Claudia Pfister weiß so gut wie nichts über die Täter – hat aber das Gefühl, die Täter wissen alles über sie.

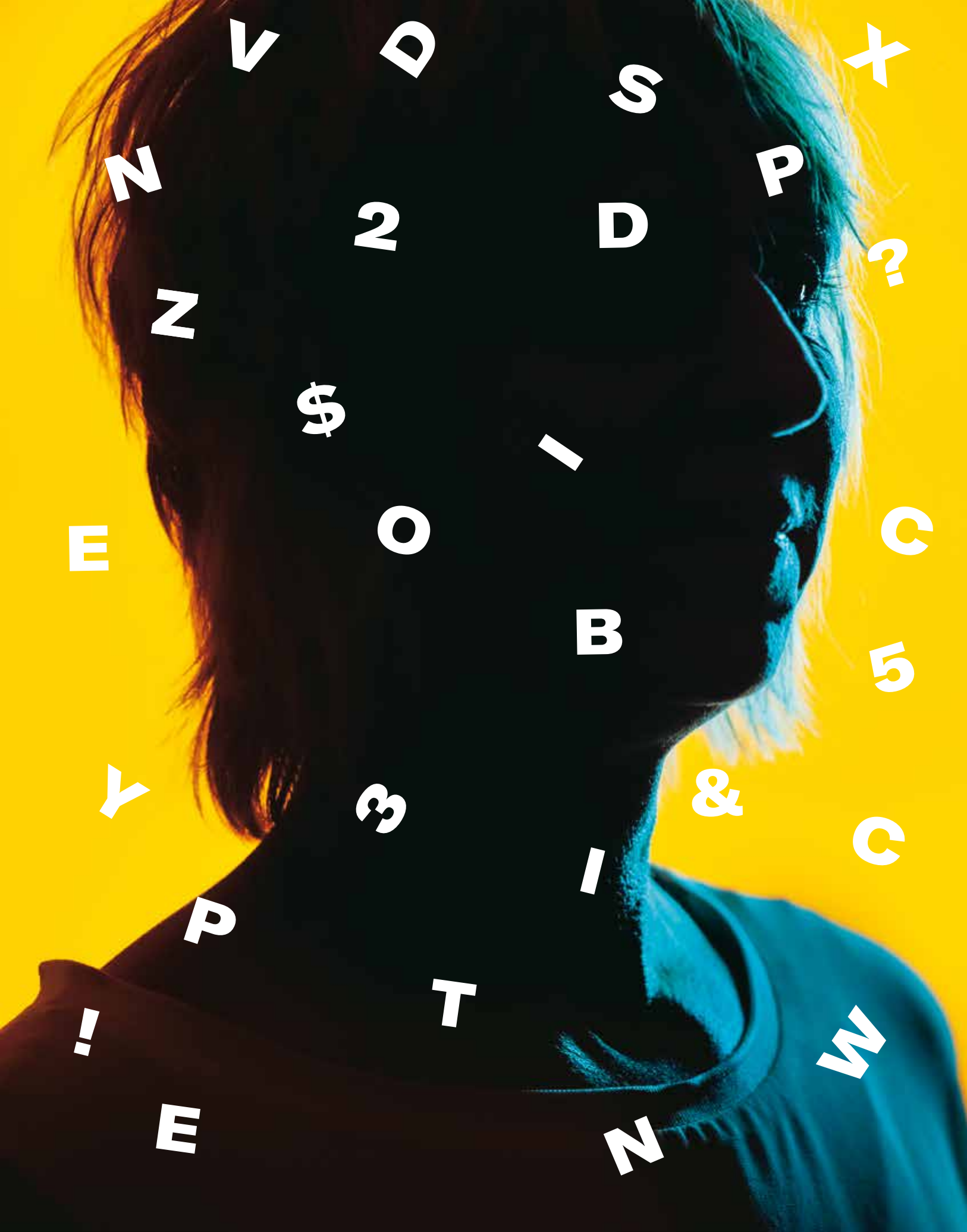
DIE BIN ICH NICHT!

