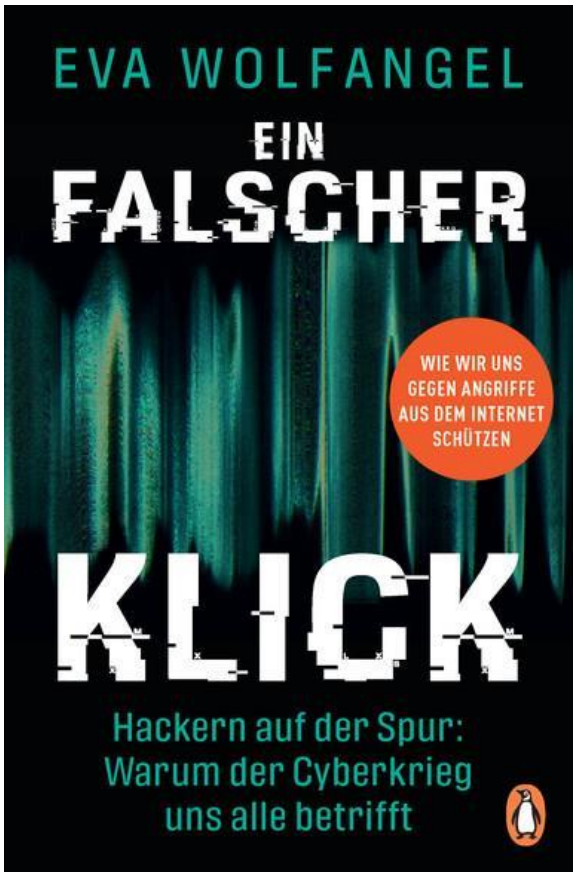

Leseprobe

Eva Wolfangel

Ein falscher Klick

Hackern auf der Spur: Warum der Cyberkrieg uns alle betrifft - Wie wir uns gegen Angriffe aus dem Internet schützen -

Bestellen Sie mit einem Klick für 18,00 €

Seiten: 352

Erscheinungstermin: 09. November 2022

Mehr Informationen zum Buch gibt es auf

www.penguinrandomhouse.de

Inhalte

Zum Buch

Spannende Reportagen aus der Welt der Hacker zeigen, wie wir uns vor Angriffen aus dem Internet schützen können

Gehackte Kraftwerke, ausgefallene Satellitenkommunikation, lahmgelegte Krankenhäuser: Der Cyberkrieg gerät außer Kontrolle. Dieses Buch erklärt packend, verständlich und an vielen konkreten Beispielen, welchen Gefahren der Online-Kriminalität wir aktuell ausgesetzt sind. Eva Wolfangel holt uns zum Ort des Geschehens: Wir sind hautnah dabei, wenn Hacker Unternehmen und Einzelpersonen angreifen, begleiten Ermittler auf der Spurensuche und Betroffene beim Versuch der Schadensbegrenzung. Die Hacks sind spannend wie ein Krimi. Nur: Sie sind nicht fiktiv. Sie sind real passiert und können jeden von uns betreffen – jederzeit. Allerdings sind wir nicht so ohnmächtig, wie wir glauben. Wer die typischen Angriffsmuster von Hackern kennt und versteht, kann viele Gefahren umgehen und erhält so die eigene Handlungsmacht zurück. „Ein falscher Klick" ist ein anschauliches Buch für alle, die bisher dachten, Cybersecurity sei nur etwas für Nerds. Spannend und wie nebenbei macht es fit für das sichere Reisen in digitalen Welten.

Autor

Eva Wolfangel

Eva Wolfangel ist preisgekrönte Wissenschaftsjournalistin, Speakerin und Moderatorin. 2019/20 war sie als Knight Science Journalism Fellow am MIT und in Harvard, wo sie unter anderem bei Barack Obamas ehemaligem Sicherheitsberater Cybersecurity studierte. Sie arbeitet frei u.a. für die ZEIT, GEO und Spiegel

Sollte diese Publikation Links auf Webseiten Dritter enthalten,
so übernehmen wir für deren Inhalte keine Haftung,
da wir uns diese nicht zu eigen machen, sondern lediglich
auf deren Stand zum Zeitpunkt der Erstveröffentlichung verweisen.

Der Verlag hat die russischen Eigennamen in der englischen Umschrift belassen, da – wie bei Eigennamen üblich – die Namensträger:innen diese Umschrift gewohnt sind und sich mit ihr identifizieren. So findet sie sich meist in den hier auch als Quellen genutzten privaten E-Mails der russischen und ukrainischen Personen.

MIX
Papier | Fördert gute Waldnutzung
FSC® C083411
FSC www.fsc.org

Klimaneutral*
Druckprodukt
ClimatePartner.com/14044-1912-1001

Penguin Random House Verlagsgruppe FSC® N001967

1. Auflage 2022

in der Penguin Random House Verlagsgruppe GmbH,
Neumarkter Straße 28, 81673 München
Redaktion: Caroline Draeger
Umschlaggestaltung: total italic/Thierry Wijnberg
Umschlagabbildung: © Shutterstock/rangizzz
Satz: Uhl + Massopust GmbH, Aalen
Druck und Bindung: CPI books GmbH, Leck
Printed in the EU
ISBN 978-3-328-10904-4

www.penguin-verlag.de

Inhalt

Einleitung

Es ist viel zu einfach

Im Herbst 2019 habe ich den IT-Sicherheitsberater des früheren US-Präsidenten Barack Obama gehackt. Damals wurde mir klar, dass die Welt dieses Buch braucht. Denn es war viel zu einfach.

Es war ein Auftragshack – und der Auftrag kam vom Opfer selbst: Eric Rosenbach, dem sogenannten Cyberzar. Unter der offiziellen Rollenbezeichnung Deputy Assistant Secretary of Defense for Cyber verantwortete er von 2011 bis 2014 die Cyberstrategie des US-Verteidigungsministeriums, von 2014 bis 2017 war er Stabschef des Pentagon. Rosenbach begleitete in dieser Zeit alle wesentlichen Entwicklungen, die den Cyberraum betreffen, und mit seinem Team gelang es ihm, allerlei Attacken teils oder vollständig abzuwenden oder zumindest im Nachhinein zu analysieren. Das waren in diesen Jahren gleich eine ganze Reihe – von Chinas Diebstahl geistigen Eigentums großer US-Unternehmen durch Spähangriffe über iranische und nordkoreanische Cyberangriffe auf kritische Infrastrukturen bis zu den immer massiveren Versuchen des russischen Geheimdiensts, sich mithilfe von Hacking-Angriffen und der Verbreitung von Falschnachrichten in die US-Politik einzumischen.

2019 erhalte ich also die Aufgabe Rosenbachs, ihm eine Spear-Phishing-E-Mail zu schreiben. Das sind sehr gezielte, auf eine Person zugeschnittene E-Mails mit dem Ziel, die Angeschriebenen dazu zu bewegen, einen schädlichen Anhang anzuklicken. Tun sie das, breitet sich ein Virus auf ihrem Computer aus, der sie wahlweise ausspioniert und Daten klaut oder alles verschlüsselt – oder gleich beides.

Eric Rosenbach unterrichtet heute Cybersecurity als Direktor des Belfer Centers an der Harvard Kennedy School. Die Phishing-E-Mail ist eine Hausaufgabe in einem Intensivseminar in Harvard, das ich zu dieser Zeit zweimal in der Woche besuche: »Cyber and Info Ops: War, Peace and the Space Between«, so lautet der Name des Seminars, der mich besonders anspricht, weil ich mich genau dafür interessiere: für Krieg, Frieden – und alles, was dazwischen in der Cyberwelt existiert. Ich bin keine reguläre Studierende, sondern habe ein Fellowship für Wissenschaftsjournalismus am MIT. Deshalb muss ich Rosenbach erst überzeugen, dass ich als Stipendiatin an seinem Seminar teilnehmen darf. »Sie müssen aber die gesamte Arbeit machen«, schreibt er mir drohend. Die Arbeit – das ist alles, was er von den ehrgeizigen Midcareer-Fellows, die mit mir an dem Seminar in Harvard teilnehmen, auch erwartet. Für mich klingt das spannend, und ich sage zu – was tatsächlich einen Berg Arbeit nach sich zieht: schier endlos lange Leselisten zur Vorbereitung jedes Termins etwa, deren Inhalt er ohne Vorwarnung vor der ganzen Klasse abfragt. Ein mehrtägiges Bootcamp mit technischen Inhalten. Gleich mehrere Quize und zu verfassende Politik-Strategiepapiere. Spontane »On the spot briefings«, bei denen wir die Rolle der Beteiligten eines Cybervorfalls einnehmen und ein Statement abgeben müssen, und vor allem Simulationen: realistisch nachempfundene Rollenspiele aus dem Verteidigungsministerium, in denen Rosenbach meist den US-Präsidenten spielt, den wir beraten müssen.

