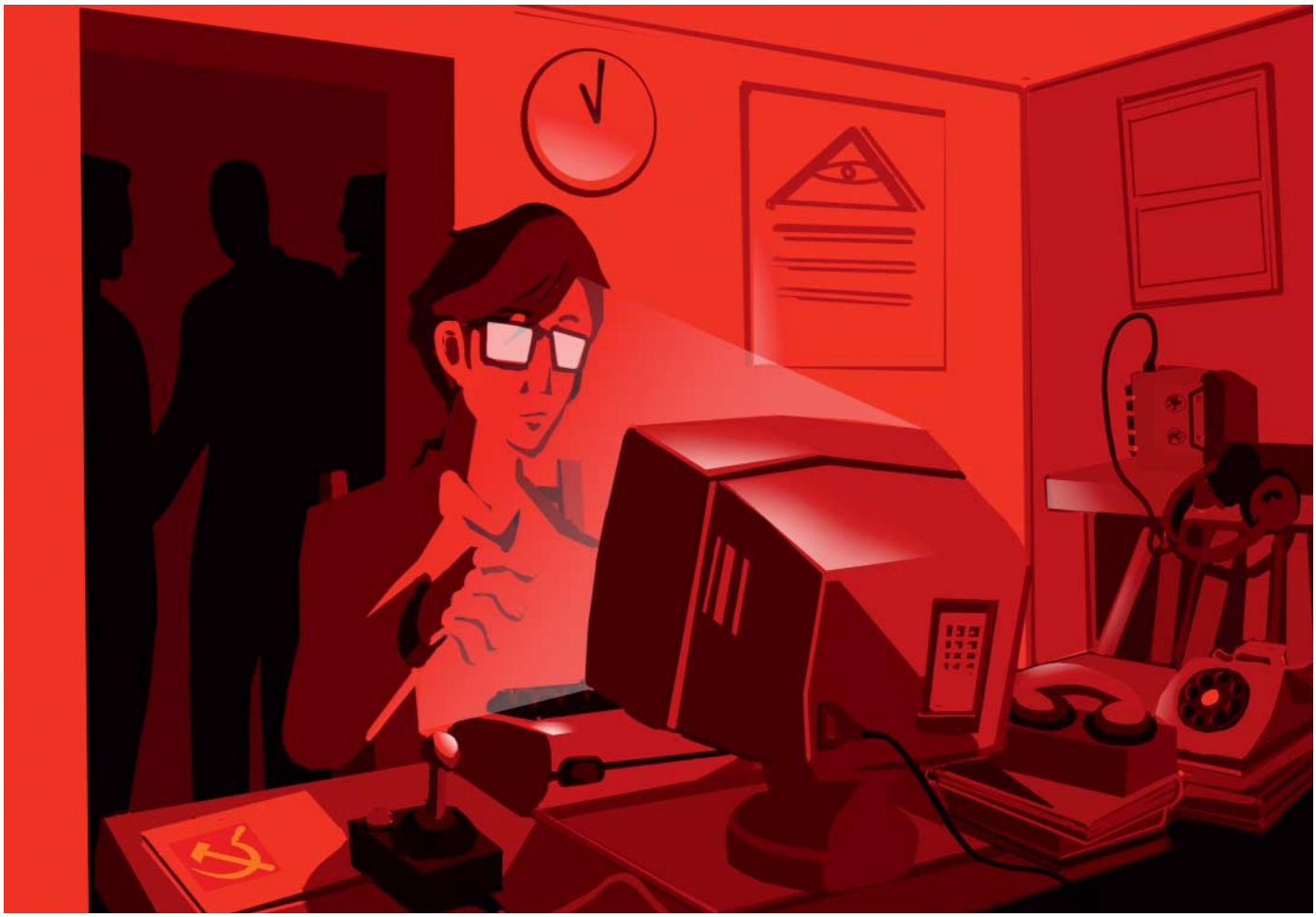

Bild: Thorsten Hübner

Der KGB-Hack

Wie Ende der 80er-Jahre fünf deutsche Hacker in die Mühlen der Geheimdienste gerieten

Pengo, Pedro, Urmel, DOB und Hagbard Celine – diese Pseudonyme stehen für die wohl kurioseste Hacker-Geschichte kurz vor dem Ende der alten BRD. Die Gruppe um Karl Koch drang in internationale Rechnernetze ein und verkaufte raubkopierte Software an den russischen Geheimdienst. Zum Verhängnis wurde ihr eine riesige Datei, die angeblich Details zur SDI-Raketenabwehr der USA enthalten sollte.

