Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

Ein Organ des Chaos Computer Club

ISSN 0930-1045 September 1995 Nr. 52 DM 3,50 Postvertriebsstück C11301F

Edito-real

Heute Bleiwüste bleifrei

(chaos-team) - Pfuinanzfragen bringen uns dazu, diesmal eine 16seitige Ausgabe zu produzieren. Im Sinne surrealsozialistischer Leistungssteigerung haben wir uns bemüht, doppelt so viele Informationen auf der halben Fläche zu verbreiten. Das Ergebnis ist die folgende Bleiwüste mit Kakteen zwischen den Zeilen.

Manche erblühen erst nach einer gewissen Textlagerzeit.

Das Einblenden von Abbildungen verschönte Windows mit einem Dialog zwischen Rechner und Scanner. Der Scanner sagte „Here is the scanner". Und Windows antwortete sowas wie „What do you want and who are you?". Doch erscheinende Abbildungen sind möglicherweise handgeklebt.

Die nächste ds wird in Berlin produziert. Mal abwarten, welche Informationspilzstruktur sich dort bildet.

Die Ereignisse überschlagen sich. Die Netzwerkalternativen zur TELEKOM entwickeln sich schnell. Wenn die neuen TELEKOM-Tarife ab 1.1.96 gelten, müßte jeder Internet-User deutlich mehr bezahlen.

Da zumindest im Osten Deutschlands schon parallel zu jeder Gasleitung und jedem Stromkabel und an den Schienen entlang Glasfasern laufen, ist an etlichen Stellen ein Alternativ-Telefonnetz möglich. Die Vermittlungsstellen arbeiten per Funk. Es werden entweder nur Daten übertragen oder aber gefaxt, aber nicht gesprochen. Mal abwarten, welche Betreiberkonstellation welche Preiskalkulation dafür macht.

Die Verflechtungen hier insbesondere im internationalen Bereich sind schier unüberschaubar. Die Landesmedienanstalten betreiben vergleichsweise Sandkastenspiele, wenn sie z. B. die familiären Verhältnisse der Familie Kirch zu durchleuchten versuchen und in NRW zwei öffentlich-rechtliche Dritte Programme aus dem Kabel fliegen, weil ein neuer Kanal vom Typ ZAP-TV und ein neuer Dauerwetterkanal ins Kabel muß. (wau)

Impressum

Die Datenschleuder
Das wissenschaftliche Fachblatt für Datenreisende
Nummer 52, Quartal III, September 1995
Adresse: Die Datenschleuder, Schwenckestr. 85, D-20255 Hamburg, Tel +49 (40) 4903757, Fax +49 (40) 4917689, BBS +49 (40) 4911085 (chaos-hh.zer), Internet: ccc@t42.ccc.de, Mailserver: ccc-serv@mail.ccc.de, Datex-J: *CCC#

Redaktion: Amok, (A)ndy, Cash, Hacko, Ron, Nomade, Wau

V.i.S.d.P.G.: Wau Holland

Herausgeber: Chaos Computer Club e.V.

Druck: St. Pauli Druckerei, Hamburg

Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion wieder.

Einzelpreis 3,50 DM. Mitglieder des Chaos Computer Club e.V. erhalten die Datenschleuder im Rahmen ihrer Mitgliedschaft. Abopreise siehe Bestellfetzen.

Adressänderungen von Abonnenten am besten schriftlich (Postkarte genügt).

ENTWURF einer Verordnung

über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind (Fernmeldeverkehr-Überwachungs-Verordnung – FUeV, Stand 02.05.1995)

Auf Grund des § 10b Satz 2 des Gesetzes über Fernmeldeanlagen in der Fassung der Bekanntmachung vom 3. Juli 1989 (BGBl. I S. 1455), der durch Artikel 5 Nr. 11 des Gesetzes zur Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994 (BGBl. I S. 2325) eingefügt wurde, verordnet die Bundesregierung:

Abschnitt 1: Allgemeine Vorschriften

§ 1 Zweck

Diese Verordnung regelt die Anforderungen und das Verfahren zur technischen Umsetzung von Überwachungsmaßnahmen nach dem Gesetz zu Artikel 10 Grundgesetz, § 100a der Strafprozeßordnung und § 39 des Außenwirtschaftsgesetzes in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind.

§ 2 Begriffsbestimmungen

Im Sinne dieser Verordnung ist

1. Betreiber: jeder, der eine Fernmeldeanlage, die für den öffentlichen Verkehr bestimmt ist, betreibt;
2. Überwachungsmaßnahme: die technische Maßnahme zur Überwachung des Fernmeldeverkehrs nach dem Gesetz zu Artikel 10 Grundgesetz, § 100a der Strafprozeßordnung oder §39 des Außenwirtschaftsgesetzes;
3. Bedarfsträger: die berechtigten Stellen nach Art. 1 § 1 Abs. 1 des Gesetzes zu Artikel 10 Grundgesetz, § 100b Abs. 3 der Strafprozeßordnung oder § 39 Abs. 1 des Außenwirtschaftsgesetzes;
4. Anschluß: diejenige technische Einrichtung, die Ursprung oder Ziel des Fernmeldeverkehrs ist und in der Regel durch eine Rufnummer eindeutig gekennzeichnet wird (physikalischer Anschluß) oder die Rufnummer, die der Teilnehmer einem physikalischen Anschluß fallweise zuordnen kann;
5. Funkzelle: der kleinste durch seine geographische Lage bestimmbare funktechnische Versorgungsbereich in einem Mobilfunknetz;
6. Kunde: eine Person, die mit dem Betreiber Vertragsbeziehungen über die Bereitstellung und Nutzung der Fernmeldeanlage für eigene Telekommunikationszwecke unterhält;
7. Anordnung: die Anordnung zur Beschränkung des Fernmeldegeheimnisses nach dem Gesetz zu Artikel 10 Grundgesetz, den §§ 100a und 100b der Strafprozeßordnung oder den §§ 39 und 40 des Außenwirtschaftsgesetzes.

Abschnitt 2: Anforderungen an die Umsetzung von Überwachungsmaßnahmen

§ 3 Bereitzustellende Informationen

(1) Der Betreiber hat im Rahmen der räumlichen Abgrenzung nach § 5 Abs. 1 zu gewährleisten, daß innerhalb des durch die Anordnung bestimmten Zeitraums die Überwachung und Aufzeichnung des gesamten Fernmeldeverkehrs ermöglicht wird, der von dem zu überwachenden Anschluß ausgeht oder für diesen bestimmt ist oder der statt dessen zu technischen Speichereinrichtungen geleitet wird oder der aus solchen Speichereinrichtungen abgerufen wird.

(2) Neben den Nachrichten hat der Betreiber dem Bedarfsträger Informationen über die mit dem Fernmeldevorgang zusammenhängenden näheren Umstände bereitzustellen, und zwar:

1. die vom überwachten Anschluß gewählten Rufnummern und Zusatzdienste, auch wenn keine Verbindung zustande kommt,
2. die Rufnummern der Anschlüsse, die den überwachten Anschluß angewählt haben, auch wenn keine Verbindung zustande kommt,
3. bei Leistungsmerkmalen, welche den Fernmeldeverkehr um- oder weiterleiten (Rufumleitung oder Rufweiterschaltung) das Umlenkziel, bei virtuellen Anschlüssen die jeweils zugeordneten physikalischen Anschlüsse,
4. bei überwachten Mobilanschlüssen die Funkzellen, über die die Verbindung abgewickelt wird,
5. Informationen zu dem jeweils in Anspruch genommenen Telekommunikationsdienst und
6. mindestens zwei der folgenden drei Angaben: Beginn und Ende der Verbindung oder des Verbindungsversuchs (jeweils mit Datum und Uhrzeit), Dauer der Verbindung.

(3) Jeder an der Schnittstelle bereitgestellte Fernmeldeverkehr ist durch ein eindeutiges Merkmal der jeweiligen Überwachungsmaßnahme zu kennzeichnen; das Merkmal darf nicht identisch sein mit Daten zum überwachten Anschluß.

(4) Die in den Absätzen 1 bis 3 genannten Bedingungen gelten entsprechend auch für Konferenzgespräche, soweit und solange der überwachte Anschluß an einem solchen Gespräch teilnimmt.

§ 4 Zeitliche Umsetzung

(1) Der Betreiber muß die notwendigen Vorkehrungen treffen, um seine Verpflichtung, die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen, ab dem Zeitpunkt, zu dem die Fernmeldeanlage den Kundenbetrieb aufnimmt, entsprechend den Vorschriften der §§ 3 bis 14 erfüllen zu können. Dies gilt entsprechend für die Einführung von Änderungen der Fernmeldeanlage oder für neue Betriebsmöglichkeiten bestehender Telekommunikationsdienste, soweit diese Einfluß auf bestehende Überwachungsmöglichkeiten haben.

(2) Die in einer Fernmeldeanlage zur Umsetzung von Überwachungsmaßnahmen erforderlichen Vorkehrungen sind so zu gestalten, daß der Betreiber eine im Einzelfall angeordnete Überwachung sofort nach Vorlage der Anordnung ermöglichen kann.

(3) Die Überwachung des Fernmeldeverkehrs eines Anschlusses erfolgt nach der ergangenen Anordnung zeitgleich mit diesem Verkehr.

