BAKER & BAKER
Consulting Group Ltd.

GLOBAL ECONOMY NEWS
November 2023

ABHÖRSICHERE HANDYS, GESCHÜTZTE MESSENGER & CO.

WIR WERDEN GEJAGT

von
Wolfgang Zimmermann

ABHÖRSICHERE HANDYS, GESCHÜTZTE MESSENGER & CO.

WIR WERDEN GEJAGT

Wir glauben an Versprechungen, Geheimnisse technisch sicher bewahren zu können. Granitdichte Software heute ist morgen wie löchriger Käse: kein Geschäftsmann 100-prozentig sicher. Konkurrenten hacken und fischen. Finanzbehörden suchen Beweise. Jeder und alles ist gläsern.

Dr. Hans ist Biochemiker und hat eine neue Formel entwickelt. Bis er sie hat patentieren lassen, darf niemand erfahren, wie sie lautet. In Deutschland kann es bis zu drei Jahre dauern, bis seine Rechte geschützt sind. Weltweit muss er auf die Patentierung fast fünf Jahre lang warten, solange über seine Zahlen und Formelzeichen wachen. Sie werden seiner Firma Milliarden Euro einbringen.

Hoffmann La Roche hat sich aus der Schweiz gemeldet. Braucht Informationen. Dr. Hans wartet ab. Pfizer bietet an, das Patentverfahren in die eigenen Hände zu nehmen. Was die wissen, reicht dem Pharmariesen aus. Das imponiert ihm. Die wissen seine teure Forschungszeit und das Ergebnis zu schätzen. Chinesen und Russen greifen an. Dr. Hans steckt in einem digitalen Weltkrieg.

Das Signal über „Signal“

Die Nachrichten von Hoffmann La Roche und von Pfizer kamen indessen von den Pharmariesen über „Signal“. „Signal“ funktioniert beim Gebrauch fast so gut wie das weitaus populärere „WhatsApp“ mit zwei Milliarden Usern, während „Signal“ im Jahr 2021 etwas mehr als 50 Millionen Nutzer hatte. Bei „Signal“ hat der Betreiber, die US-amerikanische Signal-Stiftung, keinen Zugriff auf die Nachrichten. Sie werden nicht auf den „Signal“-Servern gespeichert.

Nicht nur die CIA, der Auslandsgeheimdienst, habe aber Zugriff auf die Telefonnummern des Handys und wird nicht über den Server von „Signal“, sondern mit einer Spionage-Software die Eingaben direkt über die Tastatur des Handys auslesen können.

Edward Snowden, 40, der als US-amerikanischer Whistleblower nach Russland geflohen ist und seit 2013 mutmaßlich in Moskau lebt, vorher als Systemadministrator für die CIA, die NSA und die DIA, den US-Verteidigungsgeheimdienst, gearbeitet hat, rät trotzdem dazu, „Signal“ für die Kommunikation zu nutzen. Seit dem März 2017 ist „Signal“ für US-Senatoren und deren Mitarbeiter zugelassen, wird bei der Europäischen Kommission von und unter Kommissionspräsidentin Ursula von der Leyen, 65, verwendet.

„WhatsApp“ geknackt?

Über „WhatsApp“ hat das Hamburger Magazin „Stern“ im August 2019 berichtet, Hacker hätten die angeblich sichere Eins-zu-Eins-Verschlüsselung von „WhatsApp“ des US-amerikanischen Meta-Konzerns um Mark Zuckerberg, um den Facebook-Mitbegründer und Multimilliardär, geknackt. Es sei der Programmcode rekonstruiert worden, erklärten die Sicherheitsexperten. Deshalb könnten sie die Chats entschlüsseln.

Danach hat die israelische Softwarefirma 2020 behauptet, die „Signal“-Verschlüsselung überwunden zu haben. „Signal“ wies das zurück. Das Unternehmen „Cellebrite“ löschte die eigene Erfolgsmeldung sofort von deren Webseite. Immerhin lebt „Cellebrite“ davon, seine Hackerprogramme an staatliche Stellen zu verkaufen. Selbst angebliche Erfolge dieser Art kommen bei Auftraggebern gut an. Die glauben zurecht an die Macht der Hacker.

