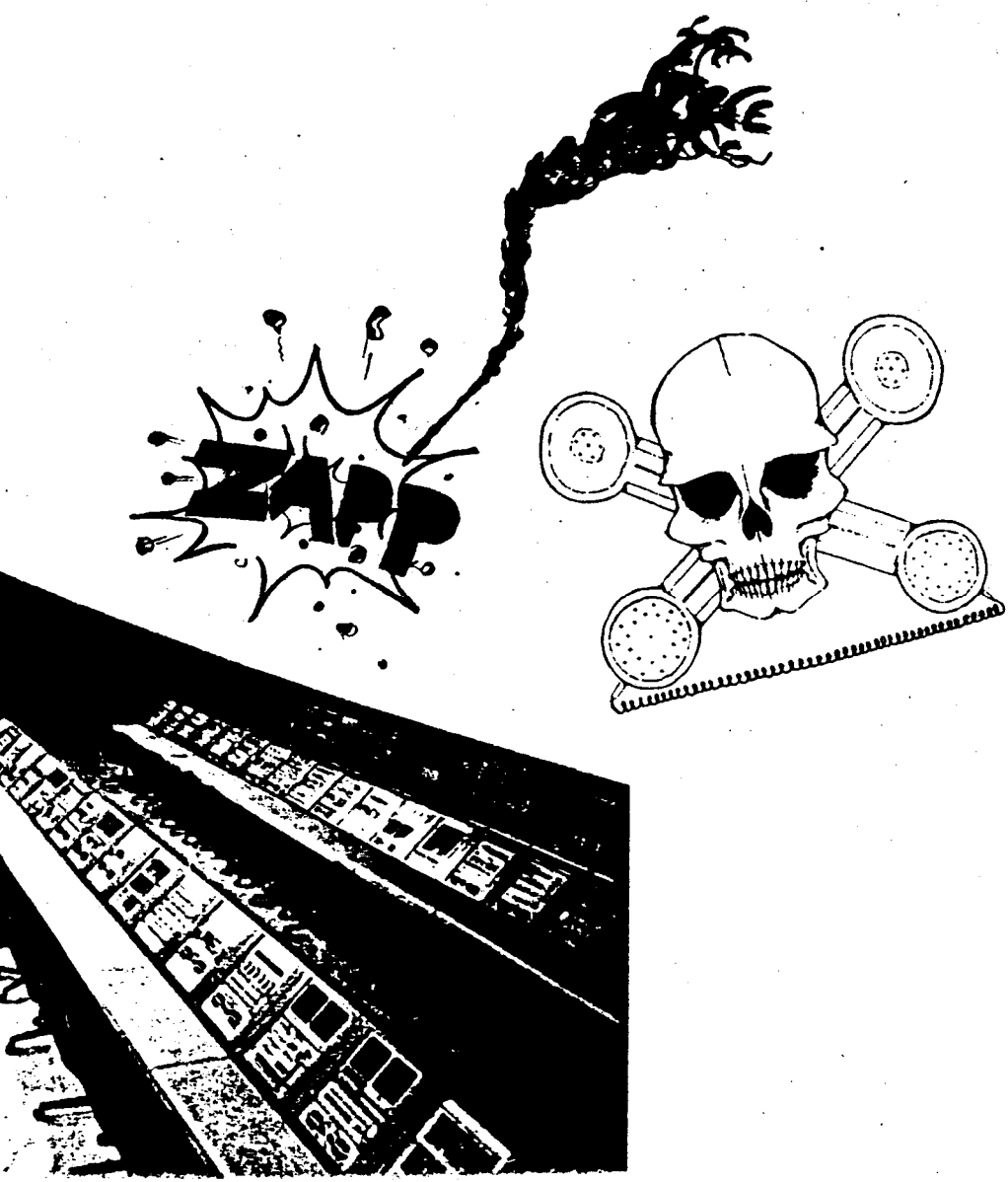
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende



DM 3,50

ISSN 0930-1045 Juni 1991 Nr. 35

Editoral

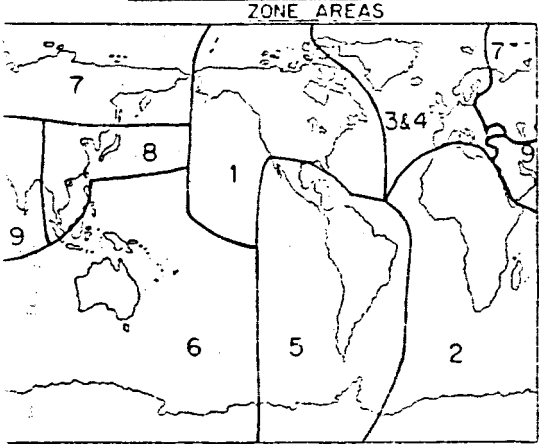
Die Killerameisen greifen an!

Hordenweise ziehen die KImeisen mordend und brandschatzend über die Tastaturen. All jener ökologischen Umstände trotzend haben wir, wie sicherlich bemerkt, eine neue DS pornographiert. Die an 16 fehlenden 4 Seiten sind den Portokosten und KImeisen und deren gigantischen Beißwerkzeugen zum Opfer gefallen. Nach eingehenden und unter großem nicht den sonellen und materiellen Einsatz geführten Diskussionen sind wir zu dem Entschluß gekommen, daß der Postzeitungsvertrieb die Lösung sei. Nun ja, das wird zur Folge haben, daß die DS jetzt „regelmäßig" erscheinen sollte. Dezentrales Chaos hatte zur Folge, daß wir mit dieser Ausgabe noch nicht im Postzeitungsvertrieb sind.

Jedenfalls sollen die sterblichen Überreste der nächsten Schleuder rechtzeitig zur Funkausstellung Berlin, also Mitte August, der P*st übergeben werden. Harren wir also der Dinge, die da kommen mögen...

spirou

WORLD NUMBERING PLAN
ZONE AREAS



Die Datenschleuder
Das wissenschaftliche Fachblatt
für Datenreisende
Heft 35 *(Zählnummer für Abonnenten)*

Wir organisieren uns irgendwie dezentral oder auch nicht, empfehlen aber unbedingt, jeweils den Kontakt mit der nächstgelegenen regionalen Gruppe zu knüpfen.

