

Die Bayerische Hackerpost



märz 1986

== Das Informationsblatt für den lebensbejahenden DFÜ-Benutzer ==

Überraschende Geschenke

'Hallo, liebe Abonnenten, Interessenten, Leser und sonstige Sympathisanten!' - So haben wir vor fast genau einem Jahr die B.H.P.#3 auf Euch losgelassen. Auf Seite zwei folgte dann der erste deutschsprachige Artikel zum Thema Computerviren mit Detailinformationen. Es sollte der Knüller des Jahres '85 werden. Inzwischen ist Schlagwort Virus schon bis zu JASMIN äh CHIP durchgedrungen. Während sich andere noch die Köpfe heißreden, ob es soetwas wie Computerviren überhaupt gibt, wenden wir uns einen neuen Gebiet zu: den sogenannten CHIPKARTEN. Nachdem das Hamburger Journalistenduo Thomas Amman / Mathias Lehnhardt die Unsicherheit der Magnetkarten bewiesen hat, ist es an der Zeit den nächsten Vorstoß in Richtung 'Plastic-Money' zu korrigieren.

Auf Seite drei dieser Nummer startet daher unser Hacker/Cracker-Rätsel. Ziel ist es zu beweisen, daß die Wunderkarte genauso unsicher, unbeherrschbar, und manipulierbar ist wie all die herkömmlichen Magnetkarten. Jeder der Interesse hat, bekommt eine Kopie sämtlicher bei uns vorhandener Unterlagen, und eine funktionsfähige Chipkarte. Das vorhersehbare Ergebnis unserer Aktion wird hoffentlich auch den letzten Bankmanager vom Techno Trip runterholen. Dann wollen wir ihnen doch mal die nötige Dosis Realität verpassen.

Über all diesen Entwicklungen wollen wir aber auch das Alltagsgeschäft nicht vernachlässigen. All die, die sehnlichst auf den B.H.P. NUA-Guide warten, können aufatmen: er ist wieder da. Versandtermin ist der 22.03.86. Es ist zwar keine vollständige Neufassung, aber sowie Version 3.0 fertig ist, erhält jeder, der dann noch will, ein Exemplar. Demnächst wird der NUA-Guide auch in elektronischer Form, d.h. auf Diskette erscheinen. Verwaltet werden die Files mittels des "Unheimlichen B.H.P.-Nuasammlers" (Natürlich Freeware), der im Laufe der Zeit möglichst vielen Rechnern angepasst werden soll.

Unser lieber Dr.Dr.Strobe bringt heute einen typischen B.H.P.-Brief, so voll aus dem Leben eines Redakteurs.

Aufgrund der positiven Reaktionen auf die erste SOURCE, in B.H.P.#7, hat sich der Platz der Duisburger mehr als verdoppelt. Wir sind auch noch offen für andere Gruppen, die bei der B.H.P. mitmachen wollen.

Genug geschwafelt:

Es grüßt wiedereimal

das Redaktorentiim



Buchbesprechung

Out Of The Inner Circle

A Hacker's Guide
To Computer Security

Der Titel des Buches, das leider nur in englischer Sprache vorliegt, verspricht ja so einiges. Der Verfasser Bill 'The Cracker' Landreth wird als 'The Teenage Computer Wizard' eingeführt. Aber als leidgeprüfter Rezensor ist man ja schon manche Mogelverpackung rund um irgendwelchen inhaltsleeren Schund gewohnt.

Dieses Buch macht da eine löbliche Ausnahme: Der Verfasser ist nicht einer der vielbeschworenen 'intimen Kenner der Hackerszene', er war auch nicht mit 'langen und aufwendigen Recherchen' beschäftigt, nein viel einfacher: Bill Landreth ist (oder war) Hacker, einer der Mitbegründer des 'Inner Circle' eines Hackerclubs ähnlich dem der 414's. Er weiß, wovon er spricht, und er tut dies auch recht ausführlich, gibt eine auch Außenstehenden verständliche Einführung in die Materie, gewürzt mit Anekdoten und Hacks aus seiner aktiven Zeit. Verschiedene Hackmethoden werden erläutert angefangen vom Scannen über Speicherauslesen bis hin zu dem was er ein Trojanisches Pferd nennt - ein Programm, das neben dem offensichtlichen Zweck noch etwas ganz anderes macht - neue Accounts einrichten zum Beispiel. Er bespricht die gegenwärtig ((c)1985) üblichen Sicherheitseinrichtungen und wie sie ein Hacker umgehen kann.

Aktuell

Die Computer nicht
den Männern überlassen ...!

Ich möchte alle Frauen, die Interesse an Computern haben - ganz gleich, ob sie was können oder nicht - auffordern, sich mal bei uns zu melden.

Damit wir vielleicht mal was zusammen anfangen können. Um das Feld Computer nicht allein den Männern zu überlassen:

Also, Kärtchen an die B.H.P. (Stichwort "Frauen und Computer") oder anrufen: 089/5784 / (^A &Z+ DATEX-P: voruebergewende Stoerung im Netz

Übrigens: Die verehrte Männerwelt ist aufgefordert, diesen Aufruf an Freundinnen und Bekannte weiterzuleiten - Es sei denn, sie hätten Angst vor computernden Frauen.

Gertie

--->

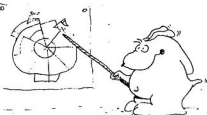
Leider endet das Buch etwas abrupt - dies ist aber nicht The Cracker in die Schuhe zu schieben, daran sind vielmehr 'several gentlemen representing the Federal Bureau of Investigation' schuld - The Cracker ist wegen angeblich unberechtigter Benutzung des GTE/Telemail-Netzes geschnappt und angeklagt worden.

Ein echter Verlust für die Hackerszene.

Bill Landreth,
Out Of The Inner Circle,
Penguin Books,
ISBN 0-14-087-139-X,
Preis U.K. £8.95

Hacker -
Preisausschreiben

??
?
? Hacker - Preisausschreiben ?
?
??