(4) Dem Bedarfsträger ist auf Antrag ein Anschluß zu den üblichen Geschäftsbedingungen des jeweiligen Betreibers zu dem Zweck zu überlassen, die technische Umsetzung der Überwachungsmaßnahmen unter sämtlichen Betriebsbedingungen zu erproben. Die Erprobung umfaßt die

Bereitstellung des von diesem Anschluß herrührenden oder für ihn bestimmten Fernmeldeverkehrs gemäß den §§ 3, 8 und 9, die Übertragung zum Bedarfsträger sowie die ordnungsgemäße Funktion der Aufzeichnungseinrichtungen des Bedarfsträgers. Der Bedarfsträger hat sicherzustellen, daß über diesen Anschluß ausschließlich der von ihm selbst zu Probezwecken erzeugte Fernmeldeverkehr ohne Beteiligung Dritter abgewickelt wird.

§ 5 Örtliche Umsetzung

(1) Die Verpflichtung des Betreibers besteht für solchen Fernmeldeverkehr, der mittels des überwachten Anschlusses über Fernmeldeanlagen im Geltungsbereich des Gesetzes zu Artikel 10 Grundgesetz, der Strafprozeßordnung und des Außenwirtschaftsgesetzes abgewickelt wird.

(2) Zum Zwecke einer eindeutigen Abgrenzung der Zuständigkeiten und Verantwortlichkeiten und der Gewährleistung des Fernmeldegeheimnisses unbeteiligter Dritter sind die Überwachung und Aufzeichnung des Fernmeldeverkehrs nicht in den Betriebsräumen des Betreibers durchzuführen. Die Bedarfsträger haben hierfür eigene Überwachungsstellen einzurichten. In Ausnahmefällen kann die Nutzung sonstiger Räume des Betreibers für diesen Zweck erfolgen, wenn diese Räume ausschließlich vom Bedarfsträger genutzt werden und dem Bedarfsträger ein Zugang zu den Betriebsräumen nicht möglich ist.

§ 6 Häufung von Überwachungsmaßnahmen

(1) Der Betreiber muß sicherstellen, daß gleichzeitig mehr als eine Überwachungsmaßnahme in Bezug auf ein und denselben Anschluß durchgeführt werden kann.

(2) Die in einer Fernmeldeanlage zu treffenden Vorkehrungen zur technischen Umsetzung von Überwachungsmaßnahmen sind anforderungsgerecht auszubauen und so zu gestalten, daß Engpässe, die in einem regional oder funktional begrenzten Teil einer Fernmeldeanlage bei gleichzeitiger Durchführung mehrerer Überwachungsmaßnahmen auftreten können, unverzüglich beseitigt werden können.

(3) Das Bundesministerium für Post und Telekommunikation kann in Technischen Richtlinien nach § 13 Richtwerte und Mindestwerte für die Anzahl der in einer Fernmeldeanlage oder Teilen einer Fernmeldeanlage gleichzeitig umsetzbaren Überwachungsmaßnahmen festlegen.

§ 7 Benennung des zu überwachenden Anschlusses

(1) Der Betreiber hat eine Überwachungsmaßnahme gegen eine Person, die sein Kunde ist, aufgrund der in der Anordnung enthaltenen Angaben zu Name und Anschrift des Kunden umzusetzen.

(2) Richtet sich eine angeordnete Überwachungsmaßnahme gegen eine Person, die nicht Kunde des Betreibers ist, muß der Betreiber die Überwachung auf der Grundlage eines ihm gleichzeitig mit der Anordnung zu benennenden eindeutigen technischen Kennzeichnungsmerkmals des zu überwachenden Anschlusses, insbesondere der Rufnummer, ermöglichen.

(3) Soweit die besonderen Eigenschaften einer bestimmten Fernmeldeanlage und die berechtigten Anforderungen der Bedarfsträger es erfordern, an einer Fernmeldeanlage verschiedenartige Kennzeichnungsmerkmale für die Bestimmung des zu überwachenden Fernmeldeverkehrs anzuwenden, hat der Betreiber sicherzustellen, daß der Fernmeldeverkehr auf Grund dieser Kennzeichnungsmerkmale überwacht werden kann. Die Kennzeichnungsmerkmale müssen im Einzelfall mit vertretbarem Aufwand zu ermitteln und geeignet sein, den zu überwachenden Fernmeldeverkehr eindeutig zu bestimmen.

§ 8 Technische Schnittstellen

(1) Der Betreiber hat den zu überwachenden Fernmeldeverkehr für die gesamte Dauer der Überwachungsmaßnahme an einer festgelegten technischen Schnittstelle bereitzustellen. Die Schnittstelle muß technisch so gestaltet sein, daß insbesondere

1. an ihr ausschließlich Fernmeldeverkehr bereitgestellt wird, der von dem überwachten Anschluß herrührt oder für diesen bestimmt ist,
2. die Qualität des an ihr bereitgestellten Fernmeldeverkehrs nicht schlechter ist als die, die dem überwachten Teilnehmer bei der jeweiligen Verbindung geboten wird,
3. die Übertragung des an ihr bereitgestellten Fernmeldeverkehrs zum Bedarfsträger mittels genormter, allgemein verfügbarer Übertragungswege und Protokolle erfolgen kann und
4. der im Rahmen einer Überwachungsmaßnahme anfallende Fernmeldeverkehr im Falle der Übertragung über Festverbindungen über einen einzigen Übertragungsweg zum Bedarfsträger oder im Falle der Übertragung über Wahlverbindungen zu einem einzigen Anschluß beim Bedarfsträger übermittelt werden kann.

Die Schnittstelle kann mit dem Ziel der Vereinheitlichung in Technischen Richtlinien nach § 13 festgelegt werden.

(2) Für die Übertragung des an der Schnittstelle bereitgestellten zu überwachenden Fernmeldeverkehrs zum Bedarfsträger sind grundsätzlich Festverbindungen oder ISDN-Wählverbindungen oder ähnlich schnell aufbaubare Wahlverbindungen zu nutzen. Soll die Übertragung zum Bedarfsträger mittels Wahlverbindungen erfolgen, muß die Schnittstelle auch die Fähigkeit zum automatischen Verbindungsaufbau zu dem vom Bedarfsträger zu benennenden Anschluß beinhalten, an den die Aufzeichnungseinrichtung angeschlossen ist. Wählverbindungen zum Bedarfsträger sind zu Beginn eines jeden für den überwachten Anschluß bestimmten oder von diesem herrührenden Fernmeldeverkehrs aufzubauen und nach dessen Ende wieder auszulösen. Die erforderlichen Zugänge zum Wählnetz sind Bestandteil der Schnittstelle.

(3) Der Betreiber hat unter Berücksichtigung der praxisorientierten Erfordernisse, insbesondere der Anforderungen nach § 4 Abs. 2 und 3, festzulegen, von welcher der in Absatz 2 Satz 1 genannten Möglichkeiten er in einer bestimmten Fernmeldeanlage Gebrauch macht. Für den Fall, daß der zu überwachende Fernmeldeverkehr nicht an einer einzelnen Schnittstelle bereitgestellt werden kann, müssen die Schnittstellen so gestaltet sein, daß Wählverbindungen zum Bedarfsträger realisiert werden können.

(4) Wenn der Betreiber die ihm zur Übermittlung anvertrauten Nachrichten durch technische Maßnahmen gegen die unbefugte Kenntnisnahme durch Dritte schützt, ha! er an der Schnittstelle nach Absatz 1 bis 3 die ungeschützten Nachrichten bereitzustellen. Falls der Betreiber dem Teilnehmer Verschlüsselungsmöglichkeiten für die Nachrichten bereitstellt, hat er an der Schnittstelle nach Absatz 1 bis 3 die entschlüsselten Nachrichten bereitzustellen oder dem Bedarfsträger die für eine Entschlüsselung erforderlicher Informationen zeitgerecht zur Verfügung zu stellen.

§ 9 Zeitweilige Übermittlungshindernisse

Falls in Ausnahmefällen die Übermittlung eines zu überwachenden Fernmeldeverkehrs an den Bedarfsträger nicht möglich ist, müssen ihm die Informationen über die näheren Umstände des Fernmeldeverkehrs in dem Umfang, in dem sie der Betreiber gemäß den geltenden

Datenschutz-bestimmungen speichert, unverzüglich nachträglich übermittelt werden. Eine Verhinderung des zu überwachenden Fernmeldeverkehrs ist nicht zulässig. Zu einer Aufzeichnung oder zeitweiser Speicherung des zu überwachenden Fernmeldeverkehrs oder von Teiler desselben über den nach den Datenschutzbestimmungen zulässigen Umfang hinaus, insbesondere der Nachrichten, ist der Betreiber nicht befugt.

§ 10 Selbständigkeit des Betreibers

Der Betreiber hat seine Fernmeldeanlage technisch so zu gestalten, daß er eine angeordnete Überwachungsmaßnahme ohne Mitwirkung anderer umsetzen kann.

§ 11 Unveränderthеit des überwachten Anschlusses

Die Umsetzung einer Überwachungsmaßnahme muß so erfolgen, daß die Überwachung von den am Fernmeldeverkehr Beteiligten nicht feststellbar ist. Insbesondere dürfen die Betriebsmöglichkeiten des überwachten Anschlusses durch die Überwachungsmaßnahme nicht verändert werden.

§ 12 Schutzanforderungen

(1) Die Umsetzung der innerhalb der Fernmeldeanlage erforderlichen technischen Vorkehrungen, auf deren Grundlage die Durchführung von Überwachungsmaßnahmen ermöglicht wird, erfolgt unter Beachtung der beim Betreiben von Fernmeldeanlagen üblichen Sorgfalt, insbesondere hinsichtlich

1. der Schutzbedürftigkeit der Informationen, welche und wieviele Rufnummern einer Überwachung unterliegen oder unterlegen haben und in welchen Zeiträumen Überwachungsmaßnahmen durchgeführt wurden und
2. der Einbeziehung von möglichst wenig Personal für die Umsetzung von Überwachungsmaßnahmen

(2) Ein Zugriff auf die Schnittstelle nach § 8 darf nur den dazu berechtigten Personen ermöglicht werden. Die Schnittstelle ist aus diesem Grund durch physikalische und organisatorische Maßnahmen vor Missbrauch zu schützen.