Es gibt sonst im Leben wohl kaum eine Gelegenheit, sich so intensiv, dicht gepackt und umfassend damit zu beschäftigen, was im digitalen Raum geschieht, welcher massive Schaden durch Cyberangriffe entsteht, wie gefährlich das Zeitalter der Cyberwars ist – und vor allem: wie angreifbar wir sind. Wir alle. Nicht die USA, sondern die Gesellschaft, die Welt.

Seither habe ich nicht aufhören können, in diesem Themenbereich zu recherchieren, und das Bild wird immer umfassender.

Neue Perspektiven kommen hinzu, bei manchen Themen gibt es unterschiedliche Einschätzungen, aber eines bleibt – meine Gewissheit: Wer sich die großen Cyberangriffe der vergangenen Jahre und die aktuelle Entwicklung anschaut, sieht, dass wir handeln müssen. Und damit meine ich nicht nur die Regierungschefs und Sicherheitsberater.

Wie sehr das jeden Einzelnen von uns betrifft, wird mir klar bei der Aufgabe, die Spear-Phishing-E-Mail an Rosenbach zu schreiben. Ich recherchiere eine Nacht lang über Rosenbach und bin erstaunt, wie viel Privates ich nach dieser Zeit schon über ihn weiß, wie viele potenzielle Angriffsmöglichkeiten sich auftun.

Für die E-Mail bekomme ich ein A, die Bestnote nach dem US-Notensystem. Das bedeutet, erklärt mir Rosenbach, dass er meine E-Mail für vertrauenswürdig gehalten hat: Wäre es eine echte Phishing-Mail gewesen, hätte er sich mit ihr einen Virus eingefangen.

Wenn es so einfach ist, einem problembewussten Menschen wie Rosenbach eine schädliche E-Mail unterzujubeln: Wie können wir uns dann überhaupt schützen? Mir wurde in dem Seminar damals plötzlich bewusst, wie viele Anhänge ich schon geöffnet hatte, weil die zugehörige E-Mail absolut vertrauenswürdig klang. Ob eine E-Mail das wirklich ist, lässt sich nur schwer überprüfen. Es muss sich nur jemand wie ich einen Tag Zeit nehmen und ein bisschen im Internet recherchieren – genau so, wie ich es mit Rosenbach getan habe. Und schon kann man eine persönliche, vertrauenswürdige E-Mail schreiben, die von den meisten Menschen arglos geöffnet würde. Die Absenderadresse zu fälschen, ist eine leichte Übung. Entsprechende Schadsoftware im Internet zu kaufen, braucht auch nur wenig Rechercheleistung. Und fertig ist der Angriff.

Die meisten Phishing-Attacken werden mit noch viel weniger Aufwand durchgeführt. Die meisten sind nicht persönlich, sondern es genügen vielfach verwendete Textbausteine – und trotz-

dem sind sie erfolgreich. Die Masse macht es. Wer genug solcher E-Mails hinaus in die Welt schickt, erwischt immer mal wieder eine leichtgläubige Person. Sobald es um größere Geldsummen geht, lohnt es sich, etwas Aufwand zu investieren und den Angriff maßzuschneidern. Das ist dann eine ziemlich lukrative Investition, wenn man bedenkt, welche Summen Unternehmen bezahlen, um ihre verschlüsselten Daten zurückzubekommen. Es gibt heute tatsächlich nur wenige effizientere Investitionen als die in Schadsoftware. Und der Schaden für uns alle ist immens.

Es braucht nur einen falschen Klick.

Wie geht es wohl dem Mitarbeiter oder der Mitarbeiterin, der oder die durch einen unbedachten Klick Kriminelle ins Unternehmensnetzwerk lässt und damit einen Millionenschaden auslöst? Das frage ich mich ganz aktuell im Februar 2022, als ich aus der Managementetage des Osnabrücker Logistikunternehmens Hellmann drei Etagen weit hinunterschaue auf den großen Vorplatz, auf dem es wie in einem Ameisenhaufen wimmelt. Dort rangieren riesige Lastwagen des Unternehmens, die Tag für Tag unzählige Güter durch die Republik fahren, auf die an ganz verschiedenen Adressen jemand wartet. Nur wenige Wochen zuvor hat hier tatsächlich alles anders ausgesehen. Die hektische Betriebsamkeit wurde jäh unterbrochen, als Hellmann kurz vor Weihnachten 2021 Opfer eines Cyberangriffs wurde. Das Unternehmen mit weltweit knapp 11 000 Beschäftigten und einem Jahresumsatz von 2,5 Milliarden Euro ging von einer Sekunde zur anderen und ohne jede Vorwarnung offline.

In diesem Fall floss kein Lösegeld, weil der Konzern den Angriff frühzeitig bemerkte – das heißt, er wurde entdeckt, bevor die Kriminellen die Daten verschlüsseln konnten. Dennoch war der Schaden enorm, schließlich war das Unternehmen einige Tage kaum handlungsfähig – und das im Weihnachtsgeschäft. Zudem standen einige Wochen später mehrere Gigabyte interne Daten

im Darknet, die für Kriminelle ebenso interessant sind wie für die internationale Konkurrenz.

Durch die Veröffentlichung der Daten wurde ich auf den Hack aufmerksam und konnte Hellmann schließlich überzeugen, mich für eine Reportage für die Wochenzeitung *Die Zeit* zu empfangen. Einfach war das nicht, die meisten Unternehmen haben große Angst, über Angriffe zu sprechen. Die öffentliche Schmach, aber auch Sorge davor, Kriminelle erst recht herauszufordern, lassen sie vor dem Schritt an die Öffentlichkeit zurückschrecken.

Aber wenn Cyberangriffe ein Tabu sind, bleiben wir für immer angreifbar. Auch im Kleinen begegnet mir oft diese Haltung: »Ich will das lieber nicht so genau wissen, ich verstehe das sowieso nicht –, und mich wird es schon nicht treffen.« Leider trifft es immer unvorbereitet, wenn man sich nicht vorbereitet. Genau diese Menschen rufen mich dann an: »Eva, ich habe da so eine E-Mail angeklickt, die klang schon ein bisschen komisch. Was soll ich denn jetzt tun?«

Allein in meinem persönlichen Umfeld hat es innerhalb eines Jahres mehrere Privatpersonen getroffen, die sich über E-Mails schädliche Viren einfingen oder auf Fake-Nachrichten hereinfielen, sowie zwei mittelständische Unternehmen, die fünf- bis sechsstellige Summen an Geld verloren haben.

Bei Hellmann sind die Kosten vermutlich deutlich höher, aber auch dieses Opfer eines Hackerangriffs ist nur eines von vielen: Der deutschen Wirtschaft entsteht laut einer Studie des Digitalverbands Bitkom ein jährlicher Schaden von rund 203 Milliarden Euro durch Cyberattacken. Es trifft die Mehrheit aller Unternehmen, rund 84 Prozent berichteten entsprechende Angriffe.

Ich habe für dieses Buch viele Recherchereisen gemacht – reale Reisen nach Russland, in die Ukraine, nach Großbritannien, in die Niederlande und in die USA ebenso wie virtuelle Zeitreisen: Ich habe mich mit Sicherheitsforscher:innen in die Geschichte des Cyberwars und der Cyberkriminalität vertieft und diese in tage-

langen Gesprächen minutiös rekonstruiert. Es ist eine noch junge Geschichte, aber nicht minder ereignisreich. Ich habe für dieses Buch einige der größten und interessantesten Cybervorfälle der vergangenen Jahre ausgewählt und deren Spuren bis in die Gegenwart intensiv verfolgt. Ich habe Hacker:innen jeder Couleur getroffen, ich habe Opfer besucht und Sicherheitsforscher:innen bei ihrer unermüdlichen Detektivarbeit begleitet.