Aus aktuellem Anlaß - die inzwischen etwas ins Gerede gekommene Scheckkarte wird ja wohl in der nächsten Zeit zu Grabe getragen, nachdem sich eklatante Mängel an der angeblichen Manipulationssicherheit des Vielzweck-Plastikkärtchens (schon mal als Türöffner benutzt?) aufateten und die auch noch in aller Öffentlichkeit breitgetreten wurden.

Der Nachfolger der Magnetkarte soll die Chipkarte werden, die auf einem anderen Prinzip basiert - nicht mehr On- (bzw. Off-)linezugriff auf das in einem fernen Zentralrechner gespeicherte Konto, sondern der Chip auf der Chipkarte wird mit einem gewissen Betrag 'geladen', den man sich dann Stück um Stück oder auch en gros von der Karte wieder runterholen kann.

Etwas ähnliches gibt es schon in Frankreich und in einsamen deutschen Enklaven in Schmalzspurverson als Telefonkarte(ohne Chip oder soetwas), die soundsoviel Einheiten draufhat, die dann Zug um Zug beim Telefonieren gelöscht werden. Im Fall der französischen Telefonkarte handelt es sich um eine Art EPROM, das im Urzustand ein bestimmtes Muster eingebrannt hat. Mit jeder Einheit, die verbraten wird, wird nun (hier trifft der Begriff 'verbraten' mal ernsthaft zu) ein weiteres Bit durchgebrannt. Es wäre nun denkbar, die Karte einfach Schicht um Schicht abzutragen, bis der eigentliche Chip vor einem liegt, das Ding mit UV-Bestrahlung wieder in den Ursprungszustand zurückzusetzen und mittels Programmiergerät wieder geschäftsfähig zu machen.

Ganz so einfach wird das bei der Bank-Chipkarte wohl nicht zu drehen sein - die Hersteller und erst recht die Verkäufer reden ja gar von einer hundertprozentigen Manipulationssicherheit. Aber das hieß es von der Magnetkarte auch.

Um genau diese Behauptung zu untersuchen, nämlich zu prüfen, ob die Chipkarte wirklich manipulationsicher ist, haben wir ein Preisausschreiben vor:

Wer mag und sich das zutraut, kann sich von uns eine kodierte Chipkarte nebst allen bis dahin aufgelaufenen Unterlagen gegen Unkostenbeitrag schicken lassen und schon gehts auf! Ziel des Spiels ist es, den Code auf der Karte auszulesen und zu ändern - zu deutsch, die Karte soll geknackt werden. Damit das Ganze noch einen weiteren Reiz hat, bekommt derjenige, der die Karte entcodiert, von uns als Hauptgewinn einen

Osborne 1 DQD - CP/M - Rechner

ACHTUNG !!! Derzeit sind wir noch dabei, eine günstige Quelle für die Karten aufzutun und Infos zu sammeln, also bitte **NOCH NICHT SCHREIBEN !!!** Bis zur nächsten B.H.P. dürfte es aber soweit sein.

Einstweilen die Auflösung der Mehrzweckkarte: Karte zwischen Tür und Türrahmen stecken und damit den Sperrriegel zur Seite drücken.



Fragen Sie Dr.Dr.Strobe



ER gibt Ihnen eine Antwort, die Sie nie vergessen werden.

Bernd Bieder aus Kleinkleckersdorf/Kreis Großkleckersdorf fragt:

Sehr geehrte Damen und Herren,

handelt es sich bei der B.H.P. um ein Periodikum oder einen Club? Könnten Sie mir im ersteren Fall Ihre derzeit gültigen Abonnementbedingungen zusenden. Im zweiten Fall erbitte ich nähere Informationen, ob es auch mir möglich wäre, in Ihren Club als Mitglied aufgenommen zu werden?

Mit der Bitte um rasche Erledigung verbleibe ich freundlich grüßend

Ihr Bernd Bieder

Dr.Dr. Strobe antwortet:

Betreff Ihr Schreiben vom ..., Ihr Zeichen ..., Unser Zeichen ...

Sehr geehrter Herr Bieder,

bezugnehmend auf Ihr o.g. Schreiben, freue ich mich Ihnen mitteilen zu können, daß die B.H.P. weder ein Frauenleiden noch ein sonst irgendwie gearteter Haufen aus mindestens sieben Leuten ist. Minwiederum gegen und dies Ihnen mitteilen zu können, freue ich mich noch viel mehr, ist die B.H.P. ein äußerst unregelmäßig erscheinendes - diese Ausgabe ist wieder mal der 10. Beweis dafür - Fachinformationsblatt für den lebensbejahenden DFU-Benutzer. Wie man dran kommt, steht auf der Rückseite!

CUL, Strobe

Und jetzt wieder ohne Krawatte, dafür mit Ringen unter den Augen:

Herr EIR aus München/Großbayerisches Reich fragt:

I hob des wörlid-schtandard-modem kaft, des tuat aa recht quat funktioniern, bloß wenn i DATEKS auf 1200 Baud chruaf, no mogs net. Was hots'n do?

Prof.Dr.Dr. Strobe antwortet:

Tja, das WS-Modem 2000 arbeitet bei 1200 Baud nur im Halbduplex-Betrieb, es kann also garnicht mit DATEX funktionieren, da DATEX nur mit Vollduplex arbeitet. Sie können also nur mit 300 Baud auf DATEX fahren, da die 600 Baud, die das WS-Modem besitzt, wiederum von DATEX nicht unterstüzt werden.

Bis zum nächsten mal verbleibe ich Euer

Dr.Dr.Strobe

Das Imperium schlägt zurück

In Berlin hat die Bundespost drei Computerfreaks die Telefone gesperrt und die Aufhebung des Teilnehmerverhältnisses (Ruch!!) in Aussicht gestellt. Dazu kommen Regressansprüche in noch nicht bekannter Höhe. (Alimente o.ä.?)

