Die Datenschleuder

Informationsdienst zu den Problemen von Datenschutz, Datensicherung und Ordnungsmäßigkeit der Datenverarbeitung

messen & prüfen

Vorweg: Schon vor der Hannover-Messe beantragten wir Formulare zur Versuchsteilnahme am TELEBOX-Dienst. Wenn die DBP uns sowas nicht schickt, müssen wir hacken, Herr Tietz!
Außerdem bitten wir das FTZ um schriftliche Bestätigung unseres Besuchs des ITT-Dialcomrechners in den USA. Amateurfunker erhalten beim Empfang entfernter Sender eine QSL-Karte als Bestätigung. Wir als Hacker brauchen beim Einstieg in fremde Rechner etwas entsprechendes.

Jetzt die Story Messen und Prüfen:
Daß Messen ausgezeichnete Veranstaltungen sind, auf denen mensch an Nummern und Passwörter kommt, ist nicht nur in Hackerkreisen bekannt. Die Deutsche Bundespost präsentierte auf der Hannover-Messe ihren neuen Telebox-Dienst. Da der deutsche Rechner (geplant sind nur 58 Ports) noch nicht voll einsatzbereit war, wurde das System in den Staaten bei ITT Dialcom (NUA 0311030100243 dann: ID DBP0xx) demonstriert. Das Passwort wurde schon fast verschenkt. DBP008, die ID (persönliche Kennung) von Herrn Christian Jonas wurde von mehreren Hackern ausgekundschaftet. Herr Jonas wollte uns und sich die Arbeit nicht zu schwer machen und verwendete seinen Nachnamen auch als Passwort.
Die Test-ID (DBP005) wurde auch noch geknackt. Ein sehr interessantes Informationssystem; Mailboxdienst mit postinternen Messages (ID's für die Telebox Mannheim - NUA 4562104000 ID POS001 bis POS040; Passwort meist vierstellig), Fluginformationssystem, ITT Mailbox sowie mehrere Presseagenturen waren dort vertreten. Ein guter Vorgeschmack auf den deutschen Teleboxdienst.
Als erstes wurden dann die Passwörter geändert. Die DBP ließ sich das Herumstöbern ganze vier Wochen lang gefallen. Dann wurde es ihr zu bunt und der Zugriff wurde gesperrt. Man wollte den Hackern wohl einen Gefallen tun und sie ein bißchen spielen lassen. Dafür herzlichen Dank. Aber was ein richtiger Hacker ist, der kommt immer wieder an den Tatort zurück. Und er kam. Mit >social engineering<. Da in dem Dialcom System ein genaues Verzeichnis aller Teilnehmer und ihrer Telefonnummern ist (schon alles auf Floppy!), konnte gezielt vorgegangen werden. Dazu erfanden wir einen Wartungsmenschen fürs SEL-System: Herrn Dau. SEL heißt Standard Elektrik Lorenz; die und Siemens schieben sich gegenseitig die Postaufträge zu.
Eines schönen Tages klingelte beim FTZ Darmstadt das Telefon. >Guten Tag, mein Name ist Dau von SEL, wir haben hier ein Problem mit dem Password Overlay<. Der freundliche Postler wurde darüber informiert, daß die halbe Passwortdatei, unter anderm auch das zu DBP003, >weg< sei. Auf die Frage, welches Passwort er denn nun gerne neu hätte, antwortetete er: >YYYY<. >Wird erledigt!< antwortete der Anrufer und schob eine kleine Frage nach: >Und wie lautete Ihr altes?< >STEFAN< kam es postwendend. Mit Mühe bewahrte der Anrufer die Fassung, bedankte und verabschiedete sich, um 5 Minuten ununterbrochen zu lachen. Anschließend gingen wir mit seinem alten Paßwort >Stefan< ins System und änderten es auf >YYYY<. Da >YYYY< nur ein vorübergehendes Passwort war, das ja immerhin dem >SEL-Techniker< bekannt war, änderte das FTZ das vier Tage später. Es ersetzte das neue durch das alte (Stefan, Sohn des Operators). Das war eine sehr intelligente Tat, somit stand uns das System für weitere Wochen zur Verfügung. Wir meinen, juristisch korrekt gehandelt zu haben. Falls nicht, bitten wir unseren Abonnenten Herrn Prof. Dr. Ulrich Sieber um Hilfe. he.
P.S.: Um weitere schöne Geschichten (die das Leben schrieb!) berichten zu können, bitten wir um eifriges Spenden auf unserer BTX-Spendenseite Berlin 19058, CEPT 20305080. Für Leser in Firmen mit BTX: Natürlich auf Firmenkosten. Danke.
(Nachdruck dieses Artikel nur mit diesem Nachsatz gestattet!)

