VERSCHLÜSSELUNG IST UNSICHER UND CYBERSICHERHEIT EIN MYTHOS

Posted on 2. November 2023

Russland, China und Nordkorea sind nicht in eine von den USA gestellte Falle getappt, aber andere 120 Nationen schon.

*Ein Meinungsbeitrag von **Felix Abt**.*

Für Crypto AG, das Schweizer Unternehmen, das laut The Economist "nach dem Zweiten Weltkrieg den Weltmarkt für Chiffriermaschinen beherrschte" und jahrzehntelang der führende Hersteller von Chiffriergeräten für die Sprachkommunikation und digitale Datennetze war, war Hans Bühler der Spitzenverkäufer, der rund 40 % des Umsatzes erwirtschaftete.

Eine lebensbedrohliche Wendung in der Karriere eines sehr erfolgreichen Geschäftsmannes: Wer und was steckt dahinter?

Er belieferte zahlreiche Staaten, insbesondere im Nahen Osten, darunter auch den Iran, mit Chiffriergeräten. Bei seinem 25. Besuch in Teheran wurde er am 18. März 1992 festgenommen und inhaftiert. Er verbrachte neun Monate in Einzelhaft im Evin-Gefängnis in Teheran, wo er jeden Tag fünf Stunden lang verhört wurde.

Der Iran warf Bühler vor, seine Verschlüsselungscodes an westliche Geheimdienste weitergegeben zu haben. Bühler wurde im Januar 1993 freigelassen, weil Crypto AG eine Kaution von 1 Million Dollar an den Iran gezahlt hatte, obwohl er nichts von einem Problem mit den Geräten wusste. Bühlers Firma entließ ihn kurz nach seiner Freilassung und verfolgte ihn persönlich, um die 1 Million Dollar Kaution zurückzubekommen.

Einige Jahre später traf ich Hans Bühler, eine große, schlanke Person, die ruhig und selbstbewusst sprach und erklärte:

> *"Bis zu meiner Verhaftung in Teheran glaubte ich an die Integrität meines Unternehmens. Aber die Iraner wussten Dinge, die ich nicht wusste. Offensichtlich fanden sie heraus, dass Geheimnisse, die sie auf den Maschinen von Crypto für sicher hielten, in Länder gingen, die ihnen feindlich gesinnt waren.*

> *Und wahrscheinlich wussten sie schon damals, dass westliche Regierungsstellen das Unternehmen gekapert hatten, um es als Spionageinstrument gegen sie einzusetzen."*

Totale Täuschung: das Geschäftsmodell eines von der CIA kontrollierten Unternehmens

Bühlers Firma setzte ihren Namen und die Sicherheitsbedenken ihrer Kunden auf die Neutralität ihres Heimatlandes, und 120 Länder, darunter auch der Vatikan, hatten die fortschrittlichste und angeblich sichere Verschlüsselungstechnologie von ihr gekauft. Da viele Staaten den in den NATO-Staaten verkauften Verschlüsselungsgeräten verständlicherweise misstrauisch gegenüberstanden, wandten sie sich an die Schweiz, eine neutrale Drittpartei. Einige wenige Länder wie China, Russland und Nordkorea waren weiterhin misstrauisch gegenüber dem Kauf eines trojanischen Pferdes im Westen und zogen es vor, stattdessen ihre eigene Verschlüsselungstechnologie zu entwickeln. Ihr Misstrauen war begründet, denn diese Geräte wurden in der Tat eingesetzt, um ihre leichtgläubigen Nutzer auszuspionieren. So berichteten sowohl die Washington Post als auch das ZDF, dass "der US-Geheimdienst jahrzehntelang aktiv die diplomatische und militärische Kommunikation zahlreicher lateinamerikanischer Staaten mit Hilfe von Verschlüsselungsgeräten überwacht hat, die von einer Schweizer Firma geliefert wurden, die sich im geheimen Besitz der CIA und des deutschen Geheimdienstes befand".

