Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

WHO SAYS

P A R A N O I A

ISN'T „IN"

ANY MORE ?

Ein Organ des Chaos Computer Club - Postvertriebsstück - C 11301 F - Einzelpreis DM 3,50 - Nr. 43, Juni '93

IMPRESSUM

Die Datenschleuder

s wissenschaftliche Fachblatt für Datenreisende

Heft 43 (Zählnummer für Abonennten)

Juni 1993

Da wir als Zentrale o.ä. sowieso nicht taugen, empfehlen wir immer und überall dezentrale Aktivität bzw. Kontaktaufnahme zu lokalen Gruppen / Menschen.

Adresse:

Die Datenschleuder

Schwenckestr. 85

D-20255 Hamburg 20

Tel.: +49-40-4903757

Vmb.: +49-40-497273 (Tonwahl erforderlich)

Fax.: +49-40-4917689

Mbx.: +49-40-4911085 (CHAOS-HH.ZER)

Internet/UUCP: ds-red@ccchh.ccc.de

Mailserver/UUCP: ccc-serv@mail.ccc.de

BTX: *CCC#

Redaktion: (A)ndy, Cash, Rababa, Hanneke, rowue, Terra, Nomade

ViSdPg: Ralf Prehn

Herausgeber: Chaos Computer Club e.V.

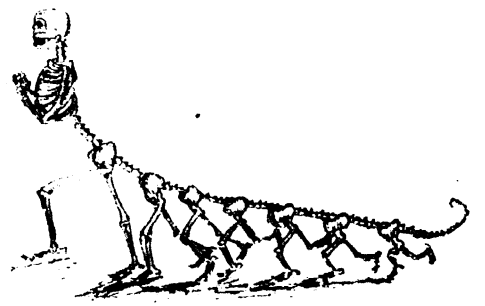
Druck: Bernd Paustian, Schwenckestraße, Hamburg

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

[*und namentliche gekennzeichnete sowieso nicht, der Sätzer*]

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

Adressänderungen von Abonennten bitte doch am besten schriftlich (Postkarte genügt).



Stanislaw Lem: Adre

Editorial

Nach einigen Stunden ue, oe, ae gegen ü, ö, ä tauschen, [*Wir bitten um EINDEUTIGE Umlaute*] kleben und Aufkleber auf unseren Körpern verteilen ist es nun soweit. Sie ist fertig. Fehlen tut das eine oder andere, wie zum Beispiel der Artikel über die Zyxel's, hier wird noch recherchiert.

Ansonsten sollten wir uns endlich mal merken, daß Farbband VOR und nicht während des Ausdruckens zu wechseln, den Grund merkt mensch beim Lesen.

Nunja, wir sind nicht ganz so SNAFU wie sonst, haben aber auch etwas länger gesetzt, vier Tage direkt hintereinander, aus geplanten 16 wurden 24 Seiten, einiges kam noch ran, und mußte unter fingerbrechenden Bedingungen bearbeitet werden. Aber trotzdem (oder gerade weil:) wenn Ihr was habt, schickt es uns, auch wenn Ihr denkt, es weiß jeder und bringt nichts: „everything counts..."

Ansonsten: zu diesem 23.05 keinen Artikel, sondern nur einfach stilles Andenken - und das Wissen: menschen zählen für einige (un)menschen nicht. Wer das nicht glaubt, der sollte mal die Zeitung aufschlagen.

Last but not least: Totgesagte leben länger.... Totgeschwiegenes ewig

Fernmeldegeheimis ?

Datenaufzeichnung bei Mobiltelefonen

Daten, die bei einem Autotelefon automatisch von Telekom aufgezeichnet werden, dürfen in einem Strafprozess als Beweismittel verwendet werden. Dieses Urteil fällte der Bundesgerichtshof in Karlsruhe gegen einen Angeklagten, der sein Autotelefon zur Anbahnung von Straftaten benutzt hatte. Die Strafkammer eines Landgerichts hatte von Telekom Auskunft über die Verbindungsdaten zu Telefongesprächen des Angeklagten verlangt, weil das Gericht feststellen wollte, von wo aus der Angeklagte zur jeweiligen Tatzeit telefonierte. Das Landgericht verwertete lediglich Datum, Uhrzeit und die Angabe der jeweiliegen Funkvermittlungsstelle, nicht jedoch die Rufnummern der Teilnehmer. Der Bundesgerichtshof stufte dies als zulässigen Eingriff in das Fernmeldegeheimnis ein. Soweit für die Aufzeichnung von Telekom eine besondere gesetzliche Grundlage erforderlich sei, müssten die Aufzeichnungen im Interesse des Fernmeldeverkehrs bis zur Neuregelung der gesetzlichen Ermächtigungen zur Datenerhebung aufgenommen werden. Eine Telefonüberwachung, wie sie nach der Strafprozessordnung nur bei Verdacht auf bestimmte Straftaten erlaubt ist, liegt nach Auffassung der Bundesrichter bei der Datenverwertung nicht vor, weil sich die Auskünfte auf die Vergangenheit bezogen, nicht aber auf den laufenden Telefonverkehr. (AZ BGH 5 StR 394/92)

[Quelle: vision No. 2 März 1993, Zeitschrift für Führungskräfte der Telekom, ISSN 0941-5556, Herausgeber: Generaldirektion Telekom, Geschäftsbereich Presse und Öffentlichkeitsarbeit,
Postfach 2000,
D-W-5300 Bonn 1]

MOBILTEL.D43 LS16

„Hacker" verhaftet

Neue Gesetze in den Niederlanden

Seit dem 1. März 1993 ist es dann so weit: nun ist Hacking auch in Holland verboten. Kaum 3 Wochen später hatte Hacker RGB aus Utrecht die zweifelhafte Ehre, das erste Opfer des neuen Computerkriminalitätsgesetzes zu sein.

RGB wurde in einem Terminalraum der „Vrije Universität" Amsterdam festgenommen. Er hatte keinen offiziellen Zugang zu dem Universitätscomputer, und soll den Account eines „regulären" Benutzers des Rechners verwendet haben. Hierfür kann mensch in den Niederlanden seit dem 1. März zu maximal 6 Monaten Freiheitsentzug verurteilt werden. Von diesem Rechner aus soll er sich auf den Rechner der Universität Delft weitergeschaltet haben, wo Ihn der Sysop bemerkte. Hierfür kann es bis zu 4 Jahren Freiheitsentzug geben.

Obwohl er nur wenige Tage von der Polizei verhört wurde, wurde er 38 Tage in U-Haft behalten. Derzeit ist unklar, wie es weiter geht, und was von Seite der Justiz noch kommt. Wahrscheinlich wird versucht, ein Exempel zu statuieren, es ist aber fraglich, ob die Beweise ausreichen, um dies zu tun. Nach der Aussage von Professor Francken, der an dem Gesetzentwurf beteiligt war, sind nicht Hacker die Zielgruppe, sondern „wirkliche" Kriminelle. In der Öffentlichkeit entsteht das Bild, als würde hier mit Kanonen auf Spatzen geschossen.

hanneke

TRIPLE YOUR READING SPEED

Lufthoheit ist Funkhoheit

Frankfurt, 29.3.93 (e.mp/wh) - Die sehr hohen Höhenflüge alliierter Flugzeuge zum Containerabwurf sind in Jugoslavien im Unterschied zum Irak notwendig, weil dem Irak jenseits zweier Breitengrade die Funkhoheit entzogen wurde. Das Einschalten des Luftabwehrradars, also das Aussenden elektromagnetischer Wellen, wurde dem Irak auf Teilen seines Staatsgebietes verboten, und Verstöße werden mit Bombadierung der Funkwellenquellen bestraft. So streng ist „man" derzeit nicht in Teilen des Gebietes, das in MEYER's Hand-Atlas von 1866 als „europäische Türkei" bezeichnet wurde.

Wie hoch über einem Land hinweggeflogen werden darf und kann, zielt auf die Unterscheidung zwischen Luftraum und Weltraum, ein juristisch schwammiger Raum. Im internationalen Faustkeilrecht gilt grob vereinfacht die Regel, der Luftraum reicht so hoch wie die Luftabwehr schießen kann und jenseits davon beginnt der Weltraum. Bekanntlich verschob sich diese Grenze vor ein paar Jahrzehnten nach oben, als es den Russen zum Erstaunen der Amis gelang, das Spionageflugzeug U2 abzuschießen. Die Flughöhe über exJugoslavien, der ehemaligen europäischen Türkei, orientiert sich auch an der von Serben bekannten Schußhöhe, da ja denen im Unterschied zum Irak der Flugabwehr-Radarbetrieb nicht verboten wurde. [*Die Kroaten haben auch leider kein Öl*]

Daß serbische Schüsse auch einem deutschen Lademeister an Bord einer Bundeswehrmaschiene lebensgefährliche Verletzungen in 3200 Meter Höhe zufügen konnten, war laut Regierungssprachregelung auf eine Art von „Materialermüdung" zurückzuführen. Diese Verkohlung wurde von ARD und Pro7 im Unterschied zum ZDF fast 24 Stunden verbreitet, ohne daß dazu in der BRD die kriegsübliche Militärzensur erlassen werden mußte. So eine freiwillige Selbstkontrolle der Kampfmoral ist angesichts der Überfülle an Fernsehsendern mit ihren Action News schon ein paar Wochen später aus dem öffentlichen Bewußtsein verschwunden und wird vom Mantel der Geschichte gnädig umhüllt. Nun pokert die Bundeswehr hoch über den Serben außerhalb des NATO-Gebietes mit fliegerischen Behelfseinsätzen. Aber die offizielle Einladung der Ungarn, in AWACS über Ungarn zu fliegen, mußte die Bundeswehr lufthoheitslogisch ausschlagen.

Wau

Kurzmeldungen

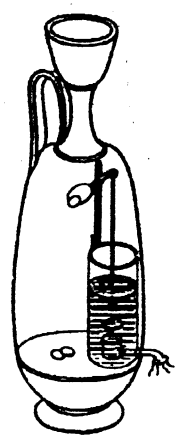
Postleidzahlen

Die 3teilung der P*st schreitet offenbar gut voran. In Berlin zumindest kann man wohl P*st-Dienst und Telekom keine übermäßige Koope-
ration vorwerfen. Das just (Mitte Juni) erschienene Telefonbuch (ca. 1.5 Millionen Auflage) enthält komplett alte Postleidzahlen.

0190er gesucht

Für ein im wesentlichen der allgemeinen Bewußtseinserweiterung dienendes Projekt im Sinne des Allgemeinwohles sucht der Erfa-Kreis Geld-Beschaffung des CCC's noch für einen Zeitraum von 4-12 Wochen eine 0190-Nummer samt PMX. Unkosten werden erstattet. Kontaktaufnahme bitte per Fax z.Hd. LS 16.

KURZ1.D43 Andy



81 Weihwasserautomat nach Heron.

DVD - Deutsche Vereinigung fuer den Datenschutz
IKÖ - Institut für Informations- und Kommunikationsökologie e.V.
Bonn, den 18.02.1992

Datenschützer:

Gesundheitsreform
teilweise verfassungswidrig

Chipkarte und EDV-Speicherung der Diagnosen und medizinischen Behandlungen zur Kostendämpfung nicht erforderlich.