In technischer Hinsicht wurde „WhatsApp“ nicht geknackt, behaupten Experten. Die „WhatsApp“-Nachrichten sind Ende-zu-Ende-verschlüsselt. Das bedeutet, dass sie nur von den Gesprächsteilneh-

mern gelesen werden können. Dritte haben keinen Zugriff darauf, selbst wenn ihnen der Zugang zum WhatsApp-Server gelingen sollte. In praktischer Hinsicht können „WhatsApp-Accounts" gehackt werden. Das geschieht in der Regel durch Phishing-Attacken, bei denen Hacker die Benutzer dazu bringen, ihnen ihren Verifizierungscode zu liefern: „Hier ist WhatsApp. Gebe sofort auf unserer Webseite zu Deiner Sicherheit Deinen Verifizierungscode ein!"

Sobald die Hacker den Verifizierungscode haben, können sie sich in das Konto des Benutzers einloggen und dessen Nachrichten lesen oder Nachrichten in seinem Namen versenden und Antworten lesen. Im Jahr 2022 gab es mehrere Berichte über Phishing-Attacken gegen „WhatsApp"-Accounts. In einem Fall gelang es Hackern, über 100.000 WhatsApp-Konten zu hacken.

Insgesamt scheint „WhatsApp" eine akzeptable Plattform zu sein: für die Familienchats, kurze Nachrichten fürs Treffen am Abend, Liebesbekundungen zum Beispiel oder was es weiter und vor allem an alltäglich Banalem zu berichten gibt – über den Einkauf, die gelungenen Schnitzel in der Pfanne mit Foto oder das schöne Wetter mit dem eigenen Gesicht.

Im Jahr 2020 waren täglich 100 Milliarden Textnachrichten per „WhatsApp" unterwegs, außerdem innerhalb von 24 Stunden 7 Milliarden Fotos. Jeden Tag. Da zeigt sich, dass der Mensch ein soziales Wesen mit einem unglaublich großen Mitteilungsbedürfnis ist und keine Rücksicht darauf nimmt, ob jemand schwerkrank im Bett liegt, im Flugzeug sitzt und nach der Landung in Südamerika mit Katzenfotos überhäuft wird, falls der Empfänger vergessen hat, den Datenempfang rechtzeitig zu deaktivieren, sonst wird es teuer. Der Empfänger zahlt in der Ferne mit. Wer nicht aufpasst, zahlt. Das gilt besonders für die eigene Sicherheit.

Nehme lieber „Signal"

„Signal" gilt als der sicherere Messenger für die Übersendung von Fotos, Textnachrichten und von Dokumenten. Empfohlen wird der Messenger von der deutschen Stiftung Warentest und der internationalen Vereinigung der Bürgerrechtsorganisationen, „European Digital Rights",

Dr. Hans schreibt und sagt nicht einmal mehr, dass es sich bei seiner Formel um den Baustein für ein Krebsmittel zur Behandlung einer verbreiteten Art der Leukämie handelt. Das hat ihm jemand vom Bundeskriminalamt geraten: gar nichts sagen. Der 56-Jährige kam extra mit seinem grauen BMW aus der Wiesbadener Zentrale angefahren. Es war offiziell außerdem ein Hauptmann von der Bundeswehr aus Berlin da, der in Diez bei Limburg und dort bei den Medizinern auf dem Schloss Oranienstein stationiert und für die Sicherheit zuständig gewesen ist, von Montag, 7 Uhr, bis Freitag um 12 Uhr in Berlin mit IT-Koryphäen für die nationale und der NATO-internationale Sicherheit arbeitet und in Diez wohnt.

Henne auf dem Ei

Der Tipp mit dem abhörsicheren Handy kam von Pfizer vom Potsdamer Platz in der deutschen Bundeshauptstadt. Auf die vielen Ratschläge und Ermahnungen des Staates wird sich Dr. Hans verlassen, und auch Pfizer macht einen guten Eindruck. Aber, oh, Du schöner Westerwald, über Deinen Höhen pfeift der Wind so kalt. In Sicherheit ist die Formel nicht. Dr. Hans ist auf sich gestellt. Er fühlt sich wie eine Henne auf dem Ei, das niemand stehlen darf. Der Staat rechnet mit hohen Steuereinnahmen. Deshalb steht Dr. Hans wie ein Verdächtiger unter Beobachtung.

Der IT-Manager von Dr. Hans schreibt jeden Morgen seinen Bericht per „Signal" aus dem Keller des zweistöckigen Hauses in den ersten Stock: gestern haben 23 Hacker versucht, ins System zu kommen, vorgestern gab es 38 Angriffe. Das ist viel. Die konnten alle abgewehrt werden. Den dienstlichen Laptop wird Dr. Hans nicht mehr aus dem Büro mit nach draußen nehmen. Einen Trojaner kann er sich auch im Büro auf den Laptop holen. Dr. Hans fürchtet sich vor Dieben und Erpressern, und wenn ihm der Laptop gestohlen wird, wird jemand Identitätsbetrug begehen und unter seinem Namen Informationen leicht anfordern können. Mit seinen Zugangsdaten geht das sowieso von jedem anderen Computer. Dafür muss sein Laptop nicht gestohlen werden. Das ist was von gestern.