»Sie wissen, wo ich wohne.
Sie lesen meine Mails.
Sie kennen meine Kontodaten.
Und sie machen in meinem Namen
kriminelle Geschäfte.«

Betrüger haben Claudia Pfister
ihre Identität im Internet gestohlen.
Hier erzählt sie ihre Geschichte

Fotos
JULIAN BAUMANN

Protokoll
THILO KOMMA-PÖLLATH


V
D
S
X
N
2
D
P
?
Z
$
I
O
C
E
B
5
Y
3
&
C
P
I
!
T
W
E
N

Ich google mich nicht mehr. Aus Furcht vor der, die mir da begegnet. Die Frau, die im Internet so heißt wie ich, die an derselben Adresse wohnt, die an meinem Tag Geburtstag hat, diese Frau bin ich nicht. Polizei und Staatsanwaltschaft in München können das inzwischen bestätigen, auch wenn sie lange gebraucht haben, um zu verstehen, was mir passiert ist. Ich heiße Claudia Pfister, ich bin 50 Jahre alt, arbeite als Unternehmenscoach in München, und man hat mir meine Identität gestohlen. Gut möglich, dass ich sie mir nie wieder ganz zurückholen kann.

Am 28. November 2019 bekam ich eine routinemäßige Nachricht meiner Kreditkartengesellschaft über die Abbuchung von 500 Euro. Die Zahlung ging an Google Ads. Ich wunderte mich, denn ich hatte keine solche Zahlung für Google-Werbung in Auftrag gegeben. Ich prüfte online die Umsätze auf meiner Kreditkarte. In der Übersicht sah ich, dass es in den zwei Wochen zuvor drei weitere Abbuchungen von Google Ads gegeben hatte, insgesamt 1600 Euro. Zu Beginn meiner Selbstständigkeit 2010 hatte ich einmal tatsächlich Anzeigen bei Google gebucht, um mein Seminarangebot in München bekannt zu machen. Seitdem nicht mehr. Wer also, wenn nicht ich, hatte die Anzeigen auf Google gebucht?

Da man Google nicht anrufen kann, schrieb ich eine E-Mail. Rund 24 Stunden später hatte ich Jasmin am Telefon, eine sehr freundliche Stimme mit osteuropäischem Einschlag, sie rief aus Irland an, dem Steuersitz von Google. Als ich mein Google-Konto verifizieren sollte, erklärte mir Jasmin, dass ich vor nicht langer Zeit ein weiteres Google-Konto eröffnet hätte, auf dem meine aktuell gültige Kreditkarte hinterlegt sei. Ich sagte Jasmin, dass ich von diesem Account nichts wisse, es müsse sich um ein Missverständnis handeln. Ich bat sie darum, die Google-Konten mit meinem Namen zu sperren, und sagte, dass ich mir das Geld von meiner Kreditkartengesellschaft zurückbuchen lassen würde. Jasmin wirkte betroffen, sie sagte, sie habe so einen Fall noch nie gehabt und werde sich schnell wieder melden.

An meinen Kreditkartenabrechnungen fielen mir weitere Ungereimtheiten auf. Da waren sieben Abbuchungen zwischen zehn und dreißig Euro, Kleinstbeträge, die ich vorher übersehen hatte. Begünstigter war die Firma Namecheap.com, die ich nicht kannte und die, wie ich später erfuhr, eine Registrierungsseite ist, auf der man im Internet Domains kaufen kann. Zusammengenommen 120 Euro. Auch eine Abbuchung von 115,83 Euro für eine Firma namens ServerMask sagte mir nichts. Heute weiß ich: ServerMask ist ein Dienst, mit dem sich Standorte von Servern verschleiern lassen.

Noch immer war mir nicht klar, in was ich da hineingeraten war. Fünf Tage später, am 3. Dezember 2019, bekam ich einen Anruf der Polizeistation Bad Bodenteich in Uelzen, Niedersachsen. Der Polizist teilte mir mit, dass er gegen einen Fakeshop namens Coffeelo.net ermittle, der vorgebe, Kaffeemaschinen zu verkaufen. Es liege eine Anzeige gegen die Betreiberin der Seite vor, eine Frau aus Suhlendorf hatte einen Kaffeevollautomaten bestellt und bezahlt, aber nicht geliefert bekommen. Die Betreiberin von Coffelo.net, sagte der Polizist, sei laut Impressum: Ich! Mein Name, meine Privatanschrift. Wie sich später herausstellte, hatte jemand für diese Seite in meinem Namen jene Anzeigen bei Google gebucht. Ich fiel aus allen Wolken.