Adresse: *Die Datenschleuder, Schwenckestraße 85, D-W 2000 Hamburg 20*
Telefon: *(040) 490 87 57*
Telefax: *(040) 491 76 89.*
Mailbox: *DS-RED@CHAOS-HH.ZER (040-491 10 85, 1200/2400 8n1)*
Internet/UUCP: *ccc@mcshh.hanse.de*
BTX: **CHAOS#*
Redaktion: *andy, cash, nomade, pirx, ron, rowue, spirou, terra, wau.*
V.i.s.d.P.: *Rolf Würdemann*
Herausgeber: *Chaos Computer Club e.V., Adresse wie Red.*
Adreßänderungen: *bitte ABOMV@CHAOS-HH.ZER mit alter und neuer Anschrift mitteilen*
Druck: Bernd Paustian, Schwenckestr. 68, 2000 Hamburg 20

Namentlich gekennzeichnete Artikel geben nicht unbedingt die Meinung der (Gesamt-) Redaktion wieder. Alle technischen Informationen, Schaltungen usw. werden ausschließlich zu Amateurzwecken mitgeteilt. Irgendeine Funktions- oder sonstige Garantie wird nicht übernommen. Die (insbesondere fernmelde-) rechtlichen Vorschriften sind zu beachten.

Einzelpreis 3,50 DM. Abonnement für 8 Ausgaben 60 DM, Sozialabonnement 90 DM. Mitglieder des Chaos Computer Club e.V. erhalten die Datenschleuder im Rahmen ihrer Mitgliedschaft.

§ Recht

Hamburger Datenschutzhefte

„Das neue Datenschutzrecht"

Da iss' es! Mit einem Geleitwort von unser'm seligen Justizsenator Wolfgang Curilla präsentiert unser lieber Manfred Krause (seines Zeichens amtierender Hamburger Datenschutzbeauftragter) das neue Datenschutzrecht!

Auf satten 122 Seiten finden sich erstmal Geleitwort, Vorwort, das Hamburger- sowie das Bundesdatenschutzgesetz. Außer dem üblichen amtlichen PiPaPo kann man/frau sich an der ergänzten, ausführlichen Senatsbegründung zum Entwurf des Gesetzes ergötzen. So hübsche Sachen wie eine Druckfehlerberichtigung, Anschriften der Datenschutzkontrollinstitutionen (32 Buchstaben) für die öffentlichen (Gericht, Staatsanwalt, Gefängnis oder Krankenhaus) und die der nicht-öffentlichen Bereiche (CCC) runden die ganze Sache ab!

Haben Sie allerdings als Ostdeutscher Fragen zu der Thematik, müssen Sie sich im Einzelfall an den Bundesbeauftragten für den Datenschutz wenden, alldiweil beim Redaktionsschluß noch keine Datenschutz-Kontrollinstitutionen eingerichtet waren. Sei's drum! Wer gerne wurschtelt, dem sei dieses Büchlein ganz warm an's Herz gelegt! Es ist kostenlos erhältlich unter dieser ehrenwerten Adresse:

Der Hamburgische Datenschutzbeauftragte, Baumwall 7, 2000 Hamburg 11, 040/3504-2044

PEB

Diverses Diffuses

CeBIT '91 - Kurzmeldungen

Freitag, 15.3.91

P.stellte ein Gerät vor, mit dem ein **ISDN-Basisanschluß** wie eine **Nebenstellenanlage** (4 Nebenstellen mit Durchwahl) benutzt werden kann. Die Teilnehmer können auch intern miteinander sprechen, Rufumleitung und ähnliche Komfortfunktionen sind möglich. Das Gerät soll über die DBP Telekom vertrieben werden und Mitte des Jahres verfügbar sein.

Eine japanische Firma stellte ein **optisches Druckerkabel** vor. Zwischen Sende- und Empfangsstecker sind 30 Meter Glasfasern verlegt. Damit lassen sich auch in gestörter Umgebung (Industrie) Drucker über große Entfernungen mit normalen Centronics-Interfaces anschließen. Näheres nach einem ausführlichen Test.

Auch **Telefax**boomt weiter. Geräte und Karten werden immer leistungsfähiger und preiswerter. Die *Datenschleuder* will demnächst einen Vergleichstest mehrerer Faxkarten, -Modems usw. veranstalten; Testgeräte wurden der Redaktion freundlicherweise von diversen Herstellern zugesagt.

Abends war der Pressetreff eines bekannten Hamburger Modem-Herstellers gut besucht. Bier, Musik und belegte Brötchen stellten eine angenehme Alternative zum 18-Uhr-Stau dar. Die Leute vom Foebud Bielefeld waren auch da, es wurde heiß und innig diskutiert – wenn ich mich jetzt noch erinnern könnte, worueber...

Dienstag, 19.3.91

Das traditionelle **Hacker-Treffen**am **Poststand** wurde von der Telekom freundlicherweise mit Getränken und Demo-Telefonkarten (je 20 Einheiten drauf, immerhin...) gesponsert. Trotzdem war der Poststand hinterher mit diversen Post-Totenköpfen verziert. Häcker und Häcksen aus ganz Deutschland waren zum Gedankenaustausch erschienen. Unser Großer Vorsitzender Terra hatte einiges betreffs neuer **ISDN-Gebühren** zu berichten (siehe seinen Artikel irgendwo in diesem Heft [*Denkste! d.S.*]).

Wer dachte, daß in deutschen Landen die Bundesbahn das Monopol auf schaurigkitschige Hausfarben hat, muß sich vom Gilb eines Besseren belehren lassen. Das neue (na ja, vorgestellt wurde es schon in einem dicken Ringbuch von ca. 1987) Erscheinungsbild der Post sieht für die Telekom **Bonbonrosa** neben **Grau** vor. Dazu schreibt siech die Telekom jetzt "T-e-l-e-k-o-m", mit Buchstaben in pink und Strichlein dazwischen in Grau. Brrr.

pirx

Perspektiven der elektronisch unterstützen Kommunikation in Krisenzeiten:

Schutz gegen Überlastungen, Katastrophenschaltung

Zum Schutz gegen Überlastungen von Vermittlungseinrichtungen, z.B. in Katastrophenfällen, sind im EWS [*Telefonvermittlungssystem der P*st, d.S.*] gestaffelte Maßnahmen vorgesehen, die je nach Rechnerbelastung automatisch in Kraft treten und eine Lastregelung bewirken.