Von Detlef Borchers

Als der Einbruch 1989 aufflog und die „KGB-Hacker“ enttarnt wurden, waren die Schlagzeilen riesig: „Per Heimcomputer tausende Daten an den sowjetischen Geheimdienst“, titelte eine Zeitung. „Computerfreaks haben dem sowjetischen Geheimdienst KGB das Einbruchswerkzeug für westliche Datennetze verschafft“, erklärte eine andere. Der Boulevard setzte noch einen drauf: „SDI verraten – sind wir jetzt schutzlos?“ SDI, das war die Strategic Defense Initiative von US-Präsident Ronald Reagan aus dem Jahre 1983, die Idee, einen Raketenschutz gegen die russische Bedrohung aufzuspannen. Von dieser Idee existierte zwar nur ein Plan, aber genau dieser sollte als Datei namens SDInet.doc dank der Hacker in russische Hände gelangt sein.

Wie der Btx-Hack (S. 66) war auch der KGB-Hack ein Medienereignis ganz besonderer Art. Dafür sorgte vor allem ein „Brennpunkt“ des NDR in der ARD, der noch am selben Abend nach einer großen Polizeiaktion gegen vier der KGB-Hacker und vierzehn mögliche Unterstützer am 2. März 1989 ausgestrahlt wurde. (Der fünfte war tags zuvor am Flughafen auf dem Weg nach Spanien verhaftet worden.) In der lange zuvor von zwei Journalisten-Teams vorbereiteten Sendung sprach Moderator Jochen Wagner vom „größten Spionagefall seit Guillaume“. Beim Zuschauer erweckte man den Eindruck, das höchst geheime

militärische Computer geknackt und deren Software an den russischen Geheimdienst verkauft worden sei. Der mit tatkräftiger Hilfe des Bundesamtes für Verfassungsschutz aufgebauschte Bericht wurde später von Wagner damit gerechtfertigt, dass die Bevölkerung für die neue Spionageform sensibilisiert werden sollte.

Tod eines Hackers

Der Sensationsbericht führte nicht nur zu den eingangs zitierten Schlagzeilen, sondern auch zu einem Auflauf von aufdringlichen Journalisten, die es vor allem auf Karl Koch alias „Hagbard Celine“ abgesehen hatten, den angeblichen genialen Kopf der Hackerbande. Er war nach der Polizeiaktion schnell wieder auf freiem Fuße und hatte eine Stelle als Kurierfahrer und Kopier-Aushilfe bei der CDU vermittelt bekommen, was die SPD im laufenden Wahlkampf weidlich ausnutzte: „KGB-Hacker in der CDU-Zentrale“.

Was der Öffentlichkeit nicht bekannt war: Karl Koch war schwer drogenabhängig, nahm eine Menge an Psychopharmaka und litt unter einer schweren Psychose. Dies wusste neben seinen Freunden nur das in dem KGB-Fall ermittelnde Bundeskriminalamt, das jedoch ein herausragendes Interesse daran hatte, ihn weiterhin für vernehmungsfähig erklären zu lassen. Einige Wochen nach der Ausstrahlung schalteten die BKA-Beamten im April 1989 vom bis dahin nüchternen Ton bei seinen Vernehmungen in einen Drohmodus.

Weiterhin von Journalisten umlagert, ließ sich Karl Koch auf allerlei Handlungen ein, posierte mit Laptop und Akustikkoppler in einer Telefonzelle. Das so verdiente Honorar wurde in Drogen umgesetzt. Dem Agenturjournalisten Jochen Sperber erzählte er zuletzt, dass Außerirdische und Illuminaten seine Gedanken lesen und beeinflussen.

Anfang Juni 1989 wird seine verkohlte Leiche neben seinem Kurierwagen gefunden. Die Obduktion ergab, dass Karl Koch am 23. oder 24. Mai starb. „Alle großen Anarchisten starben an einem 23.“, soll Karl Koch in Anspielung auf die Illuminatus!-Triologie von Robert Anton Wilson und Robert Shea gesagt haben. Aus diesem Werk über Verschwörungstheorien und über die Zahl 23 stammte sein Hacker-Name Hagbard Celine.