»AUFGEREGT VERSUCHTE ICH, DEM POLIZISTEN ZU ERKLÄREN, DASS ICH DIESE WEBSEITE NICHT KENNE«

Aufgeregt versuchte ich, dem Polizisten zu erklären, dass ich damit nichts zu tun habe, die Seite nicht kenne, keine Kaffeemaschinen verkaufe, selbst Opfer und nicht Täter bin. Der Polizist meinte, er habe sich so etwas schon gedacht. Es gebe selten Täter, die einen Fakeshop ins Netz stellen und ihre echte Adresse hinterlegen. Wenn das, was ich sage, stimme, sei ich Opfer von Identitätsklau. Es war das erste Mal, dass ich von dem Begriff hörte, der mich von nun an ständig begleiten sollte. Die Staatsanwaltschaft in Lüneburg werde die Ermittlungen leiten, sagte der Polizist und riet mir, bei der Polizei in München Anzeige gegen Unbekannt zu erstatten.

Das tat ich am nächsten Tag. Aus dem Datenmissbrauch, den ich den Polizisten meldete, machten sie »Computerbetrug«. Als hätte der Computer mich übers Ohr gehauen und nicht Menschen. Die Polizisten waren freundlich, aber ich fühlte mich fehl am Platz. Für eine Schlägerei in der U-Bahn, Hausfriedensbruch oder ein geklautes Handy, dafür mochten die zumeist älteren Polizisten geschult sein, aber Internetkriminalität, Identitätsdiebstahl? Auf die Frage, wer »meine« Kaffeemaschinenseite offline stellen könne, bekam ich keine Antwort.

Am nächsten Tag rief mich der Cybercrime-Spezialist Cem Karakaya zurück. Die Polizisten hatten mir seine Nummer gegeben. Der türkischstämmige Profiler war Polizist bei Interpol, dann baute er neben seiner Polizeiarbeit in München ein privates Beratungsnetz in Sachen Internetkriminalität auf: Blackstone432. Dort arbeiten heute Cyberermittler, Privatdetektive, Anwälte für IT-Recht, Internetforensiker.

Ein Grundproblem sei, sagte mir Karakaya, dass Identitätsklau in Deutschland – anders als in den USA – immer noch kein Straftatbestand sei. Die juristische Logik: Eine Identität ist kein bewegliches Gut, deshalb kann man sie nicht stehlen. Auch deshalb gebe es keine offiziellen Zahlen darüber. Das führt zu kafkaesken Erscheinungen, etwa dazu, dass ein Pass erst dann als gestohlen gilt, wenn er physisch entwendet wurde, und nicht, wenn seine Daten schon missbraucht werden. Das Ergebnis ist ein verdrehter Rechtsgrundsatz: Opfer müssen nachweisen, dass sie Opfer sind und nicht Täter.

Über Karakayas Netzwerk kam ich an den Anwalt Marc Maisch, der mir riet, alle Bankkonten zu ändern, ein sicheres E-Mail-Postfach anzulegen und ein IT-forensisches Gutachten in Auftrag zu geben. Die Mail-

Adresse war schnell ausgetauscht, auch ein Konto und eine Kreditkarte waren umgehend gelöscht. Doch um alle alten Bankverbindungen zu ändern, die teilweise seit Jahren, wenn nicht Jahrzehnten meinen privaten wie geschäftlichen Zahlungsverkehr regelten und die auch noch bei zwei weiteren Kreditkarten hinterlegt waren – das geht nicht von heute auf morgen. Mein Anwalt drängte: Er kenne Fälle von Identitätsmissbrauch, in denen Opfer ihre Kreditwürdigkeit verloren haben und nicht einmal mehr einen Handyvertrag abschließen konnten. Auf die in anderen Ländern ein Haftbefehl wegen Betrugs im großen Stil ausgestellt war, ohne dass sie davon wussten. Die bei der Einreise in die USA vom FBI abgeführt wurden und in Untersuchungshaft landeten. Noch immer war unklar, wie die Täter an meine Daten gekommen waren, was sie noch über mich wussten, wie sie mir möglicherweise noch empfindlicher schaden konnten. Und wie ich beweisen könnte, dass die wahre Claudia Pfister nicht die aus dem Internet ist.