Die Computerfreaks hatten mit ihren Homecomputern über zugelassene Akustikkoppler mit Hilfe ihrer Teilnehmererkennung ganz legale Datenverbindungen über den Vermittlungscomputer (PAD) hergestellt. Da es in Berlin keinen 8-Minutentakt gibt, ist es dort - im Gegensatz zum Bundesgebiet - kostengünstiger, die einmal aufgebaute Verbindung als Standleitung stehenzulassen.!. Zu diesem Zweck ist es üblich, (aha), in einem Computersystem zu parken.



VATICAL^(TM)

Ab 04.03.1986 besteht die Möglichkeit über alle autorisierten Vertriebsstellen der B.N.P. VATICAL^(TM) in der neuen Version 2.0 zu beziehen.

Erstmals ist es auch möglich VATICAL^(TM) als Hardwarezusatz für verschiedene gebräuchliche Rechner zu beziehen. Die Lieferung erfolgt in Form eines gegen unbeabsichtigtes Überschreiben geschützten WOM's (Write Only Memory).

Bei Anfragen und Bestellungen bitte Rechnerart angeben.

Nach Sevicemaßnahmen (huch, wat'n dat'n) der Post am Vermittlungscomputer trugen diese quasi Standleitungen die Teilnehmererkennung der Gesellschaft für technische Thermochemie und Physik in Hamburg (DGTHAM, Passwort PAMTYZ), obwohl sich die Computerfreaks mit ihrer persönlichen Kennung in das System eingetragen hatten. (Jawollja) Dazu sollte man wissen, daß die Kennung DGTHAM und das dazugehörige Passwort seit dem 13. Januar in der Hackerszene kursierten, denn sie ermöglichte eine kostenlose Nutzung von DATEX-P.

Angeblieh ist durch die unberechtigte Nutzung ein Schaden von DM 100.000,- entstanden, da diese Kennung bundesweit benutzt wurde (multiuserfähig). Der Post ist diese "atypische" Nutzung durchaus bekannt gewesen, (wie das) denn sie hat die GTT auf die Problematik hingewiesen. - Es liegt der Verdacht nahe, daß es möglich ist, den geheimen Teil "B" - das Passwort - aus dem Postrechner zu erfahren.

Disaster Recovery

Bemerkenswert an der ganzen Sache ist, daß die o.g. Teilnehmererkennung seit dem 18.02.86 auf Veranlassung des Inhabers von der Post gesperrt ist, besagte Berliner Phreaks, jedoch weit über diesen Zeitpunkt hinaus ihre Standleitungen in Betrieb hatten. Der nächste Verdacht drängt sich auf - daß die Post ihren Rechner noch weit weniger, als bisher befürchtet in der Hand hat. (Aber wer hat das schon?!)

Dank an Jürgen

4. Folge

Was bisher geschah:

Eigentlich garnichts, zumindest nix neues.

Die Handelnden dieser Folge:

Bonifatius Hubertus Perchl -
Ein Schicksalschlag trifft unseren Helden.

Außerdem:

IBM und eine Menge anderer völlig unwichtiger Gestalten



BAYERNSTEIN - Folge 4.:

Erste Bewegungen

Während die ostasiatischen Zwillinge in ihrem Zimmer verschwinden, das genau über der Wirtsstube liegt, in der die beiden Theologen noch immer tief ins Gespräch mit den O'Clocks versunken sind und seltsame Gerätschaften aus ihren diversen Gepäckstücken und Taschen kramen und alle Lebewesen vor dem gewaltigen Unwetter Schutz suchen, sieht man IBM's verkrüppelte Gestalt, der Naturgewalt trotzend, über die Dächer der Burg Bayernstein hüpfen um den Auftrag seines Herrn und Meisters zu erfüllen.

Lenken wir nun das geneigte Auge des Lesers jener verschwiegenen Hütte im Walde zu, in der Bonifatius Hubertus Perchl immer noch verzweifelt versucht seine Standleitung zu halten.

Der fahlgrüne Monitor flackert und langsam erscheint ein gespenstisch anmutender und doch so bekannt wirkender Unbekannter auf dem Bildschirm. Er hält etwas in Händen, das entfernt einer Kugel gleicht. Wie selbständige Lebewesen fliegen Bonifatius' Hände über die Tastatur als er versucht, die Erscheinung deutlicher auf den Schirm zu bekommen. Da - ein gleißend heller Schein, ein Krachen, das Tote erwecken könnte und der Monitor wird dunkel. Nur einmal noch flackert er kurz auf. Vor Bonifatius H.P.'s Augen entsteht eine Kugel - nein, eher ein birnenförmiges, den ganzen Schirm bedeckendes Ikon - dann ist völlige Dunkelheit. Niedergeschmettert sinkt B.H.P. über seiner Tastatur zusammen.

Wie wirts weitergehen ?

- Wohin hüpf Igor ?
- War alle Mühe umsonst ?
- Ist die Leitung jetzt futsch ?
- Wer ist die gespenstische Gestalt ?
- Ist sie vielleicht die lang gesuchte große Unbekannte (X) ?
- Was ist das für eine Birnen-Kugel ?
- Und überhaupt, was sucht eine Birne auf B.H.P.'s Apfel ?

Mehr in der nächsten Folge

 * Telefon für *
 * Fortgeschrittene *
 * Teil 4: Handwerkszeug *
 * *

Heute mal wieder ein Beitrag aus der Praxis für die Praxis, als Abwechslung für die letzten etwas trockenen Kapitel.

Häufig erwacht ja in einem lebensbejahenden DFÜ-Benutzer der Wunsch nach einem neuen Telefon, zumindest nach einem, das anders ist, als das vorhandene (womöglich noch mit Radl...). Gesagt, getan, schließen wir unser neues Telebin eben genauso an wie das alte. Ja, ganz einfach, solange wir auch bisher nur einen stinknormalen Hauptanschluß mit einem Apparillo hatten. Dann geht man mit den beiden Anschlüssen des neuen, wesentlich lebensbejaherenden Teflons einfach auf die beiden Klemmen, auf denen der bisher gebräuchliche Klapperkasten angeschlossen war. Tja, soweit, soeinfach. Aber was ist, wenn die Post beim Versuch, eine Anlage mit getrenntem Gebührenzähler, oder eine Krücke mit zwei Steckdosen und separaten Wecker, oder was der Telefonprospekt sonst noch bieten mag, nur einen heillosen Kabelsalat hinterlassen hat? Wie soll sich da ein normaler und lebensbejahender DFÜ-Benutzer noch durchfinden?