Das Ergebnis gliedert sich in vier Teile: Im ersten Teil begleite ich kriminelle Hacker, im zweiten Teil geht es um staatliches Hacking und den Beginn des Cyberwars, im dritten Teil zeige ich, wie der Cyberwar mit teils lebensgefährlichen Folgen für Unbeteiligte außer Kontrolle gerät, und im vierten Teil untersuche ich die Fragen, wieso wir so angreifbar sind und was wirklich hilft.

Wie ich werden auch Sie erstaunt und frustriert feststellen, dass die Unterscheidung zwischen kriminellen und staatlichen Angriffen nicht immer eindeutig ist, dass es Mischformen gibt, weil die einen von den anderen profitieren und umgekehrt. Das macht die Sache umso gefährlicher, denn eine Erkenntnis zieht sich durch die gesamte Geschichte der IT-Sicherheit: Auch vermeintlich »gutes«, staatliches Hacking im Kampf gegen Kriminelle schwächt in der Konsequenz die Sicherheit aller.

Was aber können wir tun? Wir müssen Sicherheitslücken schließen – im Großunternehmen wie am heimischen Schreibtisch –, und dazu müssen wir uns damit beschäftigen, wie und welche Lücken unsere Systeme für Angreifer:innen öffnen. Das tun wir in diesem Buch. Wir werden dabei auch organisatorische, ja sogar psychische »Lücken« aufdecken, denn das ist einer der Trends: Kriminelle und staatliche Hacker:innen nutzen unser Vertrauen aus. Sie werden staunen, was eine sogenannte Social-Engineering-Expertin – gewissermaßen eine Fachfrau im Überlisten und Hereinlegen – alles erreicht, ganz ohne Gewalt, ganz ohne Viren.

Mitten in die Schlussredaktion dieses Buches platzt ein Anrufer mit einer schrecklichen Nachricht: Er rufe von Europol an, auch

das FBI höre mit, sagt der Mann an meinem Handy, denn ich werde gesucht als Teil einer internationalen schwerkriminellen Bande. Er werde nun mein Bankkonto sperren, und auch mein Ausweis sei ab sofort nicht mehr gültig. In einem von mir angemieteten Fahrzeug sei vermutlich eine Gewalttat geschehen, es sei völlig verbeult und voller Blut am Stadtrand von Berlin gefunden worden, und über meine Konten werde Geldwäsche betrieben. Glücklicherweise scheint er mir aber zu glauben, dass ich mit alldem nichts zu tun habe, sondern dass offenbar jemand meine Daten erbeutet hat – nur wer? Er wolle mir helfen, sagt er. Zuallererst müsse ich den Behörden beweisen, dass mein Geld legalen Ursprungs sei. »Öffnen Sie Ihren Laptop und googeln Sie TeamViewer«, sagt er.

Sie ahnen schon, worauf es hinausläuft: Der Anrufer war ein krimineller Hacker. Er versuchte, mich zu überreden, ihn mit einem Programm auf meinen Computer einzuladen, damit er dort unter dem Vorwand, mir zu helfen, mein Konto leerräumen kann.

Natürlich tat ich das nicht, denn ich war nicht unvorbereitet. Stattdessen überlegte ich mir viele technische Ausreden, um den Anrufer auszutesten und zu sehen, was er auf Lager hat.

Ich muss gestehen: Ich war am Ende ziemlich beeindruckt, denn er hatte eine enorme Überzeugungskraft und auf alles eine Antwort. Ich wurde mehrmals weiterverbunden zu »Beamten« anderer Hierarchieebenen, die sich stets mit vollem Namen und Dienstnummer vorstellten und das »Good-Cop-Bad-Cop«-Spiel zur Vollendung spielten.

Ich bin nach der Recherche für dieses Buch natürlich kein geeignetes Opfer mehr für die Bande, doch mir wurde klar, dass sie viel investiert hatten und dass sich das vermutlich auszahlt. Und ich weiß aus erster Hand von einem Opfer, wie die Geschichte weitergeht, wenn man nicht vorbereitet ist: Im Zuge der Recherche habe ich eine junge Frau kennengelernt, die eine fünfstellige Summe an die Kriminellen verloren hat.

Wenn Sie sich jetzt fragen, wie das sein kann, lesen Sie bitte das Kapitel über Social Engineering: Es ist so aktuell wie der Anruf mitten in der Schlussphase meines Schreibprozesses. Daher gibt es in allen Bereichen dieses Buchs Hinweise auf aktuelle Entwicklungen: Eine Hackinggruppe des russischen Geheimdiensts, die sich eine ganze Zeit lang bedeckt gehalten oder im Verborgenen agiert hat und die für einige der gefährlichsten Cyberangriffe der Geschichte verantwortlich ist, ist im Zuge des russischen Angriffskriegs auf die Ukraine wieder aktiv und hat mit einer – glücklicherweise missglückten – Attacke auf ein Elektrizitätswerk gezeigt, dass sie nach wie vor eine große Gefahr darstellt – auch und gerade für westliche Infrastrukturen. Auch im Bereich der Entwicklung staatlicher Spionagesoftware und deren Missbrauchspotenzial überschlagen sich die Ereignisse: Unter anderem zeigen aktuelle Recherchen rund um die Spionagesoftware Pegasus, wie Nichtregierungsorganisationen, Journalist:innen und Oppositionelle in Diktaturen in den Fokus staatlicher Repression geraten. Cyberwaffen aus Europa helfen repressiven Regimes bei der Unterdrückung kritischer Stimmen – im Jahr 2021 war Deutschland Exportweltmeister von Spionagesoftware. Diese ging beinahe ausschließlich an nicht demokratische Regimes.

Auch die Kriminellen, die ich im ersten Teil begleitet habe, werden immer kreativer. Eine wachsende Zahl von Menschen verliert Geld, weil Kriminelle sich auf verschiedenen Wegen Zugang zu ihrem Bankkonto verschaffen. Beinahe täglich liest man von neuen Ransomware-Angriffen auf Unternehmen, die dabei Millionen verlieren. Auch hier gilt: ein falscher Klick genügt.

Als ich kurz vor Erscheinen dieses Buches auf Twitter fragte, was denn Wichtiges ins Vorwort solle, wurde mir geraten, Sie – liebe Leser:innen – im Stil von Walter Moers' *Stadt der Träumenden Bücher* zu warnen. Moers schreibt einleitend, es sei keine Geschichte »für Leute mit dünner Haut und schwachen Nerven – welchen ich auch gleich empfehlen möchte, dieses Buch wieder

zurückzulegen«[1]. In der Tat werden Sie sich möglicherweise auch bei der Lektüre meines Buchs gruseln, aber ich möchte Sie warnen: Es nicht zu lesen, könnte ebenfalls gefährlich sein. Denn Sie würden wertvolles Wissen verpassen, das Sie vor Cyberangriffen schützt. Im Gegensatz zu Walter Moers' Arbeit handelt es sich hier nämlich ausnahmslos um wahre Gegebenheiten. Vor diesen sollten Sie besser nicht die Augen verschließen.

1 Walter Moers, *Die Stadt der Träumenden Bücher: Ein Roman aus Zamonien von Hildegunst von Mythenmetz,* Piper Verlag, München 2007, S. 11.

Teil 1
Die Welt der kriminellen Hacker

**Cyberangriffe auf Bürgerinnen und Bürger
werden immer professioneller.
Für die Verteidigung ist es wichtig,
die Motive der Kriminellen zu kennen
und ihre Denkweise zu verstehen.**

Kapitel 1.1

»Wir waren arm, und Hacking galt als Patriotismus«

Die einen greifen unsere Systeme an, die anderen verteidigen sie – die Skills sind die gleichen. Was gibt den Ausschlag für eine kriminelle Karriere?

Als Sergey Pavlovich am 16. September 2004 mit Anfang 20 verhaftet wird, hat er bereits eine beeindruckende Karriere als Krimineller hinter sich. Oder als Unternehmer im Internet, der immer der Spur gefolgt ist, die Geld bringt. Das hatte ihn von halbseidenen Schummeleien zielstrebig in eine der damals größten kriminellen Hackerbanden geführt. Mehr als eine Million Dollar hat er so als krimineller Hacker bereits mit Anfang 20 erbeutet, auf raffinierte Weise geklaut von Konten europäischer und US-amerikanischer Bürger.

