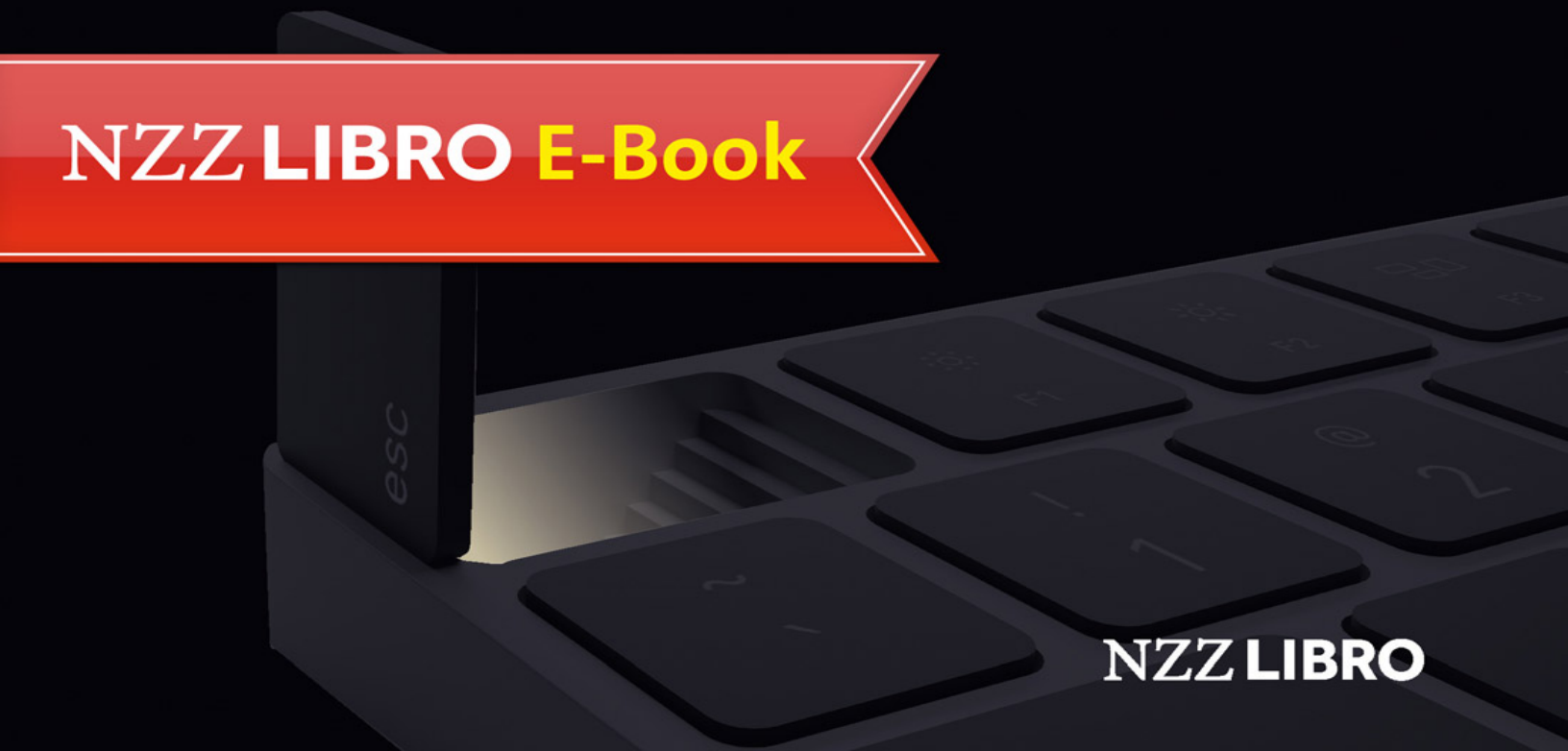
Otto Hostettler
Abdelkader Cornelius

UNDERGROUND ECONOMY

Wie Cyberkriminelle Wirtschaft und Staaten bedrohen

NZZ LIBRO E-Book



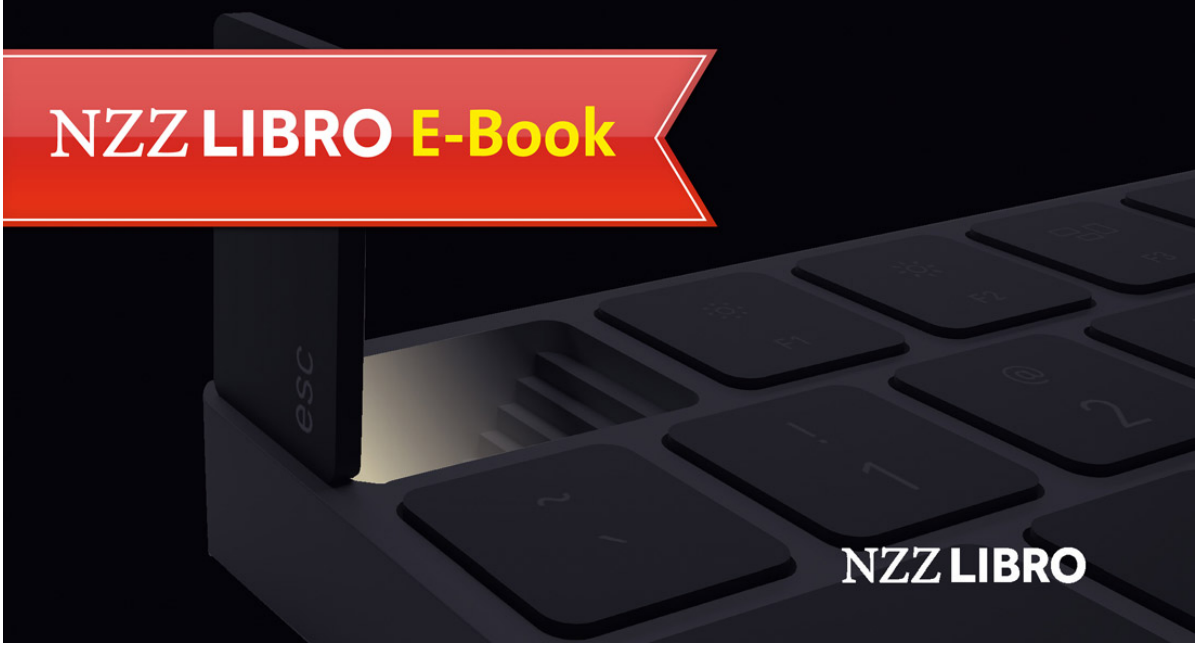
NZZ LIBRO

Otto Hostettler
Abdelkader Cornelius

UNDERGROUND ECONOMY

Wie Cyberkriminelle Wirtschaft und Staaten bedrohen

NZZ LIBRO E-Book



NZZ LIBRO

Otto Hostettler
Abdelkader Cornelius

UNDERGROUND ECONOMY

Wie Cyberkriminelle Wirtschaft und Staaten bedrohen

NZZ **Libro**

Der Verlag dankt für die finanzielle Unterstützung:

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Der Text des E-Books folgt der gedruckten 1. Auflage 2022 (ISBN 978-3-907291-67-2)

Lektorat: Karin Schneuwly, Zürich
Titelgestaltung: Weiß-Freiburg GmbH, Freiburg i. B.
Datenkonvertierung: CPI books GmbH, Leck

ISBN Print 978-3-907291-67-2
ISBN E-Book 978-3-907291-68-9

www.nzz-libro.ch
NZZ Libro ist ein Imprint der Schwabe Verlagsgruppe AG.