Um das geliebte neue Telebin anzukoppeln, müssen wir rauskriegen, auf welchen Leitungen die Sprechsignale geführt werden (im Postmund a und b genannt). Dazu basteln wir uns - je nach Geschick und Laune mehr oder weniger kompakt und wohlgeformt - einen Prüfstift zusammen. Die Schaltung ist recht einfach:

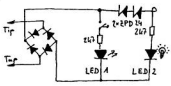


BILD 1: Prüfstift (Schaltung)

Und nun die Prüfspitzen gespitzt und ran an die Drähte, die die Post beim letzten Besuch in der Wohnung vergessen hat. Zunächst einmal lassen wir den Hörer noch auf der Gabel rumliegen. Wenn wir die richtigen Drähtelein ertapt haben, leuchtet die LED 1 auf - ganz klar, denn im Leerlauf liegt auf den Ruflleitungen eine Spannung von ca. 60 Voltis an - sobald abgehoben wird, bricht diese Spannung allerdings sinnlos zusammen und krebst hinford und heropel so in der Gegend von mickrigen 10 bis 15 Volt rum. Die LED 1 geht also beim Abhebeln des Hörers schlagartig aus. Nun aber, um uns nochmals genauer zu vergewissern, ob wir nicht irgendwelchen anderen Super - Differential- Wackeldraht - Multidreher - Schaltungen der gelben Blauröcke aufgesessen sind, drücken wir mit tastaturgestähltem Finger flugs unseren Taster - und dies ist der Moment, in dem sich a und b von allen anderen scheiden: Jetzt muß nämlich als Ersatz für die ausgegangene LED 1 LED 2 aufleuchten.

```
do while not hinhaut and
  cable in {first_cable..last_cable}
  replace(cable,another_cable);
```

BILD 2: Schematisch-algorithmische Darstellung des Verfahrens zur Ermittlung der a und b Ader in PASCAL-ähnlicher Allgemeinnotation

Dank des Gleichrichters ist es dem Prüfstift mindestens ebenso egal wie dem Telefon, wierum man ihn/es anklemt.

Lasset die Boxen blühen und die Telefone klingeln.

hacintosh



- oder was Knigge mit DFÜ vereint -

Immer wieder scheinen einige von den Basiclegasthenikern nicht zu raffan, wozu bei der DFÜ die UT-Protokolle (UT = Übertragung) da sind. Aber nicht nur den Superkrächels passiert das, sondern auch den "Super-Programmierern", die diverse Terminal-Programme und Schrott-Boxen à la M..... schreiben. Sogar diese Leute halten sich nicht an die einfachsten Regeln der Datenübermittlung. Der Schreiber dieses Artikels ist daher bemüht, ihn so verständlich wie möglich zu halten, damit nicht nur die Anfänger, sondern auch die "Experten" endlich einmal den großen Durchblick kriegen. Ich hoffe, ich drücke mich verständlich aus. Leider konnte die erforderliche Promillegrenze von über 2.5 Promille, die man für solch einen Artikel haben sollte, mangels Masse nicht erreicht werden. Jedem der meckert senden wir postwendend den Strick zum Aufhängen zu. Die Beerdigungskosten tragen wir nicht.

Vor den Protokollen erst einmal ein paar Worte zu den grundlegenden UT-Verfahren:

Halbduplex

Bei halben Duplo gibt es nur ein Protokoll. Ich will auch nicht viele Worte darüber verlieren: das Ding ist nämlich für 300 Baud Telefonboxen absoluter Schrott. Das lohnt sich nur, wenn Sie ein total chaotisches Telephonnetz haben! (Schönen Gruß an die Spanier). Bei diesem Verfahren sendet immer nur ein Computer, und der andere empfängt. Es wird auch nur ein Frequenzpaar verwendet. Das hat den Vorteil, daß der Frequenzabstand zwischen 1 und 0 größer und sicherer ist. Damit sind dann auch UT-en mit 1200 Baud durchaus sicher. Solange wir aber keine höherentwickelten Boxen haben, ergibt sich ein gravierender Nachteil: wenn man z.B. aus einer Mehlbox einen längeren Text holt, ist dieser weder anzuhalten, noch abzubrechen. Der einzige, der sich da freut, ist unser Sonnenscheinchen. Folgerung: Halb Duplo ist für unsere Zwecke und bei 300 Baud sowieso Mist.

Vollduplex bedeutet, daß beide Rechner gleichzeitig senden und empfangen können. Jeder hat ein eigenes Frequenzpaar, auf dem er arbeitet. Dadurch, daß jetzt bei der beschränkten Bandbreite des Telefons zwei UT-en gleichzeitig auf der selben Leitung stattfinden, treten natürlich mehr Störungen auf. Oberhalb von 600 Baud ist Vollduplex beim Telefon praktisch unmöglich. Weil jetzt in jede Richtung ein Kanal zur Verfügung steht ergibt sich gleich die erste und fast immer verwendete Möglichkeit zur UT-sicherung: Jedes übertragene Zeichen wird sofort zum Sender zurück übertragen (geschot). Dieser kann dann feststellen, ob ein Fehler auftrat. Aufbauend darauf gibt es mehrere Arten von UT-Protokollen. Das einfachste und am meisten verbreitete ist das XON/XOFF-Protokoll. Es dient der Synchronisation der UT-geschwindigkeit zwischen den Partnern. Alle anderen sind z.B. dazu da nachzuprüfen, ob keine Fehler auftauchen oder um Maschinenprogramme auszutauschen.