Nachdem ein Großteil der Bande hinter Gittern sitzt, betont der damalige US-Staatsanwalt in einer Pressemitteilung[2], es handele sich um den bislang »größten und komplexesten Fall von Identitätsdiebstahl«. Dem habe man nichts hinzuzufügen, schreibt das FBI auf meine Anfrage im Frühjahr 2022 hin. Was man freilich hinzufügen könnte ist, dass es heute einige solcher Banden gibt, die perfekt organisiert sind und massiven Schaden anrichten. Pavlovich und seine Kumpanen waren durchaus Pioniere – im negativen Sinne. Damals also, schon im Jahr 2004, wurden Weichen gestellt, die heute zu einem großen Problem angewachsen sind.

Deshalb wollen wir Sergey Pavlovich ein paar Schritte in sei-

2 https://www.justice.gov/archive/opa/pr/2008/August/08-ag-689.html

nem Leben begleiten. Ich habe ihn im Herbst 2021 in Moskau besucht, um mehr zu erfahren über seine Welt. Denn Pavlovich ist einer der frühen Vertreter einer Bewegung im Internet, die heute massiv wächst und die der Sicherheitsforschung große Sorgen bereitet: Kriminelle, die jede Lücke im System finden und die alle erdenklichen Schwachstellen ausnutzen, um zu stehlen. Manche tun das mit sehr viel Aufwand, sie sind häufig zu gut, um erwischt zu werden. Andere nehmen sich das, was leicht zu kriegen ist, und betreiben dafür Fleißarbeit: Sie suchen das Netz zum Beispiel systematisch nach geleakten Passwörtern ab, wohl wissend, dass viele Menschen dasselbe Passwort für verschiedene Dienste verwenden. Sie loggen sich in deren Konten ein und stehlen kleinere, manchmal auch größere Summen. Sie sind häufig unvorsichtig, werden immer mal wieder erwischt. »Aber es sind so viele, dass wir keine Chance haben«, sagt der Sicherheitsforscher Benoît Ancel, der diese Bewegung im Netz intensiv beobachtet.

Beide Gruppen – die Raffinierten und die Draufgänger:innen – haben eines gemeinsam: Ihr einziges Ziel ist es, Geld zu erbeuten. Das klingt banal, aber es lohnt, sich einmal mit den Hintergründen und der Szene auseinanderzusetzen. Denn nur wer weiß, mit wem er es zu tun hat, kann sich schützen. Im Laufe dieses Kapitels werden wir daher beobachten, wie Behörden und Sicherheitsforscher:innen manchmal danebenliegen, wenn sie sich nicht mit den Hintergründen der Kriminellen beschäftigen. Und wie wichtig es ist, sich über die Mentalität der Angreifer:innen Gedanken zu machen, um die richtigen Schutzmaßnahmen zu entwickeln.

Zurück zu Sergey Pavlovich. Er wird verhaftet, als es gerade am schönsten ist. Am Vorabend hatte er Freunde eingeladen und seine Erfolge gefeiert: Gerade einmal 20, besitzt er damals eines der erfolgreichsten Foren rund um das Hacking von Bankkunden im Internet. Als er am 16. September 2004 nach der Party in der Datscha seiner Schwiegereltern in Lipen aufwacht, einem

Dorf, 100 Kilometer von seinem damaligen Wohnort Minsk entfernt, laufen seine besten Hacker-Kumpels vor ihm nervös durchs Wohnzimmer. Da ist Dmitry Burak, der eigentlich ein Cousin ist, »aber für mich war er ein Bruder und mein bester Freund«. Da sind Kleinkriminelle mit Decknamen wie Fidel, Postal, Kaizer, und schließlich ist da noch Pavlovichs Freundin Katya.

Er habe noch nicht klar denken können nach dem vielen Wodka am Vorabend, erinnert sich Pavlovich, deshalb habe er gehofft, die Polizeibeamten seien nur deshalb gekommen, weil er am Vortag zu schnell gefahren sei. Vielleicht war es ja alles nur ein Missverständnis. Vielleicht suchten sie jemand anders. Schließlich war er hier nicht Zuhause. Doch wenige Minuten später hört er schon das Klacken der Handschellen, spürt das kalte Metall an seinen Handgelenken und findet sich schließlich auf dem Rücksitz eines Polizeiautos wieder.

Zehn Jahre sitzt er in weißrussischen Gefängnissen als Teil des »Hacking-Rings« um den berüchtigten US-Hacker Alberto Gonzalez.[3] Gemeinsam hatte die Gruppe die Daten von mehr als 40 Millionen Kreditkarten gestohlen. Pavlovichs Anteil daran heißt Dumpsmarket. Er hat das gleichnamige Forum im Internet selbst aufgebaut. Der Begriff »Dumps« steht für gehackte Kreditkartendaten, die anschließend im Internet verkauft werden. Bei Pavlovichs Verhaftung ein Jahr nach der Gründung 2003 blüht Dumpsmarket bereits. Das liegt auch an dessen gutem Ruf in der sogenannten Carding-Szene, jener Szene von Kriminellen, die Bankkunden ausnehmen, indem sie Zugangsdaten oder Kreditkartendaten erbeuten.

Seinen echten Namen nutzt er damals selten. Im Netz nennt er sich PoliceDog, manchmal auch panther757 oder FallenAngel. Seine Kunden wissen, dass auf sein Wort Verlass ist, seine Ware hat eine gute Qualität: gefälschte Kreditkarten auf der Basis gehack-

3 https://www.justice.gov/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail

ter Datensätze unter anderem aus Online-Shops. Die User seines Forums schätzen die guten Tipps, die er zu Fragen liefert wie: Wo bekomme ich gestohlene Kreditkartendaten? Wo die Rohlinge – jene weißen Plastikkarten, um Kreditkarten zu fälschen? Und wer macht das beste Design und möglichst echt aussehende gefälschte Bankkarten? Welche Anbieter für Geldwäsche gibt es?

Pavlovich selbst bietet damals immer mehr dieser Dienstleistungen selbst an. Er ist ein Geschäftsmann, seit seiner Jugend hat er ein Talent, Geld zu machen aus quasi nichts. »Wir waren arm«, sagt er. Die Mutter Apothekerin, der Vater ein Alkoholiker, der die Familie verlässt, als Sergey drei Monate alt ist. Er wächst auf in der Zeit des Turbokapitalismus nach dem Zusammenbruch der Sowjetunion. Einen moralischen Kompass zu entwickeln ist nicht einfach als Jugendlicher in dieser Zeit und in seiner Situation. Er beobachtet, wie Menschen um ihn herum plötzlich reich werden, während andere hingegen kaum über die Runden kommen. Sergey beschließt, dass er aus der zweiten Gruppe in die erste wechseln will. Er wird kreativ, wenn es darum geht, Geld zu verdienen.

Bereits als Jugendlicher kauft er Kleidung und Elektrogeräte im Internet und verkauft sie teurer weiter. Dann handelt er mit Dingen, die es gar nicht gibt oder die nicht das sind, was er von ihnen behauptet. Alte deutsche Nähmaschinen, von denen er vorgibt, sie seien aus »Nazigold« zum Beispiel. Aber spielt das eine Rolle, was etwas wirklich ist, wenn die Menschen zu gerne etwas ganz anderes glauben, fragt er heute. »Ich weiß, das ist nicht so richtig okay, aber es war auch nicht wirklich kriminell.« Mit diesem »nicht ganz okay, aber vielleicht auch nicht wirklich kriminell« wurstelt er sich durch seine Jugend – bis es eines Tages schief geht. Denn natürlich gibt es keine Abkürzung in die Welt der Neureichen, die sich alles leisten können. Doch zunächst sieht es so aus.

Mit 18 entdeckt er, wie einfach es ist, an Kreditkartendaten zu kommen. Zuerst kauft er sie in verschiedenen Foren im Netz von

Kriminellen, die sie von schlecht gesicherten Webseiten verschiedener Online-Shops geklaut haben. Schnell merkt er, wer in der Szene vertrauenswürdig ist, wo es die »guten« Karten gibt – also die, die noch funktionieren, weil die legitimen Besitzer:innen keine Ahnung haben, dass ihre Daten durch irgendein Leck eines Online-Shops verloren gegangen sind. Als das Geschäft immer besser läuft, organisiert Pavlovich Unterhändler:innen: Menschen, die mit den gefälschten Karten für ihn einkaufen oder die Bestellungen entgegennehmen und ihm weitergeben. Und sogenannte Money Mules – Menschen, die auf ihren Privatnamen ein Konto eröffnen, über das gestohlenes Geld weiterüberwiesen wird.