Inhaltsverzeichnis

Vorwort

Beinahe täglich erreichen uns Nachrichten über digitale Angriffe gegen staatliche und private Stellen: Industriegeheimnisse werden gestohlen, Finanzdaten von Gemeinden gelöscht oder Lieferketten gestört. Neben den direkten wirtschaftlichen Konsequenzen – vom Betriebsausfall und von Lösegeldforderungen hin zu potenziellen Strafzahlungen – leiden auch der Ruf und das Vertrauen in Staat und Wirtschaft im digitalen Zeitalter unter dieser Entwicklung und – unsere persönlichen Daten können betroffen sein.

Dies ist zwar nicht neu. Der Missbrauch von Sicherheitslücken und gezielte Angriffe gehören leider seit Beginn des Internets dazu, sei es aus kommerziellen oder

politischen Motiven oder einfach aus Jux und zur Aufklärung. Doch die Angriffe erlangen eine neue Qualität.

Einerseits bringt der technologische Fortschritt viele Vorteile und eröffnet uns – als Bürgerinnen und Bürger und als Konsumentinnen und Konsumenten – aber auch der Wirtschaft neue Möglichkeiten. Von der Geschäftsidee zum weltumspannenden Konzern ist es unter anderem dank digitaler Technologien oftmals kein grosser Schritt mehr. Umgekehrt können es sich auch «analoge» Firmen immer weniger leisten, auf die Vorteile der Digitalisierung zu verzichten.

Kleine und mittlere Unternehmen in der Maschinenindustrie setzen auf Automatisierung in ihren Produktionsprozessen und erfassen die Bedürfnisse ihrer Kunden dank Digitalisierung noch besser, lokales Gewerbe kann sich dank Onlineshops Absatzkanäle weit über den oftmals kleinen Heimmarkt sichern usw. Diese Ausweitung der Digitalisierung hat nicht zuletzt im Zug der Corona-Pandemie nochmals Fahrt aufgenommen. Praktisch über Nacht haben Grosskonzerne und Kleinstbetriebe dank digitaler Technologien auf Homeoffice gewechselt, neue Interaktionsformate mit Lieferanten und Kunden eingeführt oder ihr Geschäftsmodell digital neu erfinden müssen. Vielen Menschen war es nur noch über digitale Kanäle möglich, zu kommunizieren und den Kontakt zu ihren Familien aufrechtzuerhalten. Andere mussten von zu Hause aus arbeiten.

Die zunehmende Anbindung der Wirtschaft an die digitale Welt führt neben den ganzen Vorteilen aber auch zu einer gesteigerten Verletzlichkeit: Wer online ist, kann

angegriffen werden. Diese Erkenntnis scheint sich mit Blick auf die hohe Zahl erfolgreicher Cyberattacken leider noch nicht überall durchgesetzt zu haben. Hinzu kommt, dass dies nur jene Attacken sind, von denen man weiss. Nicht umsonst sagte Keith Alexander, früherer Direktor der amerikanischen National Security Agency (NSA): Entweder wissen Sie schon, dass Sie gehackt wurden, oder Sie wissen es einfach noch nicht.

Die immer grössere Zielscheibe von Organisationen im Netz wird begleitet von immer kompetenteren Angreifern. Denn die Cyberkriminellen haben, im Gegensatz zu manchen Firmen, in den letzten Jahren nicht geschlafen. Sie sind organisiert, bestens vernetzt, ausgebildet und ausgestattet für langfristige Kampagnen weltweit. Lukrative Geschäftsmodelle wie Ransomware sorgen dafür, dass dieses Problem nicht einfach verschwinden wird, im Gegenteil. Unsere steigende Abhängigkeit von digitalen Diensten macht Angriffe auf diese in Zukunft noch lukrativer. Wollen wir auf die Vorteile der Digitalisierung nicht verzichten, müssen wir Cybersicherheit endlich ernst nehmen und Cyberkriminellen entschieden entgegentreten.