Hans erzählte mir, dass er glaubte, seinen Kunden ein ehrliches Verkaufsargument gegeben zu haben, als er ihnen versicherte, dass ihre Nachrichten auf dem Weg von ihren Hauptstädten zu Botschaften, Militärattachés, Handelsbüros und Spionage-Hotspots auf der ganzen Welt und zurück völlig sicher seien. Er und seine Kunden waren schockiert, als sie erfuhren, dass dies nicht der Fall war!

Aus einer vergangenen Zeit, als die Medien noch kritisch recherchierten und berichteten

Nachdem Hans Bühler aus dem Gefängnis entlassen worden war, setzten Journalisten ihre Nachforschungen über seinen Fall fort und sprachen mit ihm. Es erschienen Berichte in deutschen Magazinen wie dem Spiegel, dem deutschen Radio International, dem Schweizer Fernsehen und allen großen Schweizer Zeitungen. Sie waren auf der Suche nach Informationen darüber, ob und wie westliche

Spionageorganisationen die Hardware von Crypto AG manipuliert hatten. Sie sprachen mit anderen Mitarbeitern von Crypto AG und forschten immer weiter nach. Um der Geschichte ein Ende zu setzen und Hans Bühler und andere Mitarbeiter zum Schweigen zu bringen, reichte Crypto AG daraufhin Klage ein. Es gelang jedoch nicht, die Medien davon abzuhalten, die damaligen Vorgänge zu erfahren. Sie bemühten sich weiterhin um die Aufklärung der Umstände: Sie fanden heraus, dass Agenten der NSA, der amerikanischen Überwachungsorganisation, Crypto AG häufig besuchten. So nahm beispielsweise die NSA-Kryptografin Nora L. Mackebee im August 1975 an einem geheimen Workshop bei Crypto AG teil, um einen neuen Prototyp eines Verschlüsselungsgeräts vorzustellen. Sie wurde auf der Besucherliste als unabhängige "Beraterin" aufgeführt, um ihre wahre Rolle als Teilnehmerin im Auftrag der NSA zu verschleiern.

Darüber hinaus gibt es stichhaltige Beweise für eine verdeckte Absprache zwischen Crypto AG und der NSA ab 1951, die durch zuvor als geheim eingestufte Papiere erbracht wurden, die 2014 von der NSA teilweise enthüllt wurden. Es besteht kein Zweifel, dass die CIA und der BND, der deutsche Nachrichtendienst, der seit langem mit der US-Regierung kollaboriert, 1970 den Kauf von Crypto vereinbarten. Aus Angst vor Enttarnung verkaufte der BND jedoch Anfang der 1990er Jahre seinen Anteil an dem Unternehmen an die USA. Die Washington Post berichtete, dass die CIA das Unternehmen bis 2018 ausnutzte, als sie die Vermögenswerte des Unternehmens an zwei private Firmen verkaufte.

Vergleichen Sie dies nun mit der Art und Weise, wie dieselben Medien kürzlich mit dem schlimmsten Terrorakt in Europa seit dem Zweiten Weltkrieg, dem Bombenanschlag auf die Nord-Stream-Gasleitung, umgegangen sind und es unterlassen haben, ernsthaft zu recherchieren: Sie würden sicherlich genauso schäbig reagieren, wenn Bühler noch am Leben wäre und zum jetzigen Zeitpunkt aus iranischem Gewahrsam zurückgekehrt wäre.

Das weltweit umfangreichste Spionageprogramm aller Zeiten

Die USA haben jahrzehntelang routinemäßig streng geheime verschlüsselte Nachrichten aus 120 verschiedenen Ländern abgefangen und entschlüsselt. Die Codeknacker des BND und der NSA konnten mit dem Schlüssel jede Kommunikation entschlüsseln, die von einem der 120 Länderkunden von Crypto AG

gesendet wurde, sobald die Chiffriermaschinen so modifiziert worden waren, dass sie den geheimen Entschlüsselungsschlüssel enthielten. Die NSA-Analysten konnten den Kommunikationsfluss so einfach analysieren, als würden sie die Morgenzeitung lesen. Darüber hinaus hat die CIA Omnisec, den Hauptkonkurrenten von Crypto AG, ein weiteres Unternehmen mit Sitz in der Schweiz, gründlich infiltriert und manipuliert, um sicherzustellen, dass ihnen wirklich nichts entgeht.