Champagner für Hacker
Der STERN berichtete in der Ausgabe Nr. 21 vom 17. Mai über Hacker. Stellungnahme von Detmar Reinnecke (Leiter des Siemens Rechenzentrums Hamburg): >In der Bundesrepublik ist ein Computer jedoch kein Suppentopf, bei dem jeder den Deckel hochheben und sich etwas rausnehmen kann<. Herr Reinnecke verspricht jedem Hacker, der in sein Datenimperium eindringt, eine Kiste Champagner. Auf unsere Anfrage bezüglich dessen, was er unter seinem Datenimperium versteht, haben wir noch keine Antwort erhalten. Siemens Hamburg 040-282 22 76/86. 1200 Baud Halbduplex. Um anonym zu bleiben, nennt euch CHAOS/SIM und hinterlasst eine Kennung, die ihr uns auch mitteilt. Wir werden die Kisten dann abfordern und auf Wunsch an euch weiter leiten. he.

Mail-Boxen mit dem Grossen Bruder
Der grosse Bruder ist immer dabei!

Wir haben eine Regierung und die hört, liest und speichert mit.
Mailboxen werden vom grossen Bruder mitgelesen. Zwar können passwortgeschützte Meldungen nicht gelesen werden, es sei denn die Mailbox-Telefonleitung wird angezapft. Jeder kann jedoch (bei den einfachen Mailboxen) den Absender sowie den Empfänger auch geschützter Mitteilungen feststellen. So lässt sich jederzeit ein Umfeld von Personen erstellen. Abhilfe schafft nur ein Mailboxprogramm, das jedem User nur die für ihn bestimmten Meldungen anzeigt. RMI (NUA 44241040341) fährt als erste öffentliche Mailbox in der BRD ein solches Programm. So können Meldungen vor Dritten verborgen übermittelt werden. Trotzdem empfiehlt sich die Verwendung eines Pseudonyms. (nur sinnvoll, wenn von Anfang an und immer benutzt!!!)
Bei der TELEBOX gibt es kaum Sicherheit, da sie staatlich kontrolliert wird. Auch der elektronische Briefwechsel unterliegt den Postvorschriften. Ein Brief darf bislang nicht verschlüsselt werden und z. B. keinen staatsfeindlichen Inhalt, was immer das sein mag, aufweisen. Er darf zwecks Kontrolle von den Sicherheitsbehörden gelesen werden.
Bei TELEBOX wird es sicher mit dem kleinen Dienstweg durch einfache Passwortweitergabe von der Post zu BKA/VS klappen. Beim Telefon geht das erst dann mit Passwort, wenn alles digital läuft. Jetzt läuft eine unangemeldete/illegale Abhöraktion durch Verdrahtung am jeweiligen AK65 (Anschlußkasten). Damit an dem entsprechenden AK65 nicht gerade dann rumgebaut wird (und amtsniedere Postler die Drähte sehen), werden solange keine Arbeitsaufträge für den Kasten erteilt. Zurück zu den Mailboxen: Mailboxen privater Firmen sind sicherer als die Telebox, weil wir dort Einblick in die Programmentwicklung nehmen können. Datenschutzaspekte werden von uns einfach mit den Sys-Op's diskutiert und die Software entsprechend ergänzt. Bessere Mailboxen arbeiten im Moment die ersten Verschlüsselungsprogramme ein. Wir werden darüber berichten.
Kurz: Wer die beste Datensicherheit, ein komfortables Programm und immer ein offenes Port bietet, wird am Markt führen!
Die Datenschutzbeauftragten, die sich auch mit der TELEBOX beschäftigen müßten, erscheinen uns nicht sonderlich kompetent. Die DBP will unsere Beratung wohl nicht; ihr Problem. Wenn sie uns nicht ernst nimmt: Firmen werden genau darüber nachdenken, WEM sie wieweit trauen. Und dann hat die Post vielleicht mehr offene Ports als Anwender. he&max

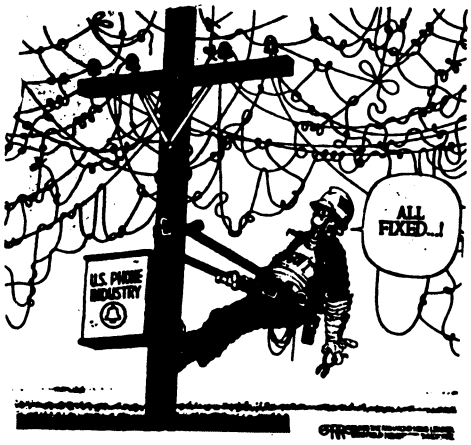
Chaos Computer Club * c/o Schwarzmarkt * Bundesstr. 9 * D-2000 Hamburg 13