DatenschützerInnen aus der „Deutschen Vereinigung für Datenschutz" (DVD) und vom „Institut für Kommunikationsökolgie" (IKÖ) haben das am Freitag vom Bundesrat verabschiedete Gesundheitsstrukturgesetz als „großen Schritt zum gläsernen Patienten" kritisiert. Mit der Chipkarte, die an Stelle des Krankenscheins treten soll, würde ein „System der Überwachung und Rationalisierung der Gesundheit" eingeführt.

Im Gesetz ist vorgesehen, daß alle ÄrztInnen die Krankheiten ihrer PatientInnen nach einem vierstelligen Zahlenschlüssel der Weltgesundheitsorganisation erfassen. Die Diagnosen sollen an die Kassenärztlichen Vereinigungen und Krankenkassen weitergegeben und dort in Computern gespeichert werden. Zweck der Erfassung und Speicherung ist nach der amtlichen Begründung die Kontrolle der ÄrztInnen, um Kosten zu sparen.

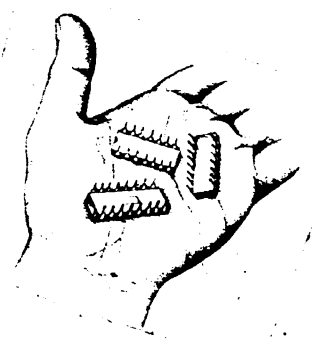
Nach dem neuen Gesetz sollen die Kosten aber vor allem durch Höchstbeträge begrenzt werden. Für Leistungen der Krankenhäuser und Ärzte sowie für Medikamente, Heil- und Hilfsmittel schreibt der Gesetzentwurf feste Obergrenzen vor. Werden mehr Leistungen erbracht, wird die Vergütung für die einzelnen Leistungen entsprechend gekürzt. Die Erfassung der Diagnosen und Behandlungen in Computern werde dafür nicht benötigt, so die DatenschützerInnen. Die „Totalerfassung der Gesundheitsdaten" sei zur Kostenersparnis überflüssig. Sie koste Milliarden für neue Computer und Software, die aus den Versicherungsbeiträgen bezahlt werden müßten.

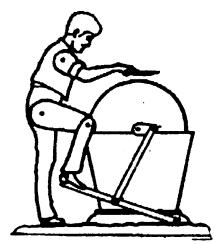
Die Erfassung und Weitergabe von Diagnosen nach dem Gesetz verstößt nach Ansicht der ExpertInnen gegen das Recht auf informelle Selbstbestimmung, das nach dem Volkszählungsurteil des Bundesverfassungsgericht verfassungsrechtlich geschützt ist. Danach darf der Staat nur so viele persönliche Daten der BürgerInnen erfassen und speichern, wie er für seine Aufgaben braucht.

Die InformatikerInnen und Juristen aus DVD und IKÖ befürchten, daß die gespeicherten Gesundheitsinformationen später benutzt werden könnten für ein „System der staatlichen Verwaltung und Zuteilung von medizinischen Leistungen", in dem die Alten und Behinderten nicht mehr ausreichend behandelt werden, weil sich „der Aufwand für sie nicht lohnt".

Datenschutz Nachrichten (DANA)
DVD und IKÖ
Reuterstr. 44
D-W 5300 Bonn 1
Tel.: +49-228-222498

DANA





Briefe...

..die wir bekommen

Schutz von Daten vor unbefugtem Zugriff

ie haben Schwächen in der Verarbeitung on Geschäftsdaten bzw. wird vermutet.

) Ihr Anrufbeantworter ist mit einer Fernbfrage ausgerüstet. Schlechte Codes wie 11, 222, bis 999, 123, 456, 789, 321, 654, 87 helfen nicht, sich vor der Abfrage durch lie Konkurrenz zu schützen. Vertrauen sie inem Gerät ohne Fernabfrage oder verwenlen Sie einen effizienteren Code.

:) Sie verwenden Raubkopien bzw. PDSoftware mit unbekanntem Ursprung. Daauf können sich sogenannte Viren befinden, lie die Software und so den Computer unbrauchbar machen werden.

3) Sie verwenden eine schnurloses Telefon oder ein C-Netz-Telefon, daß nicht abhörsicher ist.

Sagen Sie es allen Freunden (vielleicht dieser Brief per Fax) weiter und warnen Sie vor diesen Gefahren.

[*Humor ist wenn mensch trotzdem lacht, die Paranoia*] Posteingang

Anti-Viren-Mehlbox

Der NDR hat eine Anti-Viren-Mailbox eingerichtet. Dies geschah im Zusammenhang mit dem VTC. Diese ist zu erreichen unter der Hamburger Rufnummer: 54 715 235 (8N1, 2400-14.400). Dort sollen die aktuellsten Anti-Viren-Programme uploadbar sein.

[*Testet das Ding mal ein bisschen*]

NDR-Pressemitteilung

Neuer Chef beim BSI

Das Bunteamt für Unsicherheit in der Information BSI hat einen neuen Leiter bekommen, nachdem Dr. Otto Leibrich in den Ruhestand getreten ist, ist nun Dr. Dirk Heinze Präsident des BSI geworden. Dem Herrn Leibrich wurde für seine Verdienste beim Aufbau des Soft und Hardware TÜV das Bundesverdienstkreuz erster Klasse überreicht.

Bei dieser Gelegenheit gab es dann auch eine Ansprache unseres Bundesinnenministers (der für die Innere Unsicherheit Zuständig ist) Rudolf Seiters. Dieser wies auf die Gefahren für Wirtschaft und Verwaltung in der Informationsgesellschaft durch Bedienungsfehler, Mißbrauch oder Sabotage hin. Sein besonderes Augenmerk galt hierbei der organisierten Kriminalität, die die Möglichkeiten der Informationsgesellschaft weltweit nutze. (Das tut meine Bank auch) Ebenfalls habe die Sicherheit bedauerlicherweise nicht Schritt halten können mit den rasanten Entwicklungen in der Informationstechnik.

Herr Henze war früher als Leiter der „Koordinations- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung" im Bundesinnenministerium tätig.

Quelle : Innenpolitik Information des Bundesministeriums des Inneren, Nr.3/93

rowue

realer „Sozialismus"

Mitterand spinnt im Datennetz

Paris/Peking, 30.03.93 (e.mp/wh) - Ganz kurz vor der Wende in Frankreich ließ sich Mitterand eine Funkzentrale in seinen Regierungssitz bauen, mit dem er wie eine Spinne im Informationsnetz die Top-News vom Botschaftsfunk mithören kann. Außerdem ließ er zu Anfang des Jahres rund 30 französische Botschafter in seinem Sinne auswechseln. Das ist der Versuch strategischen Machterhaltes, wenn schon die sozialistischen Parteisitze von rund 250 auf etwas mehr als 50 schrumpften.

Die Volksrepublik China hat bei der SED-Nachfolgerin PDS angefragt, warum denn der Sozialismus ausgerechnet in Deutschland gescheitert ist. Vielleicht leitet die PDS die Antwort in Kopie an Mitterand weiter. Auf dem ComLink-Datennetz diskutiert die PDS über ihre Antwort an die chinesischen Genossen, falls das Scheitern des Sozialismus nicht zur parteiinternen geheimen Verschlußsache erklärt wird.

Wau

Aus Chalisti 15:

BSI: Doch ein Schrecken ?

Ein halbes Jahr existiert das neue Bundesamt für Sicherheit in der Informationstechnik schon. Im Augenblick noch in 3 Häusern getrennt untergebracht, wird das neue alte Bundesamt im August in sein Gebäude in Bonn-Bad Godesberg, gegenüber dem Hotel Maritim, einziehen.

Interessant für uns sind aber weniger die neuen Gebäude, als eher die Arbeit des Bundesamtes. Wie in der Chalisti 14 geschrieben, ist das BSI mit seinem Arbeitsbereich für den CCC ein Augenmerk wert. Die Frage, ob - und besonders wie - es seine Aufgaben wahrnimmt ist nicht nur für uns, sondern für die Gesellschaft im allgemeinen von besonderer Wichtigkeit. Wenigstens sollte es so sein, aber das Amt kann im Stillen seinem Aufbau nachgehen und bekommt von vielen Seiten - auch Journalisten - eine Schonfrist zugestanden. Wir halten im Hinblick auf die zukünftige Entwicklung der Gesellschaft zur Informationsgesellschaft die Arbeit des Bundesamtes für zu wichtig, um es jetzt einer zu langen Schonung zu gewähren. 100 Tage sind lange vorbei, also machen wir uns Gedanken über das BSI ...

Am Anfang sehen wir unsere Aufgabe darin weitere Informationen über das BSI zu geben, so wie es uns bekannt und belegbar sind. Die wichtigsten Informationen über eine zentrale staatliche Stelle sind Personen, Struktur und Finanzen. Also beschäftigen wir uns erstmal mit diesen Punkten. Dabei wollen wir versuchen besonders Zusammenhänge und Hintergrundwissen zu vermitteln. Wir tragen dabei u.a. auch Material zusammen, welches schon im Spiegel oder anderen Publikationen veröffentlicht wurde.

Struktur

An der Spitze des BSI steht als Präsident Dr. Otto Leiberich. Knapp über 60 Jahre alt, 1946 Abitur, 1947 Mathematik an der Uni Köln studiert, 1953 Promotion mit einem Thema aus der höheren Algebra, danach wissenschaftliche Tätigkeit, dann Dienst in der Zentralstelle für Chiffrierwesen (ZfCh) und dem späteren ZSI. Davon zwischen 1962 und 1974 Chefmathematiker und seit 1974 Leiter des ZSI und eben heute Präsident des BSI. Als Vizepräsident steht ihm Dr. Mertz beiseite.

Diesen beiden Personen sind die 6 Abteilungen des BSI unterstellt. Desweiteren sind diese Abteilungen in mehrere Referate unterteilt. Wir stellen sie hier dar, wie der Stand am 25. März 1991 war. Die Quelle sind die Informationen über „Struktur, Ausstattung und Planungen des BSI vom 5.4.1991". Soweit wir hier feststellen konnten, hat sich weder an der Struktur noch an den Personen wesentliches verändert. Insbesondere sind die hier als N.N. angegebenen Posten bis heute noch nicht besetzt worden.

Abteilung I „Zentrale Aufgaben", Dr. Mertz, Durchwahl: -655

Referat I 1, RR Dickopf, -313
Grundsatz, Recht, Organisation, IT-Koordinierung, Zentrale Dokumentation, Bibliothek, Öffentlichkeitsarbeit

Referat I 2, RD'n Dr. Werthebach, 346599
Personal

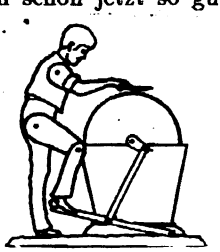
Referat I 3, Wahrnehmung durch AL I
Haushalt, Beschaffung

Referat I 4, RR Samsel, -653
Innerer Dienst, Sicherheit

Abteilung II, „Wissenschaftliche Grundlagen und Zertifizierung", N.N.