In ihrem Buch *Underground Economy* legen die Autoren Otto Hostettler und Abdelkader Cornelius klar und verständlich dar, wie es so weit kommen konnte. Sie erläutern ausserdem, wie Cyberkriminelle sich international vernetzen und Attacken koordinieren. Nicht zuletzt zeigen die Autoren auf, in welchen Handlungsfeldern Firmen nun aktiv werden müssen.

Doris Leuthard
alt Bundesrätin,

Präsidentin der Stiftung
Swiss Digital Initiative

1

Phreaking, Skript Kiddies, Cracker: wie Hacking zum Geschäft wurde

Ralph B. war noch keine 17 Jahre alt, als er an diesem Abend im elterlichen Haus gedankenverloren vor dem Kühlschrank stand. Seine Mutter mahnte ihn, nun endlich sein Zimmer aufzuräumen. Die Botschaft erreichte den Jugendlichen nicht. Geistesabwesend murmelte er: «Ich glaube, jetzt habe ich gerade etwas geschafft, das meine Zukunft verändern wird.»

Allerdings: Ralph gelang es an diesem Tag, ins Netzwerk eines grossen Schweizer Providers einzudringen. Er war gerade auf die Namen aller Kundinnen und Kunden gestossen, auf ihre Adressen – und auch auf ihre Passwörter. Er war euphorisiert und perplex zugleich. Und doch wusste er nicht, wo ihm der Kopf stand. Kurz: Er war ziemlich durch den Wind. Seine Mutter erzählt die Episode bis heute. Doch damals, 1996, konnten weder Ralph noch seine Mutter die Folgen abschätzen. Heute sagt er: «Klar, das war jugendlicher Leichtsinn.» Aber er habe die Passwörter nie verwendet, versichert er. «Die Risiken waren mir viel zu hoch.» Stattdessen gründete er – noch während seiner kaufmännischen Ausbildung – sein erstes Unternehmen. Tagsüber arbeitete er in einem Reisebüro, abends erstellte er für Firmen Webseiten. Nebenher tummelte er sich stundenlang in IT-Foren und suchte jede erdenkliche Information zu IT-Sicherheitsfragen zusammen. Ralph B. saugte alles auf.

Kein Wunder, blieb seine Ausbildung auf der Strecke. Während des Berufsschulunterrichts las er unter dem Tisch IT-Bücher, dicke Schunken. Jede Woche wälzte er mindestens ein solches Buch. Er war auch nicht wirklich erstaunt, als er die Abschlussprüfung vermasselte. Heute ist für Ralph B. klar: Mit diesem «Hack», von dem er damals seiner Mutter in der Küche beichtete und bei dem er Zehntausende von Nutzerdaten und Passwörtern aus dem Firmennetzwerk fischte, stellte er sich auf eine neue Ebene. «Mir ging an diesem Tag emotional der Knopf auf», sagt er 25 Jahre später. Was er damit ausdrücken will: Aus dem KV-Stift, der kurz darauf durch die Schlussprüfung fliegen sollte, war ein IT-Spezialist geworden.

Bis zu diesem Tag war er eher ein Gamer, nicht untypisch für die damalige Zeit. 1992, mit zwölf Jahren, erhielt er seinen ersten Computer, einen IBM XT/AT, mit 1 Megabyte Arbeitsspeicher. Sein ganzer Stolz. Nach Abschluss der obligatorischen Schule besass er eine Reihe Spielkonsolen, einige neuere X86-Rechner. Aber schlechte Zeugnisnoten. Der Berufsberater sah für ihn keine Zukunft in der Informatik, die Informatikerlehre gab es noch nicht, ein Studium kam bei den konsequent abnehmenden schulischen Leistungen selbstredend nicht infrage. So landete er in einem Reisebüro. Wenn er von der Arbeit nach Hause kam, startete er den Computer auf und setzte sich vor den Bildschirm – bis er ins Bett ging. Abend für Abend. In seinem Zimmer hatte er mit seinen verschiedenen Geräten ein kleines Netzwerk aufgebaut.