Wenn Pavlovich von dieser Zeit spricht, sprudelt es nur so aus ihm heraus. Er hat schier unendliche Mengen an Wissen zusammengetragen und gewinnbringend genutzt. Er berichtet so detailliert über diese Zeit, dass er ein Fachbuch für angehende Bank-Hacker:innen füllen könnte. Ein dickes Fachbuch. Er recherchiert damals genauestens, wie Bankkarten funktionieren, und beschafft sich Geräte, mit denen er die Informationen auslesen kann, die auf dem Magnetstreifen codiert sind – »dumps«, so nennt er diese Informationen. »Ein Magnetstreifen hat drei Tracks, die ersten beiden sind dafür da, um Transaktionen zu prozessieren, der dritte enthält technische Informationen, aber der zweite Track ist am wichtigsten: Nach der Kartennummer kommt der Name, das Ablaufdatum. Und die Zahlenfolge danach sagt etwas darüber aus, ob die Karte international funktioniert, dann sollte sie 101 lauten«, zählt Pavlovich mir atemlos auf. »201 heißt, sie gilt nur in dem Land, aus dem sie kommt. Wenn du Track 2 hast, reicht das aus, um Geld aus einem Automaten zu ziehen.«

Er kauft schließlich nur noch die Informationen von Hackern, deren Vertrauenswürdigkeit er geprüft hat. Manche trifft er persönlich, er reist viel in dieser Zeit, und die Menschen, mit denen er sich umgibt, sind irgendwie alles seine Freunde. »Es war wie eine Familie.« Er findet eine Quelle für Kreditkartenrohlinge in China, die besonders günstig ist. Und er kauft sich eine Maschine,

mittels derer er die Magnetstreifen codieren kann. Allmählich bekommt er Übung darin, die Rohlinge mittels Photoshop in einem täuschend echt aussehenden Design zu bedrucken. Nun sind die gefälschten Kreditkarten fertig für den Verkauf.

Es hätte ewig so weitergehen können, wäre nicht einer seiner Kumpane erwischt worden und hätte ihn verraten, sodass Pavlovich im weißrussischen Knast landet. Die Zeit von damals wirft noch immer einen Schatten in die Gegenwart: Das FBI sucht Pavlovich bis heute, weil die US-Behörde seine Haftstrafe in Weißrussland nicht anerkennt. Auch sein Cousin Dmitry Burak steht nach wie vor auf der Fahndungsliste. Pavlovich kann deshalb Russland und Weißrussland nicht verlassen: Sobald er eine andere Grenze überquert, würde ein Alarm ausgelöst.

Zweifelhafte Fanbase

Als ich Sergey Pavlovich im Oktober 2021 in Moskau besuche, wird klar, dass sich in seinem Leben einiges geändert hat. Heute betreibt er einen YouTube-Kanal, auf dem er unter anderem Kriminelle interviewt, und lebt von den Werbeeinnahmen. »Ich bin jetzt einer von den Guten«, sagt er. In der hippen Fabriketage im Norden Moskaus mit ihren großen Fenstern, den Backsteinmauern und Wänden aus Sichtbeton sind die Spuren einer Party vom Vorabend nicht zu übersehen. Luftballons schweben unter der Decke, der Boden ist übersät mit Glitzerplättchen, und auf Pavlovichs Schreibtisch steht eine beeindruckende Sammlung an Wodka- und Weinflaschen neben dem MacBook.

Er hat Freunde und Geschäftspartner eingeladen, um seinen Erfolg zu feiern: Seit drei Jahren besteht Pavlovichs YouTube-Kanal »Ljudi Pro«, was auf Deutsch bedeutet: »Leute Pro«. Das Pro steht für »Profi«, weil er dort Profis aller Art interviewt. Ein guter Teil von ihnen sind kriminelle Hacker, andere machen ihr Geld mit Geschäften im Darknet. Pavlovichs YouTube-Kanal ist auch

deshalb so erfolgreich, weil das Interesse der kriminellen Szene an seinen Shows enorm ist. Schließlich kann man hier von den ganz Großen lernen.

Heute ist er nicht mehr der »FallenAngel« oder »PoliceDog«. Heute ist er Sergey Pavlovich, der YouTuber mit den guten Kontakten in die Hackerszene. Der Besuch in der hippen Fabriketage in Moskau gibt wertvolle Einblicke in die Mentalität einer Szene und deren Mechanismen. Und Pavlovich ist weiterhin ein gewiefter Geschäftsmann. Mit einem feinen Gespür dafür, wofür Menschen bereit sind Geld zu bezahlen – beispielsweise dafür, dass sie in seiner Show auftreten dürfen. »I am a good guy«, wiederholt er gerne immer wieder. Aber auch hier bewegt er sich auf einer Grenze, die nicht immer ganz eindeutig ist. Denn die Werbeeinnahmen sind auch deshalb so hoch, weil die Kriminellen in seiner Show Tipps geben für den Nachwuchs.

Besonders erfolgreich sind die Videos, bei denen die Interviewten Masken tragen. Fast alle sind aktiv im Geschäft, zwielichtige Gestalten. Darunter ist einer, der seinen Telegram-Bot – also ein automatisches Chatprogramm, mit dem Telegram-Nutzer:innen kommunizieren können – »Eye of God« getauft hat: Er verspricht, alle Geheimnisse eines Menschen zu finden und zu verkaufen. Ein anderer verrät zehn Methoden, den PIN-Code eines Bankkunden zu erfahren. Wieder ein anderer verdient sein Geld mit Bitcoin-Transaktionen, und einer berichtet, wie er Pässe fälscht.

Pavlovich interviewt einmal pro Woche Leute wie den Mann in Jeans und blauer Trainingsjacke mit zwei weißen Streifen an den Ärmeln, der ihm im Herbst 2021 gegenübersitzt. Turnschuhe an den Füßen, eine sogenannte Anonymous-Maske auf dem Kopf. Die Maske, die das Erkennungszeichen der gleichnamigen Hackingbewegung ist, legt ihm ein schadenfrohes Grinsen auf das Gesicht. Unter der Maske schauen kurze braune Haare hervor, einige sind schon grau. Der Mann sitzt breitbeinig in dem großen gelben Ohrensessel, in dem Pavlovich seine Gesprächspartner immer interviewt.

Sergey Pavlovich hat den Mann noch nie zuvor gesehen. Er kennt nicht seinen richtigen Namen, und er will auch gar nicht mehr über ihn wissen. Er wird alle Daten dieses Mannes löschen. Den »geheimen Chat« auf Telegram, seine Handynummer, die er für den Notfall hat – alle digitalen Spuren. Sobald der Mann mit der Maske sein Studio verlassen hat, wird bei Pavlovich nichts mehr über ihn zu finden sein – abgesehen von der Videoaufzeichung des Interviews für seinen YouTube-Kanal. Der Mann ist professioneller Geldwäscher. Niemand soll wissen, wer er wirklich ist, denn er wird von der Polizei gesucht. Ihn gibt es nur als bekanntes Pseudonym im Darknet, im echten Leben öffentlich nur mit Maske – für ihn ist ein Auftritt in Pavlovichs Show gutes Marketing, aber auch eine Gefahr. »Bisher hat mich der Geheimdienst nie kontaktiert«, sagt Pavlovich.

Sein heutiger Gast sei ein »erfahrener Bankkartenbetrüger«, kündigt Pavlovich zu Beginn der Show an. Er habe sich darauf spezialisiert, sogenannte Money Mules anzuwerben – Menschen also, die ein Konto eröffnen, dort illegales Geld in Empfang nehmen und es gegen einen geringen Abzug weiterüberweisen. Wer Geld zu waschen hat – aus welchem Grund auch immer –, kann diesen Service bei ihm buchen. Seine Kund:innen sind Menschen, die Steuern hinterziehen oder aus anderen Gründen Schwarzgeld verwalten und Cyberkriminelle wie Pavlovich selbst einer war. Schließlich können diese ihr erbeutetes Geld nicht einfach aufs eigene Konto überweisen. Dann kämen ihnen die Behörden zu schnell auf die Schliche. Also buchen sie eine Dienstleistung, bei der das Geld ein paar Runden über andere Konten dreht. Danach ist es etwas weniger Geld, dafür ist es sicher vor den Ermittlungsbehörden.