Zu dieser Abteilung gehört unter anderem auch die Technologiefolgenabschätzung unter IT-Sicherheitsaspekten, wobei diese im Augenblick eher von Abteilung zu Abteilung geschoben wird. Es fühlt sich de facto keiner zuständig. [*Kollege kommt gleich..., der gast*] Die Hoffnung auf eine eigene Abteilung dieses komplexen Themas und Forschunggebietes kann schon jetzt so gut wie aufgegeben werden.

Geplante Unterteilung:



· Mathematische Grundlagen
· Technische Grundlagen
· Allgemeine Analyse des Gefährdungspotentials, Grundlage der Systemsicherheit und Evaluierung
· Zertifizerung, Zulassung, Normung

Abteilung III, „Mathematische Sicherheit", - RD Hange, -660

Dieser Abteilung obliegt im Rahmen des Par. 3, Abs. 1, Nr. 6 BSIG bei Bedarf auch der Entzifferung von Straftätern entwickelter Verfahren zur Verschlüsselung, z.B. aus der Rauschgiftszene.

Referat III 1, N.N.
Entwicklung mathematischer Sicherungsverfahren

Referat III 2, ORR Dr. Liebefrau, -658
Evaluierung mathematischer Sicherungsverfahren

Referat III 3, N.N.
Sicherheitsanalyse

Referat III 4, RD Bahr, -659
Software-Realisierung mathematischer Sicherungsverfahren

Abteilung IV, „Technische Sicherheit", VA Schwirkmann, -569

Diese Abteilung begleitet die Entwicklung von neuen Produkten bezügl. Sicherheitserkenntnissen und verfügt über langjährige Erfahrungen mit den zuständigen Stellen in den USA und bei der NATO.

Referat IV 1, BD Siedentop, -573
Technische Realisierung mathematischer Sicherungsverfahren

Referat IV 2, BOD Dr. Hembach, -641
Verschlüsselungssysteme

Referat IV 3, BD Koos, -423
Schlüsselmittel

Referat IV 4, BD Dr. Dorst, -546
Abstrahlsicherheit

Referat IV 5, BOR Sanne, (02254) 38-(1) 76 (ehemals BSG/BMI)
Lauschabwehr, Abstrahl- und Lauschabwehrprüfungen

Referat IV 6, RD Schnelder, (0221) 7924205
Materielle Sicherungstechnik

Abteilung V, „Sicherheit in Rechnersystemen", LRD Everts, -232
Aus dieser Abteilung kommen die bekannten IT-Sicherheitskriterien, sowie das gerade in Vorbereitung befindliche IT-Sicherheitshandbuch, welches im Herbst erscheinen soll. Der von Dr. Leiberich geäusserte Wunsch, daß sich das BSI vordringlich mit Verschlüsselung und Lauschabwehr - gerade auch im Hinblick auf neue Gefahren von innen und außen - schlägt sich hier deutlich nieder.

Referat V 1, ORR Felzmann, -234
Systembezogene Risikoanalyse

Referat V 2, ORR van Essen, -228
IT-Sicherheitstandards

Referat V 3, BD Dr. Kreutz, -229
· Maßnahmen zur Systemsicherheit

Referat V 4, ORR Dr. Kersten, -237
Evaluierung von IT-Systemen/-Komponenten

Referat V 5, ORR Dr. Ganser,
Technik für Systemevaluierung und -entwicklung

Abteilung VI, „Beratung und Unterstützung", N.N.

Die Planstellen in dieser Abteilung können frühestens 1992 beantragt werden. Allein die Beratungseinheit für den materiellen Geheimschutz existiert, weil diese vom Verfassungsschutz übernommen wurden.

Referat VI 1, N.N.
Grundsatz, Schulung, Informationsdienst

Referat VI 2, RD Meissner, (0221) 7922508
Beratungsdienst I

Referat VI 3, N.N.
Beratungsdienst II

Referat VI 4, N.N.
Unterstützung der Polizeien, Strafverfolgungs- und Verfassungsschutzbehörden, Auswertung der Sicherheitserkenntnisse.

Personal

Für das Jahr 1991 verfügt das BSI über 278 Planstellen/Stellen. Davon wurden 153 vom BND, 41 von BfV und 24 vom BGS übernommen, sowie 60 neu geschaffen. In den nächsten Jahren soll für 1992 50, für 1993 10 und für 1994 15 weitere Planstellen/Stellen geschaffen werden. Innerhalb der Abteilungen besteht folgenes Verhältnis der Planstellen/Stellen:

Abteilung I	61
Abteilung II	18

Abteilung III	18
Abteilung IV	119
Abteilung V	40
Abteilung VI	18

Zum Teil wird das Personal übergangsweise in seinen ursprünglichen Dienststellen beim BfV und beim BGS unterkommen. Den Stellenwert der einzelnen Abteilungen kann jeder Anhand der Personalzahlen und im Verhältnis zu den Aufgaben gemäss BSIG (siehe Chalisti 14) selbst ablesen. Aber auch die Finanzen können über das BSI eine Menge aussagen. Besonders zu kritisieren ist der Punkt „Beratung". Die Abteilung IV wird nur langsam erweitert und erreicht als einzige Abteilung ihre Ausbaustufe erst 1994.

Finanzen

Dem BSI stehen im Haushaltsjahr 57,1 Millionen DM zur Verfügung. Davon 22,6 Millionen DM fuer Forschung. In diesen 22,6 Millionen sind insgesamt 15 Millionen für die ehemalige BND-Unterabteilung ZSI „Chiffrierverfahren und Meßverfahren fuer kompromittierende Abtrahlung" vorgesehen. Dazu hat der Bundesrechnungshof am 10.4.1991 für die Sitzung des Innenausschuss des Bundestages am 17.4. festgestellt: „Das BSI hat keine Forschungsarbeiten durchzuführen. Diese ursprünglich im BSI-Errichtungsgesetz aufgenommene Aufgabe wurde bei den Ressortberatungen ausdrücklich gestrichen, um eine praxisbezogene Arbeitsweise des Bundesamtes sicherzustellen.". Es werden also Gelder nicht gesetzgemäß eingesetzt. Laut Auskunft eines Mitarbeiters des BSI soll aber der Bundesrechnungshof (BRH) dies inzwischen teilweise zurückgenommen haben. Allerdings konnten wir in keiner unserer Unterlagen - bis hin zum Antrag auf eine entsprechende Gesetzesänderung, die diese Haushaltsmittel betreffen - für diese Aussage einen Beleg finden.

Aber nicht nur die Tatsache ist interessant. Auch für was dieses Geld im Bereich der Forschung ausgegeben wird. Schon bestehende Verträge über Entwicklungen beim BSI regen zum Denken an:

- Entwicklung eines hochintegrierten Kryptomoduls für den universellen Einsatz in IT-Sicherheitsprodukten: 1.000.000 DM
- Entwicklung eines Schlüsselgerätes für packetvermittelte Netze (Datex-P). Dieses Gerät kann auch für Verbindungen zwischen Rechnern verwendet werden, die über das Breitband-ISDN verbunden sind: 500.000 DM

(Anm. der Redaktion: [*Challisti*] Die Verschlüsselung von DatexP und ISDN Inhaltsdaten (vermutlich auf der Ebene des HDLC) ist eine Maßnahme, die besonders für Militärs und Behörden interessant ist. Wirtschaft und noch mehr die Gesellschaft müßen genauso an dem Schutz der Verkehrsdaten (Wer mit wem wann was) interessiert sein. Entsprechende Mechanismen existieren in der Theorie, wie z.B. an der Uni Karl-

sruhe bei Dr. A. Pfitzmann, aber diesbezügl. ist beim BSI nix zu sehen. Der Staat schützt sich, vergißt aber die Bürger zu schützen. Dies ist auch ein kleiner Punkt, der aufzeigt WO das BSI SChwerpunkte setzt.)

- Entwicklung von Kleinschlüsselgeräten für den Polizeibereich, um diese weitgehend abhörsicher zu machen: 500.000 DM
- Entwicklung von hochintegrierten Kryptochips, die bei vielen Anwendungen in der IT verwendet werden: 1.600.000 DM
- Entwicklungen auf dem Gebiet der Abstrahlmeßtechnik und Lauschabwehr (z.B. Entwicklung
eines speziellen Meßempfängers und einen Röntgenmeßplatzes): 1.668.000 DM

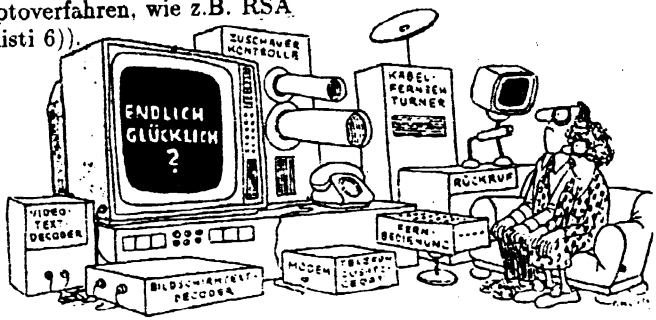
Diese sind exemplarisch für Gegenstände im Haushaltsplan die auf Grund ihrer Techniken zentral fuer Geheimdienste oder das Militär interessant sind. Dem gegenüber stehen aber auch Mittel für Aufgaben, die eher für die Wirtschaft und Gesellschaft wichtig sein könnten:

- Erprobungsmuster Schlüsselmittelverteilung (KDC): 5.000.000 DM

(Anm. der Redaktion: Dies könnte für Verfahren der elektronischen Unterschrift wie z.B. TeleTrust bei der GMD interessant sein)

- Erstellung des IT-Sicherheitshandbuches: 40.000 DM (Anm. der Redaktion: Soll im Herbst erscheinen und enthällt z.B. auch zwei Kapitel über Risikoabschätzung und Technologiefolgenabschätzung).
- Entwicklung von asymetrischen Verfahren für die Verschlüsselung von Authentisierungs- und Signaturverfahren (elektronische Unterschrift). (Anm. der Redaktion: Asymetrische Verfahren sind Public Key Kryptoverfahren, wie z.B. RSA (dazu siehe Chalisti 6)).

Bedenklich sind dann aber schon wieder angegebene Sachmittel für die Evaluierung des Betriebssysteme von Siemens BS 2000 (450.000 DM) und Sinix (40.000). Hier ist klar die Frage zu stellen, warum die Betriebssysteme von Siemens auf Kosten des Steuerzahlers evaluiert werden. Bei einer Einstufung des Systemes in die IT-Sicherheitskriterien entstehen der Firma klare Wettbewerbsvorteile gegenüber anderen Mitbewerbern und ein solcher Eingriff in den Markt ist sicher nicht zulässig. Natürlich könnte angeführt werden, daß diese Betriebssysteme in der öffentlichen Verwaltung eingesetzt werden und daher die Einstufung für den Bund interessant ist. Für den Fall ist natürlich zu fragen, ob die entstehenden Kosten der Evaluation bei Entscheidungen über neue Anschaffungen berücksichtigt werden und ob solche Firmen wie Siemens die Ergebnisse der Evaluation erfahren und damit dann auch wieder Werbung machen könnten. Dabei existiert klar die Aussage aus dem BSI, daß die Zertifizierung vom Antragssteller zu bezahlen ist und dafür gibt es auch einen entsprechende Gebührentabelle. Auf Anfrage wurde uns mitgeteilt, daß die im Haushaltsplan keine Evaluationskosten, sondern Forschungsmittel darstellen. Warum steht da aber explizit „Evaluation des Betriebssystemes BS2000" ??? Eine andere Auskunft lautete, daß diese Evaluationen noch aus der Zeit des ZSI seien. Auf der einen Seite meint das BSI, daß es nicht fair wäre immer an ihre Vergangenheit zu erinnen, da sie ja etwas neues seien. Auf der anderen Seite werden größere Summen für Aufgaben aus dieser Vergangenheit bereitgestellt. Schizophren ?