Das hausinterne Netzwerk war ihm bald zu klein. Mit dem ersten Modem, das grauenhafte Einwahlgeräusche

erzeugte, kam Ralph B. ins Internet. Dafür musste er den Eltern das Telefon ausstecken. Er fand in amerikanischen Foren Informationen über den Aufbau des Internets, etwa über technische Erklärungen, wie Daten elektronisch übermittelt werden. Und dann waren da auch die Tipps und Tricks, wie man gratis telefonieren konnte. Klar versuchte auch Ralph B., mithilfe von Tonsignalen die analogen Telefonverbindungen zu manipulieren. Diese Signale wurden von den Vermittlungsstellen benutzt, um die Verbindungen zweier Gesprächspartner herzustellen. Weil die Übertragung dieser Signale nicht vom analogen Telefongespräch abgeschirmt war, konnten sie beeinflusst werden.

«Phone» und «Freak»

Auf diese Weise konnte man schon seit den 1960er-Jahren gratis telefonieren. Als in den 1980er-Jahren die ersten Akustikkoppler auf den Markt kamen, breitete sich diese Art von Telefonmanipulation weiter aus. Die Rede war von «Phreaking». Der Begriff setzt sich zusammen aus «Phone» und «Freak» (für verrückter Typ) und wurde unter der ersten Computergeneration bald zu einem Volkssport. Allerdings waren in der Schweiz die technischen Normen anders als in den USA, und phreaking funktionierte ziemlich zufällig. Hier waren Wählscheiben verbreitet, die einen stakkatoähnlichen Impuls erzeugten und damit die Verbindung herstellten. Doch auch diese liessen sich manipulieren. Dazu musste man lediglich in einem bestimmten Rhythmus auf die Gabel schlagen und damit

den Rhythmus der Impulse simulieren, und schon wählte das Gerät eine Nummer – wenn auch eine ziemlich zufällige.

Ralph B. betrieb ebenfalls Phone Hacking, etwa zwei Jahre bevor er beim Provider die Passwörter fand. Zufälligerweise lernte er in einem amerikanischen Forum einen Jungen aus dem Nachbardorf kennen. Gemeinsam haben sie ausprobiert, was sie in den Foren gelernt hatten. «Eigentlich war es unsinnig, aber es machte Spass», sagt er heute. Immerhin schafften sie es, gratis nach Ägypten zu telefonieren. Zu Schaden kam niemand, von der damaligen PTT mal abgesehen.

Auf der deutschen Seite des Bodensees machte sich in dieser Zeit Roland Brecht in seinem Kinderzimmer daran, seine Computer zu vernetzen. Auch er war ein mittelmässiger Schüler gewesen, auch er absolvierte gerade eine kaufmännische Ausbildung und auch er steckte jeden Abend das elterliche Telefon aus – und sein Modem ein. Beide durchpflügten das Internet auf der Suche nach technischem Wissen. «Plötzlich konnte man sich vernetzen, das war neu und aufregend», sagt er fast 30 Jahre später. Wie Ralph B. durchsuchte auch Roland Brecht die damaligen Newsgroups, schrieb sich in Gruppen ein, um sich über technische Belange der neuen faszinierenden Internetwelt auszutauschen.

Der Drang, das Internet zu verstehen

In einem dieser Foren trafen sich die beiden, bald fand sich ein halbes Dutzend Schweizer und Deutsche zusammen.

Die meisten von ihnen – wenn überhaupt – waren nur knapp volljährig. Einige kannten sich bereits gut aus im Umgang mit Netzwerken, andere mit der Webseitenprogrammierung HTML oder mit Schwachstellen von Programmen und Systemen. Alle hatten eines gemeinsam: einen unglaublichen Drang, alles über dieses neue Internetding zu verstehen. Und plötzlich waren die ersten Viren und Trojaner im Umlauf. Sie wollten auch dieses neue Phänomen verstehen.

