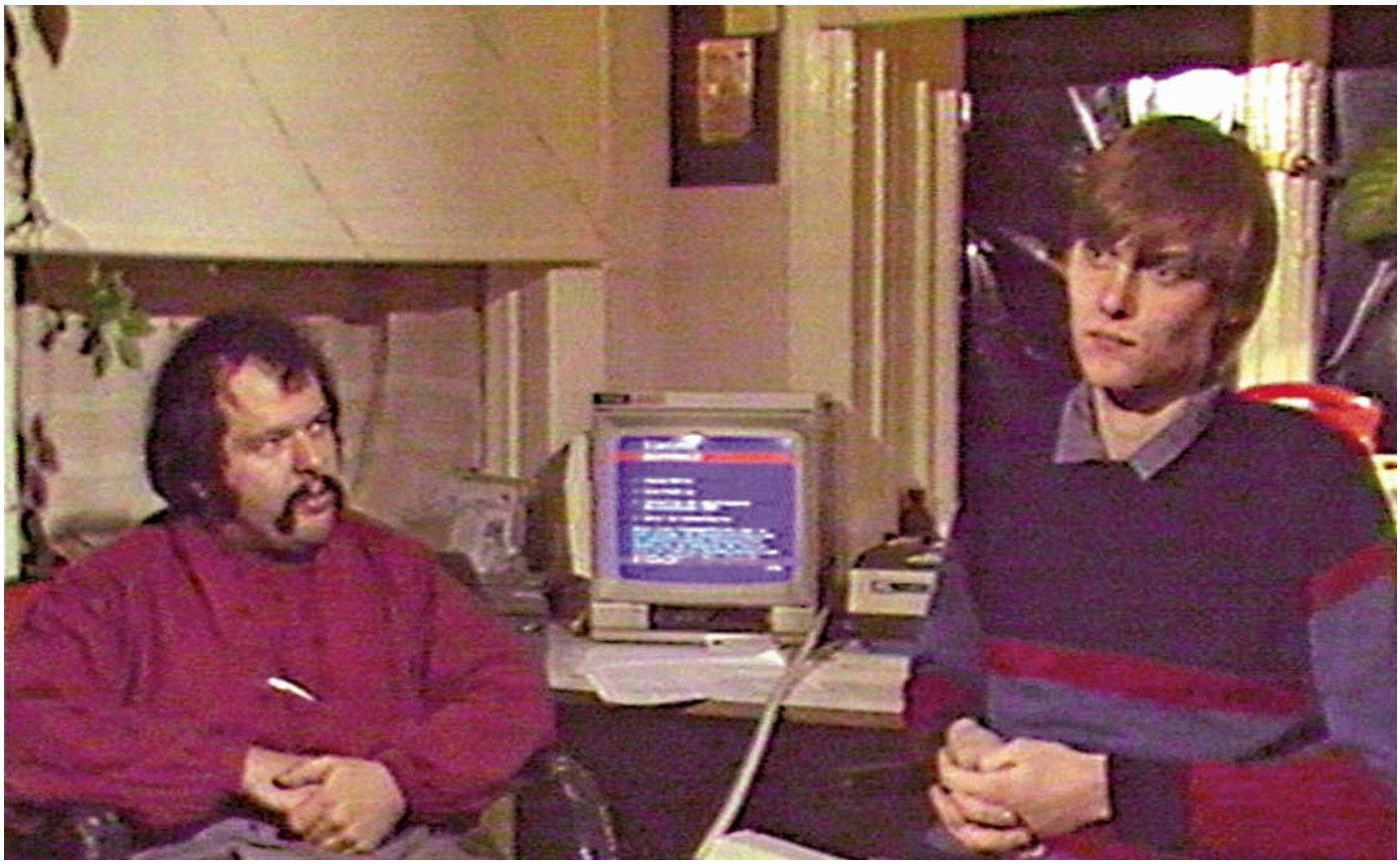

Bankraub per Telefon

Wie der Chaos Computer Club das Btx-System aushebelte

In der Nacht vom 16. auf den 17. November 1984 sorgte ein 31 Zeilen langes BASIC-Programm dafür, dass eine kostenpflichtige Informationsseite im deutschen Bildschirmtext-System (Btx) wieder und wieder aufgerufen wurde, bis beachtliche 135.000 D-Mark Gebühren zusammenkamen. Die Aktion wurde als Btx-Bankraub bekannt und machte den damals jungen Chaos Computer Club auf einen Schlag berühmt.

