„Er konnte an jedem Ort der Welt sitzen"

Hacker aus Hannover und Berlin spionierten für das KGB durch Dutzende amerikanischer Computer-Systeme

Was ist dran an der vom NDR verbreiteten Enthüllung, das KGB habe sich über westdeutsche Hacker Zugang zu den wichtigen Geheimnissen des Westens verschafft? Aller Wahrscheinlichkeit nach nicht viel. Aber die Geschichte der Hacker, ihrer Auftraggeber und ihrer Entdecker verrät dennoch eine „neue Qualität" gegnerischer Ausspähung.

Markus Hess, 27, ist weit herumgekommen. Per Computer reiste der abgebrochene Physikstudent ins Forschungszentrum Pasadena, in die US-Army-Basis Fort Buckner nach Japan und in die texanische Rüstungsfirma Richardson. Vergangenen Donnerstag nahmen Kriminalbeamte den hannoverschen Computerexperten wegen des Verdachts der geheimdienstlichen Agententätigkeit fest.

Hess ist eine der Zentralfiguren im „größten Spionagefall seit Guillaume", wie die ARD am Donnerstag in einer Fernseh-Sondersendung behauptete. Der Hacker aus Hannover soll mit zwei weiteren Computerfreaks und mit Hilfe von zwei Mittelsmännern Computerdaten aus internationalen Zentren gezapft und an den sowjetischen Geheimdienst KGB verkauft haben.

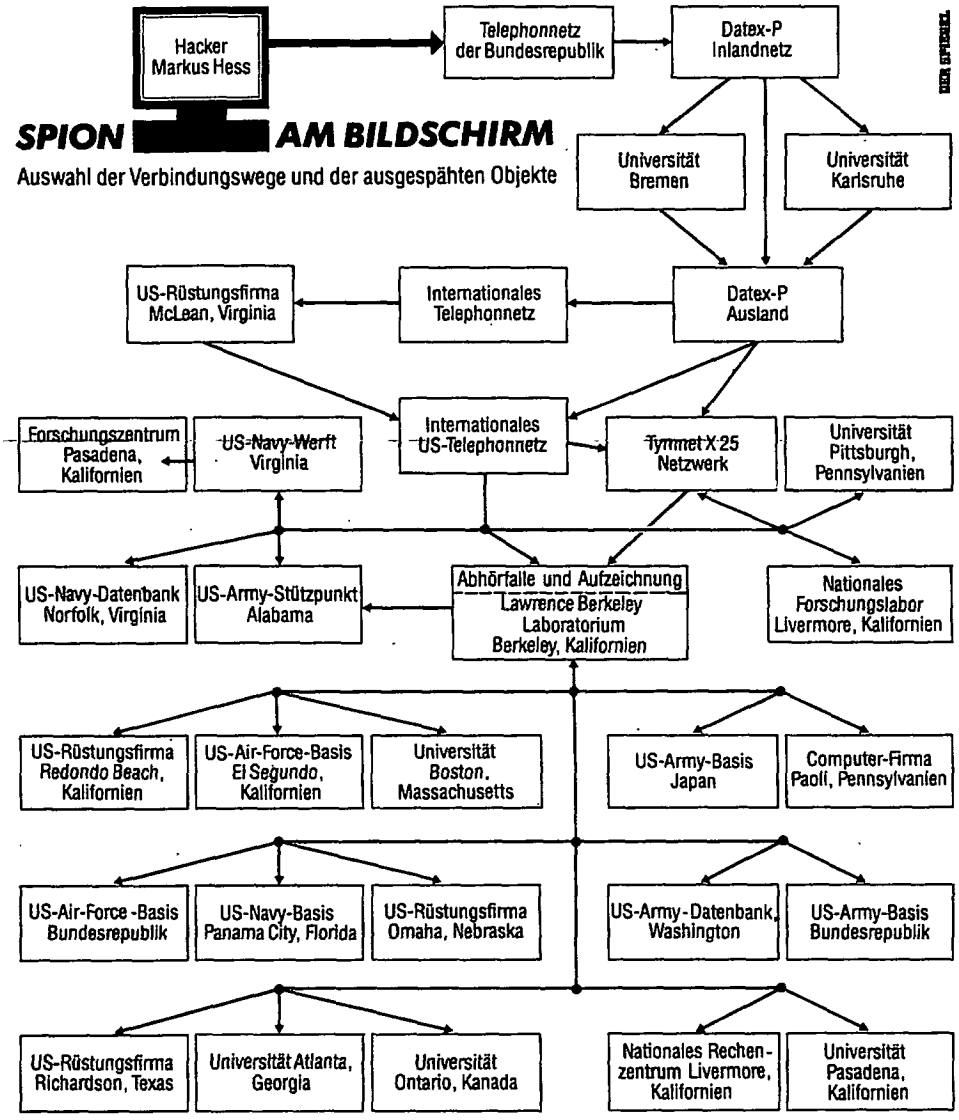
Die aufregende Geschichte sorgte vergangenen Freitag bei den bundesdeutschen Behörden für deutliche Verwirrung. Während Innenminister Friedrich Zimmermann den Sieg über einen „international operierenden Computer-Spionagering" feierte und der Verfassungsschutzpräsident Gerhard Boeden eine „neue Qualität gegnerischer Ausspähung" sah, bemaßen andere Sicherheitsstrategen den Schaden als eher gering.