Ergo: Ein 300 Baud Koppler muß nicht unbedingt halb Duplex haben. Hauptsache Answer- und Originate-Mode, aber dazu kommen wir ein andermal.

XON/XOFF

Wie schon gesagt: das Non-Plus-Ultra in der DFÜ. Eigentlich unverstänlich, warum einige Terminalprogramme das immer noch nicht raffan, wo doch selbst der einfachste Drucker mit serieller Schnittstelle mitmachen kann. Ist doch ganz einfach. Erstmal können beide Computer gleichzeitig senden und empfangen. Wenn dann ein Computer an den anderen ein XOFF (CTRL-S/\$13) sendet, so hat der andere mit dem Senden sofort anzuhalten und zwar so lange, bis der erste ein XON (CTRL-Q/\$11) sendet (Nicht etwa nach 30 Sekunden einfach weitersenden). Erst dann darf der andere Computer weitermachen und weiter Text ausgeben oder was auch immer. Das gilt sowohl für die Mehlbox als auch für die Termiten-



THE SOURCE



Hallo Leute, herzlichen Glückwunsch zur 2. Ausgabe. Die Erste scheint Euch (und uns) ja gefallen zu haben, sonst würdet Ihr hier das ja garnicht lesen. Ich hoffe die Artikel in dieser Ausgabe finden auch Anklang. Natürlich werden wir versuchen, angekündigte Serien weiter- und nicht totlaufen zu lassen.

Täglich erreichen uns WAHNSinnig viele Zuschriften. Diesmal waren es mindestens zwei (das sind gerade 5% der Zuschriften an die B.H.P. d.Hätzer); wie wär's mit etwas Kritik oder (ähm) Lob oder so. Um Euch nun die Möglichkeit der Kritik zu geben, kommt jetzt eine kurze Liste, wo wir zu erreichen sind (oder zumindest sein sollten).

RMI-Aachen	Datex-P	45241090528,ZCZC	Empfänger: G.EFFENBERG
		Passw.: MERCATOR	
GEO1 (IMCA)	Datex-P		Empfänger: H.Schröder
ZEV	Datex-P	022847911118	Empfänger: GI
Lion	Mailbox	02151/700253 (Krefeld)	Empfänger: GI's
AUS	Mailbox	0203/705827 (Duisburg)	Empfänger: GI's
MHB	Mailbox	02841/57325 (Mörs)	Empfänger: GI's

Und jetzt für all die datentechnisch Unterentwickelten, die sich noch auf Papier äußern müssen

Die GI's
Postlagerkarte Nr. 056945
Hauptpostamt
4100 Duisburg 1

Hacking on the ST - Teil 2

Während wir im ersten Teil feststellen mußten, daß die Fähigkeiten des "eingebauten" Terminals alles andere als überragend sind, schauen wir heute, was denn der vielgepriesene Softwaremarkt bietet.

Inzwischen sind bereits mehrere Terminalprogramme für den ATARI ST zu kaufen. Es empfiehlt sich jedoch grundsätzlich nur ein Programm, welches in der Lage ist, ein VT100-Terminal zu emulieren. Dies bietet den Vorteil, beim Hacken in VAXen den Bildschirmditor benutzen zu können, außerdem ist man in der Lage, PHONEnen zu können (wichtig: Vorher 'set term/vt100' eingeben, sonst weiss die VAX nix von deinem VT100!), dann kann Mann also äußerst komfortabel chatten (sowas muß man einfach mal mit einem 1200 Baud Vollduplexmodem erlebt haben). Hier nun eine kurze Übersicht der uns z.Zt. bekannten VT100-Emulatoren:

VT100-Terminal-Emulator
von RDS-Software, Frankfurt:
Terminalprogramm mit den üblichen Eigenschaften. Bietet zusätzlich allerdings einen eingebauten NUA-Scanner und frei belegbare Funktionstasten sowie Parken auf Tasten-

druck. Neue Version soll unter GEM laufen (mir noch nicht bekannt).

Leider kopiergeschützt...

Preis: DM 248.-

PC/Intercomm

von Mark Of The Unicorn:

Bestes mir bekanntes Terminalprogramm für den ST. Das einzige, was es nicht kann, ist eine Directoryanzeige. Ansonsten bietet es sogar unter anderem einen Hilfsbildschirm, der anzeigt, welche VT100-Taste auf welcher Taste des ATARI-Keyboards liegt, komplette Modemsteuerung inklusive Autodial (auf welchen Pin?), Funktionstastenbelegung. PC/Intercomm unterstützt folgende Übertragungsprotokolle: Modem7, Inter-PC/Intercomm (was ist schon ein Programm ohne eigenes Spezialformat?), Kermit, Kermit Image. Ebenfalls kopiergeschützt...

Preis: \$125.-

Das war's dann leider schon mit den brauchbaren Angeboten. Da die Preise für unser Gefühl ein bißchen happig sind, haben wir uns dazu entschlossen, außer Kopierprogrammen auch ein eigenes Terminalprogramm zu entwickeln. Sobald es fertig ist, wird es als Freeware zu haben sein.

Aus den Giftküchen deutscher Gesetzgebung:

Hackergesetz und TKO

Schon zum ersten Januar 1988 will unser Bleiminister alles zum guten wenden:

Eine TELEKOMMUNIKATIONSORDNUNG - kurz TKO genannt - soll in Kraft treten, hat er Presse-erklärt.

Neben Gebührensenkungen in 3-stelliger Millionenhöhe (geplant ist z.B., die Grundgebühr von derzeit DM 27,-- auf DM 24,60 zu senken - zuzüglich einem Telefonapparat bisher im Preis inbegriffen. Er soll nun monatlich DM 2,40 kosten.) ist noch nichts substantielles bekannt.

Insider reden aber bereits davon, daß die Post ihre Hoheit ab 1988 an der Anschlußbuchse enden lassen will.

Nachfolgend eine Aufstellung der bis jetzt bekannten Änderungen.