Die SDI-Falle

Die Polizeiaktion im März 1989 hatte ein Vorspiel. Am 27. Juni 1987 durchsuchten Polizeibeamte in Hannover die Wohnung des Programmierers Markus Hess alias „Urmel“ sowie die Firmenräume der Focus Computer GmbH. Zwei Beamte des Bundeskriminalamtes sowie vier IT-Spezialisten und ein Staatsanwalt aus Bremen waren bei der Aktion zugegen und suchten nach Beweismaterial für einen „Computerbetrug“. Als Firmeninhaber Udo Flohr die Beamten fragte, was sie denn genau suchten, war die Ratlosigkeit groß. Mehr als den Hinweis auf eine Beschriftung namens SDInet hatten die Fahnder vom US-amerikanischen FBI nicht übermittelt bekommen. Diese irgendwo gespeicherte Datei sollten sie irgendwie finden.

Doch die berüchtigte SDI-Datei war von vorne bis hinten ein kompletter Fake: Sie war eine ziemlich große Datei, die vom US-amerikanischen Admin Clifford Stoll aus allen möglichen Unterlagen zusammenkopiert worden war. Stoll war im Lawrence Berkeley Institute über einen Fehler bei der Berechnung von Computernutzungszeiten gestolpert und kam so Hackern auf die Spur, die sich in „seinem“ Rechner aufhielten. Der oder die Hacker nutzten mehrere US-Datennetze und Rechner, ließen sich aber bis nach Europa zurückverfolgen. Dort, an der Universität Bremen, verloren sich die Spuren.

Hier kam SDInet ins Spiel. Der einzige Zweck von SDInet war ihrer schiere Größe. Sie war ein früher Honeypot – Stoll nannte sie sein „Kuckucksei“: Ein Download der Datei sollte so lange dauern, dass die Universität Bremen im Verbund mit der Deutschen Bundespost und des Bundeskriminalamtes feststellen konnte, wer eigentlich derjenige war, der in US-amerikanischen Netzen via Datex-P herumschnüffelte.

Die Spur führte zu Markus Hess, der sich über eine in Hannover identifizierbare NUI-Nummer (Network User Identification) einwählte. Die Spur brachte aber zunächst wenig Klarheit, da keine Beweise gefunden wurden. Die Szenerie erinnert ein bisschen an die Situation der Soldatin Chelsea Manning, die während ihrer Stationierung im Irak eine CD mit Videosequenzen brannte und einfach „Lady Gagas new songs“ draufschrieb. „Verbrechen der US-Armee“ wäre korrekter gewesen, hätte aber kaum die US-Basis verlassen können.

In die Pleite getrieben

Für die Firma Focus Computer, die Hess beschäftigte, ging die Sache freilich weniger gut aus. Das FBI warnte US-amerikanische Computerfirmen vor der Hannoveraner Firma, die DFÜ-Programme (Daten-Fern-Übertragung) so umbaute, dass sie den FTZ genannten Segen (FernmeldeTechnischeZulassung) der Bundespost bekamen, in ihrem geheiligten Netz zu arbeiten. „Markus Hess war dafür sicherheitsüberprüft worden und derjenige unserer Entwicklung, der im Telekom-Labor ein- und ausgehen durfte“, erinnert

Bild: Claussen & Wöbke

Der Film „23 – Nichts ist so wie es scheint“ von 1998 erzählt die Geschichte von Karl Koch (2. von rechts). Im Film wurden die Namen seiner Mitstreiter geändert: Aus „Pengo“ wurde David (2. von links) und aus „Pedro“ wurde Pepe (rechts), der das Treffen mit dem KGB in Berlin einfädelte.