Verbraucherschutz

Wir zitieren einen wichtigen kritischen Beitrag zu Bildschirmtext von Herr Prof. Dr. Ulrich Sieber aus Freiburg aus der TV-Sendung über Hacker und Knacker, BR3, 28.2.84:

>Im Bereich des Bildschirmtextes werden im Prinzip die gleichen Manipulationsmöglichkeiten gegeben sein, die wir heute im Bereich der Datenfernverarbeitung haben und die insbesondere durch die Hacker in Amerika bekannt gemacht wurden. Es wird also beispielsweise bei ungenügenden Sicherungsmaßnahmen möglich sein, daß ein Täter Dienstleistungen über BTX in Anspruch nimmt, aber für diese Dienstleistungen einen anderen bezahlen läßt. Der Unterschied zwischen den BTX-Manipulationen und den klassischen Computermanipulationen besteht im folgenden: Im Bereich der klassischen Computermanipulationen sind DIE Firmen von Manipulationen betroffen, die auch für die Sicherheit ihrer Systeme verantwortlich sind. Wenn eine Firma also beispielsweise das Geld für Sicherungsmaßnahmen sparen will, dann trägt sie auch das Risiko.
Das ist im Bereich des Bildschirmtextes entscheidend anders; hier wäre es möglich, daß der eine das Risiko trägt und der andere spart. Hier muß wieder ein Gleichgewicht hergestellt werden.
Ich würde mir wünschen, daß sich zum Beispiel die Verbraucherverbände und die Öffentlichkeit stärker für die Sicherungsvorkehrungen im Bildschirmtext interessieren.
Wenn die Systeme einmal mit einem bestimmten Sicherungsstandard eingeführt sind und wenn beispielsweise mit Allgemeinen Geschäftsbedingungen das Haftungsrisiko dem Endverbraucher aufgewälzt wird, dann wird es für Änderungen zu spät sein.<

Unser Kommentar: Wenn ihr fleißig mitmacht und wir erstmal ein paar Hunderttausend auf unserer Spendenseite haben, begreift das vielleicht die Post. Bitte spendet!



Impressum: die datenschleuder 3/84 ViSdP G. Schmidt, Eigendruck im Selbstverlag. Erscheinungstag: 12.6.1984.
Auslieferung in der Reihenfolge Abonnenten, Auszüge an die Presse, restliche Meute. Wegen Überlastung unserer Haussetzerei diesmal kein Fotosatz. e-mail: DATEX-P 44241040341 an CHAOS TEAM, Infodienst im Filemenu Dir 23.

Sicherheitsgrundlagen im Datex-P Verkehr.

Der aus dem Fernsprechnetz angewählte PAD registriert die NUI's, die gewählte NUA, die Zeit sowie die anfallenden Gebühren. Wer mit einer fremden NUI arbeitet, sollte es vermeiden, Mailboxen anzuwählen, durch die ersie identifiziert werden kann.
Eine geschädigte Firma kann anhand der Aufstellung der Verbindungen feststellen, ob zum Beispiel RMI angewählt wurde. Dort ist es möglich, über die Funktion >recent callers< die Benutzerin festzustellen. Auch wer sich mit einem falschen oder frei erfundenen Namen einträgt, kann anhand der Kommunikationspartner (bei RMI geaendert!) identifiziert werden. Für Mailboxen empfiehlt sich daher die Benutzung einer eigenen NUI.
Anders ist es bei Zugriffen auf Rechner, bei denen mensch kein autorisierter User ist. Bei einem begründeten Verdacht können die Verbindungen ebenfalls überprüft werden. Durch die gewählte NUA und die Gebühreneinheiten lässt sich ein nichtautorisierter Zugang feststellen.
Der NUI-Wechsel als solcher wird nicht registriert. Jedoch lässt sich durch den festgehaltenen zeitlichen Ablauf ein Wechsel erkennen. Zur Sicherheit sollte der PAD zum NUI-Wechsel neu angewählt werden!!! Die Bundespost darf die PAD-Protokolle zwar nicht weiterleiten, die Kontrollmöglichkeiten bestehen jedoch.

Was man in einer Mailbox so machen kann!