Zu den Maßnahmen gehört u.a. die Abschaltung bestimmter Teilnehmergruppen entsprechend ihren gespeicherten Berechtigungen vom gesamten abgehenden Verkehr oder von bestimmten Verkehrsarten (Ortsverkehr, Fernverkehr). Dabei wird durch eine Anreizsperre verhindert, dass nicht berechtigte Teilnehmer durch ständige Verbindungsversuche das Zentralsteuerwerk belasten.

Die Abschaltung von Teilnehmeranschlüssen in Katastrophenfällen kann auch vom Betriebspersonal aktiviert werden.

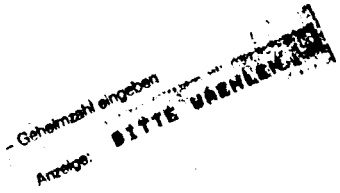
Quelle: Siemens; Elektronisches Waehlsystem EWS, Systemuebersicht EWSO LS 16

Die durch Abhörmaßnahmen von Stasi-West oder ähnlich resultierenden Störungen unserer Club-Telefonleitungen lassen sich allmählich Termin- lich fixieren. Ca. 4 Wochen vor Hagbards Todesdatum (23.5.) fing es damit auf der CHAOS-HH Leitung an - auch der aktivierte Störungsdienst der DBP Telekom (Name urheberrechtlich umstritten) konnte nicht helfen und verwies darauf, daß Stasi-West sich normalerweise induktiv ankoppelt und so keine Störungen verursacht. Überraschend und eigentlicher An- lass zum Schreiben dieses Artikels war, dass die Leitung schon am 24.5. gegen 03:00 morgens keine Störungen beim Datenverkehr mehr produzierte. Offenbar befürchten irgendwelche Stellen irgendwelche Aktionen (viel- leicht auch so ein Thema, was Diskussionsmässig noch nicht abgeha(c)kt ist) zu irgendwelchen Daten bezüglich irgendwelcher Geschichten (siehe Anzeige aus d. taz-hh hier irgendwo)...

andy

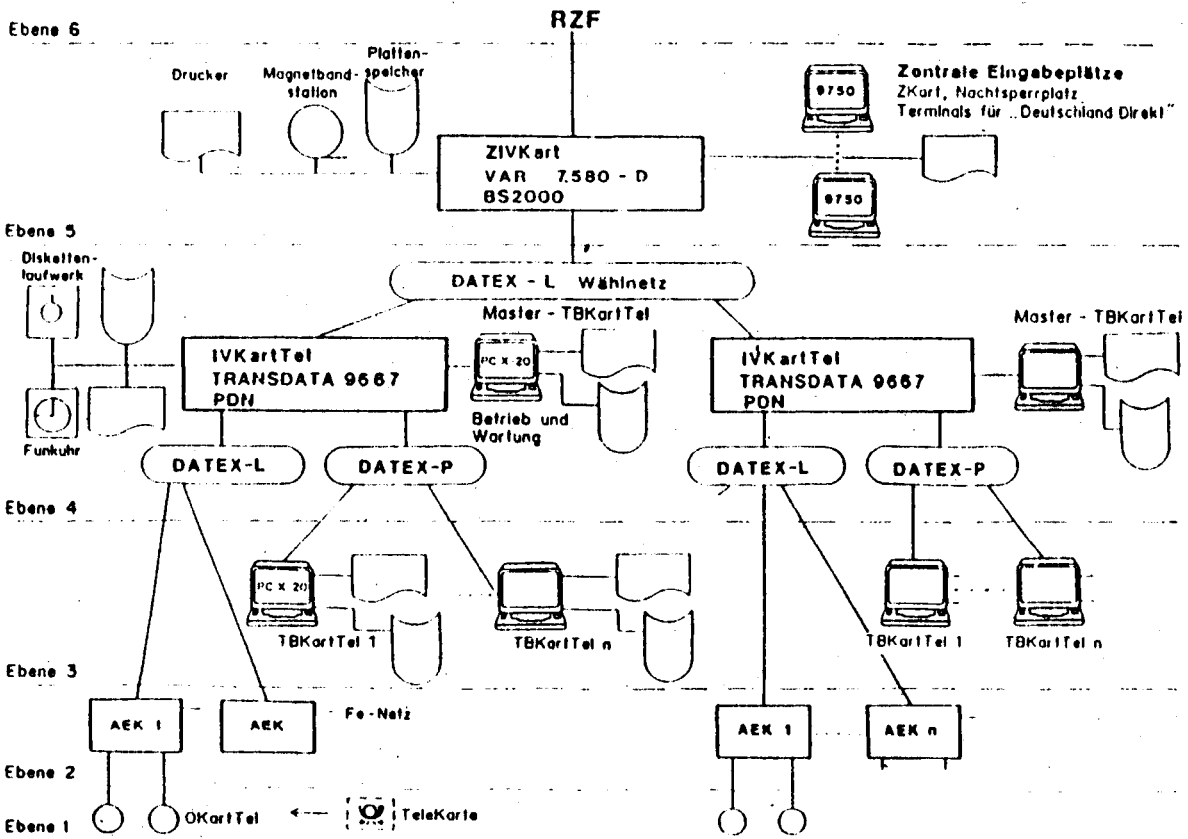
Bei Experimenten mit 0130-Nummern (siehe auch Hackerbibel Teil 1, Seite 183, 193, 194 etc. *) kann es sinnvoll sein, dies nicht vom eigenen Anschluss zu machen. (Nebenbei: Gerüchte besagen, irgendwelche Leute haben bereits Erfahrungen in diese Richtung gemacht, wüssten also schon ganz sicher, dass es besser gewesen wäre. Wer hierüber genaueres (z.B. Fakten) weiss, möge sich doch mal melden, damit auch die übrige Leserschaft etwas auf dem laufenden ist).