Dass die Menschen, die sich als Money Mules zur Verfügung stellen, dadurch natürlich ins Visier der Behörden geraten, ist dem Interviewpartner egal. Schließlich bekommen sie Geld dafür und haben meist ohnehin nichts zu verlieren. Wer so einen Job macht, ist schon ganz unten. Und meistens kommen sie durch mit der

Beteuerung, von nichts gewusst zu haben. Was sogar irgendwie stimmt: Ihre Bosse halten sie im Ungefähren, manche überwachen sie ihrerseits, um sofort zu erfahren, sobald jemand mit der Polizei in Kontakt ist.

»Wie kannst du verhindern, dass die Money Mules dein Geld einfach behalten?«, fragt Pavlovich. Schließlich ist es ja ein privates Konto, auf dem das Geld zwischengeparkt wird, bevor es über viele weitere Kanäle weitergeleitet wird, damit die Behörden den Überblick verlieren. Ach, das sei einfach, antwortet der Mann. Alles eine Frage der Organisation: Erstens solle man nie zu viel Geld auf einem Konto haben, sondern die Beträge regelmäßig weiterbuchen. Dann sei die Gefahr schon geringer, dass viel Geld abhandenkommt, sollte ein Money Mule unehrlich sein. Und zweitens sei es ratsam, die SIM-Karte des Mules zu übernehmen, sodass Nachrichten der Bank an den Auftraggeber, also den Mann mit der Maske, gehen. Dann habe der Kontoinhaber selbst keinen Zugriff mehr aufs eigene Online-Banking. Er ist dann blind, was sein eigenes Konto betrifft, während der Mann in der blauen Trainingsjacke die Geldströme genau verfolgen kann.

Mit dem Geldwäsche-Profi plaudert Pavlovich an diesem Tag ausgiebig darüber, welche Banken weniger skeptisch sind, wenn Money Mules allzu offensichtlich Konten für kriminelle Zwecke eröffnen oder in welchen Internetforen es »gute« Bankkarten gibt – also solche, die garantiert noch nicht gesperrt sind. Für 50 000 Rubel können Kriminelle sogar eine Art Versicherung dazukaufen, berichtet sein Gast: eine Geld-zurück-Garantie, falls eine gestohlene Karte nicht funktioniert oder ein anderer Krimineller ebenfalls eine Kopie der Karte hat und seinerseits Geld abhebt. Bereits für 5000 Rubel, rund 60 Euro, könne man hingegen ungeprüfte Karten bekommen, berichtet der Mann mit der Maske weiter. Das ist dann ein Glücksspiel. »Als ich angefangen habe, hat eine gestohlene Kreditkarte nur einen Dollar gekostet«, sagt Pavlovich. Mit der Professionalisierung steigen die Preise.

Falsche Spur

Diese Professionalisierung bringt bisweilen die Behörden durcheinander. Als im Juli 2014 die größte Bank der USA, JPMorgan Chase & Co, durch externe Sicherheitsunternehmen erfährt, dass sich offenbar Hacker:innen in ihren Systemen befinden, und sich nach und nach herausstellt, dass diese die Daten von 83 Millionen Kund:innen der Bank geklaut haben, ist die Aufregung groß. Denn 83 Millionen ist eine unvorstellbar große Zahl – demnach müssten mehr als die Hälfte aller privaten Haushalte in den USA betroffen sein! Zudem ist die Vorgehensweise extrem professionell: Wie die ersten Ermittlungen zeigen, sind die Angreifer:innen schon länger in den Netzwerken der Bank und haben sich extrem vorsichtig und professionell dort bewegt, ihren Zugriff auf Teile des Systems systematisch ausgeweitet und so Zugang zu immer mehr internen Daten erlangt.

Kurz zuvor hat Russland die Krim überfallen und annektiert, und die USA haben mit scharfen Sanktionen darauf reagiert. Die Welt wartet gespannt und nervös auf die erwartete Rache Russlands. Was wird als Nächstes passieren? Natürlich liegt nichts näher, als dass dieser Hack, der den ausgefeilten Methoden staatlicher russischer Hackinggruppen in nichts nachsteht, der Beginn einer großangelegten digitalen Racheaktion für die Sanktionen ist, die Russland empfindlich getroffen haben. Medien und JPMorgan Chase sind sich schnell einig: Hier sind russische staatliche Gruppen am Werk.[4]

Noch eines scheint klar auf ein politisches Motiv hinzudeuten: Die Hacker:innen in den Systemen der Bank hatten es offensichtlich nicht auf Geld abgesehen. Sie haben keinen Cent gestohlen. Wären sie Kriminelle – wäre es nicht das Erste, was sie tun würden? Also schien klar: Das sind keine Kriminellen.

4 https://www.theguardian.com/business/2014/aug/28/jpmorgan-chase-us-companies-hacking-attack-russia

Diese Vorannahmen erwiesen sich als falsch – und als teuer. Denn sie hinderten die Beteiligten daran, zielstrebig in die richtige Richtung zu ermitteln. Die Vermutung, es handele sich um den russischen Geheimdienst, schien einige Ermittlungsansätze von vorneherein auszuschließen – beispielsweise jene in die kriminelle Szene. Schließlich setzte sich das FBI gegen die IT-Abteilung der Bank durch, die weiterhin auf russische Geheimdienste verwies – und nahm im Juli 2015 drei Männer in Israel fest: einfache Kriminelle, könnte man sagen. Oder auch: begabte Kriminelle. Und wie sich schließlich zeigte, ergab es nach deren Geschäftsmodell durchaus Sinn, der Bank kein Geld zu stehlen, sondern die gestohlenen Daten zu Geld zu machen. Damit organisierten sie unter anderem Aktienbetrügereien, für die ein breit angelegtes E-Mail-Marketing die Grundlage war. Der einzige Grund für den Einbruch in die Bank war, dass die Kriminellen wussten, dass sie dort Kontaktdaten von Anleger:innen ergattern konnten. Die drei israelischen Beschuldigten scheuten weder Kosten noch Mühe, an solche Daten zu gelangen. Ihr Angriff war so perfekt, dass er offenbar an die Ausgefeiltheit staatlicher Angriffe herankam und die internen Ermittlungen der Bank gehörig durcheinanderbrachte.

Wer sich mit den Motiven von Kriminellen auseinandersetzt und deren Perspektive kennt, ist in solchen Fällen im Vorteil. Die US-Psychologin Fiona Guy beschäftigt sich seit vielen Jahren mit der Einstellung von Kriminellen und den Hintergründen krimineller Taten und hat auch den Hack bei JPMorgan Chase analyisiert. Auch sie sei überrascht, was für eine riesige kriminelle Firma hinter dem Angriff steckte und mit welcher Professionalität deren Boss Gery Shalon sie geführt habe, sagt sie im Interview mit mir. »Diese Unternehmung erstreckte sich über mehrere Länder und brachte mehrere Millionen Dollar ein.« Als sie die Vorgänge analysierte, entblätterten sich vor ihren Augen »viele Schichten von gut geölten und gut geführten Geschäftsabläufen«, sagt sie, »das

Unternehmen war sehr gut organisiert und verwaltet und äußerst effektiv.« Doch auch wenn Shalon sich die besten Kriminellen für seine Taten einkaufte, so war er doch eine Einzelperson. »Es fällt mir immer noch schwer zu begreifen, wie ein einzelner Mann ein so ausgeklügeltes Netzwerk wie dieses entwickeln und betreiben kann und damit so lange durchkommt.«

Das ging den Behörden ähnlich, nur waren diese sich darüber nicht im Klaren, dass es gerade der Grad der Professionalisierung war, von dem sie sich täuschen ließen. Weil sie das Motiv nicht auf Anhieb durchschauten, gingen sie davon aus, es handele sich um den russischen Geheimdienst.

»Kriminelle haben andere Ziele und andere Beweggründe«, sagt Fiona Guy. »Wenn man herausfindet, welche das sind, hat man schon den halben Weg geschafft, um die Täter zu finden.« Den gleichen Fall gibt es auch andersherum: Die Hacker des russischen Geheimdienstes tarnen sich tatsächlich manchmal als Cyberkriminelle, um die Aufklärung zu erschweren und eine mögliche Gegenwehr zu lähmen – beispielsweise bei NotPetya, dem teuersten Cyberangriff der Geschichte, der sich zunächst als kriminelle Ransomware – also als eine Art Erpressungsmechanismus durch Schadsoftware – tarnte und schließlich ganze Systeme unwiederbringlich löschte (Dazu mehr in Kapitel 3.1).