Da hilft es wegen der Cyberangriffe auf die Firma nicht, dass er weiß, dass nicht jeder Hacker ein Feind ist. Es gibt drei Sorten. Eine Sorte ist die Gruppe „White Hats“, eine die „Black Hats“ und die andere Gruppe ist die Gruppe „Grey Hats“. White Hat-Hacker gehören bei Dr. Hans zu denen, die er bezahlt, um sein System auf Schwachstellen hin überprüfen zu lassen. Die Black und Grey Hats wollen Daten von den Servern holen oder Unternehmen zu „Lösegeldzahlungen“ zwingen, weil sie Daten verschlüsselt haben, die wie Geiseln behandelt werden. Grey Hats sind wahlweise die Guten oder Bösen. Die kriminellen Hacker räumen auch Bankdaten ab und plündern Konten. Das wissen Unternehmen und viele Privatleute. Mittlerweile gibt es Versicherungen wie „Hiscox“, die Zahlungen in Aussicht stellen, um nachgewiesene Schäden nach erfolgreichen Hackerangriffen auszugleichen.

Dr. Hans rechnet mit Einnahmen in Höhe von mindestens einer Milliarde Euro. Versicherungen werden bei ihren Zahlungen nicht auf Vermutungen bauen. Das weiß er. Warum sollten Russen oder Chinesen zahlen, wenn der Datenklau kaum etwas kostet.

Abhörsicheres Handy

„Jede Software hat eine Schwachstelle!“, warnt der IT-Mensch: „Alles eine Frage der Zeit, bis das Handy nicht mehr abhörsicher ist!“ Es sind zwei Kryptohandys in der Firma von Dr. Hans eingetroffen und eingerichtet worden: Im T2 der Marke T.A.G. Consultation steckt ein von der Firma entwickeltes Betriebssystem, befinden sich abhörsichere Apps, verschlüsselte Datenbänke und chiffrierte Datenübertragungskanäle. Es gibt einen Schutz vor Lauschangriffen und vor denen, die die Bewegungen von Dr. Hans verfolgen wollen. Außerdem ist es einfach zu bedienen. Wirtschaftsbosse, Minister, Präsidenten, nach Dienstgrad hohe Angehörige der Streitkräfte oder der Geheimdienste nutzen das T2 T.A.G. Consultation. Stückpreis: rund 2.600 Euro.

Kommt es zum Versuch, das Handy zu hacken, löscht sich die gesamte Datenbank.

Abhörsichere Apps sind solche, die nicht von „Signal“ oder von „Meta“- „WhatsApp“ entwickelt wurden. Es sind eigenen Apps, die von T.A.G. Consultation für die Kommunikation zwischen den Kryptohandys geschaffen wurden.

Verschlüsselte Datenbänke sind wie zwei Tresore, die miteinander per Durchgang verbunden sind: von außen nicht ohne ein T2 zugänglich wie das US-Golddepot von Fort Knox im Bundesstaat Kentucky. Die Sicherheitsvalidationen wirken jetzt wie die Tausenden von Tonnen Stahl und Granit auf der Ebene des Softwareschutzes. Wie sich der Fortschritt entwickelt, potenzieren sich die Gefahren. Werden Codes des Betriebssystems, der Datenbank oder des Messengers geknackt oder gestohlen, ist das Handy nichts mehr wert. Es wird neue Hersteller und neue Versprechen geben. Codes sind Zahlenfolgen. Je schneller Computer werden, umso besser geht es, alle Varianten durchzuspielen: im Billionen-Bereich der Möglichkeiten.

Chiffrierte Datenübertragungskanäle authentifizieren sich ständig gegenseitig. Die Daten sind vor Veränderungen, dem Abfangen und bösartigen Angriffen geschützt. Scheint ein Zugriff erfolgreich sein zu können, stößt das abhörsichere Handy alles ab, was nicht in fremde Hände geraten soll. Es ist dennoch das beste Gerät für das streng geheime Telefonat oder die abhörsichere Sprachnachricht. Noch.

