2018 machte das Unternehmen Omnisec schliesslich dicht.

Die offiziellen Gründe dafür: Das Interesse an Verschlüsselungstechnologie aus der Schweiz sei massiv gesunken. Dies sagte Kammer dem Fachmagazin «Inside IT». Die Kunden von Omnisec seien mehrheitlich kleine Staaten, die sich eigens für sie entwickelte Systeme nicht mehr leisten könnten – wegen fallender Öl- und Kupferpreise auf dem Weltmarkt und sinkender Budgets.

Ein ehemaliger Mitarbeiter, mit dem wir gesprochen haben, verstand damals die Welt nicht mehr. Aus seiner Warte boomte das Geschäft. Er allein habe als Verkäufer über 10 Millionen Franken Umsatz gemacht und in den letzten Jahren lukrative Aufträge an Land gezogen. Der ehemalige Verkaufsmanager hat uns mehrere Dokumente vorgelegt: darunter unzählige Offerten und Anfragen, einen Kaufvertrag einer ausländischen Botschaft in Bern für VPN-Lösungen und Firewalls, einen Vorvertrag zwischen Omnisec und einem ausländischen Verteidigungsministerium im Millionenbereich. Doch das Management habe ihm mitgeteilt: Man brauche keine neuen Kunden mehr.

Stück um Stück wurde der Laden heruntergefahren. Die internen Vorgänge wurden immer skurriler: Der Verkaufsmanager wurde einmal angewiesen, die in Lagerhallen herumliegenden Faxgeräte der neuesten Modellreihe an seine Stammkunden zu verkaufen. Die UBS habe 5000 Stück davon bestellt, aber nicht abgeholt, sagte man ihm. Ohne weitere Erklärung.

Ende 2016 war Omnisec im Minus, wie aus Handelsregisterauszügen hervorgeht.

Wir fragen beim ehemaligen Mitarbeiter nach.

Waren Sie überrascht?

Ja. Wieso kauft Kammer die Firma Omnisec für viel teures Geld, um danach den Laden dichtzumachen?

Haben Sie eine Idee, warum?

Der einzige Grund, der für mich Sinn ergibt, war: Wir waren ein Problem für gewisse Leute.

Wir haben auch Clemens Kammer selbst um eine Stellungnahme gebeten. Er sagt: «Informationen über Kunden, Investitionen und Geschäftsabschlüsse meiner privaten Unternehmen sind vertraulich. Deshalb bitte

ich um Verständnis, dass Sie dazu keine weiteren Auskünfte erhalten können.»

Auffällig am Ende von Omnisec sind nicht nur die finanziellen Umstände. Sondern auch das Timing: Im selben Jahr stieg auch die CIA bei der Crypto AG aus – auch hier wegen angeblich sinkendem Interesse an Hochsicherheitshardware. In den gängigen Smartphone-Apps sei Verschlüsselung neuerdings digital und bereits eingebaut, wie CIA-nahe Quellen der «Washington Post» erklärten. Der Markt sei kaputt, die Crypto AG nicht mehr attraktiv genug.

NSA kontaktiert ETH-Professor

Ungeklärt in der Omnisec-Affäre ist auch die Rolle der ETH. Bekannt ist, dass ETH-Professor Ueli Maurer von 1988 bis 2015 als Omnisec-Berater fungierte. Besonders wichtig war diese wissenschaftliche Mitarbeit für den ehemaligen CEO Jürg Lindecker, da für ihn als klassischen Ingenieur das Thema Verschlüsselungstechnik «ein Buch mit sieben Siegeln» gewesen sei. Ueli Maurer und Omnisec-Gründer Pierre Schmid haben auch ein gemeinsames wissenschaftliches Paper verfasst.

Die ETH soll aber auch generell eng mit der Omnisec zusammengearbeitet haben. In mehreren Produktbroschüren, die der Republik vorliegen, wird die Kooperation der Omnisec und der Hochschule betont.

Eine ETH-Mediensprecherin sagt dazu, diese Passage aus der Werbebroschüre sei der ETH Zürich wie auch Professor Ueli Maurer nicht bekannt gewesen: «Sie ist inhaltlich irreführend und ist von der ETH nicht autorisiert worden.»