Dies ist die echte Claudia Pfister, 50 Jahre alt, Unternehmenscoach in München – und nicht jene Claudia Pfister, die Waren verkauft, die gar nicht existieren.

Eine Woche vor Weihnachten kam die von mir beauftragte IT-Forensikerin Rebecca Zinke zum Ergebnis, dass mein privater E-Mail-Account gekapert worden war. Das 25 Seiten lange Gutachten belegte, wie im Februar 2018 infolge eines Datenhacks bei der australischen Plattform Canva, die Privatleute wie Unternehmen bei der Gestaltung ihrer Webseiten unterstützt, meine komplette »Entität«, wie sie es nannte – persönliche Daten wie Name, Geburtsdatum, Postanschrift, E-Mail-Adresse, Passwörter, Usernamen –, bei einem digitalen »Container« namens Pastebin veröffentlicht und der Datensatz zum Verkauf angeboten worden war. Pastebin ist bei Whistleblowern wie Hackern gleichermaßen beliebt, weil über Pseudonym große Mengen an Daten hinterlegt werden können, sodass eine Rückverfolgung der Spuren fast unmöglich ist. Zinke sagte, eine Million gehackte E-Mail-Adressen mit Passwörtern brächten im Darknet etwa 800 Euro.

Ich erinnerte mich zunächst nicht daran, aber es stimmte: Zu Beginn meiner Selbstständigkeit hatte ich bei Canva einen Account mit meinen persönlichen Daten angelegt. Das war, wie sich jetzt zeigte, folgenreich. Ich habe meine web.de-Adresse seit zehn Jahren, in meinem Account sind rund 8000 Mails gespeichert, meine gesamte private wie berufliche Korrespondenz. Einmal habe ich meinen Reisepass verschickt, um ein Visum zu beantragen. Wer diesen Mail-Account mitlesen kann, kennt nahezu mein ganzes Leben. Er weiß, was ich verdiene, dass ich zwei Söhne habe, geschieden bin, wo meine Wohnung ist, wie meine Kontodaten lauten, er kennt meine guten Seiten und meine schlechte Laune, meine Leidenschaften, meine Geheimnisse. Mit dem Wissen fühlte ich mich beobachtet. Ich wurde nervöser und fahriger, das fiel auch meiner Familie auf. Die Gewissheit, dass im Leben immer alles gut wird, schwand schleichend. ▸

Rebecca Zinke entdeckte zwei weitere, wie sie sagte, »sehr gut gemachte« Fakeshops wie Technikkiste24.com, der Parfüm verkaufte, und Yourhandy.net, die beide auf meinen Namen angemeldet waren. Diese falschen Onlineshops waren genauso aufgebaut wie der Shop mit den Kaffeemaschinen: Alle drei Seiten besaßen ein SSL-Zertifikat, zu sehen war das an dem Schloss vor der URL. Das SSL-Zertifikat signalisiert, dass der Datentransfer zwischen Server und Browser, insbesondere die Kreditkarten-Transaktionen zwischen Besucher und Shop, verschlüsselt und sicher sind. Das Perfide war: Das stimmte auch. Nur waren in den Zertifikaten keine Informationen über den wahren Webseitenbetreiber hinterlegt. In Deutschland wäre allein das eine Straftat. Tatsächlich war die Seite von einem niederländischen Anbieter in Panama registriert worden, und dort interessiert sich niemand für falsche Zertifikate.