Die Jugendlichen teilten nicht nur ihre Leidenschaft für die neue Welt des Internets, sie teilten ihr Wissen miteinander und lernten voneinander. Kommuniziert wurde über Vorläufer heutiger Chatdienste, den Internet Relay Chat (IRC). Abend für Abend traf man sich, meist war auch tagsüber irgendjemand der Gruppe online. Solche IRC, eigentliche virtuelle Treffpunkte, bilden bis heute eine relativ abhörsichere Alternative zu sozialen Netzwerken wie Facebook und gängigen Messengerdiensten wie WhatsApp. Sie werden bis heute von Computernerds geschätzt und genutzt.

Irgendwann um 1994 nannte sich die Gruppe «Kryptocrew», Roland Brecht registrierte den Domainnamen. «Nun hatten wir eine Plattform, um das zu verwirklichen, was uns wichtig erschien: Informationen und Wissen über Sicherheitsfragen im Internet zu verbreiten.» Das Forum fand bald im gesamten deutschsprachigen Raum Beachtung. Roland Brecht wurde Seitenadministrator, Ralph B. und andere lieferten Texte. Innerhalb von rund zehn Jahren übersetzten sie Tausende von Texten aus englischsprachigen Foren, trugen Wissen

und Erkenntnisse zusammen und beantworteten Fragen anderer interessierter Internetnutzer. Analysen zu den Übertragungsprotokollen TCP/IP beispielsweise, über Netzwerke – und bald auch über Sicherheitslücken. Sie bauten die Lücken nach und versuchten sie zu schliessen. Einer der «Kryptocrew» hatte hier besonderes Talent. Er schrieb ein «Trojan-First-Aid-Kit», ein Programm, das infizierte Computer säubern konnte. Die Software war beliebt und wurde damals sogar als CD einer Computerzeitschrift beigelegt.

«Auch ich erlebte, wie mein CD-Laufwerk wie von Geisterhand auf- und zuging», erzählt Roland Brecht. Es war die Zeit, als sich viele Computernutzer nicht bewusst waren, dass bei ihrem Gerät die Netzwerkeinstellungen sperrangelweit offen waren und aussenstehende Dritte sich Zutritt verschaffen konnten. Doch die Leute der «Kryptocrew» wussten bald bestens Bescheid. Mit einem einfachen Tool suchten sie in einem festgelegten IP-Adressbereich nach offenen Netzwerken. «Wir fanden immer ein paar Dutzend zugängliche Computer.» Und so schaute man halt, was die Leute so alles auf ihrem C-Laufwerk gespeichert hatten, Briefe, Unterlagen, das private Bilderarchiv. «Aber wir waren nie kriminell», beteuert Brecht, der bis heute beruflich Websites eines Grossunternehmens programmiert.

Herumschauen und Spass haben war das Motto. Meist trafen sie sich online, immer mal wieder aber auch offline. Es war die Zeit der LAN-Partys, bei denen die Teilnehmenden ihre Computer untereinander zu sogenannten Local Area Networks zusammenschlossen.

Dazu mietete die Gruppe für ein Wochenende eine Fabrikhalle, jeder brachte einen netzwerkfähigen Computer und Unmengen Netzwerkkabel mit. In der Regel trafen sich zwischen 20 und 40 Personen. Mal in einem Industriegebiet im Aargau, mal im Grossraum Zürichs. Jeder bezahlte 5 bis 20 Franken, brachte sein eigenes Essen mit – und spielte dann «Counterstrike» und «Quake». Auf einer Einladung von 2002 steht: «Alkohol ist erlaubt, sollte aber mit Bedacht genossen werden.»

Es dürfte an einem dieser Treffen gewesen sein, als sich vier der «Kryptocrew»-Gruppe in einen Kleinwagen zwängten, jeder mit einem Laptop ausgerüstet. So fuhren sie durch ein Zürcher Industriegebiet und suchten nach offenen Netzwerken. «Plötzlich waren wir mit dem kompletten Netzwerk eines bekannten Schweizer Konzerns verbunden – vollständig unverschlüsselt», erinnert sich Roland Brecht. Sie hinterliessen dem Administrator eine Notiz, er solle doch das Firmennetz etwas besser schützen. Der Administrator fand diese Nachricht am nächsten Morgen auf einem der Drucker – in 1000-facher Ausführung.