Im Bonner Justizministerium fand ein führender Beamter, daß Zimmermann und Boeden die Sache „ein bißchen hochgeblasen hätten". Der Generalbundesanwalt Kurt Rebmann monierte eine „vorschnelle Schadensbewertung".

In Wahrheit konnten die bundesdeutschen Sicherheitsexperten vergangene Woche verläßlich lediglich sagen, daß „die Zeit der toten Briefkästen zu Ende" gehe. Mit der Vernetzung der internationalen Datenbanken gibt es für Spione ein neues Berufsbild.

Was aber die Hacker aus Hannover und Berlin gen Osten geschafft hatten, wußte niemand genau zu sagen.

Markus Hess war von seinem Computer in Hannover aus in das Lawrence Berkeley Laboratory (LBL) in Kalifornien gelangt. Von dort, so hieß es in der ARD-Sendung, habe Hacker Hess (ARD-Deckname: Speer) „seine ausgedehnten Raubzüge durch die verschiedenen Computer des amerikanischen Militärs und der Rüstungsindustrie" unternommen. Mit dem aus Westdeutschland gelieferten Material könnten sich nun die Sowjets „in die wichtigsten Großrechner in Japan, Europa und den USA einwählen". Und vor allem bei der Industrie-Spionage hätte es wertvolle Dienste geleistet.



Bei den meisten der in der langen Liste von angezapften Institutionen aufgeführten Adressen handelt es sich um wissenschaftliche Institute und Forschungseinrichtungen, vom Hamburger Elektronen-Synchrotron Desy, dem Europäischen Kernforschungszentrum Cern bis hin zur US-Raumfahrtbehörde Nasa und dem Jet Propulsion Laboratory in Pasadena (Kalifornien).

In all diesen Institutionen ist aber für östliche Geheimdienste kaum etwas zu holen. Institute wie Desy oder das (gleichfalls erwähnte) Max-Planck-Institut für Kernphysik in Heidelberg beherbergen regelmäßig sowjetische Wissenschaftler als Gäste. Dem offenen Austausch der gewonnenen wissenschaftlichen Erkenntnisse dient nicht nur die jeweilige internationale Fachpresse; ihm dienen auch die Datennetze selbst – die Verknüpfungen der Institute sind gerade *für* den Informationsaustausch geschaffen worden.

„Ich wüßte nicht, woran die Hacker bei uns interessiert sein könnten", erklärte denn auch am Freitag letzter Woche Volker Soergel, Vorsitzender des Desy-Direktoriums. „Wir haben auf diesem Sektor keine Geheimnisse."

Institutionen wie Cern oder auch das Heidelberger Kernphysik-Institut haben definitionsgemäß gerade nicht mit militärisch relevanter Anwendung von Atomtechnik zu tun. Ihre Arbeitsgebiete

Hacker Hess: „Ungeheure Möglichkeiten"

liegen bei der Grundlagenforschung über Vorgänge im Atomkern.

Dementsprechend zögerten die Cern-Manager lange, ehe sie bei der Polizei Laut gaben – jahrelang schon hatten sich Hacker im Cern-Datennetz wie auf einer Spielwiese getummelt, ohne daß die Institutsleitung das für sicherheitsrelevant gehalten hätte. Die Anzeige bei der Polizei erfolgte nur, weil die Cern-EDV-Leute sich bei der praktischen Arbeit gestört fühlten.

Gravierender erscheint, was bei der jetzt aufgeflogenen Hacker-Connection offenbar in Richtung Wirtschaftsspionage abgelaufen ist. Das genaue Ausmaß des entstandenen Schadens ist allerdings, auch in den Augen der Fachleute, schwer abzuschätzen.