Nachrichten passwortgeschützt an einen oder mehrere schreiben, lesen und weiterleiten, archivieren oder drucken. Als Telex verschicken. Telex und Teletex (ohne t) erhalten. Datenbanken aus dem Menu aufrufen (Presseagenturen usw). Mit anderen Anwendern, die gleichzeitig Online sind einen Dialog führen. BTX und Prestelseiten lesen. Das ist das Angebot einer kommerziellen Mailbox. Voraussetzung ist eine NUI um am Datex Verkehr teilzunehmen, sowie ein gebührenpflichtiger (oder nicht) Eintrag in der Mailbox.
Aufruf an alle Profi-Hacker, die an ihren hochwertigen Taschenrechnern sitzen und vor Langeweile durch sämtliche Datennetze wandern. Wir brauchen NUI's, NUA's und Passwörter. Unterlagen zu Grossrechnern und alles was sonst noch interessant ist. Meldet Euch!
Kontakt zum Chaos Team über:
RMI 44241040341 an >Chaos Team<.
RMI ist sicher, wir kennen den Sysop schon länger (wichtig, weil jeder Sysop ALLES lesen kann!). Dort ist auch der elektronische Informationsdienst mit aktuellen Nachrichten im File Menu Directory 23. Für Datex braucht Ihr zwar ne NUI, Datex ist (inter)national aber billiger. Die normalen Telefonmailboxen bieten derzeit leider oft keinen Passwortschutz. Bleibt für einige nur der Postweg in gefütterten, verschlossenem Briefumschlägen; absolut heikle Sachen nur per Boten.

Datenschleuder Abo DM 23,- plus 23% Chaos Steuer. Der Betrag wird je nach Sozialschädlichkeit mit dem Faktor 1-99 multipliziert. Für SPIEGEL Leser gilt z.B. Faktor 3 = DM 84,87. Freiabo nur für besondere Verdienste (Passwörter,NUA's, NUI's). Zahlungsmodalitäten: Entweder elektronisch durch Einzahlung bei Bildschirmtext Berlin *19058# oder (wenn fertig) CEPT 20305080. Sonst durch V-Scheck, Scheine im gefütterten Umschlag oder Briefmarken. Wir bevorzugen entweder 5 oder 50 Pfennig. Einschreiben oder gar Wertsendungen erreichen uns nicht.

Parken und testen in Datex-P

Grundsatz: Laßt euch DATEX-P von der Post erklären. Dafür werden die bezahlt! Im Telefonladen oder - per Telefon vom zuständigen Datennetzkoordinator. Wer nicht im Nahbereich eines PADs wohnt, muß eben umziehen. So verschärft die Verkabelung die Zentralisierung.
Wer in Datex-P arbeitet, muß binnen 60 Sekunden eine Verbindung haben, sonst legt der Paketrechner (PAD) auf. Wartezeiten gibt es z.B. beim Austesten einer Mailbox. Da werden Programmänderungen gemacht und es dauert 'ne Weile, bis mensch sich wieder einloggen kann. Um die 23 Pfennig für einen neuen Anruf beim PAD zu sparen (nachts ist immerhin 12 Minutentakt), muß ein anderer Rechner herhalten. Dazu nimmt mensch eine R-Nummer (R-Datengespräch heißt: Gebühr zahlt Empfänger). Da das den Empfänger die erste Minute ca. 50 Pfennig, danach ca. x (für Inlandsrechner) kostet, sollten dafür entsprechende Rechner gewählt werden. Wir sind absolut stinkig auf Leute, die z.B. bei RMI parken und damit die Kiste zumachen; wer nicht kooperativ verhält, wird schon merken, was er davon hat. Am besten sucht ihr selber R-Nummern nach eurem Geschmack. Ansonsten parkt bei der Testnummer der Post. Die Rufnummern sind:
40 PADVORWAHL4STELLIG 00002,ECHO
Z.B. München: 408900 00002,ECHO.
Da ist zwar eine NUI erforderlich, aber es kostet nur (DATEX-)Zeitgebühren, keine Verbindungsgebühren. Wenn ihr das in MODEM7 auf die AUTOLOGON-Taste legt, habt ihr eine eigene Taste zum Parken. So geht die Datex-P Echofunktion: Jede eingegebene Zeile wird vom Rechner geechot (It's Denglisch: Ich echoe, du echost).
Um wieder rauszukommen, muß Control-P CLEAR eingegeben werden (CP/M-ler: es ist günstig, MODEM7 zu patchen, Print-Funktion auf Control-O, damit Control-P gesendet werden kann!).

Wer Datexnummern scannt, sollte das per Programm tun mit einem 50-Sekunden-Timeout (geht besonders gut mit Olis M10 bzw. Tandy 100 Basic-Befehl ON TIME$=X$ GOSUB >Park-Routine<). Demnächst folgt ein komplettes Programm.