I.T.

Auf jeden Fall ist im Vergleich zu der Gesamtaufwendung, ist der Bereich der potentiell wirklich beitragen könnte bestimmte Risiken für die Gesellschaft zu vermindern recht lächerlich und wohl eher mit anderer Intention in den Plan genommen worden. Dabei ist dies auch eine Aufgabe des BSI.
Natürlich sind nicht nur die laufenden Verträge - die zum Teil noch aus ZSI-Zeiten sind - interessant, weil sie wenig über die aktuelle Arbeit. des BSI aussagen. Daher sind die demnächst vorgesehenen Vergaben noch weit aus interessanter. Geplant sind:

- Sicherheitsuntersuchung des Secury Communication Processor SCOMP der Firma Honeywell; Einsatz geplant bei NATO-Agenturen: 750.000 DM
- Untersuchung des Betriebssystemes OS/2 mit Zusatzkomponenten (Voruntersuchungen schon 1990 durchgeführt): 650.000 DM.
- Entwicklung eines Prototyps für die Datensicherung in lokalen Netzwerken (geplant für AA): 900.000 DM
- Weiterentwicklung (Anm. der Redaktion: !!!) von Protokollierungsverfahren zur Erfassung sicherheitsrelevanter Ereignisse (Datenveränderung, Manipulation, u.a.): 150.000 DM
- Nutzung von Entwicklungen der künstlichen Intelligenz zur Sicherheitsüberwachung von Anwenderhandlungen in IT-Systemen (Anm. der Redaktion: Oder anders gesagt: Little Brother is watching you, on your system): 150.000 DM
- Entwicklung und Weiterführung von „Anti-Viren"-Programmen und -Aktionen, besonders für den Bereich der Bundes- und Länderbehörden: 70.000 DM
- Studie über eine Informationsbank zur Beratung über den Einsatz von IT-Sicherheitsprodukten: 178.000 DM
- Marktstudie über PC's und Netzwerke als Grundlage für Beratung und Entwicklung: 69.000 DM
- Entwicklung eines Werkzeuges zur Spezifikation und Verifikation von IT-sicherheitsrelevanter Software
- Studie über die Sicherheit eines Bürokommunikationssystems im Bundeskanzleramt: 100.000 DM
- Entwicklung eines Überwachungssystems für Abstrahluntersuchungen an IT-Sicherheitsprodukten: 200.000 DM
- Entwicklung von Prototypen des Schlüsselgerätes ELCORVOX 1-5: 800.000 DM

Bei diesen Zahlen verwundert das Resümee des BRH nicht: „Wir haben den Eindruck, daß die neuen, durch das BSI-Gesetz festgelegten Aufgaben, die letztlich die Ursache für die Errichtung des BSI waren, über die Wahrnehmung der alten, noch aus dem BND-Bereich stammenden Aufgaben nicht ihrer Bedeutung entsprechend berücksichtigt werden. [...] Erkenntnisse aus unseren Prüfungen auf dem Gebiet der Sicherheit der Informationstechnik zeigen, daß die festgestellten, schwerwiegenden Mängel nicht aus fehlenden Chiffrierverfahren und -geräten resultieren, sondern wesentlich im fehlerhaften Einsatz und der mangelnden Kontrolle der IT begründet sind. U.E. sollte die Errichtung des BSI nicht als Fortführung der Arbeiten der ehemaligen BND-Unterabteilung ZSI mit zusätzlichen Aufgaben in einem anderen Geschäftsbereich verstanden werden; die Aufgabenschwerpunkte sollten sich vielmehr im gesetzlich festgelegten Rahmen am vordringlichen Bedarf der gesamten Bundesverwaltung orientieren."

Ein Schnitt für das BSI ?

Als CCC'ler bin ich zusätzlich der Meinung, daß genau diese Fortführung der ZSI im BSI vielfach befürchtet wurde, und nun anscheinend auch eintreten. Die Warnungen an Öffentlichkeit und Politik sind Jahre alt und wurden kaum gehört. Egal ob diese von bekannten Professoren oder verschiedenen gesellschaftlichen Gruppen vorgebracht wurden. Es ist erfreulich, daß der Bundesrechnungshof von selbst die Erkenntnis gewonnen hat, daß diese

Befürchtungen evntl. doch der Wahrheit entsprechen könnten und von seiner Seite her auch Taten folgen läßt. So hat der BRH im Änderungsantrag vom 21.5.1991 dem Bundestag vorgeschlagen, die Titel die sich auf „Kosten für Forschungs- und Entwicklungsvorhaben" beziehen sowie den damit in Zusammenhang stehenden Erwerb von Geräten, etc zu sperren. Dabei handelt es sich ingesamt um eine Summe von 12,45 Millionen DM.

Wie der BRH bin ich auch der Meinung, daß die Beratung gerade des normalen Betroffenen garnicht und die Beratung der Wirtschaft kaum berücksichtigt wurde. Leider hat das BRH sich garnicht zum Bereich der Forschung im Bereich der Technologiefolgenabschätzung geäußert. Hierfür scheint es keinen einzigen Pfennig zu geben. Dabei sollte (und laut BSIG ist es das auch) gerade dies eine Aufgabe des BSI sein. Es soll bei Gesetzen beratend tätig werden und muß auf die möglichen Risiken des Einsatzes der IT aufmerksam machen. Dieser erst nachträglich aufgenommene Punkt im Artikel 2, Abs. 7 BSIG sollte weit aus mehr in Personal und finanziellen Mitteln berücksichtigt werden.

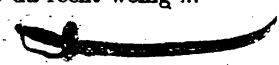
Nun folgen noch einige Randbemerkungen über das BSI, die doch den ersten Eindruck weiter verstärken.

Was ist mit den 40 Ex-DDRlern ?

Schon in der Chalisti 14 erwähnten wir einen anderen Punkt im Bezug auf das BSI. Nämlich die Ausweisung von 40 Mitarbeitern des ehemaligen zentralen Chiffrierorgan (ZCO) der DDR. Diese wurden - anders als viele andere aus dem ehemaligen Ministerum des Innern der DDR - nicht zum 31.12.1990 gekündigt, sondern wurden erstmal übernommen und dem BSI zugeteilt. Ihr Arbeitsverhältnis sollte auf Grund einer Kabinettsentscheidung, daß keine MdI-Mitarbeiter in Bundesbehörden übernommen werden sollen, am 31.3.1991 erlöschen. Auf Anfrage der Bundestagsabgeordneten Frau Ingrid Köppe von B90/Grüne aus Sachsen-Anhalt nach Verbleib dieser 30 Mitarbeiter wurde ihr mitgeteilt, daß im BSI nie Mitarbeiter des ZCO beschäftigt wurden und werden. Die damals ausgewiesenen Mitarbeiter hatte die Aufgabe des ZCO aufzulösen. Warum nun allerdings gerade SekretärInnen und Kryptgraphen (die stellen die Mehrheit dieser 40 Leute) besonders geeignet sind das ZCO aufzulösen ist ebenfalls unklar. Was aus diesen Mitarbeitern geworden ist, wird nicht deutlich.

Big BSI ist watching you ?

Das BSI nimmt natürlich auch an Forschungs- und privaten Netzen teil. Dabei wird es von den wenigstens wahrgenommen, dabei werden im BSI explizit auch die Newsgruppen (Bretter) gelesen. Dabei werden betreffende Beiträge auch genommen, gedruckt und an die betreffenden Stellen In-House verteilt. Dabei ist unklar, in wie weit Beiträge rausgefischt werden, die das BSI direkt oder nur in seiner Arbeit betreffen. Ebenfalls unklar ist, wie diese Beiträge erfaßt und archiviert werden, und vielleicht eines Tages dem Autor zum Nachteil gereichen. Dabei ist besonders zu bedenken, daß Schreiber von Beiträgen in den Netzen nicht durch das Presserecht geschützt werden. Ob hier einfach Gedankenlosigkeit oder nur die Nutzung und Freundlichkeit Einzeler gegenüber Mitarbeiter im BSI herauskristalisiert, kann nicht gesagt werden. Um aber das richtige Verhältnis dazustellen sollte deutlich folgenes gesagt werden: Es sieht nicht danach aus, als würden Nachrichten systematisch und regelmässig gelesen und weiterverteilt oder gar weiterverarbeitet. Es sprechen fehlendes Personal beim BSI sowie Äusserungen einzelner BSI'ler dagegen. Aber das Gefühl, daß ein Bundesamt wie das BSI mitliesst, wird sicher bei einzelnen dazu führen, daß sie ihr Netzgeflogenheiten ändern. Ein Bundesamt mit einem gewissen Prozentsatz von ehemaligen Mitarbeitern von BKA, BND, BfV und BGS ist, sollte sich nicht im geheimen, sondern öffentlich im Netz darstellen. Wie in der BSI-Dokumentation geschrieben, ist das BSI auf Vertrauen angewisen. Dieses muss geschaffen werden. Leugnen der Vergangenheit gilt da recht wenig ...



Das BSI rät

Nach Vorbild der amerikanischen Computer Emergency Response Teams, sollen in Deutschland und Europa Anlaufstellen für Sicherheitsprobleme eingerichtet werden. Ein Ziel solcher Anlaufstellen in den USA ist es, daß eventuelle Angriffe und Sicherheitslöcher schnell an die betroffenen und verantwortlichen Stellen weitergeleitet werden können. In den USA wird das CERT von einer Gruppe Leute betrieben, die mit möglichst wenig Formalien auskommen, allerdings ein Zugriffsverfahren unterhalten, welches regelt wer welche Informationen bekommen kann. Das BSI ist natürlich auch in den Verteilern der amerikanischen CERT's und zwar mit der höchsten Priorität.

In Deutschland ist noch unklar, welche rechtliche Grundlagen und welche Struktur das CERT in Deutschland schlußendlich besitzen soll. Diese Fragen werden im BSI gerade

angegangen und sollen bis Ende des Jahres geklärt sein. Gewünscht wird, daß dezentral Ansprechpartner als CERT vorhanden sind und dort in den verschiedenen Problembereichen helfen können. Allerdings gibt es für die spezielle Problematik „Viren" schon zwei Anlaufstellen: Das Viren-Text Center in Hamburg von Prof. Brunnstein und das Mikrobitcenter der Uni Karlsruhe. Auf weitere muß wohl noch gewartet werden.