Von Detlef Borchers

Ausgelöst wurde der Hack von den CCC-Mitgliedern Wau Holland (links) und Steffen Wernéry (rechts) bei einem nächtlichen Beutezug im Btx-System. Sie wählten sich mit der Kennung und dem Passwort der Hamburger Sparkasse in Btx ein und ließen 14 Stunden lang die eigens von ihnen entwickelte kostenpflichtige Informationsseite des CCCs mit einem idiotisch klingenden Text anwählen: „Es erfordert ein bemerkenswertes Team, den Gilb zurückzudrängen und ein Volk von 60 Millionen Menschen zu befreien.“ Jeder Aufruf dieser Seite kostete 9,97 D-Mark, die sich am Ende der Nacht nach 13510 Aufrufen zu 134.634,88 D-Mark summierten – zu Lasten der Hamburger Sparkasse.

Die beiden Hacker verfolgten mit der Aktion ein hehres Ziel: Sie wollten die deutsche Öffentlichkeit darauf aufmerksam machen, dass das von ihnen getestete Bildschirmtext-Informationssystem (Btx) unsicher ist. Das von IBM mit einiger Verspätung im Mai 1984 an die deutsche Bundespost (Spitzname Gilb) ausgelieferte Informationssystem enthielt ihrer Meinung nach so viele Fehler, dass möglichst publikumswirksam vor ihm gewarnt werden sollte. Der Gilb sollte zurückgedrängt, die massive Werbung der Bundespost für das neue System infrage gestellt werden.

Der CCC war seit dem Start von Btx im Jahre 1983 als Anbieter mit von der Partie und hatte bereits zahlreiche Fehler reklamiert und auf seinen Btx-Informationsseiten demonstriert. Indem er eine Seite nun kostenpflichtig machte und von einem anderen Teilnehmer aufrufen ließ, kam Geld ins Spiel und aus dem Protest wurde Ernst.

„Die Hacker wählten die Sprache des Geldes, um abseits ihrer Subkultur Gehör zu finden“, beschrieb der Kommunikationswissenschaftler Alexander Ehmann später die Aktion, die den 1983 gegründeten Chaos Computer Club schlagartig berühmt machte. Am 19. November 1984 gaben sie im Beisein von TV-Kameras der

Sparkasse das Geld „zurück“ – das zu diesem Zeitpunkt noch gar nicht auf der Fernmelderechnung aufgetaucht war. Journalisten spöttelten in ihren Berichten über das vom größten Computerkonzern IBM gelieferte, angeblich hochsichere System, das sich nicht einmal vor ein paar Jugendlichen schützen konnte. Irgendwie waren sie an die Login-Angaben der Hamburger Sparkasse gekommen – nur wie?

Passwort im Überlauf

Die Erklärung des CCC klang abenteuerlich: Sie hätten systematisch den Bildschirmspeicher einer Btx-Seite zum Überlauf gebracht, in dem dann auftauchenden „Datensalat“ nach verwertbaren Informationen gesucht und die Passwörter der Sparkasse gefunden. Die Bundespost bestätigte zwar den „Überlauffehler“ im Bildschirmpuffer (den IBM sofort reparieren musste), dementierte aber, dass auf diese Weise im Zeichenwirrwarr nach Passwörtern gefischt werden konnte. Diese seien in einem völlig anderen Bereich des Systems verschlüsselt gespeichert. Die Erklärung, die der Pressesprecher der Bundespost veröffentlichte, war mit der Erwähnung von „unterirdischer Kabelführung“ der Telefonleitungen nicht weniger abenteuerlich:

„Der Eindruck wird erweckt, dass es für Hacker ein Leichtes sei, Bildschirmtext mißbräuchlich zu nutzen. Dieser Eindruck ist falsch. Das Herausfinden fremder Kennungen durch computergesteuertes Probieren ist bei Bildschirmtext ausgeschlossen. Der Zugang ist durch eine zweistufige Kennung doppelt abgesichert. Die Chance, ein persönliches Kennwort herauszufinden, ist mit weniger als 1 : 100 Millionen noch geringer als sechs Richtige im Lotto zu treffen. Einzig durch das kriminelle Anzapfen eines Telefonanschlusses könnte die dazugehörige Btx-Kennung herausgefunden werden. Durch das Fehlen von Gemeinschaftsanschlüssen und die unterirdische Kabelführung ist das in der Bundesrepublik aber schwieriger als in den USA.“

Das Fazit der Btx-Techniker: Die beiden Hamburger mussten irgendwo das Passwort aufgeschnappt haben, etwa bei einer öffentlichen Vorführung des Online-Bankings der Sparkasse. Solch eine Ausspähung von Login-Daten stand übrigens nicht im Gegensatz zum CCC-Programm oder zur Hacker-Ethik: „Bei Passwörtern von Konzernen gehen wir davon aus, dass sie zur Weiterbildung unserer Jugend freigegeben sind“, stand in der allerersten Ausgabe der „Datenschleuder“ des CCC.