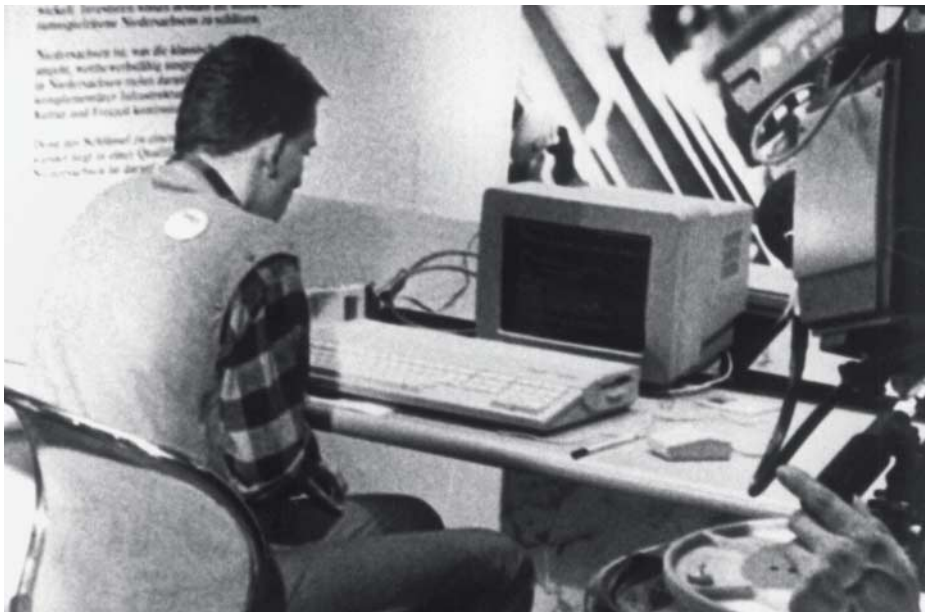

Bild: PictureAlliance/dpa

Eines der wenigen Bilder von Karl Koch. Der Hacker ließ sich auf der CeBIT 1986 nur von hinten fotografiieren.

sich Udo Flohr heute. Focus Computer verlor viele wichtige Aufträge der Forschungs- und Entwicklungsabteilung des Postministeriums und ging Anfang der 90er pleite.

Im August 1988 veröffentlichte der Chaos Computer Club das Chaos Computer Buch, in dem über die via Datex-P betriebenen Datenreisen deutscher Hacker zu Computern in der Schweiz, in den USA und Asien berichtet wurde. Leicht überheblich wurde da die Polizeiaktion in Hannover bewertet: „In der deutschen Hackerszene hat sich Dr. Clifford Stoll einen verhältnismäßig guten Ruf erworben. Hacker sind auch gute Verlierer und vereinzelt werden Stimmen laut, ‚den Stoll' zum nächsten Hackerkongress nach Hamburg einzuladen."

Mit im Buch der guten Verlierer: ein Text über die Tricks, wie Hacker auf VAX-Rechnern eindringen und sich Root-Rechte als Systemverwalter besorgen können sowie ein Bericht „Welcome to the NASA-Headquarter". Dieser Text beschrieb ausführlich, wie sich „VAXbuster" in zwei Rechner der Raumfahrtbehörde NASA einnisten und trojanische Pferde installieren konnten.

Ziel des lustig geschriebenen Textes war es, das Hacken der Jugendlichen zu entkriminalisieren. Denn im August 1986 war das „Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität" in Kraft getreten, welches den mit einer Freiheitsstrafe von drei Jahre bestrafte, der Daten, „die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft".

Die wahre Geschichte

Zurück nach Hannover. 1983 begann Karl Koch, sich für Computer zu interessieren. Zunächst nur als Arbeitsmittel, dann – bereits unter dem Einfluss von „Illuminatus!" und dem regelmäßigen Konsum von Speed und LSD – als Machtmittel. Mit Freunden gründete er einen Hackerstammtisch „als Ableger vom Chaos Computer Club", wie er in seinem Lebenslauf schrieb. Über den Stammtisch lernte er Markus Hess kennen, außerdem den Berliner Hans Heinrich Hübner, der unter dem Handle „Pengo" unterwegs war und als Spezialist für VAX-Rechner der Firma Digital Equipment (DEC) galt. Der Älteste in diesem Kreis war Dirk-Otto Brezinski alias „DOB", ein in Berlin lebender Hannoveraner, der als Spezialist für Siemens-Großrechner-Notfälle viel Geld verdiente. Er wurde für den stets klammen Koch der wichtigste Geld- und Drogengeber.

Auf der CeBIT zeigte Karl Koch im März 1986 öffentlich die Hohe Schule des Hackens an einem Atari. „Im gleißenden Scheinwerferlicht unter den Augen von Fernsehkameras demonstrierte ‚Hagbard Celine' das, was er sonst mit seinen Freunden in verschwiegenen Hinterzimmern treibt. Er drang mit einem Homecomputer in einen fremden Großrechner ein und besichtigte die Datenbestände der US-amerikanischen Caltec-University. „Der eigentlich publizitätsscheue 20-jährige Schüler gehört mit ‚Pengo' (17) und dem Kälteanlagenbauer ‚Kugelfisch' zu Hannovers eifrigsten Hackern", schreibt die Hannoversche Neue Presse zum spektakulären Auftritt. Er sollte zeigen, wie harmlos die „Computer-Freaks" beim Ausüben ihres Hobbys der Datenreise durch fremde Systeme doch waren.

