Der Fluchthelfer

Der Sicherheitsspezialist Frank Ahearn hilft **Menschen abzutauchen.** Die Digitalisierung hat sein Geschäft nicht einfacher gemacht.

INTERVIEW: ULRICH HOTTELET

Foto: Tom Monaster/ NY Daily News/ Getty Images

TR: Herr Ahearn, was ist der häufigste Fehler, den Menschen machen, wenn sie untertauchen wollen?
FRANK AHEARN: Die Leute suchen von zu Hause aus oder im Büro per Computer nach Infos über ihren künftigen Wohnort. Damit hinterlassen sie digitale Spuren wie Suchbegriffe und aufgerufene Websites auf dem Gerät. Man sollte dafür keinen eigenen Computer verwenden, sondern zum Beispiel in ein Internet-Café gehen.

Welches Motiv haben Ihre Kunden? Sind auch „normale" Menschen darunter?
(lacht) Es gibt keinen normalen Kunden. Es läuft immer auf Gewalt, Geld oder Informationen als Grund hinaus. Entweder will man Ex-Ehepartnern und Stalkern entgehen, oder man will seinen Reichtum und seine Kinder schützen, oder man weiß zu viel über seine kriminellen Geschäftspartner.

Auf Ihrer Website www.frankahearn.com empfehlen Sie, die Finger von gefälschten Identitätspapieren zu lassen, aber eine gefälschte digitale Identität zu erzeugen. Warum machen Sie da einen Unterschied?
Einen falschen Führerschein oder Pass anzufertigen ist illegal. Und woher wollen Sie wissen, dass die gekaufte Identität nicht von einer anderen Person stammt? Damit handelt man sich nur Probleme ein. Bei der digitalen Identität verhält es sich so: Die Leute suchen nach jemandem zuerst online. Am wichtigsten

beim Untertauchen ist daher Desinformation. Ich baue Webseiten mit einem Frank in London, einem in New York, einem in Cincinnati usw., bis ich zehn Franks habe. Das macht es teurer und schwieriger, nach mir zu suchen. Ich manipuliere zudem die Ergebnisse von Suchmaschinen, Blogs und sozialen Netzwerken. Man muss ein virtuelles Wesen schaffen, das mit keinen aktuellen Informationen über Sie wie Konten und Telefondaten verknüpft ist. Sie werden unter einem anderen Namen geführt.

Macht es das Internet schwerer unterzutauchen?
Geotagging hat mein Geschäft schwieriger gemacht. Techies finden heraus, wo ein Foto aufgenommen wurde. Daher muss man das Bild tatsächlich an dem Ort machen, zu dem man eine falsche Fährte legen will. Die Nutzer sind technisch versierter geworden. Sie stellen zum Beispiel in Wordpress fest, wo der Blogpost geschrieben wurde. Sobald Sie „Enter" drücken, kreieren Sie einen digitalen Fußabdruck, egal welche Anonymisierungs-Software Sie nutzen. Die Leute vergessen zudem, dass man digitale Fußabdrücke hinterlässt, wenn man beispielsweise ein Prepaid-Handy kauft.

Wie fliegt man denn beim Kauf von Prepaid-Handys auf?
In den Geschäften gibt es Überwachungskameras. Damit kann man Sie erkennen und den Zeitpunkt des Kaufs feststellen. Das kann die Polizei, das können aber auch andere, zum Beispiel Privatdetektive. Man vermeidet dieses Risiko, indem man einem Obdachlosen ein paar Dollars gibt und ihn das Handy für Sie kaufen lässt. Man darf keine Verknüpfung erzeugen. Viele konzentrieren sich darauf, online keine Spuren zu hinterlassen. Man muss das aber auch offline beachten.

Kann Ihre Kundschaft nach dem Abtauchen überhaupt noch mit irgendwem kommunizieren?
Vor allem muss sie aufpassen, wie sie es tut. Wir verabreden zum Beispiel im Vorfeld, dass ich nach dem Untertauchen eine neue Telefonnummer des Kunden dadurch erfahre, dass er beim Online-Kleinanzeigendienst Craigslist eine Verkaufsanzeige für ein gelbes Vogelhäuschen schaltet. Danach kann ich dann gezielt suchen. Oder man tauscht Botschaften per eBay, in Online-Gästebüchern und -Foren aus.

