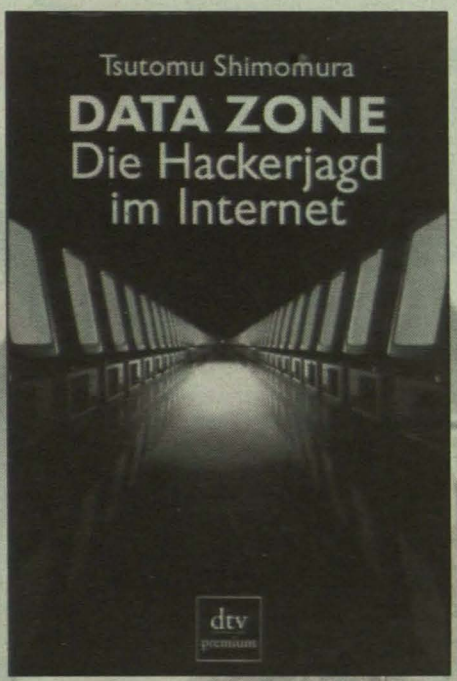
Die Hackerjagd im Internet

Data Zone

Am 16. Februar 1995 erscheint auf der ersten Seite der "New York Times" ein Artikel mit der Überschrift: "Einer der meistgesuchten Cyberdiebe gefangen in seinem eigenen Netz".

Mehr als zwei Jahre lang führt Kevin Mitnick das FBI an der Nase herum, indem er Funkverbindungen abhört und sogar die Telefonzentralen seiner Jäger manipuliert. Doch am 1. Weihnachtstag des Jahres 1994 begeht er einen folgenschweren Fehler: Mit Hilfe seines Funktelefons hackt er sich in den Computer des besten Computersicherheitsexperten der USA, Tsutomu Shimomura, und klaut ihm sämtliche E-mails samt hochsensibler Software.

Tsutomu Shimomura nimmt die Herausforderung an. 50 Tage lang jagt er den Cyberdieb durch die Datennetze, dann ist es soweit: Im Morgengrauen des 14. Februar 1995 durchquert er, begleitet von 2 Telefontechnikern und dem "New-York-Times"-Reporter John Markoff, die Vorstädte von Raleigh in North Carolina, als sein Funktelefon ihm durch ein immer lauter werdendes Piepsen anzeigt, daß Kevin Mitnick ganz in der Nähe ist und mit seinem Funktelefon in fremde Computer einbricht. Er ruft das FBI, dann dauert es nur noch Minuten...



Tsutomu Shimomuras Sieg ist ein Sieg für die Demokratie im Cyberspace. Denn wenn bösartige Hacker Daten stehlen, dann ist das ein Angriff auf das Vertrauen der großen Internet-Gemeinschaft.

■ **Alexander List**

PICS: Internet-Zugangskontrolle ohne Zensur

In letzter Zeit vermehren sich die Rufe nach einer Sperre von bestimmten (meist illegalen) Inhalten im Internet. Nach dem Willen der EU-Kommission sollen Schutzmechanismen geschaffen werden, die Eltern eine Kontrolle über die von ihren Kindern abrufbaren Informationen ermöglichen und gleichzeitig das Recht auf freie Meinungsäußerung so wenig wie möglich einschränken. Bisher wurde die »Säuberung der Inhalte« durch spezielle Programme mit proprietären Standards (CyberPatrol, NetNanny, SurfWatch usw.) bewerkstelligt. Dabei wurden von den jeweiligen Softwareherstellern Sperrlisten (sog. »black lists«) bereitgestellt, oder es wurde der empfangene Inhalt selektiv nach bestimmten Stichworten durchsucht, bevor der Benutzer die Seite zu Gesicht bekam. Das erwies sich aufgrund der gewaltigen Menge an Information, die gefiltert werden mußte, als nicht praktikabel.

Um diesem Wildwuchs ein Ende zu bereiten und eine Zugangskontrolle für die verschiedensten Internet-Dienste (WWW, FTP, IRC usw.) zu ermöglichen, wurde im Mai dieses Jahres vom World Wide Web-Consortium (W3C) der PICS-Standard vorgestellt. Namhafte Hersteller wie Netscape, SurfWatch, CyberPatrol und andere haben angekündigt, PICS-kompatible Produkte anzubieten.

Flexible Sperrung

Nicht jeder Zugriffsschutz ist für jeden Zweck sinnvoll. Eltern möchten z.B. Sex und Gewalt nicht auf dem häuslichen Computerschirm sehen, Firmen möchten die Netzbelastung durch allzu freizügiges »Surfen« während der Arbeitszeit einschränken, manche Regierungen möchten Material »indizieren«, das im Ausland legal ist, im Inland jedoch nicht.

Die Verhältnismäßigkeit einer Sperrung hängt jedenfalls von drei Faktoren ab:

1.) vom »Überwacher«, also demjenigen, der kontrolliert, was verboten ist,
2.) vom Empfänger: was für einen Fünfzehnjährigen geeignet ist, muß noch lange nicht für einen Achtjährigen geeignet sein,
3.) vom Umfeld: gegen ein Spiel oder einen Chat-Room auf dem Privat-PC zuhause mag nichts einzuwenden sein. Wenn jedoch in der Firma oder in der Schule unkontrolliert gespielt oder »gechattet« wird, ist dies nicht immer im Sinne derjenigen, die dafür die Gebühren bezahlen müssen.

PICS definiert einen allgemeinen Standard für »Labels«, eine Art elektronische Etiketten. Jede PICS-kompatible Software kann jedes PICS-kompatible Label verarbeiten. ▸