Kontakte zu den Sowjets

Ganz so harmlos blieb die Sache freilich nicht, denn noch auf der CeBIT wurde Karl Koch von zwei Holländern angesprochen, die ihm satte Honorare in Aussicht stellten, wenn er sich gezielt in von ihnen genannte Rechner einloggen und dort Dateien kopieren würde. Als er diese Geschichte am Hackerstammtisch erzählt, ist das Gelächter groß, doch wurde die Idee geäußert, dass das gesammelte Material von Datenreisen in all diesen US-Computern wohl für den sowjetischen Geheimdienst KGB von Interesse wäre. „Ich glaube, es waren DOB und sein Freund Pedro, die die Idee hatten, das Projekt ‚Equalizer' zu nennen", erinnert sich Hans Heinrich Hübner heute. Inmitten der von Gorbatschow eingeleiteten „Perestroika" für Ausgleich im Ost-West-Gefälle bei der Mikroelektronik zu sorgen, das hatte was. „Meine Idee war eher so: Hacken ist in Deutschland gefährlich, da müssen wir einen sicheren Arbeitsplatz haben, da in Ostberlin. Das war jedenfalls meine Motivation", erzählt Hübner.

Der von Hübner im Gespräch erwähnte „Pedro", bürgerlich Peter Carl, war ein ehemaliger Croupier und Gelegenheitsarbeiter, der wegen seines Drogenbedarfs ähnlich wie Karl Koch stets in Geldnöten war. Anfang September 1986 setzte Carl die eher scherzhaft geäußerte Idee um. Er warf sich in Schale, fuhr nach Berlin und marschierte direkt in die sowjetische Botschaft.

Hübner erinnert sich: „Pedro kam dann eines Tages an und erzählte, dass er drüben gewesen war und mit den Russen gesprochen hatte und die nur Software wollten. Die haben ihm 'ne Liste gegeben, was sie wollten, zum Beispiel den Cobol-Compiler Version 3.1 für die VAX. Die von der sowjetischen Handelsmission sahen in uns vor allem eine Quelle für Raubkopien. Du konntest ja damals keinen VAX-Compiler im Laden kaufen." Auf der Liste standen die Betriebssysteme Unix, VM

und VMS sowie diverse Compiler, aber auch allgemeine Angaben wie CAD/CAM, Ashton Tate oder Borland. „Das lief dann so ab, das Pedro seine Spezis abklapperte, was sie so haben und dann ist er nach Ostberlin zu Sergej“, erinnert sich Hübner. Unix wurde so aus der Firma „rüberkopiert“, in der Markus Hess arbeitete, mit HILO 2 von Genrad wanderte ein Optimierungsprogramm für das Chip-Design in den Ostblock.

„Wir wollten schon zeigen, dass wir auch was können. So hab ich mal aus den internen Rechnern von DEC selbst ‚Securepack‘, ein Shellskript runtergeladen, das hatte mir ein Freund aus Hamburg, der Obelix, dann auf Tape gezogen“, so Hübner. Einmal fuhr er mit, genoss den unbehelligten Grenzübertritt und das Kiffen auf dem Alexanderplatz, ehe es in die Leipziger Straße zu Sergej ging. Sergej zahlte jedes Mal in bar mit Hundertern. Für Unix gab es den größten Batzen, 25.000 DM, für Securepack immerhin noch 3000 DM. Dazu kam eine Besuchspauschale von 600 DM. Insgesamt kamen so 90.000 DM zusammen, von denen Pedro als Kurier die Hälfte für sich behielt, ehe er die Scheine verteilte.

Raubkopien für Putin

Nun war die Zeit, in der die westdeutschen Hacker Ostberlin aufsuchten, auch genau die Zeit des „großen Sprunges“ in der DDR. In der Mikroelektronik wollte man gegenüber dem Westen aufholen und die so entwickelten Produkte in die Ostblock-Staaten verkaufen, die unter dem CoCom-Embargo der NATO standen: eine VAX, auf der sich die Hacker amüsierten, durfte nicht in den Ostblock verkauft werden, bei Speicherbausteinen war bei 256 KB DRAM Schluss. 120 Millionen Valutamark (sprich DM) standen für die Aufholjagd zur Verfügung, in der die DDR-Lenker 1986 zwei große Ziele formulierten. So sollte das Kombinat Robotron die K1840 entwickeln, eine 1:1-Kopie der VAX 11/780 von DEC.