(3) Der Fernmeldeverkehr darf an die Aufzeichnungseinrichtung des Bedarfsträgers nur übermittelt werden, nachdem die Empfangsberechtigung der Aufzeichnungseinrichtung und die Sendeberechtigung der Schnittstelle nach § 8 nachgewiesen ist. Im Falle der Nutzung von Wählverbindungen zum Bedarfsträger ist dieser Nachweis bei jedem Verbindungsaufbau zu erbringen.

(4) Informationen über die Art und Weise, wie Überwachungsmaßnahmen in einer bestimmten Fernmeldeanlage durchgeführt werden, dürfen Unbefugten nicht zugänglich gemacht werden. Der Betreiber hat auch mit den Herstellern seiner technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen entsprechende Vertraulichkeit zu vereinbaren.

(5) Zur Verhinderung oder Verfolgung eines Missbrauchs der in den Fernmeldeanlagen enthaltenen Funktionen, mit denen die Überwachung technisch ermöglicht wird, ist der Einsatz dieser Funktionen in Bezug auf einen konkreten Anschluß lückenlos zu protokollieren. Darunter fallen auch solche Einsätze, die durch fehlerhafte oder mißbräuchliche Bedienung verursacht wurden. Es sind zu protokollieren:

1. die Rufnummer bzw. das entsprechende Kennzeichnungsmerkmal des betroffenen Anschlusses,
2. Beginn und Ende des Einsatzes,
3. das Ziel, an das der zu überwachende Fernmeldeverkehr geleitet wird und
4. ein Merkmal, welches zur Erkennung des Bedienungspersonals geeignet ist (einschließlich Datum und Uhrzeit der Eingabe).

(6) Der Betreiber hat sicherzustellen, daß die Protokolle nur seinem mit der organisatorischen Durchführung der Überwachungsmaßnahme betrauten Personal oder bei VS-Angelegenheiten nur dem Personal zugänglich gemacht werden, das die Voraussetzungen nach dem Sicherheitsüberprüfungsgesetz erfüllt. Diese Personen prüfen die Protokolle regelmäßig, spätestens alle drei Monate. Das Ergebnis der Prüfung ist schriftlich festzuhalten. Wenn die Protokolle nicht beanstandet werden, sind die Daten unverzüglich durch den vorher genannten Personenkreis zu löschen. Andernfalls sind nur die nicht beanstandeten Datensätze zu löschen, die beanstandeten Datensätze hingegen erst unverzüglich nach Abschluß der zur Klärung der Beanstandung einzuleitenden Maßnahmen. Von Beanstandungen, insbesondere von fehlerhaften oder unzulässigen Eingaben, ist unverzüglich das Bundesamt für Post und Telekommunikation zu unterrichten. In Fällen, in denen es zu Beanstandungen im Rahmen einer angeordneten Überwachungsmaßnahme kommt, ist außerdem unverzüglich der betroffene Bedarfsträger zu informieren.

(7) Das Bundesamt für Post und Telekommunikation ist befugt, Einsicht in die Protokolle und die zugehörigen Unterlagen durch Bedienstete zu verlangen, die die Voraussetzungen nach dem Sicherheitsüberprüfungsgesetz erfüllen.

§ 13 Technische Richtlinien

Die nähere technische Ausgestaltung der Anforderungen nach den §§ 3 bis 12 kann in Technischen Richtlinien festgelegt werden. Diese sind vom Bundesministerium für Post und Telekommunikation zu erlassen. Ihre Herausgabe ist im Amtsblatt des Bundesministeriums für Post und Telekommunikation bekanntzumachen.

§ 14 Geheimschutz

Der Betreiber hat die in seiner Fernmeldeanlage zu treffenden technischen Vorkehrungen so zu gestalten, daß er auch die Überwachung auf Grund einer Anordnung ermöglichen kann, die Verschlußsache im Sinne des § 1 Abs. 2 Nr. 1 des Sicherheitsüberprüfungsgesetzes ist. Der Betreiber ist verpflichtet, mit der zuständigen amtlichen Stelle Vereinbarungen über den Schutz amtlich geheim zu haltender Verschlußsachen (§ 4 Sicherheitsüberprüfungsgesetz) zu treffen.

Abschnitt 3: Zuständigkeiten und Verfahren

§ 15 Zuständige Behörde

Das Bundesamt für Post und Telekommunikation wird mit den Arbeiten zur Vorbereitung der Entscheidung über die Erteilung des Einvernehmens des Bundesministeriums für Post und Telekommunikation nach § 10b Satz 1 des Gesetzes über Fernmeldeanlagen beauftragt. Diese Beauftragung schließt eine Wahrnehmung der Aufgaben nach Satz 1 durch das Bundesministerium für Post und Telekommunikation im Einzelfall nicht aus.

§ 16 Verfahren zur Erzielung des Einvernehmens

(1) Jeder Betreiber hat vor der erstmaligen Inbetriebnahme von Fernmeldeanlagen und vor der Durchführung von Änderungen, die Einfluß auf die Ausführung von Überwachungsmaßnahmen haben können, dem Bundesamt für Post und Telekommunikation ein schriftliches Konzept zur Gestaltung der technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs vorzulegen.

(2) Aus dem Konzept muß hervorgehen

1. die technische Beschreibung der Fernmeldeanlage,

2. die über diese Fernmeldeanlage angebotenen Telekommunikationsdienstleistungen,
3. die in bezug auf diese Fernmeldeanlage nach § 3 bereitzustellenden Informationen,
4. die Beschreibung der technischen Einrichtungen, die der Bereitstellung des zu überwachenden Fernmeldeverkehrs nach § 3 dienen,
5. die Beschreibung der technischen Schnittstelle nach § 8 und
6. die Beschreibung der Vorkehrungen zur technischen Umsetzung der Anforderungen nach den §§ 4 bis 13.

(3) Entspricht das vorgelegte Konzept den Anforderungen der §§ 3 bis 13 und 17, teilt das Bundesministerium für Post und Telekommunikation dem Betreiber schriftlich mit, daß für den Fall der tatsächlichen Umsetzung des Konzeptes und des Vorliegens der Voraussetzungen nach den Absätzen 4 und 5 das Einvernehmen im Sinne von § 10b Satz 1 des Gesetzes über Fernmeldeanlagen erteilt wird. Anderenfalls fordert das Bundesamt für Post und Telekommunikation den Betreiber unter Angabe der festgestellten Mängel zur Vorlage eines verbesserten Konzeptes auf.

(4) Der Betreiber hat die tatsächliche Umsetzung des Konzeptes dem Bundesamt für Post und Telekommunikation durch schriftliche Erklärung anzuzeigen. Etwaige Abweichungen von dem vorgelegten Konzept müssen den geltenden Rechtsvorschriften, insbesondere den Anforderungen der §§ 3 bis 14 und 17, entsprechen. Solche Abweichungen sind in der Erklärung darzulegen und zu begründen.

(5) Auf Ersuchen des Bundesamtes für Post und Telekommunikation hat der Betreiber ihm die Umsetzung des Konzeptes in geeigneter Form nachzuweisen. Dieser Nachweis kann insbesondere dadurch geführt werden, daß der Betreiber den Bediensteten des Bundesamtes für Post und Telekommunikation die Besichtigung sowie die Durchführung von Messungen und Prüfungen einschließlich des hierfür erforderlichen Betretens der Geschäfts- oder Betriebsräume gestattet oder die ordnungsgemäße Betriebsbereitschaft vorführt.

Abschnitt 4: Übergangs- und Schlußvorschriften

§ 17 Übergangs- und Ausnahmeregelung

(1) Vorbehaltlich anderweitiger Regelungen sind die technischen Vorkehrungen für Überwachungsmaßnahmen in Fernmeldeanlagen, die sich zum Zeitpunkt des Inkrafttretens dieser Verordnung bereits Kundenbetrieb befinden oder die bis zum [einsetzen: Datum des letzten Tags des 9. auf die Verkündung folgenden Kalendermonats] den Kundenbetrieb aufnehmen, abweichend von § 4 Abs. 1 Satz 1 bis zum [einsetzen: Datum des letzten Tags des 12. auf die Verkündung folgenden Kalendermonats] entsprechend den Vorschriften der §§ 3 bis 14 zu treffen.

(2) Bei den technischen Vorkehrungen für Überwachungsmaßnahmen im bestehenden Funktelefonnetz C sind Abweichungen von den Vorschriften des § 3 Abs. 2 Nr. 2, 3 und 5, des § 3 Abs. 3, des § 4 Abs. 3, des § 5 Abs. 2, des § 7 Abs. 3, des § 9 und des § 12 Abs. 2, 3 und 5 im Rahmen des am 1. Januar 1995 verfügbaren technischen Verfahrens zulässig.

(3) Für einen Anschluß, der über eine herkömmliche, mit analoger Übertragungstechnik betriebene Anschlußleitung an die Vermittlungsstelle geschaltet ist, kann die Bereitstellung der Überwachungsmöglichkeit noch so lange nach dem am 1. Januar 1995 bestehenden, ausschließlich auf die Anschlußleitung bezogenen technischen Verfahren erfolgen, wie auf Grund der Leistungsmerkmale, die mit dieser Vermittlungsstelle angeboten werden, oder auf Grund der von dem Netzbetreiber auf der Anschlußleitung eingesetzten Übertragungstechnik eine vollständige und zeitgerechte Überwachung mit den bei den Bedarfsträgern vorhandenen überwachungstechnischen Einrichtungen gewährleistet ist.