Viele Grüsse von Donald Duck

Waren die Mitglieder der «Kryptocrew» Hacker? Kaum. Heute würde man von Nerds sprechen, allenfalls von Ethical Hackern oder von White Hat Hackern. Das sind Hacker ohne kriminelle Motivation, die aus eigenem Antrieb bei Behörden nach Schwachstellen suchen oder für Firmen Sicherheitstest durchführen (sogenannte

Penetrationtests oder Pentests). Damals waren es schlicht Computerfreaks oder Angefressene. Roland Brecht sagt: «Wir waren eine Art Boy Group des frühen Internets.» Es entstanden Freundschaften, bis heute stehen die meisten der Gruppe in losem Kontakt miteinander. «Wir waren eine coole Truppe», meint Brecht. Der Thrill war da, sie suchten nach Lücken, fanden sie und informierten die Betroffenen. An ein Dankeschön von Firmen, die sie auf Schwachstellen hingewiesen haben, können sich beide nicht erinnern.

Heute sagt Ralph B., er habe sich immer zum Ziel gesetzt, in eine amerikanische Behörde einzudringen, um dann mit seinen elektronischen Spähversuchen aufzuhören. Roland Brecht erinnert sich gut, wie er mit seinem Kumpel auf dem Weg nach Berlin war – zu einem Treffen mit Gleichgesinnten. Am Karlsruher Bahnhof hatten sie etwas Zeit und besuchten ein Internetcafé. Die beiden klickten sich durch verschiedene Behördenseiten, landeten bei einer «wichtigen nationalen amerikanischen Behörde», experimentierten und veränderten aufs Geratewohl die Internetadresse (url) und konnten plötzlich wider Erwarten eine ungeschützte Unterseite öffnen. Sie landeten in einem behördeninternen Verzeichnis hochrangiger Mitarbeiter – mit unzähligen Privatadressen, Telefonnummern und weiteren Informationen. Auch hier hinterliessen die beiden dem Administrator eine Nachricht. Wie genau sie lautete, wissen die beiden nicht mehr. In einem anderen Fall schrieben sie dem Administrator: «Viele Grüsse von Donald Duck».

Um 2003 oder 2004 war die «Kryptocrew» am Ende. Mehrere Mitglieder der Gruppe hatten inzwischen eine

eigene Familie, die Zeit abends vor dem Bildschirm war vorbei. Zudem hatte sich Google als Suchmaschine durchgesetzt und die Informationsseite der IT-Freaks erübrigte sich mehr und mehr. Einige der Gruppe etablierten sich zudem hauptberuflich im Bereich der Security Research, so auch Ralph B. Er ist Partner einer Firma, die längst zu den führenden Schweizer Anbietern von Cybersecurity-Dienstleistungen gehört. Noch bis vor einem Jahr betrieb er nebenbei eine eigene Informationsseite zu IT-Sicherheitsthemen – optisch aufgebaut wie die Verzeichnisse der 1990er-Jahre.

Gruppen wie die «Kryptocrew» gab es überall auf der Welt. Von lokalen Vereinigungen Gleichgesinnter bis zu international agierenden Netzwerken, meist ohne kommerziellen Hintergrund. Die wohl bekannteste und grösste Hackervereinigung dürfte der Chaos Computer Club (CCC) sein. Die Anfänge gehen in der Schweiz zurück auf Ende der 1980er-Jahre. Im Raum Basel treffen sich Interessierte etwa seit dem Jahr 2000. In Zürich besteht seit 2005 ein Verein. Seit einigen Jahren treffen sich Mitglieder des Chaos Computer Clubs auch in Bern und St. Gallen. Zusammengeschlossen haben sich diese lokalen Treffs im Chaos Computer Club Schweiz.