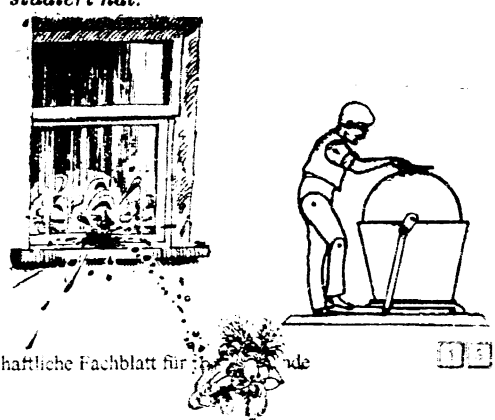
Im Augenblick existiert aber schon KITS. Dies steht für Kommunikationsplan IT-Sicherheit und soll auf Behördenebene die zügige Verteilung von Information bezügl. Angriffe und Sicherheitsproblemen gewährleisten. Falls ein solcher Fall eintritt, dann gehen die Informationen an eine Stelle im Bundeskriminalamtes. Das BKA informiert dann das Bundesinnen-, das Bundesverteidigungs- und das Bundeswirtschaftsministerium, die obersten Bundesbehörden, denn Bundestag, den Bundesrat, die Bundesbank, das Bumdesamt für Verfassungsschutz, den Bundesbeauftragten für den Datenschutz, das Bundesverfassungsgericht, den Bundesrechnungshof, natürlich das BSI, das Bundesverwaltungsamt, sowie die Landeskriminalämter. Bei Bedarf werden auch die Landesämter für den Verfassungsschutz sowie die IT-Hersteller benachrichtigt. Letzteres geschieht über ausgewählte Verbände, die entsprechend angeschrieben werden.

Quo vadis BSI ?

In und um das BSI geht es weiter neblig zu. Die Befürchtung, daß das BSI zu einem deutschen NIST bzw. NCSA oder gar NSA werden könnte, sind auch auf Grund des heutigen Kenntnisstandes nicht auszuschließen. Natürlich sind auch optimistische Töne aus dem BSI zu vernehmen. So ist geplant, daß über Mailarchive, und Textserver wichtige Informationen verfügbar gemacht werden soll. Außerdem wird das BSI, sobald seine Verbindungen ins EUnet stabil funktionieren, auch entsprechende Informationen über diesen Weg verbreiten. Im Augenblick hält mensch sich damit noch bedeckt. Verwirrende Postings mit dem Absender zsi.uucp, verlorengegangene Mails an diese Adresse, nicht beantwortete Mails an bsi.de hängen alle damit zusammen, daß die Netzwerkverbindungen beim BSI erst sicher gestaltet werden sollen. Wie sagte jemand noch aus dem BSI ? „Was könnte sich ein Hacker schöneres vorstellen, als ins BSI reinzukommen". Auf jeden Fall denkt das BSI wohl an mehr Transparenz als im Augenblick realisiert scheint.

terra

[*Dieser Artikel ist zwar etwas älter, zeigt aber die Probleme auf, die nicht nur wir mit dem BSI haben, insofern wünschen wir dem neuen Leiter Dr. Henze viel Glück, und hoffen, daß er auch einige Semester Philosophie studiert hat.*



Erfahrungsbericht

Telefonieren in Ost-Berlin

Unter dem Einfluß der deprimierenden Tatache, daß wir 1/2 Stunde nach einem ktiven Münzer in Berlin/Ost gesucht aben und schließlich gegen Mitternacht ur einen weiteren defekten Münzer fanen, entschlossen wir uns zur Selbsthilfe und lemmten einen präparierten Wählknochen rokodilhaft an freischwebende Kupferenen. Mit Erfolg. Dummerweise kam bald rauf eine Kutsche mit 3 Zivilbullen einer um uns mit vorgehaltener Win-chester uf frischer Tat zu ertappen. Mal abgeehen von einem Lachkrampf meinerseits hlug die Geschichte hier ins Nega-tive m. Beschlagnahme eines Wunderknochens, ufnahme von Personalien. Keine zwei onate später flattert eine Vorladung von en Bullen ins Haus, die wir, dem Rat erhrener Berliner folgend, ignoriert haben as rechtlich ok ist).

as nächste Schreiben vom Staat kam om Amtsgericht und nannte sich Strafefehl, das heißt etwa: „Wir sparen uns e Verhandlung und Sie bekennen sich huldig und zahlen!". Und zwar 1500.- zw. 1000.- (Tat bzw. Beihilfe). Da uns dem Schreiben allerdings auch zur Last legt wurde, wir hätten ein Kabel herisgerissen (Sachbeschädigung, Schadenserztzvorderung vom Gilb), haben wir Widerruch eingelegt, und uns von bekannten ktivisten - zugegebenerweise terminknapp eine Woche vor der sodann angesetzn Hauptverhandlung - einen Rechtsanalt empfehlen lassen. Was sich zweifelsohne s vorteilhaft erwies. Zu dieser Verhandng waren neben uns und den drei Bullen ch ein Sachverständiger von der Telekom laden. Eine Einsicht in die Akte vor Verndlungsbeginn ergab:

1) Die Telekom kann aufgrund mangelnder Technik im Osten nicht sagen, ob und wieviel Einheiten verpulvert worden sind,

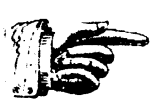
2) Das Prüfkommando von der Telekom (Sachverständiger) hat nach der Tat bei Inspektion des fraglichen Münzers keinen Schaden festgestellt, auch kein raushängiges Kabel!

Da also außer Zeugen keine Sachbeweise gegen uns vorlagen (immerhin hätten wir nun behaupten können, die Störung und diverse 0130er angerufen zu haben), da jedoch Leistungserschleichung schon durch atypische Nutzung der Kabel vorliegen könne, wurde nun zwischen Verteidiger und Richter in einem wahrhaft sehenswerten Kuhhandel kompromißhaft beschlossen:

Das Verfahren wird eingestellt (keine Vorstrafe), der Laberknochen wird einbehalten (der war tatsächlich Gegenstand des Kuhhandels) und die Delinquenten blechen je 500.- an einen gemeinnützigen Organismus (als Auflage). Fazit: Glimpflich davongekommen. Dem CCC ist zu empfehlen, sich bei einschlägigen Gerichten als gemeinnützig zu melden, offenbar fließen von Gerichten die höchsten Spendengelder. [*Ne, die fließen woanders, die Party*]

Nach der Verhandlung hat uns der Postler noch ganz interessiert gefragt, wie wir da Leistung erschlichen hätten, ohne ein Kabel anzuzapfen. Die Verwirrung legte sich erst, nachdem festgestellt wurde, daß ein drittes Telekomteam direkt nach der Tatnacht das Gerät repariert haben muß. [*gestatten: Tuttle - Heizungsmonteur*]

Ulrich Unbekannt



„Hacker-Club"

Dataterm

Ich war in der letzten Zeit total auf dem Hackertrip. [*Wo kann mensch den kaufen?, der sitzer*] Also blätterte ich in einem meiner zahlreichen Computerhefte (ohne Schleichwerbung zu machen) und da sah ich im Computerflohmarkt eine Anzeige des Dataterm Hackerclubs. Ich wunderte mich, denn soweit ich weiß ist das Hacken nach STGB [*II. WKG, der Ätzer.*] strafbar (Scheiße...). [*legal, illegal, ..., nightshift*] Aber was soll's, wenn die sich das leisten können Werbung in Zeitschriften zu machen, dann kann man denen auch nicht mehr helfen, wenn die von der Polizei oder vom Gilb an das Messer geliefert werden. [*werden?, das messer*]

Egal, ich habe mich dann einfach mal bei denen gemeldet und die haben auch gleich gesagt was Sie machen und was nicht. Ich wurde sofort mit einbezogen und auch in alles eingeweiht.

Die Führung des Clubs besteht aus vers. Hackern, die aus den neuen und alten Bundesländern kommen. Die haben zwar noch nicht soviel Pionieraktionen vollbracht wie der CCC, aber die Stimmung in der Gruppe ist super. Alles in allem kann man aber sagen, selber ausprobieren.

Nein, wenn man irgendwelche Probleme oder so hat, dann einfach melden und Posteingang = Postausgang, das heißt, daß man nach ca. 1 Woche einen Antwortbrief auf den Tisch liegen hat. Das dauert so lang, weil die nur einmal in der Woche das Postfach leeren. [*Geil, laßt mal unsere Anfragen hinschicken, der Beantworter.*]

In nächster Zeit haben die auch vor, so eine Art HACKERFETE zu machen, aber da die armen nur sehr wenig Mitglieder bei sich haben, lohnt es sich noch nicht für die so etwas zu machen. Aber wenn ca. 100 zusammen kommen, dann werden die es so schnell wie möglich machen, aber z.Zt. steht kein konkreter Termin fest.

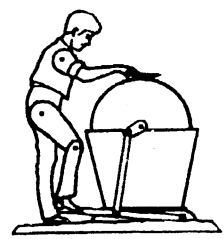
Darum möchte ich mich hier an alle wenden, die auch im CCC sind und möchte diese bitten sich doch einfach mal zu melden und einfach mal den Club zu testen und eine doppelte Mitgliedschaft kann ja auch keinem schaden, [*eine doppelte Staatsbürgerschaft auch nicht, auch wenn diese keinem nützt, der Würger*] denn der Beitrag beträgt im Monat 5.-, also noch erträglich und noch zu erwähnen wäre, daß es dafür eine 20-30 seitige Clubzeitschrift gibt und eben dann die Mitgliedschaft mit Clubausweis und der guten Stimmung. DATATERM ist garantiert keine Konkurrenz für den CCC, denn Dataterm hat keine so professionellen Hacker, wie der CCC.

Dataterm P.O.BOX 50
81741 Dippoldiswalde (8230)

Pentium

Nunja, wir sehen uns eigentlich eher als galaktische Vereinigung ohne feste Strukturen, bei uns weiß eigentlich so niemand über alles bescheid, und ist überall eingeweit. Über Clubausweise reden wir garnicht erst, wir weisen uns durch unser Denken und Handeln aus. Die Stimmung kann auch mal mit Donnerwolken verhangen sein, aber das passiert, wenn Menschen MITeinander arbeiten. Wir beschäftigen uns kritisch, kreativ mit den neuen Medien. „Professionelle Hacker" sind wir nicht. Insofern glauben wir auch nicht an eine Konkurrenz, eher an eine Bereicherung und wünschen dem Dataterm „Hacker"-Club viel Glück.

Chaos-Team



C-Netz

Geschichte

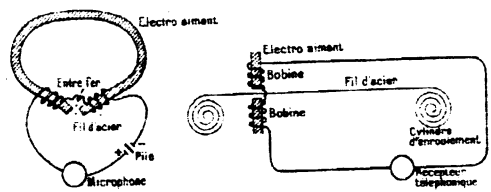
1958 faßte die Pest einige handvermittelte Funknetze, die in Schwerpunktgebieten und entlang einiger wichtiger Verkehrsverbindungen geschaffen worden waren zu dem Funktelefonnetz A zusammen. Dieses Netz hatte mit 317 Funkkanälen eine Kapazität von 10784 Teilnehmern. Da dies etwas wenig war, wurde im verlauf der 60'er Jahre das Funktelefonnetz B entwickelt, was dann 1972 seinen Betrieb aufnahm. 1972 wurde dann das A-Netz stillgelegt, um die Frequenzen wurden für das B-Netz freigegeben. Den Höhepunkt seiner Auslastung erreichte dieses Netz 1986 mit ca. 27000 Teilnehmern. Es wird vorraussichtlich Ende nächsten Jahres außer Betrieb genommen. Am 01.05.1986 wurde das C-Netz dann in den „kommerziellen" Betrieb genommen, nachdem es seit September 1985 im Probebetrieb lief.