(4) Die Bereitstellung der Daten gemäß § 3 Abs. 2 Nr. 2 kann unterbleiben, wenn der überwachte Anschluß

a) von einem analogen Anschluß angewählt wird oder

b) aus der Fernmeldeanlage eines anderen Betreibers angewählt wird und die Rufnummer nicht an die Fernmeldeanlage übergeben wird, in der die Überwachungsmaßnahme durchgeführt wird.

(5) Im Rahmen des Einvernehmens nach § 10b Satz 1 des Gesetzes über Fernmeldeanlagen kann das Bundesministerium für Post und Telekommunikation mit Zustimmung der zuständigen Bundesministerien zulassen, daß in Fällen objektiver Unmöglichkeit von der Erfüllung einzelner Bestimmungen des § 3 Abs. 2 abgesehen werden kann. Die Gründe für die objektive Unmöglichkeit sind von dem Betreiber in den Unterlagen nach § 16 darzulegen.

§18 Inkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft.

Wach, wacher, überwach

/emp - Überwachung ist kein Entwurf mehr. Am 4. Mai 1995 verabschiedete das Bundeskabinett die FÜV. Sie soll laut Bundesregierung „flächendeckende" Überwachung gewährleisten. Zum Vergleich: die BRD hörte in den letzten Jahren 10mal häufiger pro Kopf ab als die USA. Gesamtdeutsch gesehen vor 1989 (BRD+DDR zu USA) steigt der Faktor 10 weiter an. FÜV regelt in der „überwachen" BRD weit mehr als nur Abhörbarkeit der Mobilfunknetze: Abhören hat eine neue Qualität. Besondere Leistungen für „Sicherheitsbehörden" (SB): es ist schlüssig, wenn seit einiger Zeit mit der Begründung „Telefonkarten-Imitate" Daten SÄMTLICHER Telefonkarten-Benutzer werden gespeichert und eine SB-Auswertung erfolgt (Par. 6 Häufung). Nach Par. 12(4) dürfen „Unbefugte" von Überwachung nichts wissen. FÜV zwingt Sprecher der TELEKOM, gegenüber der Presse Telefonkarten-Überwachung zu leugnen.

„Verordnungen" zur Einschränkung von Grundrechten sind gefährlich. Es widerspricht demokratischem Rechtsverständnis, den grundgesetzlichen Schutz des Fernmeldegeheimnisses mit „Verordnung" einzuschränken. Übrigens schreibt der Berliner Datenschutz-Beauftragte im 94er Bericht, bei GG Art. 10 sei der Staat als Adressat verschwunden, weil die DBP (Hüter des Fernmeldegeheimnisses) nicht mehr existiert (100% privat).

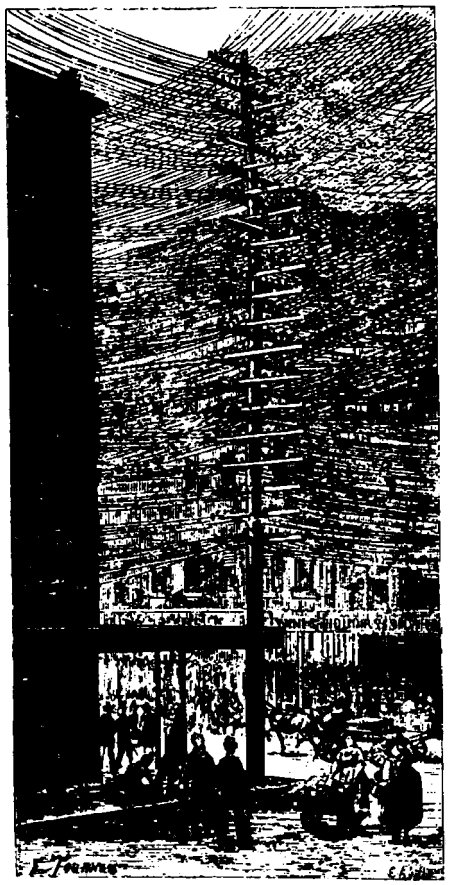
Die hier gedruckte FÜV ist erst ein Anfang. In der aktuellen BT-Stunde forderte Justizmini Schnarri am 17.5. drastische FÜV-Schnüffel-Erweiterung:

- Betreiber-unabhängige Telefonnummern-Datenbank für Sicherheitsbehörden
- internationale Abstimmung der Abhörregelungen mit wichtigen Telefonanbietern
- Regelungen für technische Neuerungen; zB Debit-Karten beim Mobiltelefon
- FÜV-Geltung für nicht-öffentliche Fernmeldeanlagen!!!

Letzteres bringt Schnüffelei in Computern und allen firmeninternen Netzen. Damit erreicht FDP-Justizmini bei Bürgerrechtsfragen ein Niveau unter Null, Beckstein und Kanther können FDP-Ehrenmitglieder werden. Noch ist die FÜV nicht erweitert. Mittelständische Unternehmer sollten überlegen, was Überwachung ihrer Computer durch den Staat bedeutet. Weitere Informationen gibts bei BT-Abgeordneten „zu Fuß", weil der Internet-Anschluß des Bundestages erst im Laborversuchs-Stadium ist. Mehr in „FIFF Kommunikation", Juni 1995, Titel „Information Highway - Im Rückwärtsgang in die Zukunft?" (DM 6; Redaktion: fiff-ko@informatik.uni-bonn.de, Tel 0228-21 95 48)

News aus dem Land der unbegrenzten Möglichkeiten

Edwards E.Cummings, auch Bernie S. genannt, wurde am 13.3.95 in New Jersey von der Straße weg verhaftet, als er gerade dabei war, an mehrere Leute 6,5 Mhz-Kristalle(Quarze) zu verkaufen. Derartige Quarze - tauscht man sie gegen die Standard-Quarze in Radio Shack Telefon Dialern aus und programmiert sie entsprechend - produzieren Töne, die Münzfernsprechern den Einwurf von Münzen vorgaukeln. Dieses Verfahren ist unter der Bezeichnung 'Red Boxes' bekannt, welches seinen Namen einer wirklichen roten Box verdankt, die irgendeine neugierige Person in den späten 70er Jahren von einem Münztelefon abgezogen hat. Die Anklage gegen Ed Cummings, der inzwischen seit ueber 5 Monaten ohne Kaution in Untersuchungshaft sitzt (die anfängliche Kaution von $100.000 wurde zwischenzeitlich fallengelassen), lautet auf : 1. den Besitz eines (laut 2600 nicht funktionsfähigen) modifizierten Radio Shack Touch-Tone Dialers, sowie 2. den Besitz von Software auf seinem Laptop, die zur Veränderung von Telekommunikationsinstrumenten benutzt werden *KANN* und gründet sich auf 2 Ergänzungsgesetze zur Verfassung, die am 21. Oktober 1994 vom Kongress aufgrund des starken Drucks der Telekom-Industrie erlassen wurden. Diese Verfassungserweiterungen stellen u.a. schon den bloßen *BESITZ* von modifizierten Telekommunikationsinstrumenten, von Scannern und sogar von Hard- und Software („used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services") unter Strafe und schließen eine Lücke, die es bis dahin unmöglich machte, bestimmte Arten von Gebührenbetrug zu verfolgen, wie z.B. das Blueboxen oder Redboxen, weil dabei kein spezifischer persönlicher Account mißbraucht wird (das alte Gesetz galt ursprünglich dem Kreditkartenbetrug). Die Terminologie der neuen Gesetze (ss1029) ist so allgemein gehalten, daß nun jeglicher Besitz, jegliche Benutzung, der Verkauf oder Verleih von allem, was „unauthorisierte Benutzung" von, oder „unauthorisierten Zugriff" auf Telekommunikationsdienste ermöglicht, einen Straftatbestand darstellt. Auch Begriffe wie „altered" , „modified" und „telecommunications instrument" bleiben wohlweislich undefiniert. So kann jegliche Veränderung



von Daten in Memory Chips von „Telekommunikationsinstrumenten" wie z.B. das Abspeichern von häufig genutzten Telefonnummern, darunter fallen. Oder jemanden anzurufen, der nicht angerufen werden will, kann als „unauthorized use" interpretiert werden. Und völlig absurd wird es, wenn man sich vor Augen führt, daß schon der Vorgang des Wählens einer Telefonnummer den Inhalt der Speicheradressen

eines Telefonchips „alters". Ed Cummings selbst hofft auf eine breitangelegte Negativ-Publicity und Lobbyarbeit gegen diese neuen Gesetze, die der staatlichen Willkür Tür und Tor öffnen. In einem Brief vom 21.Juli 1995 gibt er seiner extremen Frustration darüber Ausdruck, daß eine effektive Vorbereitung seiner Verteidigung durch die monatelange Untersuchungshaft fast unmöglich sei, da ihm der Zugriff auf nötige Ressourcen fehle. Außerdem habe er seinen Job, seine gesamten Ersparnisse und mehrere Monate seines Lebens („maybe more") verloren, seine Gesundheit sei angegriffen (ihm wurde wiederholt eine für die Wiedererlangung der Funktionsfähigkeit seines Armes notwendige physikalische Therapie verwehrt), und überhaupt durchlebe er gerade „a living hell". Es sei extrem frustrierend, sich auf die Hilfe anderer verlassen zu müssen in bezug auf Dinge, die er selber, wäre er nicht eingeschlossen, perfekt erledigen könnte. Zitat Ed : „Times like these make you realize who your friends really are."