Es fällt auf, dass Sie Verschlüsselung in Ihren Büchern nicht erwähnen. Kann man sich auch technisch nicht schützen?
Ich bin kein Technikkenner. Ich weiß nicht, ob es funktioniert. Selbst wenn, haben wir keine Garantie, dass eine verschlüsselte Mail wegen des technischen Fortschritts nicht in Zukunft entschlüsselt werden kann. Mein Rat: Wenn eine Information in Ihrer Mail kritisch ist und Sie sich darum Sorgen machen, sollten Sie lieber andere Kommunikationskanäle als eine Mail nutzen.

Sie schreiben, dass die Kundendatensätze von Banken, Fluglinien und Telefongesellschaften in falsche Hände geraten können. Wie erlangen die „Verfolger" dazu Zugang?
Sie erfinden einen Vorwand. Sie geben sich zum Beispiel am Telefon gegenüber der Bank als Konteninhaber aus, der vor einer Reise noch schnell einige Informationen braucht. Hilfreich sind auch Telefonnummern von Ex-Kollegen oder Verwandten. Es wird gelogen und Social Engineering angewendet. Die jeweilige Taktik hängt vom Gesprächspartner ab.

FRANK AHEARN

Er spürte für die Boulevardpresse Monica Lewinsky auf und arbeitete als Fahnder in Tausenden von Fällen für Gläubiger, Unternehmen, FBI und US-Regierung. Seit 2001 hilft Frank Ahearn Menschen, von der Bildfläche zu verschwinden. Dazu verwischt er ihre Spuren in der realen und in der virtuellen Welt, indem er falsche Fährten legt. Sein Wissen gibt er auch in Ratgeberbüchern preis, zuletzt in „How to Disappear From Big Brother".

Wurde jemals einer Ihrer Kunden aufgespürt?
Nicht dass ich wüsste. Einige teilten mir mit, dass sie der Meinung waren, ihnen sei jemand dicht auf den Fersen. Ich weiß nicht, ob das tatsächlich so war. Bisher gibt es keine Leichen.

Auf Ihrer Website geben Sie viele konkrete Tipps. Verraten Sie sie damit nicht auch der Gegenseite?
Detektive und Fahnder kennen diese Tricks schon. Da verrate ich keine Geschäftsgeheimnisse.

Gleichzeitig geben Sie Kriminellen wertvolle Hinweise, um abzutauchen. Haben Sie damit kein Problem?
Kriminelle brechen das Recht sowieso. Ich akzeptiere sie nicht als Kunden in meinem Beratungsgeschäft, aber jeder kann meine Bücher lesen.

Wie vielen Menschen haben Sie beim Abtauchen geholfen?
Ich führe da kein Buch mehr. Oft geht es nur darum, Informationen zu manipulieren. Das nimmt zu, weil es auch den Durchschnittsbürger betrifft. Seit den Enthüllungen von Edward Snowden sind die Leute paranoider geworden. Sie haben verstanden, dass viele Informationen über sie kursieren. Sie sorgen sich wegen Big Brother und wollen daher diese Infos zerstören. Die Kunden sind außerdem professioneller geworden und sehen ein, dass es keine gute Idee ist, Fotos ihrer Kinder auf Twitter zu posten.

Was kosten Ihre Dienste eigentlich?
Desinformation kostet mindestens 5000 bis 10 000 Dollar, Untertauchen beginnt bei 30 000 bis 40 000 Dollar, weil der Arbeitsaufwand hoch ist. Ich komme momentan jedoch an den Punkt, wo ich mit diesem Geschäft aufhören will. Ich habe immer weniger Lust, mich mit den Problemen von Leuten zu beschäftigen, und ich habe genug von extremen, fast surrealen Typen. Vielleicht schreibe ich mehr Bücher. Ich weiß es nicht.