Einbuchen, weitergeben.

Nachdem das Funktelli eingeschaltet wurde, mißt es erstmal die Empfangsqualität und stellt fest, in welcher Funkzelle es sich befindet. Nun bucht es sich im Netz ein, hierbei werden dann auch die Kenndaten des Teilnehmers übertragen, und in der Vermittlungsstelle des Kunden eingetragen, in welchem Bereich sich dieser derzeit aufhält. Dies dient dazu, damit der Teilnehmer überall zu erreichen ist, ohne daß bekannt sein muß, wo er sich aufhält (ROAMING). Nun überprüft das Telefon auch weiterhin, wo es sich befindet, um evtl. auch eine Umbuchung vorzunehmen. Hierbei wird es von der Funksendestelle auch des häufigeren aufgefordert, sich mal kurz zu melden. Tut es dies dreimal hintereinander nicht, so wird es ausgebucht. Auch wenn das Telefon innerhalb von 20 Minuten weder einen Aufruf sich zu melden, noch irgendwelche anderen Nachrichten für sich empfangen hat, betrachtet es sich als ausgebucht. Bei diesen Überprüfungen stellt das Telefon dann auch fest, ob es den Bereich einer Funkzelle verlassen hat, und bucht sich dann bei der nächsten Funkzelle ein. Während eines Gespräches wird die Signalqualität laufend von den umliegenden Funkvermittlungsstellen überwacht und gespeichert, so daß beim Unterschreiten der Grenzwerte sofort umgeschaltet werden kann (wenn ein Kanal frei ist..), da sowohl das Telefon als auch die Festsender Ihre Ausgangsleistung anpassen können, kann es theoretisch zu Verschleppungen einer Frequenz in den Bereich einer anderen Funkzelle kommen (d.h. die Verbindung läuft noch über eine Feststation, die für den Bereich garnicht zuständig ist), dies kann zu sog. Intermodulationsstörungen führen, so daß andere Telefone in Leidenschaft gezogen werden. Deshalb wird auch auf ein Überschreiten der Grenzwerte geachtet. Wenn dies der Fall ist, wird ebenfalls ein Umbuchvorgang ausgelöst. Bei diesen Umbuchvorgängen haben die Funktelefone, die gerade ein Gespräch haben vorrang vor denen, die gerade eins bekommen sollen. (Hand-Over).

Frequenzen und Übertragung

Das C-Netz verwendet die Frequenzbereiche von 450 - 455.740 Mhz (Unterband) und 460 - 465.740 Mhz (Oberband), diese werden normalerweise mit einem Kanalraster von 20 Khz betrieben (vergl. BOS-Band), können aber auch im 10 und 12.5Khz Raster betrieben werden (10Khz um das Frequenzspektrum bei Bedarf besser ausnutzen zu können, 12.5Khz um eine einfache Angleichung an das sonst häufig verwendete 25Khz Raster zu ermöglichen). Die Gespräche werden phasenmoduliert mit einem maximalen Frequenzhub von +/- 4Khz übertragen. Um das „versehentliche" Mithören von Gesprächen zu verhindern wird bei den Gesprächen das Sprachsignal invertiert. Die Informationen im OGK werden mit 5280bits/sec. übertragen, hierbei beträgt der Frequenzhub +/-2.5Khz. Diese werden mit dem Verfahren NRZ und 'nem direkt modulierten Träger (DFSK) übermittelt (siehe auch City-Ruf).



Prinzipschaltung von Poulsens Telegraphon

Organisationskanal

Der OGK ist in Zeitschlitze aufgeteilt, 32 Zeitschlitze bilden einen Zeitrahmen, dieser hat die zeitliche Ausdehnung von 2.4 sec, so daß ein Zeitschlitz 75ms lang ist. Dieser ist dann noch in Ruf und Meldeblock unterteilt. Jeweils zu Anfang und Ende eines Blocks kommen 7 Bit Pause, nach der ersten Pause kommen 33 bit Präambel, anschließend ein Leerbit (leer...), nun kommt die eigentliche Information (70 Bit) und als letztes noch die 80 bit Prüfsumme, zur Bildung dieser wird der BCH 7.15 Code verwendet, wodurch eine Korrektur von bis zu 20 Bits möglich ist.

Quelle : Unterrichtsbltter der DBP-Telecom (Mobilfunknetz
der DBP-Telecom) Jahrgang 44/91 10 Das Funktelefon-Netz C der DBP / Sonderdruck (Der Fernmeldeingenieur)

rowue

Abhörsicherheit

Mit dem Schlagwort „mangelnde" Abhörsicherheit wird - nicht nur in (Zeit-)Schriften der DBP Telekom Presse- u. Öffentlichkeitsarbeit - Werbung für digitale Funkgeräte (schnurlose und cellulare (D- Netze)) gemacht.

Hieß es noch vor wenigen Wochen beispielsweise, Funkgespräche im C-Netz Funktelefonnetz ließen sich nur mit erheblichem technischen Aufwand mithören, heißt es jetzt, dies sich C-Netz Gespräche mit für wenige hundert Mark zu jetzt legal zu erwerbenden Scannern abhören ließen.

Wer „Abhörsicherheit" will, soll sich also eines der neuen digitalen Funktelefone kaufen. Gleichzeitig wird das, was im Grundgesetz „Fernmeldegeheimniß" genannt wird - de facto genauso wie das Recht auf Asyl abgeschafft (siehe auch Artikel zum BGH--Urteil irgendwo in dieser Ausgabe).

Die Meldungen darüber, daß die D-Netze abhörsicherer seien, als es der Polizei lieb sein kann mögen zwar auf irgendwelchen temporär vorhandenen Fakten beruhen, sind aber letztlich eine Irreführung des Verbrauchers - insbesondere dem Teil der Verbraucher der auf vertrauliche Kommunikation angewiesen ist (und dafür gibt es nicht nur minder legale Beweggründe).

Solange Gespräche in Leitungen von Betreibern verlaufen, denen ein Zugriff durch staatliche Stellen gesetzlich vorgeschrieben wird, hilft nur eine Verschlüsselung vor dem gelangen der (Sprach-)Daten in eben diese Leitungen.

Und - solange dies nicht gewährt ist - hilft nur, die Telefonkommunikation genauso wie Briefkommunikation von der Sicherheit zu betrachten, wenn man davon absieht, dass mit zunehmender digitalisierung des Telefonnetzes die Speichermöglichkeit erheblich steigen: was auf dem Umschläg steht ist genauso wenig wie Verbindungsdaten in (Funk-)Telefonnetzen vor irgendwem wirklich geschützt und das, was drin steht (Gesprächsinhalte) ist letztlich auch im Zugriff. Müßen Briefumschläge noch umständlich mit Heiss-Wasser-Dampf geöffnet werden, ist es beim Anzapfen einer Leitung alles etwas einfacher.

Nebenbei: Beim BND wird seit einiger Zeit mit Sprach-Banken herumgespielt, Spracherkennung mit Listen „kritischer" Begriffe lassen die einfach mal auf allen ihnen technisch (nicht rechtlich) zur Verfügung stehenden Leitungen laufen. Technisch zur Verfügung heißt in diesem Falle (Richt-)-Funkstrecken aller Art, rechtlich nicht zur Verfügung heißt, das der jetzt geplante „große Lauschangriff" lediglich die Legalisierung der hier vorhandenen Praxis ist.

Benutzer von Telefonen mögen diese Hinweise beachten.

ABHOER.D43 Andy

N e t z - T a g e ' 9 3 (NeT)

27. August (14 Uhr) bis 29. August (17 Uhr)

Congress fuer Datenreisende und solche die es werden wollen

Allgemeines

Vom 27. bis zum 29. August finden in Kiel erstmalig die Netz-Tage statt. Auf diesem Congress sollen technische, administrative, juristische und soziale Themen im Bereich der Informations- und Kommunikationstechnik vorgestellt und diskutiert werden.
Der Congress wendet sich an alle, die sich für Computer und Netze interessieren.
Veranstaltet werden die Netz-Tage vom Toppoint Mailbox e.V., Kiel, dem Individual Network e.V., Oldenburg, dem Chaos Computer Club e.V., Hamburg und dem Freien Telekommunikations-Zentrum Hamburg e.V. in Zusammenarbeit mit der Hochschulgruppe „Elektronische Netzwerke und Kommunikation" der Universitaet Kiel, der Fachschaft Mathematik/Informatik/Logik, Universitaet Kiel, der DFN-Nutzergruppe „Studierende" sowie dem Datenschutzbeauftragten des Landes Schleswig-Holstein.

Inhalte

Der Congress wird aus mehreren Veranstaltungsblöcken bestehen.
Der Block „N e t z e + R e c h t" beschäftigt sich mit dem Fernmelderecht, dem Datenschutzrecht und der rechtlichen Einordnung von Mailboxen. Auch Fragen nach dem Sinn und Unsinn von Urheber-, Patent- und Namensrecht werden in eigenen Veranstaltungen angesprochen. Diese Themen sind durch die Schwierigkeiten des "Rainbow BBS" wieder aktuell geworden! In diesem Zusammenhang wird derzeit eine Diskussion über die eventuelle Gründung eines M a i l b o x s c h u t z b u n d e s vorbereitet. Dazu wird es noch gesonderte Informationen geben. Der Datenschutzbeauftragte des Landes Schleswig-Holstein wird einen Vortrag über die praktische Durchführung von Datenschutzprüfungen berichten und anschliessend zusammen mit Häcksen und Hackern, Datenreisenden und privaten Institutionen über die Möglichkeit einer Zusammenarbeit bei solchen Prüfungen diskutieren.
Im Block „G r u n d s ä t z l i c h e s" wird Prof. Grossmann vom Umweltforschungszentrum Leipzig ueber die Frage sprechen, inwieweit Hacker und Viren als Motor von Entwicklungen dienen. Wissenschaftler werden über die Verantwortung des Computer-Freaks, Mailboxbetreibers oder Informatikers diskutieren. Prof. Gorny (Universität Oldenburg) gibt eine Einführung in "Software-Ergonomie" und wird anschliessend in einem Arbeitskreis mit Programmierern über die praktische Bedeutung und Umsetzung von Netzanwendungen diskutieren. Auch eine Diskussion über den alten Gedanken des "Globalen Dorfes", und was daraus geworden ist, wird nicht fehlen!
Natürlich werden auch „T e c h n i k + B e n u t z e r" nicht vernachlässigt. Es wird eine Einführung in Sinn und Betrieb des "Domain Name Service" geben, und eine Einführung in die Installation und den Betrieb von Linux. Weiterhin wird über Verschlüsselungstechniken und ihre Grenzen berichtet. "MIME", "X.400", "RFC", "ModaCom" sollen nach diesem Congress für die Teilnehmer keine Fremdworte mehr sein. Desweiteren sollen nach über einen Jahr die Folgen des EMMA-Artikels diskutiert werden. Schließlich wird die Forschungsgruppe „Medienkultur und Lebensformen", Universität Trier die Ergebnisse ihrer Umfrage "Netzwerk 92/93" vorstellen.
„T r e f f e n + I n f o r m a t i o n" stehen wie selbstverständlich auf der Tagesordnung. Im Rahmen des Congresses werden sich das Individual Network (IN), die DFN-Nutzergruppe "Studierende", die diversen Projekte zur Vernetzung von Schulen (Offenes Deutsches Schulnetz, PLUTO, Niedersächsisches Schulnetz, ComPäd etc.) - zum Erfahrungsaustausch treffen. Gleiches gilt für Projekte zur Vernetzung im Umweltschutzbereich (MUT, APC, CL). Vielleicht

entstehen neue gemeinsame Projekte?
Im Block „NationaleInfrastruktur" wird die Telekom über ihre Angebote berichten. Dabei soll über die Frage gesprochen werden, wie eine nationale Datenkommunikations-Infrastruktur für Privatpersonen technisch und rechtlich möglich ist, um so auf das (teure) Telefonnetz verzichten zu können. Verschiedene Dienst-Anbieter, Vereine für private Netznutzung und Vertreter der Telekom werden in einen Arbeitskreis darüber diskutieren.