Der Ausgang seines Prozesses berührt uns auch im fernen Europa, weil sich hier auf EU-Ebene durch Antichambrieren von TRANCE TELECOM und Thomson-CSF ähnliche Entwicklungen anbahnen und vergleichbare Rechtsverordnungen in der Mache sind. Wenn etwa in diesem Text der 56 Bit DES-Schlüssel für Py-TV-Programme so enthalten wäre (Konjunktiv), daß das jeweils niedrigste Bit von Wort 20, 40, 60, 80, 100 .... nur hintereinander gesetzt werden müßte, dann wäre das Steganographie und diese Zeitschrift „kriminell" - so die EU-Planung.

Um es noch einmal deutlich zu machen : es geht im Prozeß gegen Ed Cummings NICHT um eine strafbare HANDLUNG, sondern „nur" um einen VORSATZ dazu. Die Rechtsauslegung davon ist genauso dehnbar wie der Satz „Der VERSUCH ist strafbar". Der Musterprozeß zu „verbotenen Bauteilen" birgt die Gefahr, daß die „Gesinnungsjustiz" der Nazizeit wieder eingeführt wird. Denn allein die Behauptung, daß in einem Text wie diesem hier „verbotene Bits" VORSÄTZLICH enthalten seien, könnte zu einer Bestrafung führen. Außerdem müßte die Strafbegründung geheim bleiben, weil sich ja sonst der Sinn des Urteils ad absurdum führen würde.

Zur Erläuterung von „Gesinnungsjustiz" : Zu Zeiten von Adolf Hitler hieß die Gesinnungsjustiz „Willensstrafrecht". Der „totale Staat" brauchte „totale Kontrolle", auch die des Willens. 1934 führte der Nazi-Justizminister Dr. Guertner vor der deutschen Presse aus: „es darf daher keinen Unterschied mehr machen, ob z.B. ein beabsichtigter Mord gelungen ist oder nicht. Entscheidend kann für die Strafbemessung ausschließlich der verbrecherische Wille sein. Hier liegt eine der wichtigsten Neuerungen des kommenden deutschen Strafrechts".

Rund 60 Jahre später soll auf EU-Ebene mit Hilfe von u.a. France TELECOM die Nazi-Justiz des „Willensstrafrechtes" auf Computerebene perfektioniert werden. In den USA läuft das auf Bauteilebene genauso.

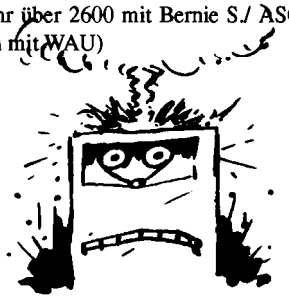
Der erste Prozeßtermin gegen Bernie S. war für den 31.Juli 1995 festgelegt worden, wurde aber inzwischen auf den 8.September 1995 verschoben. Der Richter hat auch mittlerweile einer Kautions-Anhörung zugestimmt, die allerdings erst am 7.9.95, also einen Tag vor dem Prozeßtermin, stattfinden wird.

An folgende Snail Mail Adresse kann Bernie S. geschrieben werden :

Ed Cummings 48919-066 FCI Fairton A-Left P. O. Box 420 Fairton, NJ 08320

Auch e-mails an folgenden Account werden weitergeleitet : bernies@2600.com

Nomade (Qellen:Summer Issue 2600 / Mailverkehr über 2600 mit Bernie S./ ASCII-Austausch mit WAU)



Chirac und der Atom-Kohl

Von Wau Holland

Unterirdische Atomversuche und oberirdische Satellitenplanungen haben einen Zusammenhang. Denn wer Atombomben für den Kriegseinsatz testet, braucht Spionagesatelliten.

Für den Fall, daß es da mit der deutsch-amerikanischen Koordination nicht klappt, hat Kohl die „französische Atom-Karte" im Ärmel. Deshalb sollen Deutschlands Steuerzahler drei Milliarden Markzahlen, damit Chiracs Atombomben Augen bekommen. „Wir machen mit" war die bisher wenig bekannte Haltung von Kohl.

Am 7. Juli 1995 wurde der militärische Beobachtungssatellit HELIOS 1A mit Ariane V75 gestartet. Vier Tage später traf Kohl auf dem Kurzgipfel in Straßburg Chirac und deutete ein Verschieben der Zustimmung auf September an.

Es kann sein, daß der deutsche Zuschuß von drei Milliarden Mark für französische Spionagesatelliten nur dann gewährt wird, wenn Chirac seine Atomtests auch tatsächlich durchführt.

Deutschland, so das Bonner Out-of-Area-Ministerium braucht angeblich die Sat-Aufnahmen für seine weltweiten Bundeswehreinsätze. Allerdings ist anzunehmen, daß die USA im Kriegsfall Satellitenbilder ebenso zuverlässig liefern wie sie es bisher mit Positionierdaten von anderen Satelliten tun.

Dafür gibt es ein Beispiel. Denn das satellitengestützte „Global Positioning System" (GPS) liefert in Friedenszeiten die weltweit empfangbaren Positionsdaten absichtlich gestört. Deshalb haben handelsübliche „zivile" Empfänger nur eine Genauigkeit von 100 Metern bei Längen- und Breiten-Koordinaten „Wo bin ich hier".

Das US-Militär kennt seine „Störungen". Eine relativ kleine Anzahl von militärischen GPS-Empfängern errechnet daraus die auf 20 Meter genauen Koordinaten.

Diese „bessere" Genauigkeit des Militärs hilft Menschen, die auch geistig einen festen Standort haben, zu erkennen, wann ein Krieg beginnt. Denn weil das USA-Militär beim Einmarsch in Haiti nicht genug „Mil-genaue GPS-Geräte" hatte, wurde pünktlich zu Beginn des Einmarsches die „GPS-Störung" abgeschaltet. Dadurch wußte jeder Empfänger, der seine plötzlich auf 20 Meter genaue Position bemerkte,daß „jetzt" irgendwo auf der Welt irgendwas losging. Das Einschalten der Nachrichten brachte dann das „wo" und das „was". In guten Schulen wird sowas als „kombinatorische Logik" unterichtet (etwas anders formuliert in: SATMARKT 8/95, feles-Verl., Trier).

Doch zurück zum HELIOS-System. Es gibt billigere Alternativen. Lockheed bietet bereits für 500 MioDollar ein Komplettsystem samt Start, Bodentechnik und Ersatzsatellit - allerdings ohne Garantie auf Abwesenheit von Trapdoors in der Steuerung (siehe NASA-Hack).

Zusätzlich ist das Militär nicht mehr technische Spitze. Die USA kauften im Golfkrieg „zivile" Bilder der SPOT- und LANDSAT-Systeme, weil auf Bildern von US-Militärsatelliten die getarnten SCUD-Stellungen von Saddam Hussein nicht zu sehen waren.

HELIOS als optisches System ist für Schönwetter-Spionage geeignet. Ab 1996 sollen drei weitere HELIOS-Satelliten gestartet werden und zuletzt HORUS, ein Radar-Satellit der DASA.

Für die drei Milliarden Mark zu Helios will Frankreich die deutsch-französische Rüstungsagentur nach Bonn legen und das Gemeinschaftsunternehmen DASA (Daimler-Benz Aero-Space) mit der französischen Aerospatiale genehmigen.

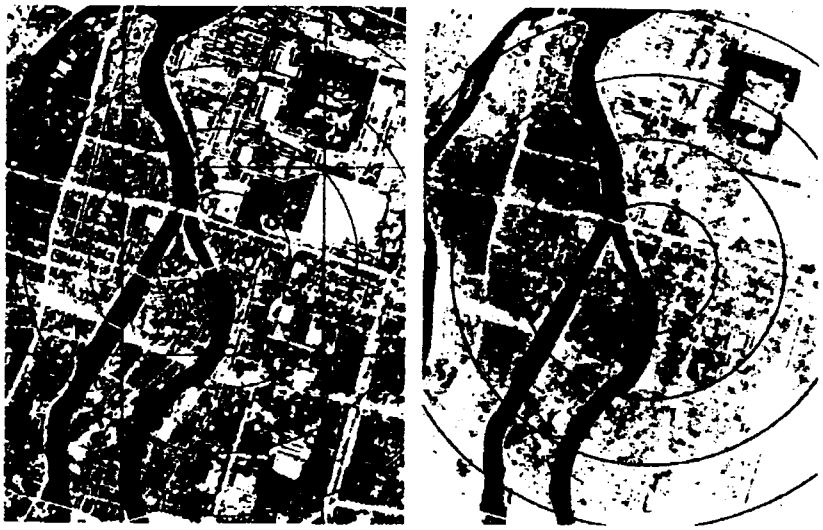
Wenn „Boykott" gegen Frankreich sinnvoll wäre, dann vielleicht gegen Kriegsvorbereitungskonzerne und nicht gegen Winzer.

Viele Infos entstammen dem Beitrag „Schluß mit dem HELIOS-Unfug!" von Wolfgang Möller-Streitbörger aus INFOSAT August 1995. Dort steht im „Steckbrief" zu HELIOS 1A u.a.:

Mission: optische Aufklärung. Auflösung: 1 Meter. Finanzierung: Frankreich 79%, Italien 14%, Spanien 7%. Federführung: franz. Verteidigungsministerium. Hauptauftragnehmer. Raumsegment: franz. Raumfahrtbehörde CNES.