Telefonzellen bieten seit einiger Zeit die Möglichkeit, dies sogar ohne den Gebrauch von Münzen/Karten zu machen. Bei Kartentelefonzellen rate ich hiervon jedoch ab; noch ist zwar nicht klar, ob die Verbindungs- daten (Absendekennung d. MünzKarTel, Anwahlnummer, Gesprächsdauer) auch ohne Einführen einer Karte übermittelt werden, die technische Infrastruktur erlaubt dieses jedoch im Zweifellsfall durch Einspielen einer neuen Software (siehe Diagramm). Ein Artikel zum genauen Funktionieren d. Kartentelefo- nierens bzw. dessen Vernetzung findet sich voraussichtlich in der nächsten Datenschleuder.



* dazu wohl auch in Hackerbibel 3 mehr. Erscheinung ca. Ende des Jahres oder später. Wer noch Ideen oder Material hat lasse das doch mal rueberwachsen

Bild 1: Öffentliches Kartentelefonsystem Übersicht



Ebenen 1 4	Prozeßebenen (technische Ebene)	RZF	Rechenzentrum Fernmeldewesen
Ebenen 5 6	Administrative Ebenen (Verwaltung)	TBKartTel	Technischer Betriebsplatz für Kartentelefone
AEK	Anschalteinheit für Kartentelefone	ZIVKart	Zentrale Informationsverarbeitung für Kartenanwendungen
IVKartTel	Informationsverarbeitung für Kartentelefone	ZKart	Zentrum für die Administration (Verwaltung) aller Kartenanwendungen bei der DBP
OKartTel	Öffentliches Kartentelefon		

Quelle: Unterrichtsblätter der DBP, Teil B (Fernmeldewesen), Jg. 42 (1989), Nr. 11

Cityruf....

...damit Sie erreichbar sind

Was ist Cityruf?

Cityruf ist ein Funkruf-Netz, welches das überlastete „Europiep"-Netz (Eurosignal, auch Europäischer Funkrufdienst, EFuRD genannt) ablösen soll, es bietet im Gegensatz zum Europiep noch die Möglichkeit der Nachrichtenübermittlung (15 Zeichen numerisch, oder 80 Zeichen alphanumerisch, je nach Empfänger) an.

Netzaufbau und Systemkonzept

Bei der Planung dieses Netzes ging mensch von einer Teilnehmeranzahl von 1 Million aus (scheint überholt, die Planung wurde teilweise in Richtung mehr mögliche Funkrufe/Minute abgeglichen).

Bei der Planung ging mensch von folgender Aufteilung der Rufklassen aus:

Nur Ton:	45%
Numerisch:	35%
Alphanumerisch:	20%

Um das daraus resultierende Verkehrsaufkommen bewältigen zu können, und im Hinblick darauf, daß Cityruf vorwiegend auf die regionale Rufversorgung ausgerichtet ist, entschied mensch sich für eine dezentrale Aufteilung des Netzes. Die BRD und Berlin(West) erhielten insgesamt acht „Funkrufvermittlungsstellen" (FuRVSt) [*und wo bleiben die FNL?, der Sitzer*], denen ca. 50 „Rufzonen" zugeordnet werden. Die FuRVSt sind in einem Netz zusammengeschaltet, so das jeder mit jedem kommunizieren kann.

Die Rufeingabe und Rufaussendung ist auf dieser Ebene völlig freizügig. Diese FuRVSt sind über Zugänge aus dem Fernsprechnetz (SWFD, Selbstwählferndienst), Teletext, Telex und Btx zu erreichen, um dort Rufe abzusetzen. An diesen FuRVSt können bis zu 30 sogenannte Funkrufkonzentratoren (FuRK) über die Funkrufnetzanschaltung (FuRNA) angeschlossen werden. An diese Funkrufkonzentratoren können wiederum bis zu 32 Funkrufsendestellen (FuRSSt) angeschlossen werden. Ein FuRK mit den angeschlossenen RuRSSt bildet eine Rufzone. Im Gegensatz zu den FuRVSt, die gleichwertig in einem Netz zusammengeschaltet sind, sind die RuRK nicht miteinander vernetzt [*ich hörte da mal was von dezentral..., der Sülzer*].

Durch diese Aufteilung in Rufzonen kommt es dazu, daß mensch den Aufenthaltsort einer Person wissen muß, um sie zu erreichen, da er hinter der Nummer noch die Funkrufzone (z.B. 40 für Hamburg, 30 für Berlin) eingeben muß.

Funkrufvermittlungsstelle (FuRVSt)

Die FuRVSt verfügt über ein Doppelrechnersystem, Funkrufrechner 1 und Funkrufrechner 2 (FuRR1 / FuRR2). Einer dieser Rechner arbeitet jeweils als Betriebsrechner, und der zweite ist als Reserve gedacht, falls der eine ausfällt, und übernimmt den Betrieb automatisch im Fehlerfall. [*Vielleicht landet der zweite ja in den FNL..., der Schwätzer*]

Die Rechner sind 16 bit Prozeßrechner, und haben über den SCSI-Bus gleichberechtigte Zugriffsmöglichkeiten. Desweiteren verfügt jeder Rechner über zwei 35MB Plattenlaufwerke. Die Datenbestände werden auf jedem Rechner identisch gehalten, um dem oben schon erwähnten Fehlerfall Rechnung zu tragen. Hierfür wird durch bestimmte Softwaremaßnahmen gesorgt. So ist ein Schreiben auf die Platten nur dann möglich, wenn sie auf beiden Platten fehlerfrei ausgeführt werden können. Die Teilnehmerdaten belegen ca. 15MB, die Statistiken über Zugänge und andere Betriebsdaten ca. 22MB. Dadurch können unter anderem Fehler bis zu 15 Stunden zurückverfolgt werden. [*Fehler: Definition durch Betreiber, der Schwätzer*]

Der Doppelrechner ist noch mit einem Bandlaufwerk ausgerüstet, um Teilnehmerdaten oder Software zu übertragen, oder um Betriebsdaten abzusichern.

Die Zugänge werden eigenständig durch die vorgeschalteten Einrichtungen bearbeitet. Das einzige, was durch die FuRR noch bearbeitet wird ist das Prüfen der Teilnehmerinformation, die Rufübergabe und die Betriebssteuerung.

Für den Betrieb der Sendestelle sind bis zu fünf Datensichtgeräte (DSG) anschaltbar. Desweiteren sind noch zwei Systemdrucker (SDR) für die Erstellung von Protokollen vorgesehen.