Ungeklärte Streitfrage

Zum 30. Jahrestag des „Btx-Hacks“ lud die Wau-Holland-Stiftung (WHS) im Jahre 2014 die beiden noch lebenden Protagonisten zu einer Podiumsdiskussion ein. Der damalige Btx-Projektleiter Eric Danke wie Btx-Hacker Steffen Wernéry wiederholten ihre seit 30 Jahren bekannten Erklärungen, ohne von ihrer Position abzurücken.

Das war nett und humorig aufgezogen, brachte aber wenig Erkenntnisgewinn, bis ein jugendlicher CCC-Anhänger forderte: „Wenn das alles noch strittig ist, dann muss man ein Rechercheteam bilden und den Quellcode untersuchen!“ Die Idee erhielt viel Beifall, doch die Btx-Rechner von damals sind längst verschrottet und die Software ist nicht mehr auffindbar, wie Eric Danke erklärte. Der letzte Btx-Zentralrechner wurde im Dezember 2001 abgeschaltet, nur das Online-Banking wurde bis 2007 weiter gepflegt.

Ob der Btx-Hack nun echt war oder ob die Passwörter ausgespäht wurden, ändert nichts am Erfolg, den der CCC mit seiner Aktion erzielte. Steffen Wernéry sprach in Berlin von einem „Hyperspace-Beschleunigungseffekt“, der den CCC zehn Jahre lang über Wasser gehalten habe. Der Btx-Hack habe auch dann noch als Mahnung gewirkt, als der Club an den Folgen des KGB-Hacks im Jahre 1989 zu zerbrechen drohte (siehe S. 60). Damals versuchten Hacker, die Ergebnisse ihrer Netzstreifzüge an Geheimdienste zu verkaufen, was im krassen Widerspruch zum Start stand, als Wau Holland vor den Kameras zum Btx-Hack verkündete: „Wir schützen den Menschen vor Datenmissbrauch.“ *(hag@ct.de)* c't

Das Btx-System

Das Bildschirmtext-System der Deutschen Bundespost wurde am 3. September 1983 nach etlichen Feldversuchen offiziell in Betrieb genommen. Insgesamt investierte die Bundespost 700 Millionen D-Mark in ein Kommunikationssystem auf Basis des Telefonanschlusses, das aus regionalen Leitrechnern bestand und den Fernseher als Terminal nutzen sollte. Dafür mussten sogenannte Btx-Decoder gebaut werden, die Informationen nach dem CEPT-Standard darstellen konnten.

Dieser 1981 verabschiedete Standard definierte einen Bildschirm mit 480 × 250 Bildpunkten und 32 gleichzeitig darstellbaren Farben aus einer Palette von 4096. Lieferant der „Server“ war IBM. Die Firma hatte überraschend den Zuschlag vor dem Hauslieferanten SEL bekommen, weil sie den Firmen, die Btx als Inhaltsanbieter nutzen wollten, Kosten im Pfennigbereich versprach. Bei IBM ging man davon aus, dass Firmen eigene Rechner ans Btx-Netz hängen, und wollte mit Lizenzen am selbst entwickelten EHKP (Einheitliches Höheres Kommunikationsprotokoll) Geld verdienen.

Die für Fernseher nötigen Decoder kamen von Blaupunkt und Loewe. Statt der versprochenen 500 D-Mark kosteten die Decoder jedoch satte 2000 D-Mark. Die Btx-Techniker begriffen zu spät, dass das Btx-Terminal zu diesem Preis den aufstrebenden Home- und Personal Computern weit unterlegen war. Letztere kosteten in Vollausstattung lediglich 500 D-Mark mehr.

Das „Bürger-Informations-Netz, das unsere komplexe Welt transparenter macht, indem es Menschen und Institutionen zusammenbringt“, wie Postminister Kurt Gscheidle Btx charakterisierte, erholte sich niemals vom Btx-Hack. Statt der erhofften 6 Millionen Kunden zählte Btx 1986 lediglich 60.000 Teilnehmer und konnte bis zur Ablösung durch das Internet-Angebot von T-Online die Millionengrenze nie überspringen.