Hauptauftragnehmer, Satellit und Bodenstationen: MATRA Marconi Space (F). MATRA ist auch im Consumer-Electronics-Bereich tätig; Verflechtungen sind bekannt. Weitere Vertragspartner: Aerospatiale (F), Alenio Spacio, Laben (I), Casa, Inisel (E).

atomkohl.txt 1.02 (c) 1995 by Wau Holland
* 03677-790 556 Fax -790 558



Hiroshima vor und nach dem 6. August 1945

Aus der Mailbox gefischt

Der TELESATELLIT-Nachrichtendienst meldet

(leicht überarbeitet)

Nachrichten vom 15.8.95 Happy Holiday

Es sei eine „interne Übertragung", die uns für rund acht Wochen den arabischen Musikkanal art 5 auf Hot Bird 1 13 Grad Ost beschert so die offizielle Version, die sicherlich nicht falsch ist. Was dahintersteckt, hat unser Mitarbeiter Martyn Williams bei Marcello Berengogardino vom italienischen „Satellite Magazine" herausgefunden. Demnach weilt der saudische Prinz al-Walid bin Talal Abdulasis al-Saud, TS-ND-Lesern durch den Aufkauf von einigen Prozenten des Berlusconischen Fernsehimperiums wohlbekannt, derzeit auf seiner Luxusjacht im Mittelmeer. Nun ist Prinz al-Walid bin Talal Abdulasis al-Saud keineswegs unerfahren mit Fernsehsendern, die ebenfalls in Italien ansässigen arabischsprachigen art-Programme gehören ihm. Und er mag sie sogar, sieht sie selbst liebend gerne sogar den Musikkanal art 5. Im Urlaub darauf verzichten? Undenkbar. Eine C-Band-Antenne auf der Luxusjacht ist technisch noch nicht machbar (ab 2,40 Meter), wohl aber der Empfang des bärenstarken Hot Bird 1 (80 cm Schüssel oder noch kleiner). Kurzerhand wurde durch die italienische Telespazio einer der freien CLT-Transponder auf dem Satelliten angemietet, für umgerechnet 640.000 DM. Die Uplink-Kosten schlagen nochmal mit 40.000 DM zu Buche. Für das Geld hätte Prinz al-Walid bin Talal Abdulasis al-Saud eigentlich alle im Programm auftretenden Künstler auf seine Jacht (richtig geraten: die auf dem Dia im Programmvorspann!) einladen und live spielen lassen können.

Ab ins Bett

Fernsehen rund um die Uhr? Nicht in Malaysia. Dort würde man wohl gerne, ein Privatsender hatte das beantragt. Abgelehnt! Den Verantwortlichen dank Zeitverschiebung nachts gezeigt werden mußte. „Informations"minister Mohamed Rahmat beklagte, viele Arbeiter hätten wegen der langen Fußballnächte tagsüber blaugemacht. Fernsehen rund um die Uhr schwäche die Produktivität der werktätigen Massen und verursache Probleme im familiären Bereich.

ACCESS ALL AREAS
London 1995

Es begab sich zu der Zeit, daß eine Hacker-Konferenz einberaumt wurde von einem Untertan Ihrer Majestät Königin Elizabeth. Stattzufinden am ersten und zweiten Tage des Monats Juli in des Königs College in London.

Durch die Gunst indischer Reiseveranstalter war es auch zwei Norddeutschen vergönnt, den langen Weg in das Königreich Britannien zu tun. Und dies ist ihr Bericht:

Nachträglich stellt sich die Frage: Was hat uns eigentlich dazu gebracht, diese Reise auf uns zu nehmen? Letztendlich waren es wohl die Gerüchte, daß sich auch 'die Holländer', 'die Bielefelder' und einige Bekannte vom HOPE auf den beschwerlichen Weg gemacht haben.

Was sich auch als wahr herausgestellt hat.

Die Konferenz selbst stellte sich dann auch als eher bewußtseinserweiternd heraus. Durch einen Einheitseintritt von 25 Pfund (etwa DM 60.–) für zwei Tage leicht entrückt, betraten wir also das zweite Untergeschoss des King's College in London und wurden als nächstes durch die großartigen Dimensionen eines 'Hackcenters' vollends in einen anderen Realitätstunnel gedrückt. Fünf PCs mit Windows und Netscape in einem LAN, welches über eine (am Ende des Tages funktionierenden) 64 kbit ISDN-Leitung ans Internet angeschlossen war. Diese Rechner waren gesponsort; eigene PCs von Konferenzteilnehmern wurden bis zum Ende der Konferenz nicht gesichtet.

Nungut, nichts ist perfekt, es konnte nur besser werden. Dachten wir. Der Blick in das Konferenzprogramm zeigte uns auf, daß wir zumindest nichts verpassen konnten, es gab nur einen wirklichen Vortragsraum, in dem alle Konferenzaktivitäten sequentiell stattfinden würden. Nun gut.

Spätestens jetzt war klar, daß die Klimaanlage wohl über das Wochenende abgestellt worden war. Bei Temperaturen von etwa 28 Grad Celsius im Schatten kein Vergnügen. Das Hakken der Klimaanlage war selbstverständlich verboten, wie auch überhaupt die aktive Hilfe der Konferenzteilnehmer nicht erwünscht war. Man hatte doch tatsächlich den Anspruch, uns für die 25 Pfund etwas 'zu bieten'.

Achja, das 'Programm': Etwa zwei Vorträge fielen aus. Machtnix. Der Mensch, der den Vortrag über Viren hielt, erklärte, was ein 'Bootsector' ist. Das Erstaunen darüber, daß er dies auf einer Hackerkonferenz tat, wurde nur noch von der Überraschung übertroffen, daß sich keiner der Konferenzteilnehmer wehrte. Die Vortragenden in Sachen POCSAC waren der eigenen Muttersprache nicht mächtig. Dafür waren die Sitze so bequem, daß es sich angenehm schlafen ließ. Zum Glück, denn das außerhalb der Konferenz stattfindende Abendprogramm ließ den Tag vergessen. Und wir haben die Party bei Annaliza („Unauthorized Access") wirklich genossen, auch wenn es etwas seltsam anmutete, daß fast keiner der Anwesenden ein Einheimischer war.

Am zweiten Tag gab es immer noch keine gekühlten Getränke, dafür einen Feueralarm, der bestimmt einige Teilnehmer aus dem dringend benötigten Schlaf gerissen hat. Inzwischen hatten wir allerdings einige lange Märsche durch die Stadt hinter uns, ein London A-Z und wir wußten, wo es Nahrung gab.

Die Teilnehmer der Konferenz waren ein Phänomen für sich. Nicht nur, daß der Konferenzveranstalter bei der fünfminütigen Abschlußveranstaltung vom Publikum in Schutz genommen wurde, was man noch mit Solidarität gegenüber dem Folk „from abroad" erklären konnte, nein auch Ausbrüche wie „Why do you talk abou this? This is not about hacking, its about laws. If I want to talk about laws, I would become a lawyer, but I do not want to become a lawyer, I want to become a hacker!" haben abends für leicht hysterische Heiterkeitsausbrüche gesorgt. Über dreihundert Teilnehmer haben für die Betaversion einer Hackerkonferenz bezahlt, aber dieses Verhalten trifft man ja öfter.

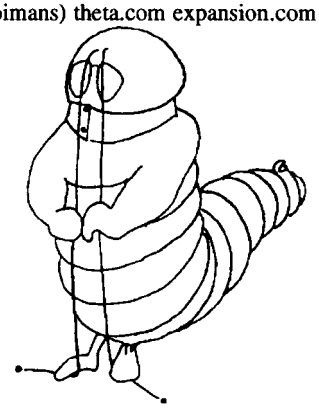
ls141

Scientology besucht Holländischen Internetprovider XS4ALL

Wie die Begründer der Hacktik mitteilten haben Rechtsdeuter des in den USA beheimateten Scientology-Konzerns vor wenigen Tagen versucht, den holländischen Internet-Provider XS4ALL (www.xs4all.nl) zu erpressen. Zwei eigens eingeschwebte Knechte aus der amerikanischen Verwaltung, ein Polizeibeamter, zwei Mietlinge aus dem EDV-Gewerbe und ein Schlosser begehrten Einlass, um die bei XS4ALL befindliche Hardware zu registrieren. Diese sollte als Sicherheit für zu erwartende Schadensersatzforderungen von Scientolgy herhalten. Die Forderungen, so meinte die Church of $cientology (CO$), könnten aus einer Klage resultieren, die von ihr gegen XS4ALL wegen des Betriebs eines anonymen remailers (der seit zwei Monaten offline ist) angestrengt wird. Der Geschäftsführung des Providers wurde, den Meldungen aus Holland zufolge, das Angebot unterbreitet, alle rechtlichen Schritte abzubrechen, wenn die WWW-Seite eines Kunden gelöscht wird, die Scientology-Kritische Informationen enthält. Diese Informationen waren zuvor weitestgehend in der newsgroup alt.religion.scientology verbreitet worden. XS4ALL hat dieses Ansinnen kategorisch zurückgewiesen. Die kriminalisierten Informationen - ein Informationspaket der US-Anti-Sektengruppe FactNet - wurden mittlerweile freiwillig von dem Kunden gelöscht. Das Paket befindet sich inzwischen auf etlichen anderen Servern, die die Seiten spontan übernahmen. Die CO$ versucht seit Ende vorigen Jahres, anonyme remailer im Internet mit allen Mitteln plattzumachen, um eine weitere anonyme Verbreitung von ihr unliebsamen Informationen zu unterbinden. So gab es Attacken mit dem Ziel, die newsgroup alt.religion.scientology zu löschen. Der Versuch dem Betreiber eines anonymen Mailers in Finnland (anon.penet.fi) eine Kinderporno-Story anzuhängen, erweckte den Eindruck einer direkten Umsetzung der scientologischen Handbücher zum Umngang mit Kritikern. Es wurden und werden außerdem kritische Beiträge in Newsgroups mittels gefakter cancel-messages gelöscht. Es gibt starke Hinweise, dass die Attacken von accounts und Systeme laufen, die Scientologen gehören.