Stasi-Akten aus der ehemaligen DDR, die ihren Weg in den Iran fanden, dürften den Iranern Informationen über das amerikanische Verschlüsselungs-Hacking geliefert haben.

Informationen, die von ahnungslosen Freunden und Feinden gestohlen wurden, werden systematisch gegen sie verwendet

Den Enthüllungen zufolge nutzten die USA Argentiniens Vertrauen in die Verschlüsselungstechnologie von Crypto AG während des Falklandkriegs zu ihrem Vorteil, indem sie abgehörte Gespräche und abgefangene Nachrichten über argentinische Militärpläne an das verbündete Großbritannien weitergaben. Dieser Verstoß gegen die argentinischen diplomatischen Regeln wurde vom ehemaligen britischen Außenminister Ted Rowlands öffentlich eingeräumt.

Die USA waren auch in der Lage, die gesamte Kommunikation des ägyptischen Präsidenten Sadat mit Kairo zu überwachen, als er 1978 in Camp David mit dem israelischen Premierminister Begin und US-Präsident Carter zusammentraf, um einen Friedensvertrag zwischen Ägypten und Israel auszuhandeln.

Die USA hatten auch immer wieder den Kauf bestimmter Ausrüstungsgegenstände als Bedingung für die Gewährung von Vergünstigungen verlangt. So erhielt Pakistan von den USA Militärkredite als Gegenleistung für den Kauf seiner Verschlüsselungstechnologie von Crypto AG.

Die USA und ihre Verbündeten haben 50 Jahre lang von der abgehörten Kommunikation in Bezug auf Handel, Diplomatie, Wirtschaft und Strategie profitiert. Sie waren in der Lage, internationale Verträge und Verhandlungen zu beeinflussen, indem sie die Verhandlungspositionen ausländischer Regierungen - sowohl von "Freunden" als auch von "Feinden" - in Erfahrung brachten. So kannten sie beispielsweise den genauen

Gesundheitszustand des Königs von Saudi-Arabien, die geheimen Finanzgeschäfte des argentinischen Präsidenten, die Verhandlungsposition der südafrikanischen Handelsdelegation in der Welthandelsorganisation, die Haltung des südkoreanischen Präsidenten zur amerikanischen Truppenpräsenz in seinem Land oder die Anti-Abtreibungshaltung des Papstes. Solche Informationen, die dem Präsidenten und dem Außenminister täglich im Rahmen ihrer geheimdienstlichen Unterrichtung zur Verfügung gestellt werden, sind sehr hilfreich und ermöglichen es den USA, mit einem Spiegel im Rücken aller anderen ein diplomatisches Pokerspiel mit hohem Einsatz zu spielen.

Der größte Überwachungsstaat der Welt lenkt von sich selbst ab, indem er mit dem Finger auf China zeigt

Ironischerweise geben die US-Regierung und ihre Partner in den Mainstream-Medien oft vor, über die Überwachung in China empört zu sein, obwohl die USA den umfassendsten und weltweit größten Überwachungsstaat aufgebaut haben, der von China, das angeblich immer noch Spionageballons einsetzt, nicht übertroffen wird. Ein China-Insider stellt sogar die berechtigte Frage:

> *"In der westlichen Panikmache wird das angebliche chinesische Sozialkreditsystem oder Sozialkreditscore hochgespielt, aber gibt es das überhaupt?"*

Die US-Regierung spioniert Menschen auf der ganzen Welt aus, auch Staatsoberhäupter, die sie als "Verbündete" und "Freunde" bezeichnet, sowie ihre eigenen Bürger. Selbst wenn Ihr Mobiltelefon ausgeschaltet ist, kann sie wissen, wann Sie nachts im Bett furzen, egal in welchem Bett und wo.