Ein Problem ist der Mensch. Er redet laut in sein Handy, klagt über die Konkurrenz, den neurotischen Nachbarn oder die infantile Freundin, die ihn, den schweren Arbeiter ohne Geliebte, für einen betrügerischen Schuft in ihrer Beziehung hält, dem sie auf die Schliche kommen werde. Irgendwer in der Nähe muss das Gerät nicht einmal anzapfen, um Bescheid zu wissen.

Zum T2 gab es für Dr. Hans eine eigene SIM-Karte für 180 Länder, also Panama inklusive. Sein abhörsicheres Handy kommuniziert nur mit einem zweiten Modell der gleichen Art derselben Herstellerfirma. Es wurden im rheinland-pfälzischen Westerwald zwei Handys eingekauft und eingerichtet.

Traue keinem ohne Freigabe

Wichtig ist der neue Jurist in der Firma als erster Ansprechpartner aus der Ferne. Der ist mit seinen 27 Jahren noch sehr jung. Kann ihm Dr. Hans nach drei Monaten im Dienst trauen?

Sicherheitsüberprüfungen hat es im Haus von Dr. Hans nie gegeben, weil er meint, dass sich jeder Lebenslauf von solventen Konkurrenten oder staatlichen Mächten spielend gut überall legal oder illegal einspeisen lässt: mit digitalen Spuren zu Schulen, Sportvereinen oder Hilfsorganisationen. Im deutschen Sicherheitssystem geben Befragte auf mehren Seiten Informationen über sich an: sogar Angaben über die Schulden. Es passiert oft, dass die, die überprüft werden, Interviews unterzogen werden, vielleicht Kontobewegungen zuhause auf ihren Rechnern vorzeigen sollen.

Bei der Masse gilt erst einmal der Grundsatz: Wer lügt, macht sich verdächtig. Wer schlüssig niederlegt, wer er ist und wie er wo bisher gelebt hat, könnte nach einer Abfrage beim Verfassungsschutz und der Anforderung des polizeilichen Führungszeugnisses auf den unteren Ebenen eine Freigabe bekommen. Das dauert bis dahin drei oder vier Monate. Das gilt für Mitarbeiter, die als Köche in den Kantinen oder als Gärtnerinnen im Park des Ministeriums, als Transportkräfte dafür sorgen, dass Koffer aus dem Flugzeug zum Förderband kommen. Gibt es keine negativen Einträge, ist viel gewonnen. Auf höheren Ebenen werden kurze und lange Gutachten erstellt, Menschen aus dem Umfeld befragt, Charakterstudien, lange Interviews vorgenommen, bis es eine Einordnung gibt, die bestimmt, ob jemand in sicherheitsrelevanten Bereichen arbeiten darf. Es geht auch ohne moderne digitale Technik.

Niemand kann sagen, dass er für Behörden und Konkurrenten nicht gläsern ist.

Einige private Sicherheitsfirmen arbeiten so gründlich wie der Staat für Unternehmen. Darüber denkt Dr. Hans nach und will den neuen Juristen ohne Verdacht für vertrauenswürdig erklären lassen. Es geht in seiner Firma um alles.

Über die eigenen Füße stolpern

Aber Dr. Peter Tieg, 61, mit dem Dr. Hans promoviert hat und zu dem er nach 40 Jahren immer noch „Sie“ sagt, mit dem er die Firma aufgebaut und die Formel entwickelt hat, wird die Gegenstelle für die Nutzung von Kryptohandy 2 sein. Der muss Informationen zusammentragen und sie durchtelefonieren. In den schneeweißen Laboren mit sehr teuren Geräten, für die er Millionenkredite unter seinem Namen und dem Namen seiner Frau Ingeborg aufgenommen hat, also im Südosten von Koblenz, tief im Westerwald, arbeiten für Dr. Hans´ mittlerweile hochqualifizierte 38 Kollegen zur Gewinnung von Erkenntnissen aus der Biochemie. Dr. Hans, 67, ist der alleinige Chef. Er muss jeden Monat für Umsatz sorgen. Da fließt Geld aus anderen Lizenzvereinbarungen zu ihm und schwimmen als Löhne und sonstige Kosten davon, aber diese Formel für ein Medikament zur Behandlung der Leukämie wird zu einem großen Erfolg werden.