Zwei Bereiche der modernen Computertechnik, so legte der ARD-Film letzten Donnerstag nahe, seien von der Ausspähung besonders betroffen:

- „CAD/CAM" – das sind Computerprogramme, mit deren Hilfe sich die Konstruktion etwa von Flugzeugen, Werkzeugmaschinen und Automobilen beschleunigen läßt, für die Ingenieure ohne diese Computerwerkzeuge Wochen oder Monate brauchen würden.
- Chip-Architektur – die mikroskopisch feinen Schaltstränge, die auf die modernen Mikrocomputer (Chips) metallisch aufgedampft werden, müssen in ihrer dreidimensionalen Anordnung hochkomplex ausgetüftelt werden; solche Pläne sind im Computer gespeichert.

CAD/CAM-Programme sind, soweit es sich nicht um firmenspezifische Varianten, etwa eines bestimmten Flugzeug- oder Automobilkonzerns handelt, auf dem westdeutschen Computermarkt frei zu kaufen. Der Export solcher Software Richtung Osten dürfte allerdings unter die Cocom-Liste fallen.

Was ein Hacker-Spion erhaschen könnte, wäre die Software für etwa solche Konstruktionsprogramme: Wenn die Einstiegstür eines Autos breiter wird, welche Auswirkungen hat das auf die tragende Dachkonstruktion? Derartige Fragestellungen beantwortet das CAD/CAM-Programm, vielfach schon in eleganter dreidimensionaler und gar farbig angelegter Bildschirmdarstellung.

Die elektronischen Blaupausen von Chips mögen auf dem Spionagemarkt heiße Ware sein. Komplexe Chip-Architektur zu entwikkeln ist zeitaufwendig und teuer. Die Vermutung allerdings, daß ausgesprochene Spitzentechnologie, wie etwa das Baugeheimnis eines Superchips, auf dem Hacker-Wege zu erlangen sei, wird von Fachleuten bezweifelt. Beispielsweise halten die Japaner auf dem Gebiet der Hochleistungschips seit Jahren einen Vorsprung vor der amerikanischen und europäischen Konkurrenz – obwohl die Japan-Chips auch unter den Mikroskopen der Konkurrenz analysiert werden können. Damit hat der Späher noch lange nicht das Know-how über die Fertigungstechnik.

„Ganz oben auf der Wunschliste" der sowjetischen Besteller, so ARD-„Brennpunkt", hätten sogenannte Compiler und Quellcodes gestanden. C-Compiler sind Programme, mit deren Hilfe ein Computer das, was ihm der Programmierer oder Benutzer über das Tastenfeld in lesbarer Sprache eingibt, in die der Maschine verständliche Sprache übersetzt. Solche Übersetzungsprogramme sind, für die verschiedenen Computertypen, auf dem Markt frei erhältlich. Deshalb erscheint EDV-Experten nicht recht plausibel, warum die Sowjets sich eine so vergleichsweise simple Sache auf so komplizierten Wegen beschaffen sollten.

Quellcodes für Betriebssysteme freilich gehören bei jedem Computersystem zum Allerheiligsten der Software. Sie sind gleichsam die Ur-Manuskripte für das Betriebsprogramm der Rechner; in ihnen sind die gesamten Kommandos für den Arbeitsablauf des Rechners und aller angeschlossenen Geräte aufgezeichnet.

Noch bis vor zehn Jahren etwa wurden bei marktgängigen Computersystemen auch diese Quellcodes an jeden Benutzer freizügig mitgeliefert, zusammen mit dem Betriebssystem. Seither aber haben sich die meisten Hersteller entschlossen, dieses gespeicherte Betriebswissen zurückzuhalten oder zu blockieren, indem sie Teile des Quellcodes unter Verschluß halten. Doch wer möchte, kann die vollständigen Quellcodes auf dem Markt gegen entsprechenden Aufpreis kaufen.

Skeptisch sind EDV-Fachleute angesichts des von den Untersuchungsbehörden offenbar erhobenen Vorwurfs, die westdeutschen Hacker hätten hochsensible militärische Daten aus amerikanischen Netzen herausgefischt. Alle Firmen, die an von außen her zugängliche Netze angeschlossen sind, sind hochgradig vergattert, keinerlei militärisch sensible Projekte über diese Netze laufen zu lassen.

Lediglich offene Netze – wie die in den Hacker-Berichten immer wieder auftauchenden Arpanet und Milnet – bieten sich für Eindringlinge an, enthalten dafür aber auch keine hochbrisanten Daten.

Auch der „Brennpunkt"-Zeuge und Anfangsfahnder beim Fischzug gegen die Hacker aus Hannover, Astrophysiker Clifford Stoll, beließ es bei der Feststellung: „Sie haben Zugang erlangt zu nichtgeheimen Computern in

Hacker-Jäger Stoll: „Wir waren Zeugen eines Spionage-Versuchs"

Physiklabors, Militärbasen und Universitäten."