Erste Modelle wurden bereits 1987 ausgeliefert, die offizielle Präsentation war auf der Frühjahrsmesse Leipzig 1988. Passend dazu wurde die Entwicklung eines eigenen Megabit-DRAM-Chips vorangetrieben, wie er in der K1840 benötigt wurde. Die ersten Exemplare dieses Chips wurden im September 1988 dem Staatslenker Erich Honecker übergeben, der sie wiederum dem russischen Staatslenker Gorbatschow als Beweis für die Überlegenheit der DDR gegenüber der Perestroika überreichte (siehe Seite 53).

Vieles spricht dafür, dass die Listen, die den jungen Hackern gegeben wurden, genau den Software-Wünschen entsprachen, die zur Aufholjagd benötigt wurden. So unterhielt Karl Nendel, der „General der Mikroelektronik“ der DDR in Moskau ein eigenes Büro zur Koordinierung der Entwicklungsarbeiten. Leider sind die Dokumente des KGB derzeit für Historiker noch nicht einsehbar, was damit zu tun haben könnte, dass der damals für Robotron zuständige KGB-Agent in Deutschland ein gewisser Wladimir Putin war.

Bild: PictureAlliance/dpa

Markus Hess, alias „Urmel“, war der fünfte Hacker im Bunde. Er arbeitete später für ein Tochter-Unternehmen des Heise Verlages.

Es gibt jedoch Indizien: Als Ende 1987 eine K1840 mitsamt Betriebssystem und Compilern nach Brasilien verkauft wurde, wütete Karl Nendel darüber, dass der Quellcode der ausgelieferten Software in der Eile nicht ausreichend genug „neutralisiert“ worden war und ihr Ursprung erkannt werden konnte: Etliche Code-Passagen enthielten Hinweise auf DEC.

„Revolver-Karl“ Nendel (so sein Spitzname) forderte eine „tiefgründige sicherheitspolitische Auswertung dieses leichtsinnigen Verrats“. Dazu kam es nicht mehr, denn die DDR brach zusammen.

Hübner alias Pengo war der erste, der sich bereits Anfang 1987 abgeseilt hatte. Übrig blieb allein Markus Hess alias Urmel, der über das erste Halbjahr 1987 die sowjetische Handelsmission belieferte – die anderen drei besaßen nicht die Fähigkeiten oder wollten wie Dirk-Otto Brezinski aus Prinzip nicht hacken. Es war die seltsame Datei SDInet, durch die die Sache schließlich aufflog.

Die Fahndung läuft

Doch auch nach den Hannoveraner Hausdurchsuchungen bei Hess und Fun Computer blieb es ruhig um die Hacker. Die Situation änderte sich schlagartig, als im April 1988 in der Zeitschrift „Quick“ ein Artikel über die Detektivarbeit von Clifford Stoll erschient. Dieser schilderte reißerisch die „Jagd auf die deutschen Hacker, die das Pentagon knackten“. Jetzt war man interessiert, mehr über die deutschen Hacker zu erfahren, die durch die Datennetze zu US-amerikanischen Computern reisten, ins Pentagon eindrangen und Militärgeheimnisse entführten.

Am 5. Juli 1988 stellte sich Karl Koch, am 20. Juli Hans Heinrich Hübner dem Bundesamt für Verfassungsschutz (BfV), beide jeweils von Anwälten begleitet. Sie folgten damit einer Empfehlung des Chaos Computer Clubs, der anlässlich der NASA-Hacks im August und September 1987 zwischen den Hackern und dem BfV vermittelte. Nach der Befragung der beiden gab das BfV die Ermittlungen an das Bundeskriminalamt weiter. Während der BfV eine Opportunitätsbehörde ist, die Ermittlungen nach eigenem Ermessen einstellen kann, arbeitet das BKA nach dem Legalitätsprinzip und ist verpflichtet, registrierte Straftaten zu verfolgen. Peter Carl, Dirk-Otto Brezinski und Markus Hess wurden verhaftet, dutzende von Wohnungen untersucht – und in der ARD lief parallel der Sensations-Brennpunkt.