Mit den Biochemikern, der Sekretärin, einem neu angeworbenen jungen Juristen wird er über Dr. Peter Tieg in Verbindung bleiben, weil Dr. Hans nach jahrelanger Arbeit endlich eine Woche lang in diesem Winter Urlaub machen kann: wo es warm ist – in Panama City, 11 Stunden lang von Paris mit Air France 474 und über den Atlantik knappe 9.000 Kilometer weit unterwegs. Es ist der 11. Januar. Panama ist zwischen dem Atlantik und dem Pazifik ein Traum. Den hat sich Dr. Hans nach 17-jähriger Forschung verdient. Seine Frau würde wie immer abwarten. Sagt sie. Er kann es nicht mehr. Er kann nicht mehr.

Sicherheit ohne Technik

Dr. Hans hat sich gemerkt: Das Wichtigste ist die Geheimhaltung. Er soll niemandem von der Formel erzählen, den er nicht kennt. Wenn jemand seine Formel stiehlt und sie früher auf den Markt bringt, könnte Dr. Hans seine Chancen aufs Patent verlieren. Ein Patent ist ein staatliches Schutzrecht, das dem Erfinder für einige Zeit exklusive Rechte einräumt. Wer die Formel nutzen will, muss ihn um seine Erlaubnis fragen und, wenn die Firma das will, viel Geld an sie für die Nutzungsrechte zahlen. Das Patentamt ist eine staatliche Behörde. Viele Sachbearbeiter kennen die Formel von Dr. Hans. Doku-

mentiert unter Aktendeckeln oder in internen Computerdateien. Der Staat haftet nicht für den Verlust. Alles Vertrauenssache?

Das andere Problem ist Dr. Hans selbst. Er telefoniert dann, wenn Menschen in der Nähe sind. Das soll er nicht mehr machen, warnen ihn seine IT-Leute ohne Verständnis für Dr. Hans´ Eigenart, immer etwas zu laut zu sein und in der Breite so zu referieren, damit es auch der Letzte versteht, was er meint. Alle also dumm, nur er nicht. Keine Telefongespräche mit dem abhörsicheren Handy im Hotelzimmer! Da könnten Wanzen sein. Er hat gebucht. Seine Daten liegen bei Air France und im Hotel Rio Plaza Panama. Wohin er mit wem fliegt und dass das Hotel im Geschäftsviertel Bellavista liegt, wissen die Angreifer längst. Daten sind wie Blumen auf einer Wiese. Die lassen sich leicht pflücken. Ein abhörsicheres Handy hilft nicht, falls sich Dr. Hans nicht einen Ort aussucht, an dem er nicht mit einem Richtmikrofon abgehört werden kann. Panama City ist nicht der Ort, an dem Geheimdienste nicht schon ihre großen Erfolge erzielt und gefeiert haben. Ausgerechnet Panama …

Fernhalten

Wie wäre es mit einer privaten Katamaran-Fahrt ohne Anmeldung auf dem Atlantik, so weit draußen, sodass noch eine gute Verbindung zum Festland besteht, die Gischt schäumt und der Skipper mit anderen Dingen beschäftigt ist als ausgerechnet diesem Deutschen aus dem Westerwald? Es ist tatsächlich wie im Krimi.

Dr. Tieg schlägt seinem Chef Dr. Hans vor, ohne Handy und ohne Laptop in den Urlaub zu fahren. Er habe alles im Griff, versichert er Dr. Hans. Frau Hans findet die Idee gut. „Aber doch nicht jetzt!“, wendet Dr. Hans ein, und er hat recht. Er muss wissen, wie es um den Patentantrag steht und hat um ein Angebot von Pfizer gebeten. Dr. Hans nimmt seinen Urlaub, und es wird nichts passieren, was seiner Firma schadet. Das hat er erwartet. Er hat nur Glück gehabt. Passiert auch, aber selten.

Hinweis: Sowohl Pfizer wie Hoffmann La Roche wie auch die Firma mit ihren Angestellten dienen der fiktionalen Beschreibung, um Probleme bei der sicheren Kommunikation besser lesbar zu verdeutlichen.

Sie brauchen Hilfe?

Wir beraten unsere Klienten umfassend und kompetent, um Transaktionen so diskret wie absolut möglich einzuleiten, zu verhandeln und erfolgreich abzuwickeln.

Global, überall vernetzt, vorausschauend.
Das ist unser Geschäft seit Jahrzehnten – legal, nicht gefährlich.

Wir wissen, wie´s zu tun ist.

Ihr Wolfgang Zimmermann

November 2023

BAKER & BAKER
Consulting Group Ltd.
Repräsentanz Germany I Hohenstaufenring 62 I D-50674 Köln
phone: +49-221-400 6836
phone: +49-221-400 6837 (Assistant Wolfgang Zimmermann)
info@baker-consultancy.com (Headquarters)