Zum Selbstüberprüfen des Systems ist ein automatische Wähleinrichtung für Datenübertragung (AWD) eingebaut. Der Prüfvorgang wird entweder manuell für einen einzelnen Telefonzugang gestartet, oder über „Zeitaufträge" automatisch für alle Zugänge. Dabei wird eine Prüfnummer

eingeben und der Rechner wertet die Reaktionen auf dem Zugang aus.
Da die Sender auf den gleichen Frequenzen arbeiten, werden die Frequenzen in Zeitschlitzen gewechselt, um Störungen zu vermeiden. Für diesen Zweck sind die Rechner mit funkgesteuerten DCF77-Uhren ausgestattet, um die Rechner zu synchronsieren.

Zugänge

SWFD	0164()	(Nur Ton)
	0168()	(Numerisch)
	01691()	(Alphanumerisch)
	016951	(Auftragsdienst)
Telex	1691	
Teletex	1692	
Btx	*1962#	

Die Klammern () beim SWFD bedeuten, daß nach der Nummer noch die Cityrufnummer(+Rufzone) eingwählt werden muß. Bei dem numerischen Zugang erfolgt die Eingabe über MFV (Touch-Tone), bei dem alphanumerischen Zugang mit 300 Baud (8n1) und Rechner.

Ablauf

Wenn jetzt über einen der Zugänge ein Funkruf abgesetzt wird, so wird in dem Zugang eine Plausibilitätskontrolle unterzogen. Dies ist dadurch möglich, daß die ersten drei Stellen der siebenstelligen Teilnehmernummer die Zugehörigkeit zu einem maximal 10 000 Teilnehmer umfassenden Nummernblock kennzeichnen. Die Nummernblöcke werden durch die jeweiligen Fernmeldeämter im Bereich der FuRVSt zugeordnet, und die Teilnehmernnummern daraus vergeben. In jeder FuRVSt existiert eine Liste über die Zugehörigkeit zu den Nummernblöcken, werden darin Veränderungen vorgenommen, so werden die Listen in allen FuRVSt sofort über den Datenverbund aktualiesiert. Sobald ein Funkruf angestzt wird, wird festgestellt, auf welchem Rechner die Teilnehmerdaten sind, und fragt diese ab. Danach wird die Funkrufanforderung über das Netz an die entspechende FuRVSt weitergeleitet (wenn die Rufzone „gebucht" ist) und von dort über den FuRK an die FuRSSt weitergeben, wo sie dann abgestrahlt wird. (Das Umsetzen der Anforderungen in POCSAG Nachrichten geschieht in der FuRVSt).
Ist dann daß Gerät eingschaltet, und wird die Nachricht empfangen, so wird dies dem Benutzer [*User sind unter uns, der Kätzer*] über einen Piepton und eine LED angezeigt, „Optional ist auch die Signalisierung durch einen Vibrator möglich" (ANT Nachrichtentechnische Berichte, Heft 6 Oktober 1989)

Geräte und Rufklassen

- Nur Ton — Vier verschiedene optische oder akustische Signale können übermittelt werden.
- Numerik — 15 Ziffern von 0 bis 9 und fünf Sonderzeichen, sowie zwei „nur Ton" Rufzeichen.
- Alphanumerik — 80 Zeichen nach DIN 66003, ebenfalls zwei „nur Ton" Rufzeichen.

- Einzelruf — Ein Empfänger wird mittels einer individuellen Rufnummer gerufen.
- Sammelruf — Mehrere Empfänger werden mittels einer Sammelrufnummer durch sequentielle Aussendung von Einzelrufen nacheinander gerufen.
- Gruppenruf — Mehrere Empfänger haben eine weitere gleiche Addresse und werden über diese gerufen.

Zum Schluß

In den Staaten ist das Erwerben von Cityrufempfängern für menschen unter 21 inzwischen verboten. Diese Geräte wurden sehr stark für nicht gesetzliche Geschäfte benutzt (alt.activism). In den Staaten gibt es auch Telfönnummern, wo derjenige, der sie anwählt Gebühren an den Inhaber zählt, sog. 900er Nummern. In New York erschien auf einmal eine Nummer dieser Art auf allen Cityruf-Empfängern. Etwa 50.000 Inhaber dieser Geräte haben diese Nummer angewählt...

rowue

BSI
Geheimdienst oder Notwendigkeit?

„Die glücklichen Sklaven sind die erbittersten Feinde der Freiheit"
(Marie v. Ebner-Eschenbach, Ausspruch eines Teilnehmers auf dem BSI-Workshop)

In nur einer halben Stunde Diskussion wurde am 24. Oktober 1990 im Deutschen Bundestag ein Gesetz beschlossen, dessen Reichweite heute noch nicht zu überblicken ist. Nicht nur hat der Gesetzgeber dort ein neues Amt mit über 200 Mitarbeitern geschaffen, sondern definierte auch den Begriff der Sicherheit in der Informationstechnik (IT) im Hinblick auf Wirtschaft und Gesellschaft. Es kann bekanntlich davon ausgegangen werden, daß die Produktionsgesellschaft sich endgültig in eine Informationsgesellschaft wandelt und sich damit direkt und ursächlich in Abhängigkeit von der verwendeten Technik, insbesondere der Informationstechnik, begibt. Einem Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt damit automatisch eine zentrale Rolle in der zukünftigen Entwicklung zu.

Die Vorgeschichte

Wenn nun an dieser Stelle von einem neuen Bundesamt gesprochen wird, so ist erstmal zu erwähnen, daß zwar der Status als Bundesamt neu ist, allerdings die Behörde an sich schon älter ist: Mitte der fünfziger Jahre wurde schon die Zentralstelle für das Chiffrierwesen (ZfCh) gegründet und dem Bundesnachrichtendienst (BND) zugeordnet. Die Existenz des ZfCh war lange Zeit unbekannt, da davon nur unter der Rubrik "vertraulich" neben der Regierung der Innenausschuß des Bundestages informiert war. Das ZfCh befaßte sich insbesondere mit kryptographischen Verfahren zur Verschlüsselung von Nachrichten und Verfahren zum "brechen" von verschlüsselten Nachrichten, sowie Koordination und Standardisierung solcher Verfahren im Rahmen der NATO.