Von allen drei Shops führten durch die freie Verschleierungs-Software Cloudflare anonymisierte Datenspuren zu einem Konto in die niederländische Provinz Südholland, in allen drei Fällen tauchten der Name von Gert B. auf sowie eine niederländische Telefonnummer. Rebecca Zinke sprach von »Finanzagenten«, über die das Geld nach Osteuropa weitergeleitet werde, in meinem Fall in die Slowakei, wo sich mutmaßlich die wahren Täter aufhalten würden. Die Finanzagenten wüssten oft nicht, dass sie Teil eines illegalen Netzes seien. Auf 450-Euro-Basis verbuchten sie Beträge für seriös auftretende Firmen, von deren eigentlichem Geschäft sie nichts wüssten oder nichts wissen wollten. Im Fall von Yourhandy.net belegte Rebecca Zinke, dass rund 200 co-gehostete Seiten mit dem Fakeshop in Verbindung stehen, also verlinkte URLs und IP-Adressen, Unterseiten und Urheberlinks, welche zu Pornoseiten und Instagram-Accounts führen, die genauso heißen wie der falsche Handyshop. Zinke zeigte, dass Nutzer, die diese Seiten besuchen, doppelt geschädigt werden: Die Täter verkaufen an sie Ware, die es nicht gibt, und spielen jedem, der die Seite benutzt, Schadsoftware wie Keylogger-Chips auf den Computer, mithilfe derer die Täter alles mitlesen können, um wiederum die Identitäten dieser Nutzer zu missbrauchen, so wie sie meine missbraucht hatten.

Ich schämte mich dafür, dass sich in meinem Namen so viel Betrug und Gemeinheit ausbreiteten, aber ich konnte es nicht verhindern. Inzwischen weiß ich, dass es vielen so geht wie mir. Laut dem Bundesamt für Sicherheit in der Informationstechnik hat die Zahl falscher Onlineshops während der Corona-Krise sprunghaft zugenommen, etwa um Schutzmasken zu verkaufen, die es nicht gibt. Das Betreiben von Fakeshops ist heute ein wesentliches Betätigungsfeld für Internetkriminelle. Trotzdem: Am 8. Januar 2020 stellte die Staatsanwaltschaft München I mein Verfahren wegen »Computerbetruges« ein, »weil der Täter bisher nicht ermittelt werden konnte«. Weiter hieß es: »Sollte der Täter im Verlauf weiterer Ermittlungen bekannt werden, so erhalten Sie Mitteilung.« Wirklich? Im Verlauf welcher weiteren Ermittlungen sollte es denn je dazu kommen? Ich fühlte mich im Stich gelassen.

»ICH WAR NIE KUNDIN BEI CONGSTAR GEWESEN, WIE KONNTEN SIE EINE EINZUGSERMÄCHTIGUNG BEKOMMEN?«

Unterdessen gingen die Abbuchungen von meinen Konten weiter. Diesmal betraf es ein Girokonto von mir, das ich noch nicht geändert hatte und über das die Telekom-Billigtochter Congstar mittels Einzugsermächtigung zweimal je knapp 100 Euro abbuchen ließ. Ich war nie Kunde bei Congstar gewesen, wie konnten sie eine Einzugsermächtigung bekommen? Als ich das Geld für die Google-Anzeigen vom November von meiner Kreditkarte zurückgebucht haben wollte, leitete mir das Kreditkartenunternehmen verwundert eine E-Mail weiter, in der ich mich auf Englisch darüber beschwert hatte, dass keine Google-Anzeigen ausgeführt worden waren, »obwohl mein Bankkonto gedeckt« gewesen sei. »What's next?«, stand am Ende der Mail von der Adresse pfisterclaudia10@gmail.com, die mir nicht gehörte. Das waren die Täter! Sie schrieben E-Mails in meinem Namen! Mir lief es kalt den Rücken hinunter.

Dauernd wollte jemand etwas von dieser Claudia Pfister. Eine Firma namens Lottohelden wollte bei der Schufa meine Bonität prüfen lassen, ich lehnte ab. 1&1 wollte Mitte November 2019 einen Vertrag mit mir fertigstellen, von dem ich nichts wusste. Kurz vor Weihnachten läutete ein kräftiger Mann bei mir zu Hause an der Tür und wollte eine Kaffeemaschine kaufen, in den Tagen danach klingelte mehrmals mein Festnetztelefon, unbekannte ausländische Stimmen wollten jemanden sprechen, den ich nicht kannte. Als ich über die Weihnachtstage ein paar Tage Auszeit auf dem Bauernhof meiner Eltern nahm, überlegte ich mir, ob der oder die Täter auch in meine Wohnung einsteigen würden. Sie kannten ja meine Adresse, ich fühlte mich so machtlos. Als ich zurückkam, hatte jemand den Aufkleber mit meinem Mädchennamen entfernt, mit dem ich mein Klingelschild überklebt hatte. Die Täter? Der Hausmeister? Ein Nachbar?