Maurer äusserte sich gegenüber der Republik ausführlich in einer schriftlichen Stellungnahme. Darin erklärt er, er sei in den 2000er-Jahren von Omnisec gebeten worden, einige von der Firma entwickelte Algorithmen auf deren Sicherheit zu untersuchen: «Ich fand nach eingehender Prüfung keine Schwachstellen.» Als Berater sei er aber nicht in die Produktion der Geräte von Omnisec involviert gewesen und wisse auch nicht, wie diese Algorithmen in Produkten eingesetzt worden seien.

Interessant ist Maurers Antwort auf die Frage, ob er in Verbindung mit Geheimdiensten gestanden sei: «1989 wurde ich in der Tat vom amerikanischen Geheimdienst kontaktiert. Diese Kontaktaufnahme startete unauffällig auf der Ebene eines wissenschaftlichen Diskurses. Im Lauf der Diskussion eröffneten mir die NSA-Kontakte, dass sie mit Omnisec zusammenarbeiten möchten. Ich erklärte, keinerlei Einfluss auf Omnisecs Produkte zu haben und dass ich Manipulationen nicht mittragen würde.»

Darauf habe er den CEO von Omnisec kontaktiert, um ihn zu warnen, sagt Maurer: «Es kam danach zu einem Treffen der NSA-Mitarbeiter, des Omnisec-CEO und mir, an welchem der CEO eine Zusammenarbeit kategorisch ausschloss und sehr klar und definitiv den Kontakt beendete. Ich habe keine Informationen oder Indizien, dass der CEO den Kontakt zur NSA weitergeführt hat. Ich habe auch die nachfolgenden CEOs und den Chef-Kryptologen über diese Kontaktaufnahmen informiert.»

Dass Kryptografieexperten von Geheimdienstagenten angegangen werden, sei nicht per se ungewöhnlich, sagt Maurer. «Entscheidend ist, sich dieser Gefahr bewusst zu sein und sich nicht auf eine Zusammenarbeit einzulassen.»

Unklar bleibe, inwiefern die Geräte abgeschwächt worden seien und welche Komponenten betroffen sein könnten, so Maurer. «Auch wenn ich über keinerlei Indizien verfüge, kann ich persönlich eine Unterwanderung der Omnisec durch einen Geheimdienst letztlich nicht ausschliessen.»

Viele offene Fragen

Die Enthüllungen rund um die Vorgänge bei der Firma Omnisec werfen viele weitere Fragen auf.

- Wer war neben der UBS die weitere betroffene Grossfirma?
- Warum hat der Bundesrat trotz dieser Vorfälle weiterhin Omnisec-Handys erworben, wie etwa im Jahr 2013 die Mira-Handys? Wurde die Schweizer Regierung belauscht?
- In welchem Dienst agierte die Omnisec? Waren es wirklich die Amerikaner oder auch noch weitere ausländische Geheimdienste?

Klar ist: Je tiefer man gräbt, desto mehr Hinweise darauf lassen sich finden, dass die Schweiz einerseits als Trittbrettfahrerin von einer weltweiten Abhöroperation profitierte, andererseits aber auch selbst Opfer von Spionage war – und das von Schweizer Firmen. So hatte nicht nur die Schwesterfirma der Crypto AG, Infoguard, ursprünglich den Auftrag, manipulierte Geräte an die Privatwirtschaft zu verkaufen. Es wird nun auch klar, dass die Verschlüsselungsfirma Omnisec, die ein bis dato sehr sauberes Image pflegte, mitgeholfen hat, den Schweizer Staat zu belauschen.

Das alles gäbe mehr als genug Stoff für eine vertiefte Aufarbeitung durch eine Parlamentarische Untersuchungskommission (PUK).

Wenn die Politik denn wollte.

Unterstützen Sie uns!

Wir konnten sämtliche Verkaufsbroschüren und Unterlagen der Omnisec auftreiben. Dabei liegt uns die Dokumentation für Faksimile-Modelle (OC 500) und IP-Encryptors-Modelle (OC 400) sowie von Funkgeräten und Kryptophonen der Firma Omnisec vor. Sollten Sie sich mit diesen Modellen auskennen oder weitere Informationen zu Omnisec-Produkten haben, melden Sie sich bitte bei adrienne.fichter@republik.ch (für verschlüsselte Nachrichten via Adrienne Fichter). So helfen Sie uns, die Aufarbeitung eines wichtigen Kapitels der Schweizer Geheimdienstgeschichte weiterzutreiben.