Ein Hacker hinterläßt keine Spuren

Jeder, der einen Rechner nach langen Mühen aufgemacht hat, behält dieses Erlebnis selten für sich. Schon allein um tiefer in das System einzudringen, wird er seine Erkenntnisse anderen mitteilen. Vier Augen sehen bekanntlich mehr als zwei. Vereinzelt mussten wir jedoch feststellen, daß die Passwörter unbedacht weitergegeben werden. Das ist zwar nicht sehr schön, lässt sich aber kaum vermeiden.
Nur: warum müssen einige umbedingt ihre Spuren in Systemen hinterlassen? Das geht soweit, daß der Sys-Op (Systemoperator) den Zugriff sperrt. Und davon haben wir jedenfalls nichts. Ein Hacker hinterlässt keine Spuren; jedenfalls nicht solche, die sofort gefunden werden.
Es gibt gute Informationssysteme, die man immer mal wieder gebrauchen kann.
Also verhaltet Euch ruhig in Systemen, arbeitet sauber (korrektes Logoff) und weist nicht gleich alle mit der Nase auf Eure Anwesenheit hin. Chattet nicht unbekannte Teilnehmer in fremden Systemen an. Es könnte der Gilb sein.
Auch wenn ein Chat von DBP003 mit DBP003 spannend sein kann: Welcher der beiden ist der Hacker? Beide?

BTX heißt Bildschirm-TriX

Vorweg: Wer nichts über BTX weiß, soll sich sonstwo informieren. Im nächsten Telefonladen liegen genügend Prospekte rum. Wenn da ein BTX-Gerät steht: Vorführen lassen! Unsere gebührenpflichtige Seite (PRESTEL 99 Pfennige) kommt nach *19058# und wenn CEPT läuft, ist es ganz einfach: 20305080.
Für jeden Aufruf unserer Spendenseite kriegen wir echtes Geld!!! Bittet auch Postler um entsprechende sinnvolle Tätigkeit. Angesichts unserer riesigen Telefonrechnungen ist das nur gerecht.

1. Sys-Op's (System-Operateure) → gibts bei Post und BM
dem Rechnerlieferanten). Sie können - je nach Priorität - >alles<. Also Seiten einrichten, löschen, ändern, Anbietern zuteilen, wegnehmen, Passwörter einsehen, ändern, Verknüptungen herstellen, alle möglichen Statistiken und Abrechnungen erstellen (wer - wem - wann - was). Da erfolgt die Datenweitergabe an Verfassungsschutz usw. bei >Abhören< nach den entsprechenden Gesetzen (oder ohne sie). Zwar gibt es noch Streit zwischen Hinz und Bund, wer was wie Abhören darf, aber: Sie werden's schon regeln.

2. Gewöhnliche Teilnehmer können Informationsseiten abrufen oder Antwortseiten ausfüllen oder Bestellen oder an der Schließung ihrer Bankfiliale um die Ecke arbeiten oder anderen Mitteilungen zukommen lassen. Sie können kaum rumtrixen. Und sie dürfen zahlen, zahlen, zahlen.
Auch alle amtlichen Datenschützer sind so arme Schweine. Sie kriegen gerade eben aus Verbraucherseite mit, wie die BTX-Verarschung läuft. Wie wenn sie bei der Neuerrichtung eines Einkaufzentrums schon mal vorab mit dem Wägelchen da durch tappen können und die schönen bunten Warenkörbe anglotzen. Von Kundenlenkung, Impulskäufen, Werbepsychologie und Videoüberwachung zur Verhaltensanalyse (Griffhöhe usw.) ahnen sie gerade etwas. Wir wollen zwar keinesfalls diese unsere Datenschützer als Sys-Ops (das wäre schrecklich), aber als BTX-Teilnehmer sind sie lächerlich.

3. Informationsanbieter haben bei Mehrkosten - mehr Möglichkeiten. Sie können Informationsseiten erstellen/ändern und Gebühren kassieren. Beachtlich ist, daß die Programme zur Abrechnung nicht funktionieren. Auch sowas wissen nur die Anbieter, weil sie die Zahlungen mit der Post wie auf einem Informationsbasar aushandeln. In dem Zusammenhang ist systemtheoretisch interessant, daß ab einer bestimmten Systemgröße totale Kontrollstrukturen nicht mehr realisierbar sind, da sie komplexer als das Gesamtnetz werden. Sollte BTX schon jetzt mit den paar tausend Teilnehmern so komplex sein, daß eine genaue Abrechnung (wer hat wann welche gebührenpflichtige Seite von welchem Anbieter geholt?) unmöglich ist?!?
Dann gibt es noch eine Reihe von Trix. Anbieter können ihre Identität (Systemzeile) verschleiern und unbemerkt kassieren (Verknüpfung zu automatischer kostenpflichtiger Folgeseite, zurück zur Grundseite), bei geschicktem Vorgehen Teilnehmerdaten >unbemerkt< abrufen usw. Auch die >geschlossenen Benutzergruppen< sind interessant. Dort lagern >nicht öffentliche< Informationen von z.B. großen Firmen oder Interessengruppen.