Viele Opfer von Wohnungseinbrüchen erleiden eine emotionale Belastungsstörung, Juristen sprechen von »emotional distress«, einem Unsicherheitsgefühl, das sich hartnäckig hält und deshalb schadenersatzpflichtig ist. Aus seiner Wohnung kann man ausziehen, aus seiner Haut nicht. Zum Jahresbeginn verließ ich meine Wohnung zwei Wochen lang nicht mehr und sagte alle Termine ab. Ich fühlte mich, als würde mir jemand den Boden unter den Füßen wegziehen. Da war alles gleichzeitig: Angst, Hilflosigkeit, Ärger.

Drei Wochen lang hatte ich plötzlich Ruhe. Ich begann zu hoffen, dass der Albtraum vorüber sei. Dann kam der 31. Januar. Sparkasse Dingolfing, das Konto hatte ich als Jugendliche eröffnet und nun nicht mehr daran gedacht. Binnen weniger Tage wurden in mehreren Tranchen insgesamt 4800 Euro abgehoben. Wieder für Google-Anzeigen. Zuvor hatte Google Ads 53 Cent auf das Konto gebucht, um zu prüfen, ob das Konto aktiv ist. Was war jetzt los? Die Kaffeemaschi-

nenseite war vom Netz genommen. Verzweifelt versuchte ich, Jasmin oder Vinzent zu erreichen, meine beiden Ansprechpartner bei Google. Wie konnte es sein, dass weiter Anzeigenplätze gebucht wurden, wo mein Google-Ads-Account doch seit Ende November gesperrt war? Für welchen Shop im Netz sollte ich diese Anzeigen diesmal gebucht haben? Da ich mir auch dieses Geld innerhalb von sechs Wochen von meiner Bank zurückholen konnte, würde in diesem Fall Google um das Geld geprellt werden. Wollte Google gegen die Täter vorgehen? Aber Jasmin oder Vinzent waren nicht mehr zu sprechen, stattdessen kam die stets gleichklingende schriftliche Antwort, das »Legal Team« wisse Bescheid. Die Mails wurden nun offenbar von einem Bot generiert, einem Programm, das zwischenmenschliche Kommunikation simulieren kann.

Ich fragte Viktor Mraz, der mit seiner IT-Sicherheitsberatung zum Blackstone-Netzwerk gehört und der vorher als Information Security Engineer bei Google gearbeitet hat, also verantwortlich dafür war, dass Google selbst nicht gehackt wurde: Wie kann das sein, dass Google seinen geschädigten Kunden anscheinend nicht helfen will? Seine Antwort: »Für Identitätsklau interessiert sich bei Google keiner, weil die Verfolgung aufwendig und wenig aussichtsreich ist und man damit kein Geld verdienen kann.« Wie zum Hohn fiel mir zufällig eine Hochglanzbeilage von Google in die Hände. Darin las ich von 300 Mitarbeitern, die sich im »Google Safety Engineering Center« darum kümmern würden, »dass privat eingestufte Daten auch privat bleiben«. Sitz von Googles größtem Zentrum für Sicherheit und Datenschutz weltweit: meine Heimatstadt München. Während ich darum kämpfte, wieder ich selbst sein zu dürfen, saßen die Google-Fachleute keine zehn Minuten von mir entfernt. Zwischen diesem Zentrum und mir kam es nie zu einem Kontakt.

Ende Januar 2020 legte mein Anwalt Marc Maisch Beschwerde gegen die Einstellung des Verfahrens ein. Wie sich herausstellte, hatte der zuständige Polizist das forensische Gutachten von Rebecca Zinke meiner Akte nicht beigefügt, die an die Münchner Staatsanwaltschaft gegangen war. Mein Anwalt schrieb, ich sei »Opfer von organisierter Kriminalität im großen Stil« geworden. »Unzählige Fakeshops im Internet« würden, »höchst professionell gestaltet«, die »Kreditkartendaten und Wohnsitzadresse von Frau Pfister« missbrauchen. Es gebe eine »Täteridentität in Südholland«, und die durch das IT-Gutachten gefundenen Informationen deuteten auf ein »Netzwerk mit mehreren Hundert Websites hin, die sich derzeit im Aufbau befinden«.