Lügen, betrügen, stehlen: der Modus Operandi der mächtigsten Regierung der Welt

Im Jahr 2018, dem Jahr des Todes von Hans Bühler, verlor die CIA ihr Interesse an Crypto AG, nachdem bekannt wurde, dass es sich um ein geheimes CIA-Projekt handelte. Sie ist aber zweifellos immer noch daran interessiert, Verschlüsselungstechniken gezielt zu verschlechtern, um sie zum Ausspionieren ihrer Nutzer zu verwenden. Und sie wird zweifellos an den Grundsätzen festhalten, die Mike Pompeo, ein

ehemaliger CIA-Chef, so formulierte: "Wir haben gelogen, wir haben betrogen, wir haben gestohlen!" Zu diesem Zweck besitzt es höchstwahrscheinlich eine Reihe anderer Unternehmen oder hat sich Zugang zu ihnen verschafft.

Wie leicht ist es, Ihre Geräte zu infiltrieren?

Die CIA und die NSA fügen auch Hintertüren ("backdoors") in von ihnen entwickelte oder gekaufte Anwendungen ("Apps") ein, um sicherzustellen, dass nicht nur Regierungen, sondern auch Unternehmen und Privatpersonen gründlich ausspioniert werden können.

Eine Ende-zu-Ende-Verschlüsselung ("end-to-end encryption"), wie sie von Zoom, Signal, Telegram und WhatsApp verwendet wird, kann nicht umgangen werden, es sei denn, eine Partei hat Zugriff auf den Inhalt der Übertragung oder erhält die Schlüssel oder Chiffren. Dies kann nur durch Hacking geschehen. Die Endpunkte (Smartphone, PC oder andere Geräte) sind jedoch das schwächste Glied in der Kette, da sie mit ziemlicher Sicherheit unsicher sind und auf unendlich viele Arten kompromittiert werden können. Nutzer von Software, die vorgibt, Sicherheit für die Ende-zu-Ende-Kommunikation zu bieten, sollten sich dessen bewusst sein. Und selbst wenn die Verschlüsselung verhindert, dass der Inhalt Ihrer Nachrichten gelesen werden kann, sind die Metadaten nicht verborgen oder verschlüsselt, was bedeutet, dass es möglich ist, festzustellen, an wen Sie Nachrichten gesendet haben, und möglicherweise auf den Inhalt zu schließen. Selbst wenn Sie alle Ihre Geräte perfekt schützen und sicher sind, dass niemand Zugang zu den darauf befindlichen Nachrichten hat, können Sie nicht sicher sein, dass das Gerät Ihres Gesprächspartners nicht kompromittiert ist. Es könnte Ihnen auch Schadsoftware senden. Die Ende-zu-Ende-Verschlüsselung ist da keine Hilfe.

Was den bei weitem größten und am stärksten in die Privatsphäre eingreifenden staatlichen Überwachungsakteur betrifft, so hat die NSA ihre Supercomputer eingesetzt, um viel kompliziertere Verschlüsselungsalgorithmen zu knacken und Systeme auf beschlagnahmter Hardware und/oder Kommunikation von ausländischen Geheimdiensten zu entschlüsseln. Mit dieser Fähigkeit gibt es wahrscheinlich nichts, was die NSA nicht hacken könnte, und sie wird es auch tun, wenn sie es will. So kann

sie z. B. problemlos die iPhone-Kommunikation entschlüsseln, ohne die Schlüssel von Apple zu erhalten.

+++

Felix Abt ist Mitbegründer des asiatischen Internetmagazins Eastern Angle.

+++

Wir danken dem Autor für das Recht zur Veröffentlichung dieses Beitrags.

+++

Bildquelle: TippaPatt / Shutterstock.com