Scientology hat sich kürzlich in nahezu allen Bereichen des Lebens unbeliebt gemacht. Neulich sah sich sogar der wahrlich nicht für übermäßige Skrupel bekannte Ring Deutscher Makler zu einem Ausschluss von Scientology-infizierten Firmen veranlasst. Im Gegensatz zu den USA ist die CO$ in Europa unter heftigem Druck. In der Wirtschaft und bei vielen staatlichen Stellen ist der religös verbrämte Psychokonzern als potentieller Verfassungsfeind vorgemerkt. Untenstehend eine kleine Liste von interessanten Domains, die zu zum Scientology-Imperium gehören. Sicherlich kann man sich dort nach weiteren Informationen umsehen.

scientology.com scientology.org earthlink.com (Verwalter aller anderen genannten doimans) theta.com expansion.com



(A-Toll)

Fünf vor zwölf anrufen irgendwo in Frankreich und „Anti-Atom. Anti-Chirac. Protest. Boykott" sagen, versteht jeder Franzose und kostet dreißig Pfennig. Nach der 0033 kommt zentral organisiert entweder eine 1 für Paris und dann acht Nummern oder nur acht Nummern. Ein Bildschirmschoner macht sowas kostenfrei und legt beim ersten Klingeln auf. Infos über Kommunikationszugänge von Atom-Behörden und Umfeld finden sie via Tel. 030-2544 9250 oder WWW.jura2.uni-hamburg.de/ccc

KURZMELDUNGEN

Kartentricks I

/emp - Um eine leere Telefonkarte zu einer Pay-TV-Karte für MTV umzubauen, könnte ein „Telefonchip" sorgfältig von den Kontakten isoliert werden. Das machen personenzugelassene Elektriker z.B. durch Anlegen von 230 Volt an die Chipkartenkontakte mit einem Heizlüfter als Vorwiderstand. Dann könnten die paar benötigten Kartenchipkontakte für u.a. Serial I/O und Masse mit Leitsilber weitergemalt werden. Angeschlossen wird eine notfalls handverdrahtete Schaltung aus 80C31, 74HCT374, 27256 (mind. 2764) und noch einem IC. Das ist die „billigste" Methode. Etwas teurer, aber immer noch unter 25 DM ist die Herstellung einer Platine im verlängerten Chipkartenformat. Einzelheiten finden sich in Mailboxen mit Sat-Technik unter dem Stichwort „LUDICARD". Ludwigs Beschreibung enthält ein ausdruckbares Platinenlayout und praktische Hinweise für Materialbeschaffung und Nachbau. Mit diesem Aufbau und einem Dekoder für Videocrypt I (nicht II) ist es möglich, MTV und BSkyB-Sendungen zu dekodieren. Da MTV im Rahmen einer Sendungsreihe über Jugendrebellion in Europa den CCC Ende Juni 1995 aufgefordert hat, den Code zu knacken, ist der Aufbau einer solchen Schaltung zumindest CCC-Mitgliedern als Forschungstätigkeit anzurechnen.

Kartentricks II

/emp - Chipkarten werden beim Telefonieren und beim Arzt benutzt. Neu ist die Verwendung der Krankenkassenkarte zur Erfassung der Arbeitszeit. Das geschieht schon jetzt in etlichen Zahnarztpraxen. Für die Mitarbeiter dort ist das einfach „praktisch". Krankenkassen sind sauer, weil durch diese ungeplante Verwendung Chipkartenprobleme für „Otto Normalverbraucher" verständlicher werden und Nachdenken anregen. Bei der AOK war eine andere Nutzung der Krankenkassenkarte angedacht: AOK-Versicherte sollten mit ihrer Krankenkassen-Chipkarte samstags auf innerstädtischen AOK-Parkplätzen parken können. Dies hat die AOK-Projektleiterin „Versichertenkarte" beim Bundesverband jedoch sofort unterbunden. Gegen die Verwendung der Chipkarte zur Arbeitszeiterfassung kann sie nichts tun.

Kartentricks III

/emp - Manche Banken lassen auf ihren Parkplätzen nur ihre Kunden parken: die mit der richtigen Bankleitzahl auf dem Magnetstreifen. Mit welcher ec-Karte man auf alle Parkplätze kommt, wissen einige. Das Risiko, ec-Kartendaten an einer Parkschranke zu hinterlassen, ist in der Regel nicht einmal den Rechtsanwälten bewußt, die Bankkunden verteidigen, deren Karte gefälscht und/oder mißbraucht wurde.

Kartentricks IV

(crd) - Schon vor Jahren wurde auf einem Chaos Communication Congress über Risiken von Chipkarten - auch Telefonkarten - berichtet. Bücher und Zeitschriften brachten etliche Fachbeiträge zum Thema. Nun scheint es passiert zu sein: organisierte Kriminelle produzierten Telefonkarten in größeren Stückzahlen. Die TELEKOM badet nun die Altlasten mangelnder Sicherheitsplanung ihres Rechtsvorgängers teuer aus und hat selbst noch nicht genug dazu gelernt. Wenn dann noch ein TELEKOM-Mitarbeiter für 1,8 MioMark (oder war es eine Million Dollar, als der Kurs noch höher war?) ausplauderte, wie Telefonkarten nachgeladen werden können, weist das auf Loyalitätsprobleme hin. Wenn eine 50-DM-Nachbaukarte leer ist, dann - so wurde vernommen -kann sie sich 63mal wieder voll laden. Die Summen, um die es geht, sind enorm: 63mal 50 sind rund 3000 DM und bei einer angenommenen Auflage von 10 000 Stück kommen schon 30 Millionen zusammen.

Heute kann jeder Schüler in den Computerzeitschriften lesen, wie er seine Krankenversicherungskarte mit dem PC im Kinderzimmer modifizieren kann. Es ist nicht nur unmöglich, Chipkarten-Knowhow geheimzuhalten, sondern das Wissen über viele Internas ist in der Informationsgesellschaft Allgemeingut. Der Technologievorsprung schrumpft.

Halbwegs sichere Lösungen

/emp - Gute Sicherheits-Systeme zeichnen sich durch Konzepte aus, die öffentlich bis in die Einzelheiten bekannt sind und trotzdem genügend sicher sind. Ein Beispiel ist PGP, Pretty Good Privacy. Dieses Verschlüsselungssystem liegt im Quellcode vor und ermöglicht die Übermittlung persönlicher Nachrichten und Daten in einer Form, die das Mitlesen unbefugter Dritter drastisch einschränkt oder zumindest für die nähere Zukunft unmöglich macht. Sorgsame Anwendung ist Voraussetzung wie der Haustürschlüssel, der nicht unter der Fußmatte liegt. Zusätzlich kann die eigene Festplatte mit Software wie SFS (secure file system) verschlüsselt werden - eine Empfehlung insbesondere für redaktionelle Arbeiten. Es ist gerade angesichts von „Sperrfristen" in der Medienbranche jedem Journalisten zu empfehlen, in seinem engeren Umfeld für sich einen öffentlichen PGP-Schlüssel zu erstellen und zu nutzen.

Zur Abhörlage der Nation

„Warentest spezial Mobilfunk" der Stiftung Warentest berichtet unter der Überschrift „Mit Vollgas in die Datenfalle" u.a. zum Stand der Abhörmöglichkeiten in Funknetzen " ... in sehr begrenztem Umfange könne bei D1 mitgehört werden, so DeTeMobil-Sprecher Muth. Und D2-Betreiber Mannesmann Mobilfunk spricht von einerm „hohen technischen Aufwand", wenn es um das Abhören seiner Kundschaft geht. Nur im neuen E-Netz seien die erforderlichen Vorkehrungen getroffen, teilt dessen Betreiber mit." Der Streit, so Warentest weiter, drehe sich im wesentlichen um die Bezahlung der Abhöreinrichtungen. Mit Kosten, die allein der Erfüllung staatlicher Aufgaben dienten und keinen Gegenwert im Sinne einer Dienstleistung darstellten, würde Mannesmann seine Kunden nicht belasten, betont Unternehmenssprecher Christian Schwolow. Klartext: „Der Bund soll bezahlen." Danach findet sich der Hinweis: „Wir raten ab: Vom C-Netz, wenn vertrauliche Gespräche geführt werden sollen - das Abhören ist technisch einfach." Gerätetest in „Der Funkamateur" 9/95.

Computer im Kindergarten

/emp - Nach dem Motto „Nie allein, nie länger als eine halbe Stunde und keine schokoladeverklebten Finger" wird der Computer in der Kindertagesstätte (Kita) Seestraße in Berlin-Reinickendorf genutzt. Noch vor zwei Jahren war dieses Projekt bundesweit einmalig. Jetzt sind allein in Reinickendorf vier weitere Kitas dabei. Der Computer ist ein Spielzeug wie jedes andere: es wird benutzt und weggestellt. Beim Erfahrungsaustausch mit anderen Kitas ergab sich: Kinder sind auch vor dem Bildschirm kreativ und kommunikativ. Sie lernen in komplexen Systemen zu denken. Ganz zappelige Kinder können sich vor dem Computer besser konzentrieren. Die These, Kinder würden zu kommunikationsunfähigen und einsamen Wesen vor dem Computer, hat sich nicht bestätigt.