»MEIN ANWALT GEHT DAVON AUS, DASS DER MÖGLICHE TATVERDÄCHTIGE NIE KONTAKTIERT WURDE«

Ende Februar verfügte die Generalstaatsanwaltschaft in München die endgültige Einstellung des Verfahrens. Es gebe »keine erfolgversprechenden Ermittlungsansätze«. Mein Anwalt geht davon aus, dass die niederländische Telefonnummer nie gewählt und der mögliche Tatverdächtige Gert B. nie kontaktiert wurde. Die Generalstaatsanwaltschaft schrieb: Der entstandene finanzielle Schaden sei nicht groß genug gewesen, sodass, »wie aus zahlreichen gleichgelagerten Verfahren bekannt«, Rechtshilfeersuchen in die USA »nicht erfolgversprechend« und »auch nicht verhältnismäßig« seien. Die Täter würden Bestellungen nicht unter ihren Echtpersonalien tätigen, und sie würden mit den Kreditkartendaten »virtuelle Waren bezahlen, deren Lieferwege anders als körperliche Waren nicht nachvollzogen werden können«.

Warum im Bescheid der Generalstaatsanwaltschaft von den USA die Rede ist, habe ich nie erfahren. Um Google zu fragen, wer da meine Identität missbraucht? Aber warum nicht gleich gegen die Täter direkt ermitteln, da doch die Spuren der verschleierten IP-Adressen von Panama über die Niederlande in die Slowakei führen? Das deutsche Strafrecht beruft sich auch in Zeiten des Internets auf das »Territorialitätsprinzip«, so hat es mir mein Anwalt erklärt: Es fühlt sich erst mal nur für Taten zuständig, die auf deutschem Staatsgebiet verübt werden. Da ist es natürlich ungünstig, wenn Internetkriminalität zwischen Panama, den Niederlanden und der Slowakei hin- und herspringt.

Eine Woche später klingelte das Telefon. Es war ein Polizist von einem Münchner Kommissariat, mit dem ich bisher nichts zu tun gehabt hatte. Er wolle mir mitteilen, dass bei ihm Anzeigen eingegangen seien von Kunden, die bei mir über Yourhandy.net Smartphones gekauft, diese aber nicht erhalten hätten. Er rechne damit, dass bis zu 100 Anzeigen eingehen würden, mit einem durchschnittlichen Schaden von je 1000 Euro. Er sagte, wenn ich unschuldig sei, solle ich Anzeige gegen Unbekannt erstatten.

Und nun? Die Polizei in Bad Bodenteich und die Polizei in München ermitteln weiter, einmal gegen die Kaffeemaschinenseite, einmal gegen den illegalen Handyshop. Dass sie beide gegen dieselben Täter ermitteln, wissen die Dienststellen nicht, die Ergebnisse des forensischen Gutachtens von Rebecca Zinke kennen sie nicht. Das Gutachten wurde nur in dem bereits eingestellten Verfahren zu den Akten genommen. Mein Anwalt meint, ich müsse damit rechnen, dass die Täter nie gefasst werden.

Die Frage nach meiner eigenen Sicherheit kann mir niemand beantworten. Selbst wenn ich alle Bankverbindungen, E-Mail- und Internet-Accounts geändert habe, reichen mein Name und mein Geburtsdatum, um mit meiner Identität illegale Geschäfte zu tätigen. Ich überlege, den Namen meines zweiten Mannes anzunehmen. Ich will mich endlich wieder googeln können – ganz ohne Furcht.

THILO KOMMA-PÖLLATH

hat nach wochenlanger Recherche des Falls von Claudia Pfister viele Empfehlungen, wie persönliche Daten im Netz sicherer zu machen sind. So kann man bei haveibeenpwned.com selbst prüfen, ob der eigene E-Mail-Account schon einmal von einem Datendiebstahl betroffen war und man besser schnell das Passwort ändern sollte. Man kann sich auch die Netflix-Serie *Don't fuck with Cats* anschauen, die Einblick gibt in die Welt der IT-Recherche. Es ist die Lieblingsserie von Rebecca Zinke.