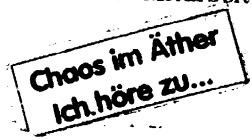
Darüberhinaus wird der CCC Ulm über studentische Netzzugänge berichten. Die Nutzergruppe "Studierende im DFN" wird Projekte vorstellen, die Studentenwohnheime direkt an die Universitätsnetze anschließen. Die Congress-Redaktion der Netz-Tage wird mittels E-Mail den direkten Kontakt zu einer dänischen Tageszeitung herstellen und so den praktischen Einsatz von Netzen in der Redaktionsarbeit demonstrieren (und hoffentlich dabei noch Zeit finden, den Tagungsband fertigzustellen).
Zum Abschluß der Netz-Tage ist ein Streitgespräch zwischen Prof. Joseph Weizenbaum (MIT), Prof. Robert Jungk (Publizist und Zukunftsforscher) und Wau Holland (CCC) über die Möglichkeiten und Folgen des Einsatzes moderner Kommunikationstechnik in der Gesellschaft geplant. Beispiel wird die Nutzung von NotePads, Multimedia und Funknetzen in einem Krankenhaus des Jahres 1997 sein.

Ausstellung und Technik-Center

Es wird auf den Netz-Tagen '93 eine Ausstellung bzw. ein Technik-Center geben. Vereine und Einzelpersonen können dort ihre Leistungen oder Ideen präsentieren. Weiterhin wird auch Zugang zu Mailboxen und der weiten (Netz-)Welt realisiert. Wer hier etwas beisteuern möchte, ist herzlich willkommen und wende sich bitte rechtzeitig an die Adresse „raider@tpki.toppoint.de", denn der verfügbare Platz und die Anzahl der Telefonanschlüsse sind begrenzt.

Cafe + Uebernachtung

Zur Entspannung und Erfrischung wird es ein Cafe geben. Ebenfalls wird ein Archiv mit Materialien aus der Computer-Szene vorhanden sein. Ein Fotokopierer steht dort zur Verfügung.
Eine Liste von Übernachtungsmöglichkeiten wird mit dieser Congress-Ankündigung verbreitet. Ein Themenfahrplan und genauere Informationen zum Ablauf der Veranstaltung werden Ende Juli in allen Netzen verbreitet werden.
Es sind noch weitere Themen vorgesehen, die jedoch nur dann realisiert werden können, wenn noch weitere aktive Mitarbeiterinnen und Mitarbeiter zu uns stoßen. Als Veranstalter der Netz-Tage '93 hoffen wir auf Eure Mitarbeit für weitere



Vorträge, Diskussionen und Arbeitskreise! Keine ungerechtfertigte Scheu!- Wenn Ihr Vorschläge oder Anfragen habt, so richtet sie bitte an net-antwort@sol.ccc.de oder net-antwort@sol.zer Wir freuen uns auf Euch!

Veranstaltungsort und Preise

Universität Kiel Veranstaltungstrakt der Mathematik + Informatik Ecke Olshausenstrasse, Westring Bus-Linie 2, 12, 22 und 41 vom Bahnhof

Tageskarten

DM 20,– (Samstag),
DM 15,– (Freitag oder Sonntag)

Dauerkarte

DM 45,–

Vorkasse

DM 40,– (nur als Dauerkarte)
Bei Vorkasse ist die Teilnahmegebuehr zu überweisen auf das Konto
Martin Seeger, Sonderkonto NeT,
Vereins- und Westbank Kiel
BLZ. 21030000
Kto. 91/050922

Wohnheime am Netz

ür viele Studenten gehört die Arbeit
it Rechnern und auch die Verwendung
on Netzdiensten mittlerweile zum Alltag.
ews, Electronic-Mail sowie eine Vielzahl
kaler Informationssysteme an Univer-
täten helfen ihnen, ihr Studium besser
planen, Gedanken und Ideen auszu-
auschen und sich über das eigentliche Stu-
ienfach hinaus weiterzubilden. Außerdem
gnen sich solche Netze natürlich auch für
ktivitäten mit mehr „Freizeitwert" ;-).
inzige Voraussetzung hierzu ist ein ent-
prechender Rechner- und Netzzugang. Und
bwohl es immer noch Rechenzentren gibt,
ie ihren Studenten einen solchen Account
erwehren, scheint sich hier eine ingsgesamt
ositive Entwicklung anzudeuten, insbeson-
ere seitdem die Nutzergruppe Studierende
n DFN ihre Arbeit aufgenommen hat.
eben dem reinen Account gibt es allerd-
gs noch eine zweite Voraussetzung, die,
eil allzu selbstverständlich, oft vergessen
ird : der physikalische Rechnerzugang.
ier ist es immer noch die Regel, dass
ich Studenten von Terminal- oder PC-
ools in das weltweite Netzgeschehen ein-
linken. Diese öffentlichen Räume haben
edoch zwei gravierende Nachteile: erstens
uß sie der Student dazu extra aufsuchen,
as bei manchen Universitäten und Studien-
ichtungen eine Fahrt durch die halbe Stadt
edeuten kann, und zweitens sind diese Räu-
e oft überfüllt oder abends abgeschlossen.
ine andere, nicht ganz so häufig genutzte
öglichkeit ist der Zugang per Modem.
ie jedoch jeder weiß, ist das Telefonnetz
icht gerade das ideale Medium fuer dig-
tale Datenübertragung. Mit stark begren-
ter und heutigen Ansprüchen nicht mehr
enügender Bandbreite, sowie zeittarifiert,
ann man es eigentlich mit nur zwei Worten
eschreiben : langsam und teuer. Deshalb
at sich der CCC-Ulm zusammen mit dem
iesigen Rechenzentrum ein Projekt über-
egt, welches feststellen soll, inwieweit ein
ostenloser und schneller Rechner- und Net-
zugang von den Studenten akzeptiert und
enutzt wird. Da sich ein hier gerade im
au befindliches Studentenwohnheim für
inen solchen Versuch geradezu anbietet, entstand nach einigen Überlegungen folgender Plan : Im Wohnheim wird mittels Unshielded-Twisted-Pair Leitungen ein lokales LAN aufgebaut, an das die Studenten ihre Rechner über entsprechende Dosen in ihren Zimmern anschließen können. Gleichzeitig befindet sich ein zentraler Server im Netz, der zum einen die Aufgabe hat, Wohnheimsinterne oder für alle interessante Daten zu speichern, und der zum anderen als Verbindungstor zur Universität und damit zum gesamten Internet dient. Dies geschieht wohl am sinnvollsten über eine (oder mehrere) gemietete ISDN-Standleitung(en). Seine Aufgaben wären Dinge wie Mail-Routing, News-Polling und nicht zuletzt eine Firewall-Funktion, um allzugroßen Unfug innerhalb des Wohnheims vom Uni-LAN und dem Internet insgesamt abzuhalten.

Es sind natürlich auch andere technische Lösungen denkbar, diese erscheint uns aber als die Sinnvollste. Neben den Informatikstudenten und sonstigen „Rechnerfreaks" an der Universität, bei denen ein solches Projekt natürlich helle Begeisterung wachruft, dürfte es allerdings insbesondere durch ein anderes Projekt des Universitätsrechen-

Chaos Mailserver

Ja, es gibt jetzt einen im usenet per Mail erreichbaren Chaos Mailserver, der brav aktuelle Infos, Chaos Pressespiegel, Challisti-, Datenschleudertexte, nen bisserl nützliche Soft und andere interessante Texte verschickt. Momentan noch im Aufbau befindlich, kann mensch dort noch nicht so arg aus dem Vollen schöpfen, aber auch das kommt noch.

Einfach ne Mail an ccc-serv@mail.ccc.de schicken.

In der Mail sollte etwas wie:

HELP

oder

BEGIN
HELP
SEND INDEX
END

stehen.

Cash

zentrums auch bei den anderen Studenten, die bisher eher weniger mit Rechnern in Berührung kamen, auf großes Interesse stoßen. Ich meine hier das sog. UDINE Projekt, welches ein campusweites elektronisches Informationssystem an der Universität schaffen soll. Geplant ist, hier eine Vielzahl von Daten abzulegen, die von unmittelbar studienrelevanten Dingen wie Stundenplänen, Klausurterminen sowie kurzfristigen Verschiebungen, über (multimediale) Vorlesungsskripte bis hin zu Daten von externen Informationsanbietern reichen können. Neben der Universität Ulm bereitet auch die Universität Olden- burg ein ähnliches Projekt vor und zusammen mit Terra wollen Flynn und ich über die Nutzergruppe Studierende das Interesse des DFN an diesen Vorhaben, welches wir „Dezentrale Informationssysteme für Studierende" genannt haben, wecken, um somit eine weitere Verbreitung und vielleicht auch einen noch größeren finanziellen Rückhalt zu erreichen. Langfristiges Ziel unserer Bemühungen ist es, die Arbeit mit Rechnern und Computernetzen zu einem selbstverständlichen Teil studentischer Arbeit zu machen, wie es auch Telefone oder Textverarbeitungssysteme darstellen. Vielleicht herrschen ja irgendwann einmal auch bei uns „amerikanische Verhältnisse"; dort jedenfalls sind Wohnheime, die sich auf dem Campus der Universität befinden, wesentlich häufiger in die lokalen Rechnernetze integriert, als bei uns.