Trotz alledem waren Sicherheitsexperten vergangene Woche voller Anerkennung über „Phantasie" und „Leidenschaft" der Hacker.

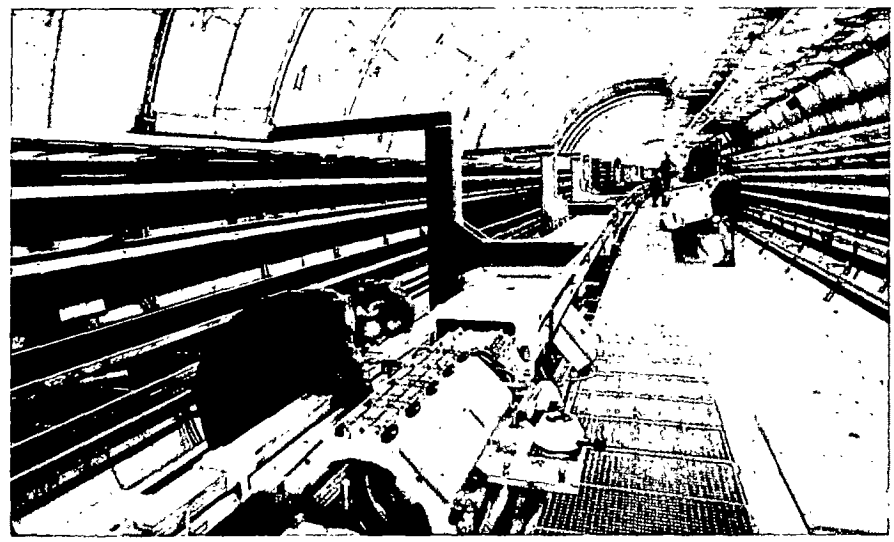
Das Geld aus Moskau war für die in Hannover und Berlin beheimateten Hacker ganz offenkundig nicht der ursprüngliche Anlaß für ihre elektronischen Weltreisen. Markus Hess und sein Hacker-Kollege Karl Koch, 23, gehören zu jener Spezies Mensch, für die die Nacht vor dem Computer „zur Sucht geworden ist", wie ein Verfassungsschützer sagt.

Auf regelmäßigen Hacker-Partys, die oft bei Koch in der Wohnung stiegen, kam eine Handvoll Freaks zusammen, versammelte sich um den Bildschirm und fing an zu tüfteln. Vom späten Nachmittag an, die Nacht hindurch bis in den frühen Morgen knobelten die Hacker Wege aus, die in fremde Rechner bis nach Japan und in die USA führten, hinein in die Rechenzentren von Konzernen, Universitäten und Verwaltungen.

Die Hacker berauschten sich an ihren Möglichkeiten: Durch raffinierte Manipulation verschafften sie sich sogenannte Benutzer-Privilegien, irritierten Systeme und sperrten auch schon mal Systemmanager von ihren eigenen Computern aus.

Wo der Rausch des „Wissens um die ungeheuren Möglichkeiten" (Koch) nicht reichte, half Kokain. Das war nötig, damit zumindest Koch die Nächte vor dem flimmernden Schirm überhaupt durchstehen konnte.

Mit dabei war gelegentlich auch Markus Hess, eigentlich mehr ein einsamer Hacker, der nur selten die Verbindung zu den Kollegen suchte. Er galt als der fähigste Programmierer der hannoverschen Hacker-Truppe. Hess hinterließ in vielen Großsystemen überall auf der Welt sein eigenes Programm „.d", ein sogenanntes Trojanisches Pferd, mit dem er allen Benutzern, die er davon informierte, einen Zugang zu speziellen Systemprivilegien verschaffen konnte.



Elektronen-Synchrotron Desy

Gäste auf den Partys waren bald auch drei Berliner: der findige Hacker Hans Hübner (Spitzname „Pengo"), der Programmierer Dirk Brezinsky und sein Freund Peter Carl. Kumpel Carl, eine windige Figur, hatte mal als Croupier gearbeitet und soll nach Angaben eines Beteiligten immer gut mit Kokain bestückt gewesen sein. Brezinsky, ein Mann mit aufwendigem Lebensstil, war als elektronischer Trouble-Shooter bei Firmen wie Siemens und Institutionen wie der Bundesversicherungsanstalt für Angestellte in Berlin immer dann von Nutzen, wenn der Computer streikte und niemand mehr weiterwußte. Ein Verfassungsschutzmann hält Brezinsky für „eine Art Genie", das für seine Tätigkeit mit 20 000 Mark im Monat entlohnt wurde.

