

Werner Heine: Die Hacker - Von der Lust, in fremden Netzen zu wildern.- Reinbek: Rowohlt 1985, 190 S., DM 10,80

Wenn es ums Hackern geht, dann knistert es irgendwie, denn es geht um 'fast-Einbrüche', um den Schutz des Eigentums an Information und um Datensicherheit. Im Herbst 1987 meldeten die Zeitungen, daß jugendliche Hacker erfolgreich in den NASA-Computer eingedrungen seien. Im Frühjahr 1988 findet man eine Notiz, daß ein Münchner Schüler ein amerikanisches Computersystem geknackt hat und sich in die Lage versetzte, den VAX-Computer bei dessen Produzenten (DEC)

zu beherrschen. Hackern, das Stöbern in 'fremden Netzen', hat auch in der Bundesrepublik Deutschland schon häufiger öffentliche Aufmerksamkeit auf sich gezogen. Schließlich war es Hackern schon vor der offiziellen Einführung von BTX gelungen, in Mailboxen einzudringen, Buchungen bei Banken zu veranlassen und auch sonstige Verwirrung zu stiften. Neben dem gelegentlich 'sportiven' Stöbern in der Datenwelt gibt es allerdings auch Meldungen in der Tagespresse, die von einem bargeldlosen Bargeldklau berichten: Die geheime vierstellige PIN (persönliche Identifikationsnummer) wird nicht nur vom befugten Kontoinhaber, sondern auch von Unbefugten dazu benutzt, sich über einen Geldautomaten Bares zu verschaffen. Heine berichtet vom Eindringen in den BTX-Rechner bis hin zur gezielten Fehlbuchung. Zur Begrifflichkeit und zur Etablierung der neuen Bewegung gibt er einleitend Auskunft und stellt einen Zusammenhang her zwischen der Entwicklung lernfähiger Computer und einer neu entstehenden Bewegung, die es sich zum Ziel gesetzt hat, die Computertechnologie mit einer 'Hacker-Ethik' zu konfrontieren. Als Vorläufer der Hacker gelten die 'phone freaks'. Ab Mitte der sechziger Jahre umgingen diese mit verschiedenen Tricks die Gebühren für Telefonate und kommunizierten kostenfrei rund um die Welt. Die geschädigten Telefongesellschaften haben allerdings erfolgreich durchgesetzt, daß die 'Informationsgesellschaft' auch auf die Zahlung von Leistungen besteht. Hierzulande spricht die juristische Würdigung von 'Automatenmißbrauch' (nach dem StGB § 265ff) und von 'Erschleichungen von Leistungen'. Auch bei den 'phone freaks' ging es bereits um die Frage, worin in dem speziellen Falle das Eigentum bestünde. Die 'phone freaks' nahmen sich etwas, was keinem anderen abging. Hacker argumentieren in Sachen Eigentum etwas anders. Alles bleibt an seinem Platz, es wird nur mehrfach genutzt: "Was ist schon Eigentum angesichts des Rechts auf Freizügigkeit für Informationen und Meinungen". Diesem Anspruch der Hacker steht entgegen, daß der alte Eigentumsbegriff juristisch auch in den internationalen Netzen gilt.

Was dann folgt, sind Erläuterungen zur Datenvernetzung (Bild, Datenbank, Fernabfragen, IDN, ISDN) als Mittel und Medium, um an Daten und Informationen heranzukommen. Das Taschenbuch berichtet von diversen und in der Regel gelungenen Versuchen, in fremde Rechnersysteme einzudringen, wobei nicht immer der Computer das wesentliche Vehikel sein muß, wenn es darum geht, sogenannte 'Fehlbuchungen' zu veranlassen. Auch wenn diesbezügliche Fälle spannungsreich dargestellt werden, so handelt es sich letztlich um Lücken in der Kontrolle einzelner Banken und Betriebe, die auch früher schon in der 'alten' Technik einige Buchhalter für sich auszuschöpfen wußten. Näher am Computer dran sind dann wieder die Erläuterungen zur 'Kryptologie'. Hier wird nachvollziehbar und anschaulich gemacht, wie mit fortschreitender Entwicklung der Informationsverarbeitungstechniken der Bedarf nach neuen Sicherheitsmechanismen immer gewichtiger wird. Die Sache schaukelt sich auf, denn - wie Sicherheitsexperte Norman seufzend formuliert - "Im allgemeinen ist der erschwerte Zugang eine Herausforderung für den Angreifer, so wie der schwierige Gipfel den Bergsteiger anzieht" (S. 105). Solche Befunde rechtfertigen es wohl, den kryptographischen Techniken und der Entwicklung der Chiffretechniken nachzugehen, die ursprünglich exklusiv für militärische und Spionagezwecke entwickelt wurden.

Wenn sich trotz ausgefeilter Techniken immer auch Lücken entdecken lassen, so verweist dies darauf, daß bei der Sicherung der 'Information als Eigentum' zwar alte juristische Regeln greifen, nicht aber alte Sicherungsmechanismen. Insofern ist auch die Kapitelüberschrift 'Elektronische Burgen', unter der die praktische Umsetzung der Kryptographie in der Computertechnik behandelt wird, eher irreführend.

In dem Film 'War Game' dringt ein 15-jähriger von seinem Homecomputer aus in das Rechnersystem des Pentagon ein. Wie nahe die Realität schon an solche Fiktionen elektronischer Einbrüche heranreicht, wird bei der Lektüre des Buches deutlich. Da sie sich keine Vermögensvorteile verschaffen, will Heine die Hacker allerdings nicht kriminalisiert sehen, und es gelingt ihm in diesem Sinne, den Blick auf das 'Tatwerkzeug' Computer zu lenken. Schließlich hat man es mit einer kulturellen Erscheinung zu tun, die der computerisierten Gesellschaft ihre Schwachstellen nachweisen möchte. Um dies zu demonstrieren, nehmen die Hacker auch Verstöße gegen geltende Normen in Kauf. Exemplarisch beruft sich ein im Buch zitierter Hacker auf die Schlußakte von Helsinki, die den freien Informationsaustausch garantiert. Damit ist zugleich auch der Streitpunkt zwischen Hackern und Datensicherungsexperten benannt. Beide warnen vor mißbräuchlicher Informationsverwendung und weisen nach, daß der Eigentumsschutz bei Daten anders aussehen muß als bei dinglichen Objekten. Der digitalisierte Transport und die elektronische Speicherung von Daten verschaffen der Information erstmals den ihr eigenen Charakter von Allgemeinheit. Hacker und Cracker (jene, die Kopiersperren bei der Software knacken) machen sich auf dieser Grundlage daran, die Grenzen der freien Verfügbarkeit von Wissen und Information zu demonstrieren. Mit dem erfolgreichen Eindringen in fremde Netze belegen sie, daß die Kontrolle und mithin der Datenschutz bislang nicht gelungen ist.

Claus J. Tully