Bild: Acme Klein Bottle

Clifford Stoll stellte den Hackern damals die entscheidende Falle. Heute verkauft er über Acme Klein Bottle wundersame Flaschen im Internet.

Nachsichtige Richter

Bis zu ihrem Prozess vor dem Staatsschutzsenat in Celle mussten Carl und Brezinski die Zeit in Untersuchungshaft verbringen, während Markus Hess dank günstiger Sozialprognose bald die Haft verlassen konnte: Er hatte eine Stelle als Programmierer bei der CosmoNet GmbH angetreten, einer damaligen Tochterfirma des Heise Verlages.

Mit dem Tod von Karl Koch war Hans Heinrich Hübner zum einem der wichtigsten Zeugen im Prozess gegen die drei verbleibenden KGB-Hacker geworden. Der andere war Clifford Stoll, dessen Buch „Kuckucksei“ Prozesslektüre wurde. In der Befragung durch den vorsitzenden Richter Leopold Spiller machte Stoll deutlich, dass die hoch geheime Datei SDInet nichts weiter war als ein Sammelsurium willkürlich zusammenkopierter Dokumente mit erfundenen militärischen Namen. Auf Nachfragen von Spiller konnte keine Softwarefirma genannt werden, die einen erlittenen Schaden geltend machte.

Nach zwölf Verhandlungstagen erging das Urteil: Peter Carl erhielt eine zweijährige Freiheitsstrafe, Markus Hess bekam ein Jahr und acht Monate, Dirk-Otto Brezinski ein Jahr und zwei Monate. Alle Strafen wurden zur Bewährung ausgesetzt und von den 90.000 DM mussten 18.000 an die Staatskasse gezahlt werden: Aus der Tatsache, dass die Hacker statt der gewünschten Million nur 90.000 bekamen, schloss das Gericht, dass die Sowjetunion das Material nicht zu nutzen wusste: „Viel Wertvolles kann in den Lieferungen an den KGB-Agenten Sergej in Ost-Berlin nicht gewesen sein“, meinte Richter Spiller zum Schluss. Die Angeklagten nahmen das Urteil erleichtert an.

Epilog

Als die Bombe platzte, war der Schock beim Chaos Computer Club groß. Wau Holland, damals der CCC-Übervater, veröffentlichte in der „tageszeitung“ einen Artikel, dass Hacker von Natur aus nicht mit Geheimdiensten zusammenarbeiten würden. Es widerspreche der Hackerethik, Daten an Agenten zu verkaufen – daher seien die KGB-Hacker eben keine Hacker. Als moralische Leitplanke würde vielmehr gelten „Hände weg von Militär und Geheimdiensten“.

Pragmatischer äußerte sich Steffen Wernéry, damals Vorsitzender des CCC auf einer Gedenkveranstaltung für Karl Koch im Jahre 2014: „Im Grunde genommen war mir klar, dass so etwas früher oder später passieren würde.“ Auf eben jener Veranstaltung schilderte Andy-Müller Maguhn, wie der CCC damals nah dran war, sich aufzulösen, und der Club gegen eine Panik ankämpfen musste: „Dass einige diese Deals machten, das war schon kritisch, da gab es auf mehreren Ebenen Vertrauensprobleme. Die Abgrenzung zwischen dem harmlosen NASA-Hack und diesem KGB-Team fiel nicht nur uns, sondern auch dem BKA schwer. Und dann die gegenseitigen Verdächtigungen. Einige sind da dann aus dem CCC ausgetreten.“ Insgesamt verlief die Sache aber glimpflich. „Damals passierte so viel, nicht nur in der DDR. Wir hatten dann nach der Barschel-Affäre die Medienhoheit wieder.“ *(hag@ct.de)* c't

Literatur

[1] CCC und Jürgen Wieckmann (Hrsg.): Das Chaos Computer Buch, August 1988

[2] Thomas Amann, Matthias Lehnhardt, Gerd Meißner, Stephan Stahl: Hacker für Moskau, Juni 1989

[3] Clifford Stoll: Das Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten. August 1989

[4] Katie Haffner, John Markoff: Cyberpunk. Outlaws and Hackers on the Computer Frontier, März 1991

[5] Hans-Christian Schmid, Michael Gutmann: 23 – Die Geschichte des Hackers Karl Koch, Januar 1999