Anfang 1986 reifte in dieser Gruppe der Plan, die heißen Infos aus den Einbrüchen in die sicherheitsempfindlichen Computersysteme zu Geld zu machen. Die Idee dazu kam, so erinnern sich Teilnehmer der Runde, von den Berliner Partnern.

ARD-„Brennpunkt"-Sendung: Größter Fall seit Guillaume?

Koch, der sich nach dem Held des Science-fiction-Schmökers „Captain Hagbard Celine" nur „Hagbard" nannte und gelegentlich in der dritten Person von sich sprach, sprang darauf an. Ihm war das Geld ausgegangen. Anderthalb Jahre lang hatte er allein durch die Hackerei monatliche Telephonkosten von über 2000 Mark; teure Computeranlagen und Datenreisen auf eigene Kosten verschlangen große Summen. Koch hatte am Ende ein 100 000-Mark-Erbe durchgebracht und keine Einnahmen: Er saß nur noch vor dem Computer.

Auch Hess, der ebenfalls keinen Job hatte und irgendwie sein Fernstudium der Informatik an der Universität Hagen finanzieren mußte und außerdem endlich einmal einen „anständigen Computer" haben wollte, biß, laut Zeugen, auf das Angebot der Berliner Computerkumpel an. „Pengo" brauchte Geld für eine eigene Software-Firma. Brezinsky, so berichten Teilnehmer der Runde, stellte den Kontakt mit den Sowjets in Ost-Berlin her.

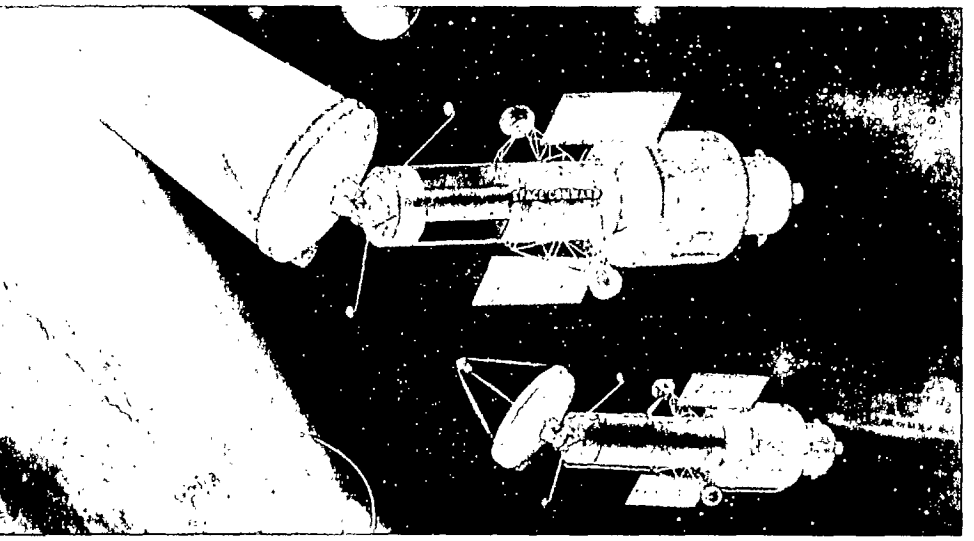
Von Mai bis November 1986 soll die Hacker-Crew mindestens fünf Disketten in die DDR geliefert haben, vollgepackt mit Netzwerk-Know-how über Datensysteme in aller Welt. Dazu gehörten Codes, um in die Systeme einzubrechen. Pro Stück bezahlten die Sowjets mindestens 15 000 Mark und gingen bald, wie Eingeweihte behaupten, dazu über, System-Software- und Chip-Design bei den Hackern zu bestellen. Doch im November 1986 war Schluß: In Amerika wie auch in der Bundesrepublik waren Computerexperten auf die emsigen Nachtarbeiter aufmerksam geworden.

Das Hess-System wies eine Schwachstelle in Bremen auf. Der Hacker hatte sich des dortigen Universitäts-Rechners bedient, um jenseits des Atlantiks in die großen Datenbanken einzudringen.