Am 1.6.1989 machte das ZfCh seine erste Wandlung durch und wurde in Zentralstelle für die Sicherheit in der Informationstechnik (ZSI) umbenannt. Damit anheim ging eine Erweiterung der Aufgaben auf den Bereich Sicherheit in der IT. Dies war die direkte Folge — des weit überschätzten — Eindringens in Systeme der NASA, sowie des sogenannten KGB-Hacks.

Mit Wirkung vom 1.1.1991 hat nun das ZSI erneut seinen Namen geändert und heißt nun BSI. Gleichzeitig wurde das BSI der organisatorischen Anbindung an den BND entlassen und nun direkt dem Bundesministerium des Innern (BMI) zugeordnet. Damit ließ das neue Bundesamt aber seine Entwicklung nicht am Nagel der Geschichte hängen. Die Aufgaben des Bundesamtes waren deutlich über den geheimdienstlichen Bereich erweitert worden, so z.B. die Bera-

tung der Wirtschaft und der Bundes- bzw. Landesbehörden in Fragen der Sicherheit, der Unterstützung der Datenschutzberater, etc. Allerdings wurde das BSI der Abteilung Innere Sicherheit 4, zuständig für Geheim- und Sabotage- schutz, als nationale Sicherheitsbehörde zugeordnet. Leiter des BSI ist und bleibt Dr. Leiberich, der davor schon das ZSI und davor seit 1957 im ZfCh tätig war und seit 1974 deren Leiter war.

In dem Gesetzgebungsverfahren ist dem BSI noch die Aufgabe der Technologiefolgenabschätzung (TFA) in Par. 3, Absatz 1, Punkt 7 mit auf den Weg gegeben worden und der Bundesinnenminister machte dies in seiner Rede vor dem Bundestag nochmal deutlich. Allerdings hat die organisatorische Anbindung ans BMI schon im Vorfeld dem BSI die Möglichkeit genommen, erstmal ohne Mißtrauen betrachtet zu werden. Die Diskussion über die nationale Sicherheitsbehörde der USA, der National Security Agency (NSA) war noch nicht vergessen und die Befürchtung, daß endgültig ein neuer Geheimdienst im Bereich der IT geschaffen wird, wurde immer häufiger laut.

Das BSI lädt ein...

Ende April trafen sich Experten aus dem Gebiet der Wissenschaft, Wirtschaft und der Behörden zu einem Workshop in Boppard. Das BSI hatte unter der Überschrift "IT-Sicherheit: mögliche Folgen fehlender oder unzureichender Sicherheitsvorkehrungen" an den idyllischen Ort am Rhein in die Bundesakademie für Öffentliche Verwaltung der Nähe von Bonn geladen. Die Liste der geladenen Teilnehmer las sich wie ein "Who is Who" der in IT-Sicherheit engagierten. Teilnehmer aus den diversen Universitäten, dem Virus-Test-Labor Hamburg, Firmen wie Debis, Siemens und IABG, Landesdatenschutzbeauftragte aus Berlin und NRW, Projektträger, Ministerialräte aus den diversen Ministerien, sowie gesellschaftliche Gruppen wie DGB, Gesellschaft für Informatik (GI) oder Chaos Computer Club waren vertreten.

Die zentralen Aussagen auf diesem Workshop sollen hier dargestellt werden.

In der Begrüßung würdigte der BSI-Präsident Dr. Leiberich das Erscheinen von ca. 50 Teilnehmern und lobte den Initiator der Veranstaltung, Dr. Ulrich, für sein Engagement.

Dr. Ulrich hat sich in der Fachwelt schon einen Namen durch seine Publikationen im Bereich der TFA und der Restrisiken in der Informationssicherheit gemacht und arbeitete nun sein kurzen im BSI. Schon die Begrüßung wurde von einigen Teilnehmern als Distanzierung zu Dr. Ulrich und der Veranstaltung aufgefaßt, und auch im weiteren Verlauf der Veranstaltung kam der unbefangene Teilnehmer nicht umhin zu vermuten, daß der Bereich TFA, im Bundesamt durch Dr. Ulrich vertreten, ein Novizendasein führt.

Als erster Referent ergriff Prof. Roßnagel von der FH Darmstadt das Wort. Er legte dar, daß die bisherigen Bemühungen um IT-Sicherheit zu technikzentriert sei und die gesellschaftliche Einbettung des Sicherheitsproblems nur unzureichend berücksichtigen. Informations- und Kommunikationssysteme seien Systeme mit Auswirkungen auf die Gesellschaft und seien daher als soziotechnisches System aufzufassen. Wie die meisten Teilnehmer war auch er der Meinung, daß die Verletzlichkeit der Gesellschaft nicht nur durch technische Massnahmen zur Verhinderung von Fehlern und Mißbräuchen veringert werden muß, sondern daß auch die Abhängigkeit der Gesellschaft von Informations- und Kommunikationstechnik und das dadurch bestehende Schadens- und Katastrophenpotential beeinflußt werden muss.

Es gehört eben nicht nur zur IT-Sicherheit, die möglichen Fehler eines Systems zu betrachten, sondern auch im Verhältnis das Risiko, das allein durch den Rechnereinsatz entsteht.

Als Beispiel wurde ein einfacher Lesefehler einer Festplatte bei der Pariser Justiz angeführt, der dazu führte, daß aus mehreren Bescheiden wegen Verkehrssünden plötzlich Delikte wegen Drogenmißbrauch und Prostitution wurden.