Im Zuge des russischen Angriffskriegs auf die Ukraine bietet sich aktuell ein einmaliger Einblick in die Organisationsstruktur einer anderen kriminellen Hackinggruppe aus Russland: Conti gilt als eine der gefährlichsten, wenn nicht als die gefährlichste Ransomware-Gruppe. Sie wird offensichtlich aus Russland gesteuert. Als Russland im Februar 2022 in die Ukraine einmarschierte, erklärten sich zahlreiche internationale Hacker:innen solidarisch mit der Ukraine und begannen, russische Infrastrukturen anzugreifen. Im Gegenzug erklärte Conti, die Gruppe werde Russland verteidigen und Vergeltung üben für alle, die ihr Heimatland angriffen.

Das behagte offenbar einem Insider nicht, der daraufhin unter

dem Namen »Conti-Leaks« begann, zahlreiche interne Dokumente zu veröffentlichen – unter anderem waren dies Chats und Textnachrichten, die die Befehlskette und die Organisation des kriminellen Unternehmens sichtbar werden ließen. Diese Leaks zeigen eindrücklich, dass Conti nicht eine zufällig zusammengewürfelte Untergrund-Gang ist, sondern wie ein professionelles Unternehmen organisiert ist – mit Personalabteilung, Bonuszahlungen und einer klaren Rollenverteilung unter anderem in Zuständige fürs Coding, für die Systemadministration und für die Verschlüsselung, zudem gab es ein eigenes Offensiv-Team.[5] Für jede Aufgabe gibt es Spezialist:innen. Nur wer sich dies vor Augen hält und davon ausgeht, dass Angreifer:innen aus dem Darknet ebenso straff organisiert und professionell sein können wie ein erfolgreiches Start-up, kann solche Aktivitäten richtig einordnen.

Aber wieso entscheiden sich offensichtlich begabte Menschen nicht dafür, mit ihren Fähigkeiten etwas Legales zu tun? Diese Frage treibt Fiona Guy immer wieder um. Sie erinnert sich noch gut an den Fall von Zain Qaiser, einem 17-jährigen Jungen, der zu Hause bei seinen Eltern in London lebte und von dort eine massive Cybercrime-Unternehmung startete. »Er war ein sehr begabter Hacker und hatte das nötige Selbstvertrauen, um ein russisches Ransomware-Syndikat anzusprechen.« Die Strafverfolgungsbehörden gehen in diesem Fall davon aus, dass er in kurzer Zeit mehr als vier Millionen Pfund einnahm – womit er als der erfolgreichste Cyberkriminelle Großbritanniens gilt. Es gebe keinen vergleichbaren Fall, erklärte der Richter, der ihn schließlich zu mehr als sechs Jahren Haft verurteilte.[6]»Man kann sich des Eindrucks nicht erwehren, dass dieser Junge mit seinen Fähigkeiten, seinem Tatendrang und seiner Motivation auf legalem Weg viel Beeindruckendes hätte erreichen können«, sagt Fiona Guy zu mir

5 https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/

6 https://www.bbc.com/news/uk-47800378

im Gespräch. Warum tat er es nicht? Wieso wird ein junger Mann mit Fähigkeiten, die ihm viele legale und durchaus lukrative Möglichkeiten eröffnet hätten, zum Kriminellen?

Die Frage nach der Motivation beschäftigt auch den Sicherheitsforscher Benoît Ancel, den ich im Sommer 2021 im idyllischen dänischen Skanderborg besuchte, wo er für ein Sicherheitsunternehmen arbeitet. »Mit meinen Fähigkeiten hätte ich auch im Gefängnis landen können«, sagt er. Als Jugendlicher hat er viel gemein mit Gleichaltrigen, die später in der kriminellen Hackingszene gelandet sind. Er treibt sich damals in Computerforen herum, deren Mitglieder sich gegenseitig in Sachen Hacking weiterbilden. Er hat viel Zeit, denn Schule findet er weniger wichtig. Stattdessen tüftelt er nächtelang am großen Rätsel der Computersprache. »Im Nachhinein denke ich oft: Die ganze Sache hätte auch schiefgehen können, aber ich habe zum Glück den richtigen Weg gewählt, denn als Jugendlicher ist die dunkle Seite natürlich interessant«, sagt er.

Heute scrollt er beruflich oft durch das Internet. Nicht auf der Suche nach Filmen, Musik oder Schnäppchen wie wir, sondern auf der Spur von Kriminellen. Als ich ihn besuche, sitzt Benoît Ancel im Büro des dänischen Unternehmen CSIS Security Group in Skanderborg, der Kleinstadt in der Nähe des dänischen Arhus, zwischen Bildschirmen und vor einem Fenster mit Blick auf einen malerischen See. Draußen scheint die Sonne, der Garten des Unternehmens endet am See, es gibt sogar einen eigenen Badesteg für die Angestellten. Aber Ancel hat nur Augen für die Zahlen und Buchstaben auf seinem Bildschirm. Dieses scheinbar ziellose Scrollen ist Herzstück seiner Tätigkeit. Für sein Unternehmen und dessen Kunden – darunter viele Banken – will er vorhersehen, was da anrollt: Von welchen IP-Adressen aus verbreiten sich Viren und Trojaner? Welche Schadsoftware ist gerade wo unterwegs? Und wer sind die kriminellen Hacker:innen, die dahinterstecken?

Die scheinbare Ziellosigkeit seines Scrollens folgt in Wirklichkeit einem Muster, wenn auch einem undurchsichtigen. Ancel folgt seinem Bauchgefühl. »Andere durchsuchen das Netz automatisch«, sagt er. Automatisch heißt mit eigens dafür entwickelten Programmen, die auffällige Muster suchen, die auf kriminelle Aktivitäten hindeuten könnten. Er lässt sich lieber von seiner Intuition leiten. »So sieht man mehr. Ich spüre mehr.« Dieses Gespür ergibt sich aus vielen kleinen Eindrücken im Vorbeisurfen und aus jahrelanger Erfahrung. Es ist die Haptik des Internets. Das Bauchgefühl eines Sicherheitsforschers, der sich mit Computern beschäftigt, seit er als Achtjähriger der einzige in 50 Kilometern Umkreis war, der überhaupt einen besaß.

Mit Leuten wie Pavlovich oder seinen Mitstreiter:innen im Forum hat der junge Benoît Ancel eine Leidenschaft gemeinsam, die er in seinem analogen Leben in einem französischen Dorf mit niemandem teilen kann. Wieso es nicht schiefging? Ancel ist überzeugt, dass es der gute Einfluss seiner Eltern war und deren konsequente Ehrlichkeit. Die letztlich behütete Jugend. Geld war unwichtig, moralische Werte wichtig. »Meine Eltern haben mir von klein auf gesagt, dass ich tun muss, was richtig ist, und nicht, was einfach ist«, erinnert er sich.

Aufmerksam verfolgt er als Jugendlicher, wie einer seiner Freunde schließlich in ein gut geschütztes Forum von Kriminellen im Darknet eindringt, was ihm nur gelingt, indem er jahrelang an seiner Reputation als krimineller Hacker arbeitet und schließlich eine Einladung erhält. Auch Ancel ist fasziniert von dem, was die Hacker:innen dort können, von ihrer Macht. Doch dann kommt die Überraschung: Sein Freund gibt alles, was er dort vorfindet, direkt ans FBI weiter. Und Ancel beschließt: Das möchte er auch eines Tages machen.

Heute sieht er in seinem Beruf als Sicherheitsforscher das Leid, das kriminelle Hacker:innen anrichten. Er selbst ist als Sohn einer Krankenschwester und eines Sachbearbeiters in einem Elektrizitätswerk im ländlichen Frankreich bescheiden aufgewachsen.

»Wir waren nicht reich, aber mir hat es nie an etwas gefehlt«, sagt er. Doch nicht auszudenken, was passiert wäre, wenn jemand das Familienkonto geplündert hätte!

Bis heute gibt Ancel den Ermittlungsbehörden regelmäßig Tipps, welche Hacker derzeit wo auf der Welt aktiv sind, von welchen IP-Adressen aus sie sich mit dem Internet verbinden, in welcher Stadt sie möglicherweise leben, welche Ziele sie im Visier haben und vieles mehr. Solche Tipps führen immer wieder dazu, dass Hackingringe zerschlagen werden und Kriminelle wie Pavlovich im Gefängnis landen.