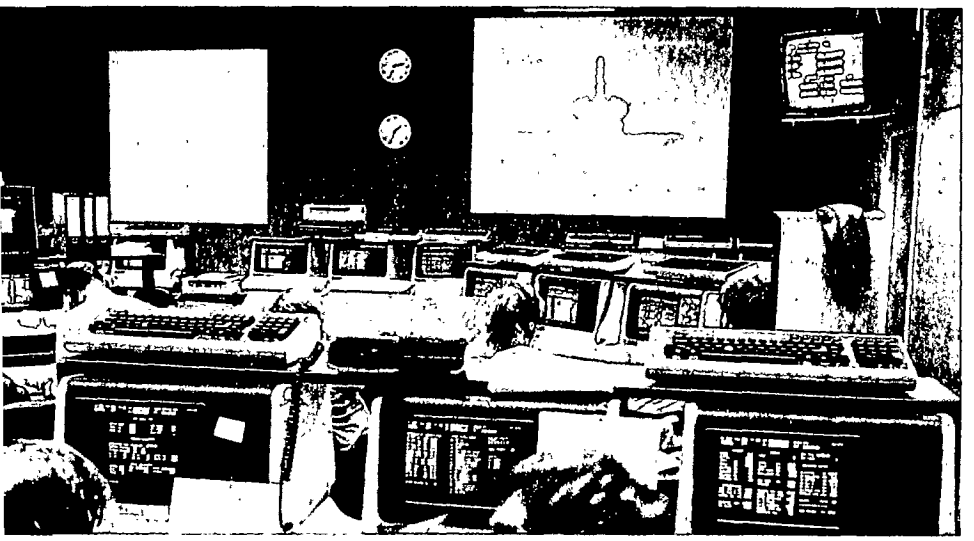
Die Bremer Computerexperten wunderten sich, daß sie ständig unerklärlich hohe Rechnungen für ausgedehnten Datenverkehr mit den USA erhielten. Als es ihnen zuviel wurde, erstatteten sie im Dezember 1986 Anzeige bei der Staatsanwaltschaft, zunächst gegen Unbekannt.

Währenddessen war Markus Hess im fernen Kalifornien ebenfalls mit der Buchhaltung ins Gehege gekommen. Neben dem Bremer Umweg war der Hacker auch direkt, über das Postnetz Datex-P, in den USA tätig.

Der unbekannte Gast fiel im Rechnungswesen des Lawrence Berkeley La-



SDI-Darstellung



Deutsche Forschungs- und Versuchsanstalt für Luft- und Raumfahrt

Hacker-Ziele: „Zugang zu Computern in Physiklabors und Militärbasen"

boratory auf. In dessen dortigen Rechnern, die für interessierte Wissenschaftler und Universitäten offen sind, erschien ein neuer Kunde, ohne allerdings eine Anschrift zu hinterlassen, an welche die Rechnung für benutzte Computerzeit geschickt werden sollte. Zwar handelte es sich stets nur um ein paar Dollar, doch die Monatsabrechnung war nicht auszugleichen.

Clifford Stoll, Systemmanager am LBL, verdächtigte zunächst einen Studenten von der benachbarten University of California, der sich – wie zuvor öfters geschehen – Zugang zum bequemen Lesen von LBL-Forschungsunterlagen verschafft hatte.

Doch eine Nachricht vom National Computer Security Center (NCSC), einer Abteilung des US-Geheimdienstes NSA in Fort Meade, bewog Stoll, den Computerzeit-Schnorrer diesmal nicht als Ulk-Studenten abzutun. Laut NCSC hatte jemand von einem LBL-Computer aus versucht, über das mehrheitlich von Militärs und Rüstungsfirmen genutzte und seinerzeit noch als relativ einbruchsicher eingeschätzte Datennetz Milnet in die NCSC-Rechner einzudringen. Stoll, ein schlaksiger Computerfreak mit wirrem Haarschopf, wähnte zwischen dem LBL- und NCSC-Problem einen Zusammenhang und beschloß, den Eindringling zu verfolgen.

Zunächst sperrte Stoll dem Fremdling das Konto. Der Ertappte ließ sich davon nicht abschrecken. Offenbar verfügte er über Paßwörter, die ihn als Systemmanager auswiesen und ihm so Zugriff auf sämtliche LBL-Programme sicherten: Um den einzigen Anhaltspunkt, der ihn bisher verraten hatte, zu beseitigen, versuchte der Eindringling, die von ihm benutzten Konten auszugleichen.

Stoll stellte ein kleines Team von Kollegen zusammen, mit denen er gemeinsam daran ging, die Aktivitäten des unerwünschten Computernutzers aufzuzeichnen, seine Eigenarten, seine Kniffe und Zugangswege auszuforschen.

Das Stoll-Team richtete eine Art Logbuch ein. Die Computerexperten hielten in den folgenden Monaten nicht nur Zeitpunkt und Dauer aller illegalen Computerzugriffe fest, sondern auch jede sich abzeichnende neue Spur, jedes neue Verdachtsmoment.

Da es galt, den Eindringling über die angelaufene Fahndung und gegen ihn gerichtete Sicherheitsvorkehrungen zu täuschen, verständigten sich die LBL-Fahnder über das Telephon statt – wie in Computerkreisen üblich – per elektronischer Post.