ComRam (aka Frank Kargl)
KARGL@MAIN01.RZ.UNI-ULM.DE
CCC - Ulm

Nachtlektüre für Hacker

Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

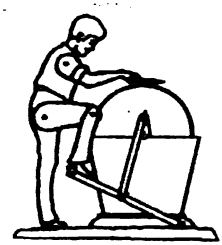
Wenn mensch sich einige Anreize für kleine Stöberaktionen holen möchte, oder sich einfach nur über die Probleme der Datensicherheit im öffentlichen Bereich informieren möchte, so kann mensch ihm unter anderem den „Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragen" empfehlen. Neben den rechtlichen Grundlagen, Mängeln und Ihrer Lösung findet mensch dann auch den einen oder anderen kleinen Rüffel für die Datensammler, die Computer als Informationsinstrument und nicht als Kommunikationsmedium ansehen: so steht dort zum Beispiel unter dem Punkt 18.3 (Verfassungsschutz: Automatisierung der Referatsarbeitskartei):

„Leider war die Systementscheidung ohne ausreichende Beteiligung des Hamburgischen Datenschutzbeauftragten getroffen worden, so daß die grundlegenden Sicherheitsbedenken gegen die vorgesehene Systemkonzeption nicht mehr bei der Auswahl berücksichtigt werden konnten.
Das vorgesehene System weist durch die spezifische Kombination von Hard- und Software strukturelle Unsicherheiten auf,...
...Umso bedauerlicher ist es, daß offenbar die Systementscheidung von anderen Behörden wegen des beim Landesamt für Verfassungsschutz vermuteten hohen Sicherheitsstandards übernommen wurde."

Zu überlegen ist, ob die Herren vom VS aus eigener Erfahrung wissen, daß Datenschutz eine Illusion ist, oder....

Auch die Mailboxen werden in diesem Bericht angesprochen, dort die Problematik des mailspannernden Sysops. Nunja fast jeder Sysop hat es mal gemacht, und fast jeder Sysop hat früher oder später (meistens früher) das Interesse verloren. Was bringt es auch - die öffentlichen Nachrichten sind interessanter. Gesetze werden dort nicht viel bringen, eher schon die Verschlüsselung, die ja auch wegen der G10 Änderung angebracht ist. Als Tip: PGP - RSA Verschlüsselung mit eingebautem uuen-decode.

rowue



CHAOS- MITGLIEDS- ABBOFETZEN

Chaos Computer Club

Schwenckestraße 85
D-W-2000 Hamburg 20
Telefon (040) 490 37 57
Fax (040) 491 76 89

Postgiro Hamburg
(BLZ 200 100 20)
Konto 599 090 – 201

Name: _____

Adresse: _____

Mitgliedschaft im CCC e.V. Schließt Datenschleuder-Abo mit ein.

evvw	*20,00 DM*	Einmalige Verwaltungsgebühr bei Eintritt
evnm	*120,00 DM*	Normalmitgliedschaft (Jahresbeitrag)
evsoz	*60,00 DM*	Mitgliedschaft für Studenten, Schüler, Arbeitslose (Jahresbeitrag)

Reine Datenschleuder–Abos *Ein Abo gilt für 8 Ausgaben.*

nabo	*60,00 DM*	Normalabo der Datenschleuder
sabo	*30,00 DM*	Abo der Datenschleuder für Studenten, Schüler, Arbeitslose
pvst	*??,?? DM*	Porto/Verp./Spende/Trinkgeld

Summe: DM _____, _____ ○ bar ○ V-Scheck ○ Überweisung

Rechtsgültige Unterschrift _____

Chaos: E ADRESSEN BE ERL

CHAOS-HH - CCC Hamburg
Treffen jeden Dienstag ab 19 Uhr, Ort ist an der Aussentür ausgeschildert. Mailbox CHAOS-HH unter +49-40-4911085 Voice +49-40-4903757 Voice MBX +49-40-497273 Fax +49-40-4917689 Briefpost: CCC-HH, Schwenckestraße 85, D-W-2000 HAMBURG 20

CHAOS-B - CCC Berlin
Treffen jeden Dienstag ab 20 Uhr bei gutem Wetter: Am See im Park in der Brunnenstr. gegenüber der Polizeiwache. (U-Bahn Linie 8: Rosenthaler Platz). bei schlechtem Wetter: Zettel an der Tür vom Cafe Art Acker, Ackerstr. 18, D-O-1040 Berlin. Briefpost: CCC-B c/o Müller, Postfach 840, 10048 Berlin. An der sonstigen Erreichbarkeit wird derzeit noch gearbytet (DAL bzw. Prio. f. EAS/BAS gesucht).

Redaktion Chalisti/CCC Nordwest
c/o Frank Simon Strackerjanstr. 53, D-W-2900 Oldenburg Tel.: +49-441-76206 chalisti@sol.zer, chalisti@sol.north.de

CHAOS-HL - CCC Lübeck
Treffen am ersten und dritten Freitag im Monat, 19 Uhr in der Röhre (gerade von der Mengstraße ab).
Briefpost: CCC-HL, c/o Benno Fischer, Bugenhagenstr. 7, 2400 Lübeck 1 Voice: +49-451-34799 Mbx: MAFIA InfoSys +49-451-31642 300-38.400 Bps

CHAOS-RH - CCC Recklinghausen
Treffen alle zwei Wochen oder so.
Voice: +49-2364-16349
Fax: +49-2361-652744
Mailbox: LITB +49-2363-66378 und LIVE-TIMES +49-2361-373214

CHAOS-RM - CCC Rhein-Main
Treffen finden statt oder auch nicht
Voice: +49-6103-4100
Mailbox:BITMAIL vielleicht unter +49-6103-45287
Briefpost: CCC-RM, c/o Engelter, Postfach 1201, 6073 Egelsbach

SUECRATES

Stuttgarter Computerrunde mit Zeitschrift D'Hacketse

Garantiert keine Satzungsdebatten - Mitglied im Bundesverband gegen Vereinsmeierei e.V. Kontakt: T.Schuster, Im Feuerhapt 19, 7024 Filderstadt 3 E-Mail: norman@delos.stgt.sub.org

2600 Magazine

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-Line: +1-516-751-2608
Voice-Mail-System: +1-516-751-6634

2600 Meeting in Germany

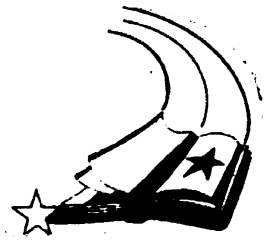
Jeden ersten Freitag im Monat um 18:00 Uhr im Münchener Hauptbahnhof in der ersten Etage bei Würger King und den Telefonzellen.
Erreichbar als 2600@sectec.hanse.de, Voice-Mailbox +1-904-366-4431, auf den Treffen im Hauptbahnhof ueber die anrufbaren Zellen +49-89-591-835 und +49-89-558-541 (bis 545, hier handvermittelt über Operator).

Hack-Tic

Postbus 22953
NL-1100 Dl Amsterdam
Voice: +31-20-6001480
Fax: +31-20-6900968

CHAOS-RN CCC Rhein Neckar

Treffen jeden Dienstag 20 Uhr im „Vater Rhein" in HD.
Wegbeschreibung von der Stadthalle: „Gehe über die Fußgängerampel, Gehe nicht über LOS. Durchquere den Minipark. Gehe halb links. Jetzt stehst Du davor. Begib Dich in den linken Flügel der Gaststätte. Hinten rechts siehst Du einen Haufen Leute mit Schlepptops, Funkgeräten und ähnlichem Kram. Das sind wir. Trau Dich zu fragen, wir beißen nicht."
Mailbox CHAOS RN unter +49-6221-904727
Briefpost: CCC-RN, Postfach 104027, 6900 Heidelberg



FoeBuD-BI

Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V., Bielefeld Treffen jeden Dienstag, 19:30 Uhr im Café „Spinnerei", Heeperstraße 64, D-W-4800 Bielefeld 1, voice +49-521-62339
Monatliche „Public Domain"-Veranstaltung zu Themen aus Randbereichen der Computerkultur jew. am 1. Sonntag im Monat (außer Januar, Juli und August) ab 15 Uhr, im Bunker Ulmenwall, Kreuzstraße 0, 4800 Bielefeld 1. Termine siehe BIONIC.
Voice: +49-521-175254 Fax: +49-521-61172
Mailbox BIONIC unter +49-521-68000
Briefpost: FoeBuD c/o Art d' Ameublement, Marktstraße 18, 4800 Bielefeld 1
e-mail: ZENTRALE@BIONIC.ZER / zentrale@bionic.zer.de

CCC-Ulm

Treffen jeden Mittwoch, 19 Uhr im Café „Einstein", Uni-ULM
Kontakt: Framstag, framstag@rz.uni-ulm.de (Ulli Horlacher, Landfiedbühl 5, 7900 Ulm) und Deep Thought (brenner@tat.physik.uni-tübingen.de (Martin Brenner) oder CCC-ULM, ccc-ulm@sol.zer und ccc-ulm@sol.north.de
ohne Gewähr

CHAOS-
BESTELLFETZEN

Chaos Computer Club

Schwenckestraße 85
D-W-2000 Hamburg 20
Telefon (040) 490 37 57
Fax (040) 491 76 89

Postgiro Hamburg
(BLZ 200 100 20)
Konto 599 090 – 201

Postvertriebsstück, Gebühr bezahlt – C 11301 F

Name: _____

Adresse: _____

_____

_____

Chaos-Literatur *(auch im Buchhandel erhältlich)*			
vergriffen	*habi1*	*33,33 DM*	Die Hackerbibel, Teil 1 (260 Seiten A4)
vergriffen	*habi2*	*33,33 DM*	Die Hackerbibel, Teil 2 (260 Seiten A4)
Chaos-Literatur *(im Buchhandel eher nicht erhältlich)*			
in Vorb.	*ts-plan*	*10,00 DM*	„Taschen-Synthi"
____	*stud*	*7,50 DM*	Studie für die Grünen
____	*mutst*	*16,00 DM*	Elektronische Informationssysteme für den Umweltschutz
Infopakete / Software & Co.		*z.Zt. nur 5 1/4" Disketten möglich*	
____	*pcd*	*25,00 DM*	PC-DES für MS-DOS: Private Verschlüsselung
____	*psynth*	*20,00 DM*	PC Soundprogramm für blaue Töne
____	*pocsac*	*10,00 DM*	Pocsac - Decoder - nur für Schulung
Backer *PVC wassergeschützt / gestanzt, wenn nicht anders angegeben*			
____	*3ks*	*3,33 DM*	3 Stück „Kabelsalat ist gesund" mit Chaos-Knoten
____	*ah*	*3,33 DM*	Bogen mit 64 Stück „Achtung Abhörgefahr", Papier, zum Selbstausschneiden, postgelb
____	*cia*	*5,00 DM*	Bogen mit 68 Stück „Chaos im Äther", Papier, zum Selbstausschneiden, rot
____	~~*ooo*~~	~~*5,00 DM*~~	~~18×„Außer Betrieb,"8×„Out of Order,"1×„Guuste"~~
____	*post*	*5,00 DM*	Bogen mit Post-Totenkopf-Klebern verschiedener Größe
____	*glob*	*5,00 DM*	Bogen mit 10 Stck „Globales Dorf, Rechtsfreier Raum"
____	*zula*	*5,00 DM*	Zulassungszeichen („ZZF-Prüfnummer")
Ganz Wichtiges Gedenkt bitte unserer immensen Portokosten! Rückporto *mindestens* **erbeten!**			
____	*pvst*	*??,?? DM*	Porto/Verp./Spende/Trinkgeld

Summe: DM _____, _____ ○ bar ○ V-Scheck ○ Überweisung

Rechtsgültige Unterschrift _____

Chaos: E _____ BE _____ ERL _____