Prahlen und Patriotismus

Pavlovich hingegen hätte gerne Ruhe vor dem FBI. Doch davon kann keine Rede sein. Die US-Behörde sucht ihn noch immer und macht kein Geheimnis daraus, dass sie ihn sofort in den Knast stecken würde, sobald er den Fuß in ein Land setzte, das an die USA ausliefert. Zwei seiner früheren Mitstreiter aus der Ukraine und aus Estland ist das passiert: Einer war im Türkeiurlaub, ein anderer in Deutschland. Sie waren auf der Interpol-Fahndungsliste, auf der auch Pavlovich bis heute steht.

»Ich würde das so gerne klären mit Interpol«, sagt Pavlovich bei meinem Besuch in Moskau, während er in seinem Büro das Geschenkpapier eines länglichen Päckchens löst und einen Baseballschläger aus der Verpackung nimmt. Seine Besucher:innen haben ihm so viele Geschenke zum Jubiläum mitgebracht, dass er noch am nächsten Tag jede Gesprächspause nutzt, um weiter auszupacken. Der Schläger ist blau lackiert, darauf sind weiße Blumen gemalt. Ein Baseballschläger mit Margeriten? »Das ist Kunst.« Pavlovich schwingt ihn durch die Luft, dann streicht er über den Lack als prüfe er die Qualität eines besonders wertvollen Stücks Holz. »I am a good guy now«, sagt er wieder wie ein Mantra, »ich bin jetzt einer von den Guten.« Der Baseballschläger ist das Ge-

schenk eines befreundeten Galeristen. Wobei die Unterscheidung zwischen Freund und Geschäftspartner kaum möglich ist, denn Pavlovich macht möglichst mit jedem Geschäfte. Auch der Galerist wird bald darauf in Pavlovichs Show auftreten. Dafür zahlt er gerne 5000 Dollar, denn für ihn ist das Marketing.

Aber Pavlovich beschäftigt derzeit mehr, wie es mit seiner Freiheit weitergeht. »Ich saß zehn Jahre im Knast, wieso reicht das nicht für das FBI?« Sein Anwalt versucht gerade, die US-Behörden davon zu überzeugen, dass er für seine Taten ausreichend gebüßt hat, auch für die, unter denen Millionen amerikanischer Bankkunden gelitten haben. Kürzlich habe ihn ein FBI-Beamter persönlich angerufen und versucht, ihn zu überreden, in die USA zu reisen. »Sie wollten mir ein Spezialvisum ausstellen, ich hätte es innerhalb einer Stunde bekommen.« Aber kann der Mann am Telefon garantieren, dass er nicht verhaftet wird? Nein, habe der Mann gesagt, das könne er nicht. Man müsse die Sache verhandeln, wenn er vor Ort sei.

Pavlovich hat sich vorerst dagegen entschieden. Er wird in Russland bleiben. Lediglich seine Heimat Weißrussland ist noch sicher vor dem Zugriff internationaler Behörden. »Aber da herrscht ein Diktator, da will ich nicht hin.« An allen anderen Grenzen würde er aufgrund des Eintrags auf der Interpol-Liste vermutlich verhaftet. Auch sein Cousin und einstiger bester Freund Dmitry Burak ist abgetaucht, er hat ihn seit seiner Festnahme nicht mehr gesehen. Das sagt er zumindest. »Ich vermisse ihn sehr, ich hoffe, er kann das mit dem FBI irgendwann klären.«

Wäre er nur nicht auf diese Interpol-Liste geraten! Wieso er sich damals wohl für diesen Weg entschieden hat? Typische Beweggründe sind laut Fiona Guy: »Die Verlockung des Geldes ohne harte Arbeit und die Option, flexibel von zu Hause aus zu arbeiten. Und der Nervenkitzel, etwas zu tun, von dem man weiß, dass es falsch ist, und damit davonzukommen«, sagt sie. »Für Jüngere hat das Ganze einen gewissen Glamour.« Oft locke zudem die Aussicht auf »protzige Autos, schicke Anzüge und Geld«, mit

denen die Hacker dann prahlen. Das wurde Zain Qaiser zum Verhängnis: Er geriet in Verdacht, weil er offenbar plötzlich zu Geld gekommen war.

»Nenn es Patriotismus«, sagt Pavlovich, wenn man ihn darauf anspricht. »Wir fanden, es gibt so viele reiche Europäer und Amerikaner – und wir waren arm.« Nach dem eigentlichen Interview sitze ich mit Pavlovich und einem Kollegen im Büro. »Vlad, mein CEO«, stellt Pavlovich den jungen Mann vor. »Ich musste mich vergrößern, das Geschäft läuft so gut.« Mit mehr als einer Million Abonennt:innen auf YouTube sowie Tausenden Fans auf diversen Telegram-Kanälen und einem Gewinn von 46 316 Dollar allein aus YouTube-Werbeeinnahmen im vergangenen Jahr fand er: Jetzt ist es Zeit für eine Professionalisierung. Zusammen mit seinem CEO will er Verträge durchgehen: Vlad gibt ihm eine Liste all der Kund:innen, die für ihre Auftritte in der Show bezahlen. »Dem müsstest du bald den Entwurf für das Marketing-Element schicken«, sagt Vlad und zeigt auf einen Vertrag. Der Kunde bezahlt 2000 Dollar dafür, dass Pavlovich ihn zu Beginn seiner Sendung erwähnt.

Pavlovich hat jetzt also einen CEO, außerdem einen Mitarbeiter für die Sendung, der sich mit Kryptowährungen auskennt, einen Marketingmitarbeiter, einen Techniker und zwei Anwälte. »Letztes Jahr war ich noch ganz allein«, sagt er nachdenklich. »Letztes Jahr war ich noch Putzkraft«, erwidert Vlad. Andere würden zusammenzucken bei einem solchen Geständnis des eigenen Geschäftsführers. Aber Vlads Chef schaut ihn an wie ein stolzer großer Bruder und sagt: »Er ist erst einundzwanzig und arbeitet, seit er fünfzehn ist!« Vlad kommt aus der Ukraine, seine Familie ist ebenfalls arm. Und so habe er sich aufgemacht, um Arbeit zu finden, berichtet er. Zwei Jahre war er in Israel als Koch, drei Jahre in Deutschland als Fahrer, Putzmann und Hausmeister – und als Pole. »Denn als Ukrainer bekommst du in Deutschland keine

Arbeitserlaubnis.«[7] Deshalb verdienen die einen ihr Geld mit Ausweisfälschungen, während die anderen mit den gefälschten Ausweisen im EU-Ausland arbeiten. »Wir werden kriminell, weil wir arm sind«, sagt Pavlovich.

Aber ist es so einfach? Wovon hängt es ab, ob jemand irgendwann erkennt, dass der Weg in die falsche Richtung geht und die Notbremse zieht? Auch Benoît Ancel ist nicht in besonders üppigen Verhältnissen aufgewachsen. Sind es wirklich die Eltern mit ihrem prägenden Einfluss, von denen Ancel sagt, dass er ihnen Ehrlichkeit schuldig ist? »Das ist die uralte Debatte um Natur und Veranlagung«, sagt die Psychologin Fiona Guy. So spielen ihrer Beobachtung nach die Erfahrungen in der Kindheit durchaus eine große Rolle bei zukünftigen Entscheidungen und dem weiteren Lebensweg. »Gleichzeitig gibt es Menschen, die einen schrecklichen Start ins Leben hatten und als Kinder sehr gelitten haben, sich aber dennoch zu ausgeglichenen und völlig gesetzestreuen Bürgern entwickelt haben.« Was Menschen wie Ancel und Pavlovich dazu bewegt hat, dass sie heute Gegenspieler sind – diese Frage ist nicht einfach zu beantworten.

Einsames Geschäft

Benoît Ancel hat sich in seinem Leben schon viel in die Leben von Kriminellen gehackt. Er hat ihre Schicksale verfolgt, mit vielen hatte er persönlichen Kontakt. Die Begeisterung für die Technik ist eine große Gemeinsamkeit. Er kann sich in sie hineinversetzen. »Ich behandle sie nicht von oben herab, sondern mit Respekt«, sagt er. So etwa den 17-Jährigen, den er eines Tages ausfindig machte und mit dem er bis heute in Kontakt ist. Er hatte beobachtet, wie der junge Franzose in zwei Jahren mehr als eine Mil-

7 Das Gespräch fand vor dem russischen Angriffskrieg statt – aktuell dürfen ukrainische Geflüchtete in Deutschland arbeiten.