Stoll hatte nämlich bemerkt, daß der geheimnisvolle Hacker bei seinen Besuchen regelmäßig die elektronischen Mitteilungen des LBL filzte – offenbar in der Hoffnung, dort leichtsinnig hinterlassene Paßwörter abzuziehen, die ihm Zugriff zu weiteren Rechnern gesichert hätten. Um den Eindringling zusätzlich in Sicherheit zu wiegen, deponierte das Stoll-Team eine Reihe von fingierten Nachrichten in elektronischen Briefkästen, die Hess regelmäßig durchstöberte.

Stoll stand die ganze Zeit unter dem Eindruck, es mit einem einzigen Hacker zu tun zu haben. In Wahrheit war die Gruppe um Hess zu viert.

Während Hess meist aus einem kleinen Software-Büro tätig war, in dem er einen Job angenommen hatte, hackte Koch auf höchst private Weise. Er ging abends mit seinem tragbaren Laptop-Computer in öffentliche Telephonzellen und setzte von dort zur Computerreise nach Amerika an. Zu Recht hoffte Koch, daß mögliche Spürhunde den Weg in eine öffentliche Telephonzelle nicht würden zurückverfolgen können.

Höchst aktiv betätigte sich bei US-Hacks auch ein 19jähriger junger Mann namens Hans Hübner, der unter dem Künstlernamen „Pengo" als Berlins hoffnungsvollstes Hack-Talent gehandelt wird. Ein vierter Hacker war in Hannover tätig.

Hess und Hübner machten sich einen Spaß, der unter Hackern als elegante Pflichtübung gilt. Beide drangen gleichzeitig in den LBL-Computer ein und unterhielten sich via Computer darüber, wie sie am besten in den Rechner der Stanford-Universität gelangen könnten.

Die lockeren Tricks konnten jedoch nicht darüber hinwegtäuschen, daß Stoll und sein Team auf Dauer gewinnen mußten: Kriminalbeamten gleich, die verräterische Fußabdrücke oder Reifenspuren am Tatort mit Gips ausgießen, plazierten die kalifornischen Hacker-Jäger eine Reihe von Spurensicherungsgeräten. Sie hatten festgestellt, daß der Hacker über bestimmte Zugänge in den LBL-Computer gelangte.

In jede Kommunikationsleitung, durch die der LBL-Computer mit Rechnern in aller Welt verbunden ist, schalteten sie entweder einen Drucker oder einen Personal-Computer. Die Geräte hielten jedes Paßwort, jeden Computerbefehl fest, den der Hacker eingab. Wichtiger noch: „Lückenlos" (Stoll) konnten die LBL-Experten mit ihren aufgestellten Hacker-Fallen sämtliche Aktivitäten dokumentieren, die der Ein-

dringling von dem als Operationsbasis dienenden LBL-Computer aus entfaltete (siehe Graphik Seite 112).

Da nicht auszuschließen war, daß der Eindringling Schaden anrichten würde, bewehrten sich Stoll und seine Freunde mit „Beepern". Die kleinen Elektronik-Pieper sprangen automatisch an, wenn Hess – zumeist ab neun Uhr abends Hannoveraner Ortszeit – sich in den LBL-Rechner hineinzuhacken begann. Beim ersten Piepser eilte das Stoll-Team an die Monitore oder Drucker, um die Absichten des Hackers zu beobachten.

Wenn sich Hess beispielsweise anschickte, Daten zu löschen, zu verändern oder möglicherweise vertrauliche Daten auf seinen eigenen Computer zu überspielen, reagierten die Überwacher in Berkeley unverzüglich. Sie unterbrachen

entweder die Verbindung oder legten ein Störsignal auf die Leitung.

In vielen Fällen informierten sie die Systemmanager von attackierten Computern und veranlaßten sie, ihre Systeme für Hess zu blockieren. So wurde der Eindringling gezwungen, nur noch mit LBL zu kommunizieren.

Dieser Feuerwehreinsatz lohnte. Denn der mögliche Schaden konnte begrenzt werden. Nicht in 450 Computer, wie vielfach berichtet, drang Hess ein, sondern allenfalls in 220. Und selbst bei diesen wurde ihm der Zutritt mangels richtiger Paßwörter meist verwehrt. „Richtig reingekommen", so Stoll, „ist er in gut 30 Computer."

„Erheblich beeindruckt" allerdings war Astrophysiker Stoll von der Hartnäckigkeit und Geduld des Eindringlings, der sich überdies als kenntnisreicher Profi auswies. Hess – und, nach Ansicht eines westdeutschen Computerexperten, „auch andere" – nutzte alle hinlänglich bekannten Schwachstellen in den einzelnen Betriebssystemen aus. Zudem durchkreuzte er den Fahndern gekonnt die Absicht, ihn zu lokalisieren.