Diesen eher harmlosen Folgen stehen aber auch katastrophe Fehler im Rechnereinsatz entgegen, wie ein Softwarefehler in einem Programm zur Steuerung einer Bestrahlungsapparatur in einem Krankenhaus. Weil ein bestimmter Zustand vom Programmie-

rer nicht vorgesehen waren, wurden 2 Patienten mit erhöhter Strahlung behandelt, was zum Tode der Betroffenen führte.
Ebenso machte Prof. Roßnagel darauf aufmerksam, daß ein Fehler in Rechensystemen weitaus stärkere Folgen hätte als gemeinhin angenommen. Durch die Verkettung der Gesellschaft würde der Ausfall von zentralen Rechnern in einigen Großstädten sich im gesamten System fortpflanzen und eine Gefahr für die Gesamtheit darstellen. Ein „Chaosmanagement" wäre aber dann auch nicht mehr möglich, weil die gesamte dafür notwendige Infrastruktur ebenfalls ausgefallen wäre. Eine schreckliche Vorstellung für jedem im Katastrophenschutz.
Das BSI hat — ähnlich wie ihre Vorgänger in anderen Staaten — den Weg der technokratischen Sicherheit gewählt und sich damit auf einen Wettlauf zwischen steigender Verletzlichkeit und Sicherungstechnik eingelassen, die letztere kaum gewinnen kann.
Prof. Brunnstein vom Virentestlabor in Hamburg führte in seinem Beitrag ebenfalls aus, daß er beim BSI eine Fehlentwicklung sieht, weil sich das BSI allein auf technische Massnahmen konzentriert. Da es aber keine sicheren Systeme geben kann, müssen technisch und sozial beherrschbare Systeme gefordert werden. Unter beherrschbaren Systemen müssen aber Systeme verstanden werden, die von Menschen noch erfaßt und damit kontrolliert werden können.
Da aber die gesamte heutige Computertechnik auf den Ideen John von Neumanns aufbaut, ist dies faktisch unmöglich. Von Neumann hatte den Rechner mit seinem Bus, Speicher, CPU, etc. verglichen mit dem Aufbau des menschlichen Gehirns und ging dadurch von einer möglichen Transparenz zwischen Mensch und Maschine aus. Heute wissen wir, daß diese Ähnlichkeit nicht besteht, also der Rechner an sich dem Menschen immer fremd bleiben muß.
Dr. Büllesbach von der Daimler Benz Informationssysteme (debis) und früherer Datenschutzbeauftragter Bremens ging das Sicherheitsproblem von der Entwicklungsseite an. Er kritisierte das nachträgliche Aufspüren von Sicherheitslücken mit Hilfe von Tiger-Teams, also professionelen, angestellten Hackern, und legte dar, daß bei der Entwicklung von Software in Zusammenarbeit mit den Betroffenen (Betreiber, Benutzer, Anwender) die Basis für "Security Managment" gelegt werden muss. Gleichzeitig muss über Sicherheitsprobleme öffentlich diskutiert werden, denn diese Transparenz ist die Basis für den Fortschritt. Zwar stehen dem Sicherheitsbedenken der Hersteller oder Abwender entgegen, aber in der Regel sei Verheimlichung kein Sicherheitsgewinn.
Eine ganze andere — eher pragmatische — Sichtweise wurde von Dr. Bunge, Ministerialrat beim Bundesrechnungshof, vorgestellt. Der BRH stellt häufig Sicherheitsmängel fest, die allerdings nicht bekannt werden. Dadurch werden aber ähnliche Mängel in anderen öffentlichen Einrichtungen nicht beseitigt. Daher ist der Rechnungshof dazu übergegangen, solche Mängel anonym zu veröffentlichen.
Dabei werden diese aber abstrakt dargestellt, um Nachahmungstäter zu vermeiden. Die Details gelten als vertraulich. Sicherheit ist für den BRH ein wichtiger Punkt, da er über den angemessen und wirtschaftlichen Einsatz staatlicher Gelder wacht. Auf der einen Seite kostet Sicherheit aber Geld, ein evtl. Schaden kann auch große finanzielle Aufwendungen nachsichziehen. Inzwischen muss daher bei Antrag auf den Einsatz von Rechnern ein Nachweis Über Angemessenheit und eine [*??? d.S.*] eingereicht werden.
Das BRH beschäftigt sich darüberhinaus nicht nur mit der punktuellen Sicherheit einzelner Systeme, sondern auch im Gesamtkonzept Mensch-Organisation-Technik. Beispielsweise findet im Augenblick eine Diskussion über den Einsatz von Unix im Hinblick auf Sicherheit, wirtschaftlichkeit und Risiko statt.
Am 2. Tag der Veranstaltung erläuterten Dr. Pfitzmann von der Uni Karlsruhe und Prof. von Henke von der Uni Ulm die Anforderungen an IT-Systeme bezügl. Funktionalität und Korrektheit. Dabei wurde erläutert, daß in der Regel Fehler in der Software und seltener in der Hardware liegen.
Kleine Fehler in FORTRAN-Programmen können Raumsonden um Hunderttausende

von KM ihr Ziel verfehlen lassen (und Cruise Missiles um paar Meter).
Ein Lösungsansatz wurde z.B. beim Airbus 320 verwendet: zwei vollkommen eigenständig entwickelte Systeme, die ihre Ergebnisse vergleichen. Solange ihre Ergebnisse übereinstimmen, kann davon ausgegangen werden, daß das Ergebnis richtig ist. Bei Nichtübereinstimmung können entsprechende Maßnahmen eingeleitet werden. Allerdings hat das System auch seine schlechten Seiten, wie der Absturz bei einer Airbus-Vorführung in Paris gezeigt hat.
Als abschliessendes Referat brachte Herr Lau von der Uni Rostock noch einen Einblick in die Situation in der ehemaligen DDR. Eine Abteilung Datensicherheit war der Abt. Geheimnisschutz des Ministerrates in der DDR unterstellt. Datenschutz an sich gab es in der DDR nicht. Datensicherheit selbst wurde aber auch an den Universitäten gelehrt. Für Informatiker waren da 30 Semesterwochenstunden Pflicht. Ob das so bleiben wird, ist unklar. Geplant ist demnächst ein Workshop von der Uni Rostok un der Uni Bremen zur Rechtsangleichung des Datenschutzes.

Was nun, BSI ?

Wo sieht das Bundesamt aber seine zukünftige Aufgabe? Die Teilnehmer waren einer Meinung, daß die Arbeit des BSI auf Grundlage des Errichtungsgesetzes geschehen müsse, aber dieses genug Freiräume zum Setzen von Schwerpunkten und Prioritäten lassen würde.