4. Hacker
. . . kennen - warum auch immer - Sys-Op-, Teilnehmer- oder Anbieterkennung und tun so, als ob. Das BTX-Gesetz droht durchaus Strafen an. Soweit bekannt, wurde noch niemand bei Verwendung fremder Kennungen und Passwörter geschnappt, der in einer Telefonzelle stand und nicht länger als 5 Minuten wirkte. Wenn die Telefonzelle nicht gerade im Hauptpostamt steht, sondern im >Nahbereich<, dauert allein eine Fangschaltung mehrere Minuten. Und in Orten ohne elektronische Vermittlung genügt es in der Regel, die eigene Vorwahl zu wählen um im Fernnetz zu

landen. Dort wirken noch keine automatischen Fangschaltungen.

5. BTX im Ausland, u.a. in Schweiz und Österreich. Allerdings gibts dahin in der Regel keinen Acht-Minuten-Takt. Von Postlern wird berichtet, daß sie ihr Diensttelefon so manipuliert haben, daß, wenn abends dort angerufen wird, ein Mechanismus abhebt und die ankommende Leitung auf eine abgehende schaltet. Dann gibt es weltweit den Acht-Minuten-Takt (nachts 12 Minuten). Bauanleitungen bitte an uns einsenden. In GB: Datex-P 23411002002018 (Teletype, no grafik), 23411002002017 (USA Videotex), 23411002002000 (for international use, was immer das ist) Nummern für hier gibts bei der Post bzw. bei DECATES nachschauen.

6. Der Grafik-Standard
Prestel ist der einfache Standard, der in England benutzt wird. Er läßt sich auch auf einem einfachen VC64 (Atari?) darstellen; entsprechende Programme werden von englischen Hackern eifrig genutzt. Sie wuseln z.B. auch in Anbieterseiten rum, die nicht angekündigt sind, aber zugreifbar existieren, das Sperren und Entsperren von Seiten ist lästig. Und wer außer Hackern schaut schon nicht angekündigte Seiten an.
Der vielgepriesene CEPT-Standard ist - wie alle modernen Normen - geschichtet. Es gibt sieben Ebenen, die oberen sind aber noch nicht genau definiert. Die unteren sind's. Der LOEWE-Dekoder kann ein bißchen CEPT, der MUPID2 ein bißchen mehr (Level C2). Mehr als MUPID2 kann z.Z. kein Gerät am Markt.

7. Daten verschenken
Wer einen anderen liebt, schenkt ihm Daten. So können Leserbriefe geschrieben werden (per Programm), die entweder tausendmal oder mehr wiederholen >die heutige Bild-Zeitung war SO toll, ich kann das garnicht oft genug wiederholen, so toll war sie<. Oder den Text >Das ist ein Systemtest. Dein Briefkasten wird auf Überfüllungsfestigkeit getestet.< Oder einfach irgendwelche Zufallsdaten.

8. Rechnerverbund
Eine Reihe externer Rechner sind an BTX angeschlossen. Bei Kenntnis der entsprechenden Zugriffsprozedur lassen sich vielfältige Effekte erreichen. Die Methode des >shipping refrigerators to Alaska< ist da die simpelste.

9. Banken in BTX
Banküberweisungen sind wie folgt abgesichert:
Der Kontoinhaber identifiziert sich gegenüber der Bank durch Kontonummer und Geheimzahl (durch Wanze im Telefon zu erfahren). Von der Bank erhält er per Einschreiben eine Liste von TAN, Transaktionsnummern. Für jede Geldbewegung wird irgendeine dieser Nummern verbraucht und muß auf der Liste

durchgestrichen werden. Um das zu mißbrauchen, muß die Telefonleitung nicht nur angezapft, sondern >getürkt< werden, ein Kleinstcomputer wird - bei Datenverkehr - automatisch dazwischengeschaltet. Der gibt die Daten fast immer einfach weiter. Nur bei einer Buchung gibt er sie nicht zur Bank weiter, sondern speichert die TAN und meldet dem Teilnehmer >Buchung brav ausgeführt<. Mit dieser TAN kann anschließend das Konto geräumt werden.
Eine zweite Möglichkeit liegt im >Verbrennen< der Bankbuchung per BTX. Wenn irgendjemand versucht, in ein fremdes Konto reinzuhacken, also mehrfach eine falsche Geheimnummer eingab (Geburtsdaten und eigene Telefonnumern sind erst seit März 84 verboten, vorher klappte sowas oft), wurde das Konto für BTX-Buchungen gesperrt. Wenn der richtige Teilnehmer was überweisen will, erfährt er von dem Hack-Versuch und muß eine TAN opfern, um sich zu identifizieren und eine zweite, um zu überweisen. Der Dazwischen-Computer kann auch einfach so tun, als sei gehackt worden und einfach ne TAN abfragen. . .

10. Die Illusion der Beweisbarkeit
Die elektronische Anonymität (Die Daten sind sich alle gleich, lebendig und als Leich'; Grüße an Wolf B!) macht es sehr schwer, festzustellen, wer wirklich was bestellt/gebucht/veranlasst hat. Bekannt ist das von amtlich Anonymen. Journalisten, die auf ner Demo einen knüppelnden Bullen nach seiner Dienstnummer fragten, kennen das Spielchen: 110. Oder 0815. Sowas findet sich auch bei geklauten Programmen. Die Seriennummer soll die Herkunft (den registrierten Käufer) beweisen. Da steht aber 4711/007. Trotzdem glauben viele an Merkwürdigkeiten wie >Solange die Daten noch in meinem MUPID-Speicher sind, hat das Beweiskraft. Ausdrucken genügt nicht<. Es mag ja Juristen geben, die sich sowas einreden lassen, sachlich ist es Unsinn. Genauso wie sich Beliebigkeiten drucken lassen, können Speicher gefüllt werden. Electronic graffiti.

12. Sicherheit und Lottoglück
Die Post argumentiert, ihre Systeme seien so sicher (d.h. Hackers Besuch so unwahrscheinlich) wie 6 aus 49. Das ist richtig. Jede Woche mindestens ein Hauptgewinn. Wir haben zwar noch nie im Lotto einen bekommen. Aber erstens freuen wir uns auch schon bei kleineren Gewinnen und zweitens lassen sich Passwörter - im Gegensatz zu Geldgewinnen - durch Weitergabe verdoppeln!!! Und überhaupt: siehe unseren Artikel über Telebox.

Weitere Informationen vorhanden,
aber noch absolut unreif für Veröffentlichungen. Wir können aber noch jede Menge Informationen gebrauchen. Insbesondere zur bundesweiten Einführungsphase von BTX suchen wir noch eine Menge Menschen (auch und vor allem Nicht-Computer-Besitzer!), die bereit sind, das System dann auszutesten. Dazu brauchen wir noch viele, viele Passwörter. Überbringt sie uns bitte direkt, AUF GAR KEINEN FALL PER POST! Wie ihr das macht, müßt ihr euch selbst überlegen. Auch sowas gehört zum Hacken.

Weltpostkongreß in Hamburg
Im Juni findet im hamburger Kongreßzentrum der Weltpostkongreß statt. Es werden Vertreter aus aller Welt erwartet. Wir werden dort unser Anliegen, das **Menschenrecht auf weltweiten freien und ungehinderten Informationsaustausch** vertreten! Wir erwarten viele Freunde und wollen u. a. mit Betreibern der verschiedensten Bulletinboards über Mailboxen und Standardisierung reden und >sonstige< Erfahrungen austauschen. Wir planen, zum Weltjahr der Jugend 1985 per Mailboxen mit Jugendprojekten in aller Welt in Verbindung zu stehen! So als klitzekleine Überlegung: Die industrialisierte Welt hat einen riesigen Informationsvorsprung vor den >Entwicklungsländern<! Das führt in der Zukunft noch zu harten Auseinandersetzungen; Ökonomisches Stichwort: wer kann per Satellit die besseren Erntevoraussagen machen? Wer Lust hat, sich an der damit zusammenhängenden Arbeit zu beteiligen, soll sich umgehend bei uns melden. Wer Unterkunft in Hamburg sucht, hat vielleicht beim C.C.C. Chancen; Anmeldung entweder in einer Mailbox oder mit gelber Post. wau.

Das NUA-Telefonbuch
Angeblich will die DBP ein NUA-Telefonbuch verbreiten. Es wird unvollständig sein, da nur die Firmen eingetragen werden, die das auch wollen. Wir wollen auch eins verbreiten. Und zwar viel besser und komfortabler als die Post. Unser NUA-Verzeichnis wird als FREEWARE entweder auf Papier, auf Floppies oder als File in irgendwelchen Mailboxen existieren.
Die Master-Daten werden unter dbase2 (notfalls DataStar) aufbewahrt. Eine genaue Formatbeschreibung wird noch erstellt. Sie enthält (jetziger Stand):
NUA - Portzahl - Firmenname/Anschrift - Rechnertyp - ID, Passwort - Kommentar
Das Ding wird mit jeder Ergänzung durch euch besser. Und wenn es als FREEWARE (Zahlungen an uns werden dankbar entgegengenommen, sind aber freiwillig!) verbreitet wird, ist es vollständiger als irgendeine kommerzielle Liste. Denn unser Projekt lebt von der freiwilligen Mitarbeit der vielen und jeder Mitarbeiter hat als Lohn die aktuellste Version zur Verfügung!
wat.

Rechnerspezifische Modemprobleme wollen wir mit Ergänzungsblättern, für jeden Rechner eins, zum Modembauplan lösen. Wer schon online ist: Bitte technische Info an uns!

Fallt nicht auf Billiganzeigen von Modems rein! Mit Bell 103 ist nicht viel zu machen (Tandy-Modem ok). Sonst baut unsers nach. Teile ca. 300 DM, Bauplan 10 DM

Der CCC hat im BTX eine Spendenseite *19058# (Berlin) eingerichtet. Im Kaufhaus oder so mal ausprobieren.

Wer mit Chaos-Sympathi¢santen in seiner Umgebung Kontakt aufnehmen möchte, sende ein Schreiben in mehrfacher Ausfertigung an uns. Wir versenden die Kontaktwünsche mit der Datenschleuder an unsere Abonnenten. Pro Ausfertigung benötigen wir den Portomehraufwand von 30 Pfg.. Wir geben keine Adressen weiter. (Manchmal dauert aber unsere Weiterleitung!)

Es gibt viele Methoden, sich die eigene Hardware zu finanzieren. Von einem Boy hörten wir, daß er sich gerade sein 2. Laufwerk auf dem Strich verdient. Eine Frau aus dem Ruhrpott machte das mit Blutspenden; eine Körperfüllung reicht etwa für ein Laufwerk. Und ein dritter hat aus seiner Briefmarkensammlung (Hobbywechsel...) die >postfrischen< an uns verkauft. Deshalb frankieren wir diesmal vorwiegend mit Sondermarken. Eigentlich sollte die Drucksache uns 47,5 statt 50 Pfennig kosten, aber mit den 5% Rabatt hat der Schüler seine Bahnfahrt zum C.C.C. nach Hamburg finanziert.

Ein Computerclub schrieb uns: >Wir unterteilen zwei Gruppen. Zum einen gibt es den Mob. Dem verkaufen wir die Programme und versaufen das Geld. Dann gibt es die User. Denen schenken wir die Programm. Ach ja, und dann gibt es noch die Tiere. Das sind die Menschen ohne Computer.<

Der Chaos-Knoten als Aufkleber für DM 10,- ist noch verfügbar. Alle Abonennten erhalten mit dieser Ausgabe einen gratis. Eine Klein& Billigausführung (so wie die Radfahrkleber PARKE NICHT AUF UNSEREN WEGEN) ist in Vorbereitung

Die Hamburger Sparkasse hat neue Magnetkärtchen eingeführt. In einigen Filialen läßt sich damit der Kontostand ermitteln. Ohne Passwort!!!

In einigen Hamburger Computerläden gab es Razzien, Suche nach fernöstlichen Äpfeln und deren EPROMS.

Der Modembauplan ist für DM 10,- zu beziehen. Die Schaltung wird mit dem Baustein AMD 7910 aufgebaut. Alle schon bezahlten Baupläne liegen dieser Ausgabe bei.

Die Telefonrechnung des CHAOS-TEAMs beläuft sich z.Z. auf rund 800 DM im Monat. Die Hälfte davon sind DATEX (ca. 10 DM bzw. 5 Stunden pro Tag), die andere Hälfte meist Voice, ein klein wenig direkte Boxen. In den Spitzenzeiten sind alle drei Anschlüsse belegt. Auf dem einen wird in DECATES was nachgeschaut, auf dem zweiten mit anderen Hackern debattiert und auf dem dritten bereits am Problem gearbeitet. Einen vierten Anschluß, um noch anrufbar zu sein, hat die Post wegen Leitungsmangel verweigert.

Lang dauern auch Telefonate mit Hackern, wenn die nicht da sind. Frauen, die es mit Hackern aushalten, sind in der Regel sehr interessant...

Nach dem Versand dieser Datenschleuder werden alle Adressen von Nichtabonnenten gelöscht. Neuabonnenten bitten wir anzugeben welche Ausgaben sie schon erhalten haben.

TEDAS: 089-59 64 22, DECATES: 06154-514 33, (nur abens: MCS 040-65 23486). Weitere suchen!

Weitere Kurzmeldungen, die nur für Modembesitzer interessant sind, findet ihr bei RMI! Platzmangel!

Chaos Computer Club * c/o Schwarzmarkt * Bundesstr. 9 * D-2000 Hamburg 13