Da Hess über das internationale X.25-Netz in den Berkeley-Computer hineinkam, „konnte er an jedem Ort der Welt sitzen", sagt Stoll. Als weitere Schwierigkeit erwies sich die Hess-Taktik, einmal aufgebaute Verbindungen nur kurzzeitig zu nutzen. In meist nur wenigen Minuten ließen sich mit Fangschaltungen, gelegt von den Betreibern des Tymnet-Netzwerkes, keine Treffer erzielen.

Doch dann ging der Hacker trotzdem in die Falle: Das Stoll-Team schaffte es mit einem verlockenden Köder.

Daß Hess und Kollegen mehr als geschickte Computerfreaks waren, die aus purer Hacker-Lust durch die Datennetze reisten, glaubten ihre amerikanischen Verfolger relativ früh erkannt zu haben. Ihr Interesse konzentrierte sich offenbar auf militärische Einrichtungen und Pläne.

Bei jedem ihrer Besuche von Computern auf US-Militärbasen oder in Rüstungsfirmen verrieten sie umgehend ihre Absichten. Die Hacker wiesen die geknackten Computer an, ihre Dateien nach brisanten Schlüsselwörtern zu durchforsten. Immer wieder lauteten die Suchbefehle: „SDI" (Strategisches Raketenabwehrsystem im Weltraum), „KH-11" (Spionage-Satellit) oder „Norad" (Nordamerikanisches Luftverteidigungszentrum).

Diese Fixierung wurde Hess zum Verhängnis. Stoll stellte eine Datei zusammen, die kurze Berichte über den Computereinsatz bei der SDI-Forschung enthielt. „Weitere Berichte", hieß es in einer Nachricht, „können per Post bestellt werden" – angeblich in Berkeley bei einer LBL-Sekretärin, deren Namen ebenso gefälscht war wie die gesamte Nachricht.

Hess entdeckte die Ankündigung. Im LBL piepten die Beeper. Das Stoll-Team eilte an die Monitore und beobachtete erfreut, wie der Hacker diesmal die Verbindung länger als eine Stunde aufrechterhielt. Die Zeit reichte für die Telephonfangschalter aus, den Anschluß ausfindig zu machen. In Berkeley wurde der erfolgreiche Coup gefeiert – „mit Milch-Shakes aus kalifornischen Erdbeeren" (Stoll).

Drei Monate später wurde der Sieg wider Erwarten abgerundet. In Berkeley traf ein Brief, adressiert an die nicht existente Sekretärin, ein, in dem um das angekündigte SDI-Material gebeten wurde.

Doch der Brief kam nicht aus Deutschland, sondern aus Pittsburgh (Pennsylvania). Absender war ein gewisser Laszlo Balogh, der den US-Behörden als internationaler Waffenhändler mit saudiarabischen Verbindungen bekannt war und der auch als KGB-Agent verdächtigt wird.

Wie war die falsche Adresse von Deutschland nach Pittsburgh gekommen? Wohl von Hannover über die sowjetische Connection, wie die Fahnder inzwischen vermuten. Der Professor in Berkeley hatte es vorweg geahnt: „Wir wurden uns bewußt, daß wir Zeugen eines Spionage-Versuchs wurden" (Stoll).

Wer in der Bundesrepublik der Hakker war, hätte Stoll freilich niemals herausbekommen – hätte nicht die Bundespost geholfen. Am 8. Dezember 1986 wandten sich die Amerikaner um Hilfe an die Post wegen der „Eingrenzung einer Belästigung", wie die Beamten notierten. Gut einen Monat später hatten die Spezialisten zunächst die Bremer Universität und dann Markus Hess geortet (Kennwort DURMEL – D für Deutschland und Urmel, der Spitzname des Hackers).

Allerdings hatten die Postler dabei eine Fangschaltung benutzt, die einer richterlichen Genehmigung bedurft hätte. In der Eile hatten die Post-Horcher die Erlaubnis nicht eingeholt. So kam es, daß der Bremer Staatsanwalt Hans-Georg von Bock und Pollach sein Ermittlungsverfahren gegen Markus Hess nicht weiterführen durfte.

Aber dann bekam das Unternehmen im vergangenen Sommer neuen Schub. Die Polizei durchsuchte die norddeutsche Hacker-Szene und unterzog die einschlägigen Personen eindringlicher Befragungen. Karl Koch und ein zweiter Hacker gestanden alles.

Koch glaubt fest daran, daß die Welt von fünf Menschen beherrscht wird und daß es seine Aufgabe ist, einen dritten Weltkrieg zu verhindern. Vergangenen Donnerstag hatte die Realität ihn wieder.