Dabei wurden denn Punkten Öffentlichkeitsarbeit, Kooperation mit der Wissenschaft, Unterstützung der Datenschutzbeauftragten und der Technologiefolgenabschätzung hohe Stellenwerte eingeräumt. Es kam der Wunsch auf, daß die Technologiefolgenabschätzung eine eigene Abteilung im BSI werden würde und nicht stiefmütterlich am Rande zum Vorzeigen verwendet werden würde.
Die parlamentarischen und ausserparlamentarischen Kontrollmechanismen werden einen besonderen Augenmerk auf die TFA werfen, die ja erst im letzten Augenblick in das Gesetz aufgenommen wurde.
Die Teilnehmer der abschliessenden Podiumsdiskussion sprachen sich durchweg für die Verbindung zwischen Technik und Gesellschaftlicher Verantwortung aus. Sicherheit darf nicht nach dem olympischen Prinzip (höher, weiter, schneller), so Prof. Dierstein, betrachtet werden, sondern auch nach TFA und Verfassungskonformität. Auch wurde die Zusammenarbeit zwischen Juristen, Techniker, BSI und Betroffenen angemahnt, sowie regelmässige Treffen zum Bereich der TFA vorgeschlagen.
Die Abschlußrede blieb Dr. Leiberich vorenthalten. Er bedankte sich bei den Teilnehmern und lobte die Diskussion. Dann erläuterte, wo er die Schwerpunkte des BSI sehen würde, nämlich im Bereich der Verhinderung des Abhörens kommerzieler und staatlicher Links. Diese Gefahr erläuterte er recht ausführlich.
Das in nächster Zeit wirklich nicht mit einer änderung der Einstellung zu rechnen ist, zeigt die 2. Deutsche Konferenz über Computersicherheit, die Mitte Juni vom BSI und BIFOA veranstaltet wird.
Von über 30 Vorträgen beschäftigt sich keiner mit TFA. Dafür gibt es aber eine Podiumsdiskussion über "Techno-Terrorismus" und Kongressgebühren von über 1000 DM. Ob damit der Gesellschaft geholfen ist ? Und in wie weit es sinnvoll ist, daß die von der ehemaligen ZSI entwickelten Sicherheitskriterien für Software kein Wort der TFA enthält und die Überprüfung von Software nach diesen Kriterien - neben drei TÜV-Anstalten - auch von der IABG in München vorgenommen werden, also einer Firma, die zu grossen Teilen dem Bund gehört und bis jetzt stark für die Geheimdienste und dem Verteidigungsministerium gearbeitet hat, spricht ebenfalls nicht dafür, daß das BSI ernsthaft um eine Trennung von seiner Vergangenheit bemüht ist.

Terra

Chaos Computer Club – Schwenckestr. 85 – D-W-2000 Hamburg 20
Telefon (040) 490 37 57 – Fax (040) 491 76 89 – Mbx (040) 491 10 85 – Btx *CHAOS#

Als Normalbrief schicken – Einschreiben gehen zurück!
Ohne Vorkasse können wir leider nicht liefern.

Mitgliedschaft im CCC e.V. Schließt Datenschleuder-Abo mit ein.			
____	*evvw*	*20,00 DM*	Einmalige Verwaltungsgebühr bei Eintritt
____	*evmm*	*120,00 DM*	Normalmitgliedschaft (Jahresbeitrag)
____	*evsoz*	*60,00 DM*	Sozialmitgliedschaft für Studenten, Schüler, Arbeitslose etc. (Jahresbeitrag)
Reine Datenschleuder-Abos. *Ein Abo gilt für 8 Ausgaben.*			
____	*nabo*	*60,00 DM*	Normalabo der Datenschleuder
____	*sabo*	*30,00 DM*	Sozialabo der Datenschleuder für Studenten, Schüler, Arbeitslose etc.
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)
in Vorb.	*habi3*	*33,33 DM*	Die Hackerbibel, Teil 3 (ca. 250 Seiten A4)
____	*wund*	*28,00 DM*	Das Chaos Computer Buch (250 Seiten A5)
____	*mosk*	*26,00 DM*	Hacker für Moskau *(unzensierte 1. Auflage)*
Chaos-Literatur *(im Buchhandel eher nicht erhältlich)*			
____	*stud*	*7,50 DM*	Studie für die Grünen über politischen Computereinsatz im Bundestag — und überhaupt
____	*mutst*	*10,00 DM*	*Mensch-Umwelt-Technik* Studie: Elektronische Informationssysteme für den Umweltschutz
____	*kamj*	*10,00 DM*	Der elektronische Kammerjäger / Über Wanzen, Abhörmethoden und Erkennung derselben
____	*doku*	*5,00 DM*	Dokumentation zum Tod von Hagbard (Karl Koch)
____	*frnk*	*7,50 DM*	Perspektiven einer neuen Kommunikationsmoral für das Zeitalter der Kybernetik, *von Prof. G. Frank*
Infopakete / Software & Co.			*z.Zt. nur 5 1/4" Disketten möglich*
____	*vir*	*25,00 DM*	Infopaket Computerviren (inkl. MS-DOS Demovirus)
____	*pcd*	*25,00 DM*	PC-DES für MS-DOS: Private Verschlüsselung von (Text-) Dateien. *Gewerbliche Version bei BainON! Heidelberg*
Backer *PVC wassergeschützt / gestanzt, wenn nicht anders angegeben*			
vergriffen	*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
____	*ooo*	*5,00 DM*	Bogen mit 18× „Außer Betrieb," 8× „Out of Order" und 1× „Guasto"
____	*post*	*5,00 DM*	Bogen mit Post-Totenkopf-Klebern verschiedener Größe
____	*zula*	*5,00 DM*	15 × Chaos-Zulassungszeichen Z A023/042Z mit Post-Totenkopf
Ganz Wichtig: Gedenkt bitte unserer immensen Portokosten! Rückporto *mindestens* erbeten!			
____	*pvt*	*??,?? DM*	Porto/Verp./Spende

Summe: _____ DM
(Versand erfolgt frühestens nach Geldeingang)

Zahlweise *(bitte bekreuzigen oder so):*
- ◯ bar
- ◯ V-Scheck
- ◯ Rostwertzeichen *(nicht über 1 DM!)*
- ◯ Überweisung (Postgiro Hamburg / BLZ 200 100 20 / Konto 599 090 – 201)

Datum,
Unterschrift: _____

Name: _____

Adresse: _____

_____

_____

_____