* ab 1988 soll die einheitliche Anschlußgebühr 65 Märker kosten - egal wieviel Krepel und Buchsen man sich zusätzlich bestellt.

* private Zusatzgeräte wie Anruf-beantworter werden genauso kostenlos wie der Gebührenzähler.

* DATEX-P wird es endlich bundesweit zum Ortstarif mit einheitlicher Nummer geben. Vermutlich aber in Minuten-Takt ... Ende Mai soll der Postverwaltungsrat dazu sein endgültiges Jawort geben.

In der nächsten B.H.P. werden wir ausführlicher auf die Änderungen, besonders bei der Datenfernübertragung eingehen. Die Post ist hier sehr zugeknöpft, was Informationen angeht. Was uns aber bekanntlicher Weise nur sehr selten stört

In der nächsten Ausgabe erfolgt auch eine endgültige Würdigung des "Hackergesetzes", das am 27.2.86 vom deutschen Bundestag beschlossen wurde und zum 1. Juni in Kraft treten soll. Es verdient jetzt - Opposition sei Dank - diesen Namen weit weniger, als ursprünglich befürchtet.

```
PACKAGE BODY HAKERSPIEL IS  
TASK ORGANISATION IS  
  ENTRY USER-ID;  
  ENTRY PASSWORD;  
  END ORGANISATION;  
TASK BODY ORGANISATION IS SEPERATE;  
END HAKERSPIEL;
```

```
SEPERATE (HAKERSPIEL);  
TASK BODY ORGANISATION IS  
  DUMMY: STRING;  
  HACKING: BOOLEAN;  
BEGIN  
  SET LINE LENGTH(50);  
  WHILE HACKING LOOP  
    ACCEPT USER-ID(OK:OUT BOOLEAN)DO;  
      SET COL(15);PUT("USER-ID");  
      GET(DUMMY);  
      NEW LINE  
    OK:=FALSE;  
    END USER-ID  
    ACCEPT PASSWORD(OK:OUT BOOLEAN)DO  
      SET COL(15);PUT("PASSWORD");  
      GET(DUMMY);  
      NEW LINE(2)  
    OK:=FALSE;  
    END PASSWORD  
    HACKING:=TRUE;  
  END LOOP;  
END ORGANISATION;
```

Die Össis
sind doch die Schnellsten

Ein neuer Geschwindigkeitsrekord im Sperren einer NUI wurde in Österreich aufgestellt. Braucht die deutsche Post zum Sperren einer NUI ca. ein bis zwei Wochen, so schafft unser kleiner Nachbar das in nur zwei Tagen, und das auch noch am Wochenende!

Am Freitag den 24. Januar 1986 wurde festgestellt, daß auf der NUI des Vogel-Verlags (Ihr wisst schon, das ist die NUI, die mit 'D' anfängt) herumgehackt würde. Obwohl hier wie dort Beamten am Ruder, sitzen zeigten die Össis, daß man schnell reagieren kann. Am Sonntag den 26. (immer noch selber Monat) ging nichts mehr!

Auch wenn man es dem Vogel-Verlach wegen diverser Vergehen gegen die Menschlichkeit (Chip, HC und anderes) wünschen würde, es war leider nur blinder Alarm. Ein neuer Port hat falsche Daten geliefert, und den Tracer verwirrt.

programme. Ich weiß gar nicht, wo für einige Programmschleifer da die Problems sind. Checken die das nicht oder was? Ein häufiger Fehler: Das Termprog. reagiert nicht auf einen XOFF von der Mehlbox. Das äußert sich folgendermaßen: Nehmen wir an, ein längerer Text soll in eine Mehlbox in einem Stück abgelegt werden. Sagen wir mal 10 KB. Ja, ich weiß, die meisten verkraften nur 50 Zeilen à 80 Zeichen (ca. 4KB). Aber es gibt auch andere, bessere Boxen (Hilfe! Die 64'er wollen mich lynchen). Also! Solche Mailboxen haben meist einen Zeichenpuffer, der auch nicht größer ist, als der der anderen Boxen. Nun sind aber die wenigsten Laufwerke in der Lage 4-5 KB zwischen dem Empfang von zwei Zeichen auf die Disk zu schreiben (es sei denn, die Box hat einen soft/hardware Zeichenpuffer in der seriellen Schnittstelle. Das ist aber noch sehr sehr selten). Die Box braucht also Zeit zum abspeichern. Sie sendet ein XOFF an das Terminalprogramm und speichert ab. Das Programm aber läßt das XOFF kalt und der Schweinepriester sendet einfach weiter. Dadurch gehen dann natürlich Daten verloren. Peinlich. Keine Arme, keine Kekse. Bei manchen Programmen kann man natürlich XON/XOFF an und abstellen, aber wenn es bei an (enable) immer noch nicht klappt, hat da wohl irgend jemand einen Fehler gemacht (Wahrscheinlich der Goofy, der den Müll verbockt hat). Wie gesagt, das sind aber Schwächen, die nur dann auftreten, wenn jemand nicht programmieren kann (an dieser Stelle auch einen Gruß an Apple; wie war das noch mit APPLE ACCESS V1.07).

Mit XON/XOFF ist es natürlich noch lange nicht möglich Nicht-ASCII-Files/ Maschinenprogramme zu übertragen. Leuchtet doch ein, oder? Denn erstens haben wir ja nur einen eingeschränkten Codebereich (\$20-\$7E) und außerdem: sobald ein CTRL-S auftaucht und gesendet wird, hängt die UT-. Um das zu übergehen, wurden noch verschiedene andere UT-protokolle entwickelt. Das läuft meistens so, daß normalerweise mit XON/XOFF gearbeitet wird und erst dann, wenn ein File übertragen oder gelesen werden soll, auf das jeweilige Protokoll umgestellt wird. Doch darüber mehr in der nächsten Folge.

Urteil der Experten:

Ode an den ST

Lasset uns zusammen die unbeschreiblichen Fähigkeiten des Atari 520ST rühmen:

Oh lieber Tramiel, wie können wir Dir dafür danken, daß wir alle 20 Minuten das System neu starten dürfen?