200 DM kassieren und spenden

/emp - Eine „Mißgeburt" nannte Jean Pütz den telekomischen Satelliten „Kopernikus" auf 23,5 Grad. Die „aktive Reserve" für den einzigen „nationalen deutschen TV-Satelliten" TV-Sat2 strahlt noch gut ein Jahr DSR aus, das „Digitale Satelliten-Radio". Ende 1996 laufen die DSR-Mietverträge der Sender aus, was dann passiert, ist unklar. Wer sich im Vertrauen auf die Rechtslage beim einzigen deutschen TV-Satelliten, der genehmigungsfrei zu empfangen war, eine Sat-Antenne kaufte, ist in den Mors gekniffen, weil die TELEKOM TV-Sat2 verschoben hat auf einen anderen Parkplatz am Himmel und auch verkauft: der DSR-Empfang auf der „amtlichen deutschen Himmelsposition" 19,2W fiel weg. Aufgrund „schlechten Gewissens" - so Jean Pütz - zahlt die TELEKOM jedem 200 DM, der ihr nachweist, daß er eine Sat-Schüssel für DSR-Empfang via TV-Sat2 gekauft hat. Die Zeitschrift Infosat sieht sogar die Chance, mit einer Klage gegen die TELEKOM mehr als 200 DM zu bekommen. Der Einfachheit halber: Wie die 200 DM von der TELEKOM zu bekommen sind, beschreibt Jean Pütz im „Hobby-Tip" zur Augustsendung der Hobbythek. Bitte einen mit 1,50 DM frankierten und mit

„Büchersendung" und der eigenen Adresse versehenen Rückumschlag im Format C5 (!!!) zusammenfalten (!!!) und in einen gewöhnlichen kleinen (!!!) Brief stecken und schicken an: WDR Hobbythek „Raumklang", 50 610 Köln. Der Chaos Computer Club wäre erfreut, wenn ein Teil der 200 DM als Rechthilfe-Spende beim CCC landen würde.

Zeitung hat Angst vor Microsoft

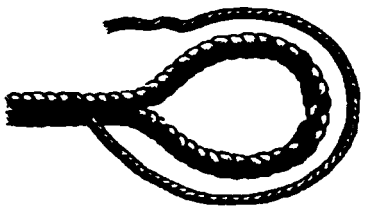
/emp - Die Zeitung „Seattle-Post" weigert sich, Geld für Anzeigen zu nehmen. Wohl weil in der Nähe von Seattle der Microsoft-Sitz Richmond ist, wurde eine CompuServe-Anzeige nicht gedruckt. CI$ gab den Hinweis, daß Microsoft-Network sich in der Entwicklung befindet und keine Chance am Markt hätte, wenn es nicht mit Windows95 gebündelt verkauft würde. Vergleichende Compuserve-Werbung ist in USA so zulässig wie von Apple verteilte T-Shirts mit der Software-Gleichung „Windows'95 = Mac'89".

ct: keine Angst vor Weißem Haus

/emp - Weil deutsche Nachwuchshacker sich angeregt von einem c't-Bericht in Computer des „Weißen Hauses" einhackten, bekamen einige CERT-Leute Schaum vorm Mund und regten sich über „Verantwortungslosigkeit" der Presse auf. Dabei hatte c't verantwortungsvoll berichtet und einige Feinheiten nur angedeutet. Wer davon nichts wußte, fiel beim Betreten der vom Washingtoner Artenschutzabkommen nicht geschützten Computer des Weißen Hauses eben auf. CERT-USA soll lieber ihren Job machen anstatt sich über Kids aus Deutschland aufzuregen und Zeitschriften zu beschimpfen!

CCC-Mitgliederversammlung

(crd) - Weil ds voll und Bericht nicht fertig, diesmal nix von der MV. Better luck next time.



Adressen

CHAOS-HH – CCC Hamburg
Treff jeden Dienstag ab 20 Uhr in den Clubräumen. Danach meistens bei Costa. Adresse siehe Impressum.

CHAOS-B - CCC Berlin
Treffen jeden Dienstag ab 20 Uhr in der Kronenstr. 3, Berliner-Mitte (U6/2-Station Stadtmitte) im dritten Stock (über dem Friseur). Fax c/o Botschaft +49 (30) 2292429 (eigene beantragt). Briefpost: CCC, Kronenstraße 3, D-10117 Berlin.

CHAOS-HL - CCC Lübeck
Treff am ersten und dritten Freitag im Monat, 19 Uhr in der Röhre (gerade Querstraße, geht von der Mengstraße ab). Briefpost: CCC-HL, c/o Benno Fischer, Bugenhagenstr. 7, D-23568 Lübeck, Voice +49 (451) 34799, Mailbox Mafia +49 (451) 31642.

CHAOS-SüdThür
Treff Di 18-20 Uhr Porzellanfabrik Martinroda neben dem Schornstein (von Norden auf der B4 kurz hinter DOS-Dorf). Briefpost CCC-SüdThür Arnstädterstr. 26/7, 98693 Martinroda, Voice +49 (3677) 790556, Fax +49 (3677) 790558

CHAOS-Ulm - Treffen jeden Mittwoch, 19 Uhr im Café „Einstein"

SUECRATES - Stuttgarter Computerrunde mit Zeitschrift d'Hacketse. Kontakt: T.Schuster, Im Feuerhaupt 19, D-70794 Filderstadt, e-mail: norman@delos.stgt.sub.org

2600 Magazine - Amerikanische Hackerzeitschrift Overseas $30 individual, $65 corporate. Back issues available for 1984-88 at $25 per year, $30 per year overseas. Adress all subscription correspondence to: 2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0099. Office Line: +1 (516) 751-2600, Fax +1 (516) 751-2608

Foebud-BI - Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V., Bielefeld Treffen jeden Dienstag, 19:30 Uhr im Cafe „Spinnerei", Heeperstrasse 64, dort voice: +49 (521) 62339 Monatl. „Public Domain"-Veranstaltung; Themen und Termine siehe Mailbox BIONIC. Voice: +49 (521) 175254, Fax +49 (521) 61172, Mailbox BIONIC +49 (521) 68000. FoeBuD, Marktstraße 18, D-33602 Bielefeld, e-mail: zentrale@bionic.zer.de

Künstliches Auge

Zu guter Letzt: der Bestellfetzen

Chaos Computer Club e.V. Schwenckestr. 85 D-20255 Hamburg Telefon + 49-40-4903757 Telefax + 49-40-4917689	Vorname _____ Name _____ Strasse _____ PLZ, Ort _____ Telefon _____

B E S T E L L F E T Z E N - FÜLL AUS, IF Überweisung THEN fax:=vaild
Version 27B/6-1 ELSE einschicken + V-Scheck or money

Mitgliedschaft im Chaos Computer Club e.V. - Abo in Mitgliedschaft inklusive

__ __	1,- DM	Satzung des Chaos Computer Club e.V.
__ __	20,- DM	Einmalige Verwaltungsgebühr bei Eintritt
__ __	120,- DM	Normal-Jahresbeitrag. Dauerauftragalternative: 10,- pro Monat
__ __	60,- DM	Sozial-Jahresbeitrag. Dauerauftragalternative: 5,- pro Monat

Datenschleuder Abonnement für 8 Ausgaben, erscheint vierteljährlich

__ __	60,- DM	Abonnement, Normalpreis
__ __	30,- DM	Abonnement, Sozialpreis

Bücher bzw. diverse Druckschriften

vergr.	33,33 DM	Die Hackerbibel, Teil 1 (260 Seiten A4), Erstellung 1981-1985
vergr.	33,33 DM	Die Hackerbibel, Teil 2 (260 Seiten A4), Erstellung 1985 - zur Zeit vergriffen
__ __	7,50 DM	CCC-Studie für die Grünen über politische Computereinsatz
__ __	16,00 DM	Elektronische Informationssystem für den Umweltschutz
__ __	5,00 DM	Dokumenation zum Tod von "KGB"-Hacker Karl Koch
__ __	20,00 DM	Zerberus-Mailbox-BenutzerInnen-Handbuch
__ __	50,00 DM	"Lock Picking" Dokumentation über das Öffnen von Schlössern
__ __	15,00 DM	Dokumentation zum Chaos Communication Congress '93

Softwaresammlungen, Diskettenformat angeben: 5.25", 3.5", 360/720/1.2/1.44

__ __	25,00 DM	Sammlung von Verschlüsselungsprogrammen, neues PGP + Handbuch
__ __	25,00 DM	Programmiersammlungen für blaue Töne, POCSAC-Decoder etc.

Aufkleber, spritzwassergeschützt, wunderschön und überhaupt

__ __	3,33 DM	3 Aufkleber Chaos-Knoten + "Kabelsalat ist gesund"
vergr.	5,00 DM	15 Aufkleber "Achtung Abhörgefahr" - auch für Mobiltelefone
vergr.	5,00 DM	Bogen mit Postknochen-Aufklebern verschiedener Größe
vergr.	5,00 DM	Bogen mit 10 Aufklebern "globales Dorf - rechtsfreier Raum"
vergr.	5,00 DM	Bogen mit 15 A023/042Z Zulassungszeichen
__ __	5,00 DM	Bogen mit 64 Aufklebern "Chaos im Äther - ich höre zu"

__X__	5,00 DM	Portopauschale
-->		Der Sozialtarif gilt für Schüler und minderbetuchte Studenten etc.
-->		Da unser Versandpersonal ehrenamtlich tätig ist, bitten wir um Verständnis für Lieferzeiten bis zu max. 6 Wochen

_____ DM Gesamtbetrag (bitte die Protopauschale, und bei Mitgliedschaft die Verwaltungspauschale NICHT vergessen)

__ __ Bargeld anbei __ __ V-Scheck __ __ Überweisung auf Konto 599090-201 Postbank Hamburg (BLZ 200 100 20) erfolgt am: _____._____._____

Eingang Betrag erhalten Erledigt: