

Hacker

Mittwoch/Donnerstag, 21./22. November 1984

Hamburger Computerclub entdeckte Fehler im Bildschirmtext-System Geheimes Kennwort eingefangen

Über Nacht 135000 Mark von einer Sparkasse aufs eigene Konto „überwiesen“
Die Post in der Hansestadt: „Äußerst peinlicher Vorgang“ — Klage der Bank?

HAMBURG — Einem Hamburger Computerclub ist der Nachweis gelungen, daß das Bildschirmtext-System elektronischen Bankbetrug ermöglicht. Die Nachricht löste bei der Bundespost und ihren Kunden erhebliche Aufregung aus.

Durch Zufall hatte der „Chaos Computer Club“ das im Btx-System „umherirrende“, eigentlich als „Geheim“ deklarierte Kennwort und die Anrufnummer der Hamburger Sparkasse (Hspa) eingefangen. Mit diesen Informationen konnte sich der Verein gegenüber der Post als „Mitglied“ ausweisen und durch den Anruf von gebührenpflichtigen Bildschirmtext-Seiten jeweils 997 Mark auf das eigene Btx-Konto überweisen. Durch ständige Wiederholung des Aufrufs sammelten sich mit diesem Trick über Nacht 135 000 Mark auf Kosten der Sparkasse an. Die Mitglieder des Vereins wollten mit ihrem Experiment, wie sie sagten, auf „schwere Fehlerquellen“ im Btx-Netz aufmerksam machen.

Während ein Sprecher der Hamburger Oberpostdirektion den Vorgang „äußerst peinlich“ nannte und den „nachgewiesenen Fehler“ im Programm eingestand, beteuerte das Bundespostministerium, die „unmittelbare Schädigung eines Btx-Kunden sei grundsätzlich ausgeschlossen“. Der Hamburger Programmierer habe sich nur auf Funktionen „innerhalb der Btx-Vermittlung“ auswirken können, da diese durch die Kontoführung von Banken, nicht jedoch durch die Identifizierungsnummern abgesichert sei. Das Ministerium betonte, daß die über Btx-System entstandenen Kosten nachträglich zu ihrem Urheber zurückverfolgt werden könnten.

Inzwischen wurde der Computerfehler bei der Hamburger Oberpostdirektion behoben. Wie ein Sprecher der Behörde betonte, sei in Zukunft das unverlangte Auftauchen eines Kennwortes nicht mehr möglich.

„Das System schreitet zielgerichtet ins Chaos“

Als Einbrecher im Datennetz werden die Hacker in den USA längst gefürchtet. Hierzulande sind die digitalen Freibeuter noch dünn gesät. Die Lacher allerdings haben sie schon jetzt auf ihrer Seite

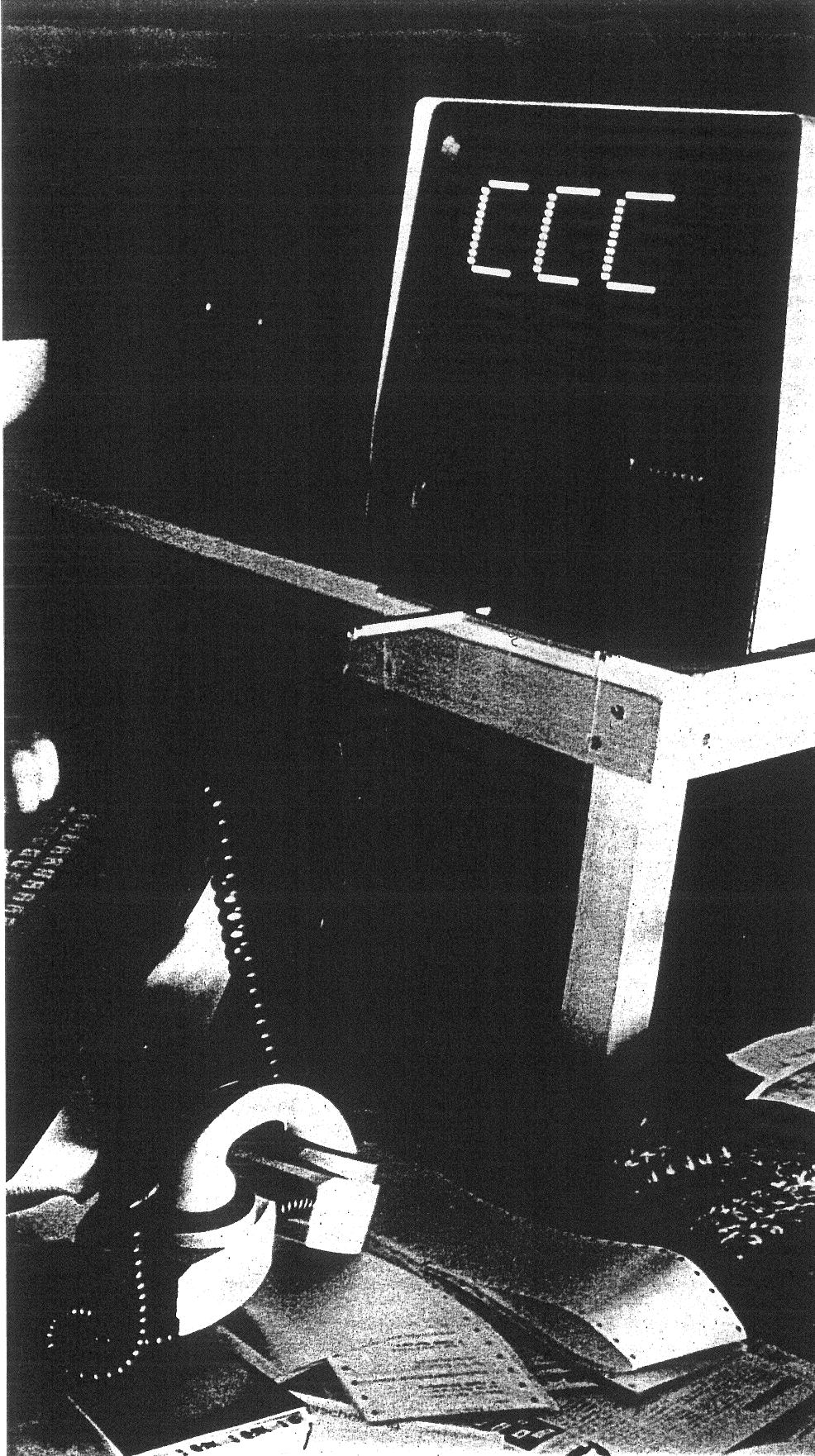
Von Jochen Siemens

Es war wohl eines der ersten sonnigen Wochenenden des Jahres: Peter Michel*, Sachbearbeiter im Fernmeldezentrum der Bundespost in Darmstadt, hatte es jedenfalls eilig an diesem Freitag. Eine halbe Stunde vor Feierabend räumte der Postler gerade seinen Schreibtisch auf, als doch noch das Telefon klingelte. „Guten Tag, Herr Michel, mein Name ist Dau von SEL. Wir haben ein Problem, soeben ist uns hier das gesamte Passwort-Overlay

abgestürzt, die Hälfte der Kartei ist weg“, klagte der Anrufer. Michel stöhnte mitfühlend. Als Datenspezialist wußte er, was es heißt, ein Overlay (ein Speicher) wieder zusammenzuflicken. Der arme Herr Dau werde wohl die ganze Nacht daran zu werkeln haben. Doch der Anrufer machte einen verständlichen Vorschlag: „Sagen sie mir doch schnell ein neues Passwort, ich bau das dann erst einmal ein“, drängte der Mann von der Technik. Michel wurde mißtrauisch, man las ja soviel über Datenmißbrauch. „Welche Pri-

orität haben sie denn?“ wollte Michel wissen. Die Priorität ist ein postinterner Dienstgrad, der die Zugangsberechtigung zum Computer ausdrückt. „Sieben“, behauptete der Anrufer. Michel war beruhigt, er hatte ja nur „fünf“. Dau kam demnach von oben. „Machen sie doch vier Y“, drängelte nun Michel; das Passwort war einfach und sollte ja nur ein Übergang sein. „Danke, machen wir. Ach, sagen Sie mir noch schnell ihr altes?“ fragte der Anrufer. Michel war fast an der Tür: „Stefan“, murmelte er und legte auf.

*Name von der Redaktion geändert



Dieses Telefongespräch wurde im Mai geführt und löste tosendes Gelächter aus. „Ich habe mich erst mal vor Freude gewunden und konnte die Tastatur vor Lachen nicht bedienen“, erzählt Henning Dau heute. Der Hamburger ist natürlich kein gestreifter SEL-Techniker und rief auch nicht von einem Arbeitsplatz in Darmstadt an. Henning Dau gehört zu der kleinen Gruppe Hamburger Computerpiraten, den Hackern. Hacker sind Computerfreunde, die sich mit Leidenschaft an großen Datennetzen bedienen

und mit technologischer Respektlosigkeit große Rechner aufs Kreuz legen. In den USA sind Hacker längst gefürchtete Einbrecher im Datennetz, die auch vor Kontorräumungen und Datenvernichtung nicht Halt machen. Gegen Hacker gibt es so gut wie keine Sicherung. Mit unendlicher Geduld und Phantasie fragen sie Großcomputer so lange mit möglichen Passwörtern ab, bis die Rechner den Weg freigeben. In der Bundesrepublik sind die digitalen Freibeuter eher dünn gesät. Post und Banken streiten obendrein hef-

tig ab, daß Hacker in ihrem System eine Chance hätten. Dennoch: Schätzungen beziffern den bisherigen Verlust illegaler Computermanipulation schon auf einige Millionen. Zum erstenmal haben Hamburger Hacker nun vorgeführt, was die Post für unmöglich hält, den Einbruch in einen von der Bundespost bewachten Computer. Die Geschichte dieses Dateneinbruchs zeigt, daß erst die Bundespost die entscheidenden Tips gab.

Die logistische Vorbereitung der Tat begann im April in Halle 3 der Hannover-Messe. „Da waren wir natürlich auf die Neuigkeiten der Bundespost gespannt“, erzählt Henning Dau. Die ließ sich nicht lumpen und stellte einen Computerterminal vor, der das neue Mail-Box-System der Post demonstrieren sollte. Unter dem Namen „Tele-Box“ wollen die Briefträger ihr angeschlagenes Image bei Industrie und Management wieder aufpolieren. „Tele-Box“ ist nichts weiter als ein Postfach in Gestalt eines Computers. Über den hauseigenen Terminal kann eine Firma dort beispielsweise Aufträge und Baupläne ablegen, die dann von anderen Teilnehmern, vorausgesetzt sie besitzen das richtige Passwort, abgerufen werden können.

Wo anders als auf der größten Managerversammlung Europas, der Hannover-Messe, konnte die Post besser für ihren digitalen Briefkasten werben? Nur, die Briefträger vom Staat hatten wieder einmal verschlafen. „Tele-Box“ konnte in Hannover noch nicht vorgeführt werden – der Rechner war noch im Bau. Deshalb behielten sich die Briefträger mit einem ähnlichen System, dem „ITT Dialcom“, einem analogen Rechner, der bloß in den USA steht. „Da wurden wir neugierig“, erinnern sich die Hacker. Hacker Dau ließ sich von den Datenpostlern alles erklären, technikbegeisterte Jugend sah man ja gern am Stand. Dau achtete allerdings nur auf die vielen Ziffern, die in den Computer eingegeben wurden. Als ihm der Postberater Christoph Jonas dann erklärte, „Und nun fehlt noch ein Passwort. Nehmen wir doch einfach meinen Nachnamen“, und daraufhin der Computer zu Diensten stand, war Dau fassungslos. Ihm war allerdings klar, daß nach der Messe nichts mehr ging. Die großen Firmen tauschen nach Messen ihre Passwörter vollständig aus. Die großen Firmen schon – aber die Post?

Zurück in Hamburg, fütterte Hacker Dau seinen Apple-Computer sofort mit den Messeerlebnissen. Noch am selben Abend staunte er nicht schlecht: Mit dem Passwort Jonas war Dau in die Hallen des Mail-Box-Computers in den USA eingestiegen. „Da gab es viel zu gucken“, berichtet Dau. Flugpläne vieler Flughäfen, die Angebote aller Nachrichtenagenturen, Hausverkaufsangebote, Stellenangebote und allerlei Daten, die der Hacker zunächst nicht identifizieren konnte. Dennoch sah Dau sofort, daß ihm der Bildschirm auch eine Reihe von neuen Zugangsnummern lieferte. „Unfaßbar, die Post änderte die Passwörter nicht, eigentlich unverantwortlich.“ Freilich erzählte der Computer keine Staatsgeheimnisse, doch alles war wohl nicht für Hackeraugen bestimmt. Und: Der Hamburger Hacker kapierte, wie sich die Bundespost den späteren Schutz ihrer Telebox vorstellte. „Die Adresse, die man eingeben muß heißt DBP008 und so weiter. Das Pass-

wort ist meist vier- bis sechstellig. Eigentlich ganz einfach“, freute sich der Hacker. Das mußte es auch sein, denn nach vier Wochen änderten die Postler alle Passwörter.

„Da war ich persönlich beleidigt“, erinnert sich Hacker Dau. Mittlerweile war sein nächtlicher Gang in den Rechner schon zur Gewohnheit geworden. „Da wollte ich wieder rein.“ Aber wie? Dau, der sich die schönsten Daten schon kopiert hatte, sah seine Beute durch. Unter anderem hatte er mal die komplette Teilnehmerliste der Benutzer des Computers gespeichert, inklusive Telefonnummern. Dau rief Peter Michel, einen der Benutzer an. „SEL installiert für die Postler die Anlagen, das zog. Als er mich allerdings nach der Priorität fragte, kam ich ins Schwitzen.“ Hacker Dau pokerte. Er wußte, daß die meisten Firmen die Prioritäten von eins bis zwölf haben. „Mal von unten, oder von oben. Sieben war etwa in der Mitte.“ Sieben traf, Datenverarbeiter Michel hatte nur fünf. Nach dem Telefongespräch war der Hamburger Hacker wieder am Computer. „Wochenlang“ spionierte Dau alles aus, was Post und Firmen dort ablegten. Eines Nachts spürte er sogar einen Hackerkollegen aus Berlin im System auf. „Dem hab ich Angst gemacht, der dachte, ich wäre der Postler, und verzog sich schleunigst“ – Hacker im selben Revier. Nachdem also der Hamburger Pirat brav Michels Kennwort von „Stefan“ in „YYYY“ geändert hatte, wechselte Michel es nach einer Woche wieder aus – in das alte „Stefan“, so heißt sein Sohn. „Die meisten verwenden als Passwort den Namen von Frau, Sohn oder Tochter“, weiß Dau aus Erfahrung. „Die Erfahrung wird in den Chefetagen der Post geteilt. „Wir wissen natürlich, daß es sich die Benutzer mit den Passwörtern einfach machen“, erzählt

ein Bearbeiter im Fernmeldetechnischen Zentrum Darmstadt. Doch Referatsleiter Walter Tietz findet die ganze Aktion „hart an der Grenze zum Illegalen“. Das sei „Einbruch“ und „Diebstahl fremden Eigentums“, meint der Postler. Doch er wiegelt ab. „Die Telefonbox gibt es doch noch gar nicht. Deshalb kann von einem Einbruch nicht die Rede sein“, versichert Tietz. Dennoch, auch die Bundespost erschrak, als sie sah, daß es Computere-freaks so einfach gemacht wurde, in die geschützten Systeme einzudringen. Auch wenn es nur ein Probetrieb war, „haben wir der Post einen Gratis-Test geliefert“, glauben die Hacker. Postmann Tietz findet das allerdings „unseriös“. „Das ist böswillige Täuschung gewesen und Einbruch“, so Tietz.

Wohl nicht ganz. Hacker Dau hat keine der Daten gelöscht oder an andere weitergegeben, „nur kopiert“, wie er sagt. Und den Tatbestand der Datenkopie gibt es im Strafgesetzbuch noch nicht. Postler Tietz bedauert das, weiß aber, daß es schwierig ist, einen Hacker auf frischer Tat zu ertappen. Computerhacker hinterlassen keine Spuren und sind nicht festzuhalten. Falls Hacker Dau im System erwisch worden wäre, hätte er sich seelenruhig ausgeklinkt, „in Sekunden“. Der Post ist es unmöglich, Eindringlinge zu verfolgen. Deshalb fürchten die Briefträger auch jede Publikation derartiger Pira-terien. Denn wenn ruchbar wird, daß es ein Kinderspiel sein kann einzusteigen, dann würden Großindustrie und Management wieder auf Telefon und Fernkopierer setzen. „Die ganze Geschichte wäre umsonst, uns traut doch keiner mehr“, fürchten Postler in Hamburg.

Die Hamburger Hacker freuen sich noch über die niedrigen Gebührenrechnungen für ihre nächtlichen Ausflüge. Denn bezahlt wird nur bis zum „Da-

tenzubringer“, dem Datenschalter der Post in der Schlüterstraße in Hamburg. Das kostet den Hacker, der über Telefon kommt, ein Datengespräch von 35 Pfennig pro 12-Minuten-Takt. Den Rest, den langen Weg über den Satelliten in die USA und zurück nach Darmstadt, muß der Nutzer berap-pen. Bei den Hackern ist das immer der Besitzer des Passwortes – die Post.

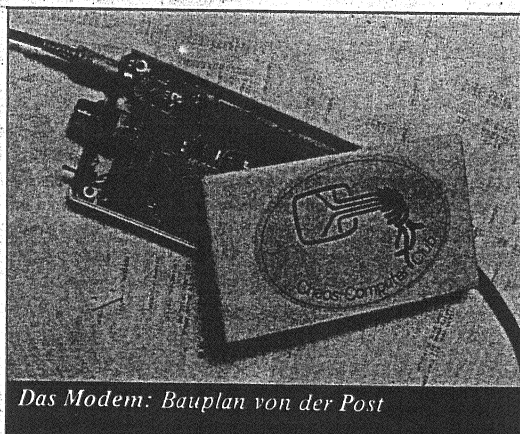
Trotzdem tüfteln Dau und Kollegen auch an technischen Spielereien herum, die die Leitungen zum Nulltarif freigeben. „Selbstverständlich nur, um die Post zu warnen“, versichern die Bastler. In Hamburg haben sie einen Club gegründet, den „Chaos Computer Club“. In dieser illustren Runde wird viel gefachsimpelt und ausgetauscht. Das neueste Werk der Computerchaoten ist ein Bauplan für einen Akustik-Koppler zum Selbermachen. Bisher mußten diese Geräte, die den Telefonhörer mit dem Rechner verbinden, gekauft und bei der Post angemeldet werden. Der Eigenbau „könnte den Behörden Arbeit und den Benutzern Kosten ersparen“, meint dazu ein Hacker. Material für ihren Koppler fanden die Bastler denn auch dort, wo es keiner vermutet: im Heimwerkermarkt. So besteht der Koppler neben der Elektronik noch aus zwei normalen kleinen Radiolautsprechern, die in Gummidichtungen für WC-Rohre verpackt werden. „Da paßt der Hörer genau rein“, haben die Hacker erfreut festgestellt. So ausgerüstet, wird der Koppler an einen tragbaren Kleincomputer angeschlossen, der dem Hacker das Hobby aus jeder Telefonzelle erlaubt.

Noch sind sie wenige, doch der Zuspruch aus allen Winkeln der Bundesrepublik wird täglich größer. Dafür sorgt unter anderem das Zentralorgan der Hamburger Hacker, die „Datenschleuder“. Das vier-seitige, chaotisch zusammengeschriebene Blättchen wird bei Post, Polizei und Banken ebenfalls mit Interesse gelesen. „Wir haben dort schon manche Anregung gefunden“, gesteht Walter Tietz aus Darmstadt.

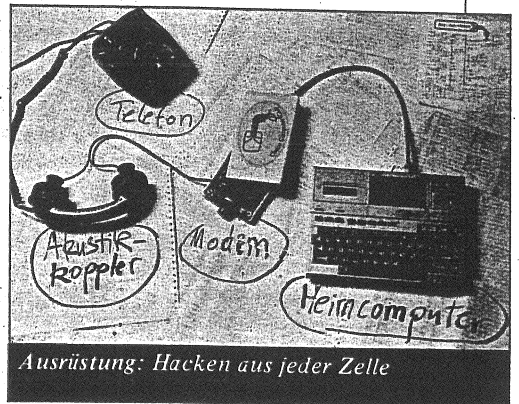
Andere auch. Zwischenzeitlich wurde der noch im Aufbau befindliche Rechner



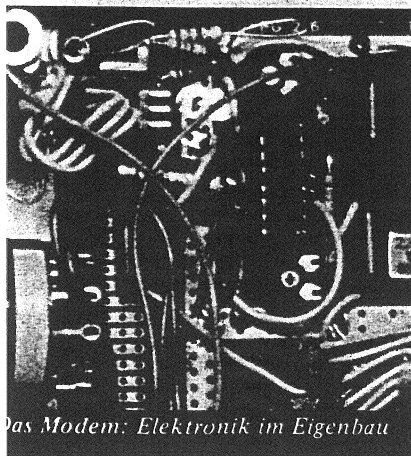
Der Koppler: Selbstgemacht



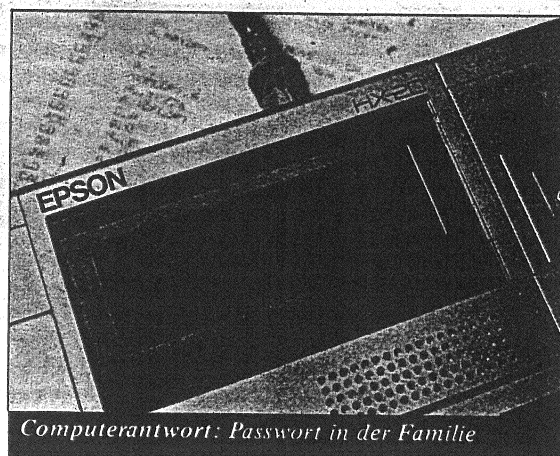
Das Modem: Bauplan von der Post



Ausrüstung: Hacken aus jeder Zelle



Das Modem: Elektronik im Eigenbau



Computerantwort: Passwort in der Familie

„Telebox“ von ungeduldigen Hackern schon so ausdauernd mit Passwörtern befragt, daß „Telebox“ nicht mehr wollte und seinen Geist aufgab.

Aus der „Baustelle Telebox“, so Tietz, wurde im Nu eine Ruine, die Post verzweifelte.

Hamburgs Hacker fühlen sich nicht allein. Henning Dau staunte heftig, als er eines Nachts im Postcomputer die Mitteilung fand: „Das System schreitet zielgerichtet ins Chaos.“ Der Autor dieser Zeilen war ein Postbeamter.