Heute sieht sich der CCC als Anlaufstelle der alternativen IT-Szene. Die Exponenten setzen sich ein gegen Vorratsdatenspeicherung, Zensur, Kontrolle im Netz und für andere gesellschaftliche Fragen im digitalen Raum. Ein zentrales Anliegen des CCC: die Förderung der Kryptografie als Mittel zur digitalen Selbstverteidigung. Sein Kredo: öffentliche Daten nützen, private Daten

schützen – und grundsätzlich allen Autoritäten misstrauen. Von sich reden machte der Chaos Computer Club unter anderem bei der Diskussion um biometrische Ausweise oder das Sicherheitsprojekt der Postcard von Postfinance. Die Exponenten wiesen auf technologische Gefahren hin und legten bei der Schweizer Debitkarte auch Sicherheitslücken offen.[1]

In Deutschland dürfte der Chaos Computer Club mit rund 8000 Mitgliedern die grösste Hackervereinigung in Europa bilden. Seit 1984 organisiert der CCC Deutschland jährlich den Chaos Communication Congress. Exponenten des CCC haben sich einen Namen gemacht mit Expertengutachten, Vorträgen und Demonstrationen, mit denen sie soziale Auswirkungen technischer Entwicklungen offenlegen. Immer wieder tritt der CCC Deutschland öffentlichkeitswirksam in Erscheinung. So etwa wenn es um technische Fragwürdigkeiten geht bei Wahlcomputern oder die staatliche Überwachungssoftware (Staatstrojaner).

Letztes Jahr legte eine CCC-Aktivistin Schwachstellen der Wahlkampf-Kommunikations-App der CDU offen. Ungeschützt und frei übers Netz zugänglich waren die persönlichen Daten von 18 500 Wahlkampfhelferinnen und Wahlkampfhelfern, dazu persönliche Daten von 1350 Parteiunterstützern sowie eine halbe Million Datensätze über politische Einstellungen. Die ehrenamtliche Sicherheitsforscherin meldete die Panne der CDU und den zuständigen staatlichen Stellen. Die Partei schaltete die App ab und reichte gegen die Aktivistin eine Strafanzeige ein.[2]

Den Begriff Hacker verwenden bis heute sowohl Exponenten, die sich dem Ethical Hacking verschrieben haben, als auch IT-Sicherheitsfachleute. In der Bevölkerung verbindet man hingegen mit dem Begriff primär eine kriminelle Tätigkeit. Die kriminelle Motivation reicht bis in die Anfänge des Internets zurück. Einer der ersten kriminellen Hacker war der Amerikaner Bill Landreth, der Anfang der 1980er-Jahre als Teenager unter dem Begriff «cracking» einen Club mit dem Namen The Inner Circle anführte. 1984 wurde er als gerademal 20-Jähriger verurteilt, weil er verschiedene Computersysteme gehackt hatte. Unter anderem griff er auf Daten der NASA und des Departement of Defense zu.

Von «Brian» über «Aids-Trojaner» zu «Melissa»

Als die erste unkontrolliert verbreitete Schadsoftware (sogenannte Malware) für das damals häufigste Betriebssystem MS-DOS gilt das Virus «Brian». Das war im September 1986. Das Virus infizierte nicht die Festplatte, sondern sogenannte Boot-Sektoren der damals gebräuchlichen Floppy-Disk. Diese Sektoren wurden vom Virus als defekt bezeichnet und konnten folglich nicht mehr überschrieben werden. So wurde das Laufwerk langsamer oder die Floppy-Disks wurden unbrauchbar. Die beiden pakistanischen Brüder Amjad und Basit Farouk Alvi beteuerten später in einem Interview mit dem finnischen Security-Spezialisten Mikko Hyppönen, «Brain» sei «ein sehr freundliches Virus» gewesen. «Als wir das Virus schrieben, hatten wir keine Absicht, irgendetwas zu