Du hast sicher auch daran gedacht, das ehemalige 64er User ohne 30 dB Lärm einer Floppy nicht leben können.

Und dieses einmalige Basic! Es war sicher Arbeit, über 300 unvollständig funktionierende Befehle zusammenstellen. So wurde für alle Zeiten gesorgt, daß das Programmieren nie langweilig wird. Ohne einen GET-Befehl lernt man ja dann ausserdem noch Maschinensprache. Vielen Dank dafür.

Die Hardware so unzugänglich zu konzipieren ist mit Sicherheit auch reif für das Guinnessbuch der Rekorde.

Oh ihr Ingenieure, wie kamt ihr auf die herrliche Idee, das man einen Dosenöffner braucht, um seinen Prozessor zu sehen?

Mit den Nadelimpulsen auf der Masseleitung habt ihr der Anlage ja dann den letzten Schluß gegeben.

Wie könntet Ihr ja auch zulassen, daß der Atari mit einem normalen handelsüblichen Modem für Mailboxen genutzt wird...

Das wäre ja gegen die Postgesetze! Da habt ihr mit eurer unbeschreiblichen Güte dafür gesorgt, daß jedes Modem an dem Rechner verrückt spielt.

Ach, das wolltet Ihr nicht?

Ok, das nächstmal nehmen wir Optokoppler um das Modem vor den Atari zu schützen und programmiere die RS232C neu!

Zum Schluß möchten wir der Firma Atari noch für Ihre einmaliges Stecker danken. So werden wir nie in Versuchung kommen, ein fremdes Gerät an den ST anzuschließen.

Ein gefrusteter Atari Besitzer

Manche Leute scheinen noch nicht geschickt zu haben was FREWARE ist. Freeware, das sind Programme, die beliebig kopiert, weitergegeben und getauscht werden können. Einzige Einschränkung: niemand darf sich daran eine goldene Nase verdienen. Und da erreichen uns doch glatt Briefe, in denen eine zweite oder dritte Disk, für Freunde oder Bekannte bestellt wird. Sollte es tatsächlich Computerbesitzer geben, die nicht einmal eine ungeschützte Diskette kopieren können??? Wir sind froh über jede Disk, die wir nicht kopieren müssen, und dann sowas.

Nichtsdestodennoch, das Freewareangebot wird immer weiter ausgebaut:

- C-64 Sammeldiskette (ca. 250kByte)
 - connection 64 (Terminal)
 - Term V1.7 (Terminal)
 - tsps (Phreak-Utility)
 - vidtex (Terminal)
 - megacon v4.0 (Hackprogramm)
 - proterm-64 g (Terminal)
 - norad (Mailbox)
 - nua-list (NUA-Liste, gelle)
 - first-term (Terminal)
 - first-dial (Nummernscanner)
 - micro-term (Terminal)
 - pro-microterm (Terminal)
 - data-hacker (Scanner)
 - sherlock (selber nachschauen)
 - proterm-64+ (neue Version)
- Apple II Sammeldiskette (ca. 280kByte)
 - Modem 7 in Source (Terminal)
 - Kermit (nur Apple II mit SSC)
 - Terminal-Prog in Turbo-Source
- Kaypro II Sammeldiskette
 - * Modem 7 in Source (Terminal)
 - Kaypromodem (Terminal)
 - Kaypro Yam (Terminal)
 - Squeeze (Dateien schrumpfen)
 - Unsqueeze (andersrum)
- Osborne Sammeldiskette
 - * Modem 7 in Source (Terminal)
 - Osborne Yam (Terminal)
 - Squeeze (Dateien schrumpfen)
 - Unsqueeze (andersrum)
- Sanyo (CP/M) Sammeldiskette
 - * Modem 7 in Source (Terminal)
 - Sanyo Yam (Terminal)
 - Squeeze (Dateien schrumpfen)
 - Unsqueeze (andersrum)

- IBM-PC Sammeldiskette I (ca. 320kByte)
 - PC-TERM (Terminal)
 - KERMIT-MS 2.26 (Terminal)
 - Q-Modem (Terminal)
 - Basic-Mailbox (ratet mal)
- IBM-PC Sammeldiskette II
 - ARC (wie Squeeze/Unsqueeze)
 - RBBS V1.3.1 (Mailbox)
- IBM-PC Sammeldisketten III + IV
 - FIDO (Mailbox)
- DEC RAINBOW Sammeldiskette
 - KERMIT-MS 2.26 (Terminal)
 - * PC-TERM (Terminal)



- WANG PC Sammeldiskette
 - KERMIT/MS 2.26 (Terminal)
 - * PC-TERM (Terminal)
- MS-DOS Sammeldiskette (ca. 700kByte)
 - * KERMIT-MS 2.26 (Source+Dok.)
- Apple DOS 3.3 - Sammeldiskette
 - Disktransferer (ganze DOS 3.3-Disk übertragen)
 - ACESS // Patch
 - Test Serial Card
 - DFÜ-Kosten mit Multiplan
- DEC VT180
 - KERMIT-80 (Terminal)
 - * MODEM 7 in Source
- ATARI 520
 - Megroid (Spiel)
 - Joshua (RAM- u. Diskmonitor)
 - ST-Writer (Editor)
 - Neochrome (Malprogramm)
 - S-Term (Terminal)
 - Hack (Terminal m. VT100)
 - KERMIT (Terminal)
- KERMIT-allgemeine Dokumentation
 - KERMIT Users Guide (436 kByte)
 - KERMIT Protocol (230 kByte)
 - KERMIT Byte-Artikel (95 kByte)
- * heißt, daß u.U. noch Anpassungen (Patches) für diesen Rechner erforderlich sind.

PRINZIPIELLES:

Wenn hier für 'nen bestimmten Rechner eine Sammeldiskette angeboten wird, dann sind alle oder die meisten Programme bereits auf diese Krücke angepasst und lauffähig. Für die sportlicheren Naturen können wir natürlich auch so fast alles auf anderen Formaten liefern, wie z.B. Modem 7 auf Osborne Executive oder so. Bei exotischeren Formaten bitte an die Redaktion wenden. Und nicht vergessen: Wenn die Installation erfolgreich war, seid so gut und schickt die neuen Patches zurück an uns, dann gibts eben auch für Euren Rechner eine Sammeldiskette und für Euch ein Freiabo.

KERMIT:

Bei KERMIT handelt es sich um ein Terminal- und Dateitransferprogramm. Kermit wurde von der Columbia University in New York entwickelt. Zum Transfer werden alle Dateien (auch 8-Bit) per Protokoll in DRUCKBARE ASCII-Zeichen umgewandelt, so daß auch die meiste Leitung, die nur 7 Bit und keine Steuerzeichen überträgt, kein Hindernis darstellt. Der o.g. KERMIT-MS (Source) beinhaltet bereits Anpassungen auf andere MS-DOS-Rechner (Wang, HP150 sowie DEC-Rainbow).

Mit KERMIT-80 in Source für CP/M-80 dauert's gerade noch etwas, da wir auf die neue Version 4 warten. MODEM7 unter CP/M wird in Source und fertig für Apple II / Softcard / Super Serial Card geliefert. Ebenfalls für'n Apple mit o.g. Ausstattung gibt es KERMIT-80 Vers#4 bereits.

YAM:

YAM ist sozusagen ein Konkurrenzprodukt zu MODEM7, es ist im Gegensatz zu ihm nicht in Assembler, sondern in C geschrieben. Man benötigt also, wenn man mit der Source arbeiten will, einen passenden Compiler, in diesem Fall den BDS-C-Compiler V1.50. Source kommt demnächst.

DOKUMENTATIONEN:

Bei den KERMITen gibt es in jedem Fall ein oder mehrere Help-Files dazu. Außerdem sind getrennte, sehr (umfang-)reiche Dokumentationen über KERMIT im Programm (s.o.). Zu MODEM7 gibt es ebenfalls einiges an Anleitung auf der Diskette. YAM ist auch dokumentiert. Bei den anderen Programmen muss man sich halt von Fall zu Fall selber durchwurschteln. Aber ein echter Hacker macht das ja mit links.

ATARI ST520:

Hack wurde uns von Andreas Schwerendt aus Düsseldorf zur Verfügung gestellt. Es bietet nicht nur ein Terminalprogramm, sondern vollwertige VT100-Emulation mit Funktionstastenbelegung, Up- und Download etc. Hier & da (in gewöhnlich schlecht informierten Kreisen) heißt es, daß der Kermit nicht laufen würde - weit gefehlt, man muß ihn nur über Command und nicht übers TOS aufrufen, da sonst der Rechner wieder mal abstürzt.

C-64

Die C-64 Disk ist auf beiden Seiten bespielt, also nicht meckern, sondern erst auf der Rückseite nachschauen. Kurzzeitig wurde auf der C-64 Disk die Mailboxliste des CAC mitgeliefert. Sie musste aber aus Platzgründen den neuen proترم 64+ weichen. Die in dieser Nummer abgedruckte Kurzanleitung für proترم 64 ist auch auf der Disk. Wenn das Freewareangebot wie bisher weiterwächst gibt es bald zwei verschiedene Disks.

DISKETTENFORMATE:

Im Prinzip können wir fast jedes 5 1/4" Format liefern. 3", 3.5" und 8" geht auch, dauert aber länger und kostet mehr (so ist das ja meistens im Leben).

Beim Bestellen müsst Ihr Euch halt ausrechnen, wieviel Disketten das Gewünschte ausmacht und entsprechend Knete beilegen.

PREISE:

Eine Diskette 5 1/4" kostet DM 10,- Exotenformate (3", 3.5", 8") das Doppelte.

Notizen - Meinungen

Kurzmeldung

Wie wir aus gut unterrichteten Kreisen erfahren haben, wurden an der Technischen Universität München einige Studenten mit mehrwöchiger Rechnersperre bestraft, weil sie auf der VM/370-Anlage ein Programm geschrieben hatten, das die VM/SP-Einschaltmeldung auf dem Terminal simuliert und nach Eingabe von ID und PW und deren Abspeicherung in einer Datei einen Systemfehler vortäuscht...



Wahr - unwahr

Wahr ist, in Halle 2 auf der CeBIT massenweise Aktenvernichter zu sehen sind.

Unwahr ist hingegen, daß für spezielle Gäste auch Modelle vorgeführt werden, die das Material vor der Vernichtung noch Mikroverfilmen.

Contrôlé par

Gekontrolleerd door

<--- SERIAL NUMBER

Die Bayrische Hackerpost erscheint in unregelmäßigen Abständen, solange die Welt nicht untergeht und uns nix Besseres einfällt.

Wer da dran auch teilhaben will, muß sich entweder einen Doofen suchen, der die B.H.P. abonniert hat und dort abkopieren, uns ein Austauschabo zukommen lassen, oder in Gottes Namen halt DM 50,-- (i.W. einen Fuffi) bzw. DM 20,-- (für Schüler, Studenten, ZDLer, Arbeitslose, Rentner, Kleinkinder und andere Mittellose) für 10 fortlaufende Nummern schicken.

Für Rechenzentren, Großfirmen und andere Massenverbraucher gibt es ab sofort auch ein preisreduziertes Großabo: 20 B.H.P.'s einer Ausgabe für NurNochDM 70,--. Wir bitten ehrlicherweise unter dem richtigen Namen zu bestellen. Es wird niemand diskriminiert, bei uns hat noch jeder sein Fett abbekommen.

Im Ausland gelten die Preise entsprechend. Bitte den Bestellwisch anfordern.

Adresse für Anregungen, Bestellungen, Spenden, Anfragen, Kritik, Hinweise, Infos und was Euch sonst noch einfällt, ist:

++++ B.H.P. c/o BASIS, Adalbertstr. 41b, D-8000 München 40 ++++

Introduction