CHAOS COMPUTER CLUB

Der ungeklärte Btx-Hack

Vor 30 Jahren gelang Mitgliedern des Chaos Computer Clubs ein spektakulärer Hack, bei dem sie der Hamburger Sparkasse mit Hilfe des Btx-Systems 135.000 Mark in Rechnung stellten. Über den genauen Ablauf sind sich Hacker und Btx-Verantwortliche bis heute uneinig.

18. November 2014, 8:04 Uhr , Hanno Böck

(Bild: Wikipedia [https://de.wikipedia.org/wiki/Datei:Bildschirmtext_Logo.svg])

Der Bildschirmtext der deutschen Post sah noch eine Trennung von Anbietern und Nutzern vor.

Die Wau Holland Stiftung [https://www.wauland.de/] und der Chaos Computer Club (CCC) haben zum 30. Jubiläum des sogenannten Btx-Hacks zu einer Diskussionsrunde ins Berlin Congress Center (BCC) eingeladen [http://ccc.de/de/updates/2014/veranstaltung-zu-30-jahre-btx-hack] . Der Btx-Hack brachte 1984 den CCC zum ersten Mal bundesweit in die Schlagzeilen.

Das Bildschirmtextsystem [https://de.wikipedia.org/wiki/Bildschirmtext] der damaligen Deutschen Bundespost, abgekürzt Btx, war ein Onlinenetzwerk, das 1983 in Betrieb ging. Stefan Wernery, damals bereits Mitglied im CCC, erklärte, dass sich die meisten Hacker zu dieser Zeit eher für VAX-Netzwerke interessierten, er persönlich fand das neue System jedoch sofort spannend. Nach einiger Zeit gelang es den Hackern auch, erste Sicherheitsprobleme in Btx zu finden, die sie - schon damals der Hackerethik [http://www.ccc.de/en/hackerethik] folgend - der Post mitteilten. Als die Post jedoch die entdeckten Sicherheitslücken schlicht leugnete, wollten die Hacker diese bei einer öffentlichen Pressekonferenz vorführen. Doch das schlug fehl, die Post hatte die Sicherheitslücken mittlerweile geschlossen. Diese Pressekonferenz war laut Bernd Fix von der Wau Holland Stiftung der Grund, weshalb die Hacker sich beim nächsten Hack dazu entschieden, die Post nicht vorab über die Sicherheitsprobleme zu informieren, sondern stattdessen direkt an die Öffentlichkeit zu gehen.

Das eigene Angebot abgerufen

Das damalige Btx-System sah kostenpflichtige Inhaltsseiten vor, und der Chaos Computer Club besaß selbst einen Anbieterzugang, mit dem er derartige Btx-Seiten einstellen konnte. Mit einer Teilnehmerkennung der Hamburger Sparkasse (Haspa) riefen die CCC-Hacker permanent dieselbe Seite aus dem eigenen Angebot auf. Ein einzelner Abruf kostete 9,97 Mark, am Ende hätte die Sparkasse dem CCC 135.000 Mark geschuldet. Der CCC verzichtete jedoch auf die Zahlung des Geldes und machte den Hack öffentlich.

Strittig ist bis heute, wie der CCC in Besitz der Zugangsdaten der Hamburger Sparkasse gelangte. Nach Darstellung von Stefan Wernery und dem inzwischen verstorbenen CCC-Gründer Wau Holland gelang es mittels eines Buffer Overflows im Publikationssystem von Btx, zufällige Daten aus dem System auszulesen. Dabei seien die Hacker nach mehreren Versuchen auf die Zugangsdaten der Haspa gestoßen. Derartige Fehler sind im Übrigen bis heute ein Problem, der Heartbleed-Bug funktioniert vom Prinzip her genauso.

Streit um die Zugangsdaten

Eric Danke, der damals für das Btx-System der Post verantwortlich war, bezweifelt jedoch bis heute diese Darstellung der CCC-Hacker. Die Post und die verantwortlichen Programmierer von IBM bestätigten zwar den Buffer Overflow, es sei jedoch nicht möglich gewesen, dass dadurch Zugangsdaten ausgelesen werden konnten. Diese seien verschlüsselt abgelegt gewesen. Es sei den Hackern auch nicht gelungen, bei einer Vorführung dem Hamburger Datenschutzbeauftragten Henning Schapper den Hack vorzuführen, sagte Danke. Schapper hatte damals den Vorfall untersucht, der als Ordnungswidrigkeit nach dem Bildschirmtext-Staatsvertrag verhandelt wurde.

Nach Darstellung der Verantwortlichen der Post kamen die Hacker vermutlich auf ganz andere Art an die Zugangsdaten. So hatte es wenige Tage vorher eine öffentliche Veranstaltung der Hamburger Sparkasse gegeben, bei der das Btx-Angebot der Bank vorgestellt wurde. Dort wurde öffentlich die Funktionsweise des Btx-Systems gezeigt, dabei wurden die Zugangsdaten der Haspa verwendet. Dabei seien diese auf irgendeine Weise ausgespäht worden.

Buffer Overflows, damals wie heute

Aus technischer Sicht ist die Darstellung der CCC-Hacker plausibel. Selbst wenn die Zugangsdaten verschlüsselt waren, wären sie nach einem Login der Haspa in jedem Fall für kurze Zeit unverschlüsselt im Speicher vorhanden gewesen. Möglicherweise war es schlicht ein Zufall, dass die Hacker den Buffer Overflow im richtigen Moment ausgenutzt haben. Dass Betreiber eines Systems die Auswirkungen von Sicherheitslücken unterschätzen, ist keine Seltenheit [https://www.golem.de/news/heartbleed-keys-auslesen-ist-einfacher-als-gedacht-1404-105825.html] .

Ob der genaue Hergang des Hacks jemals geklärt werden kann, ist zweifelhaft. Auf Nachfragen aus dem Publikum, ob nicht der Quellcode der damaligen Btx-Software veröffentlicht werden könne, um die Behauptungen zu prüfen, antwortete Danke, dass die entsprechende Hardware inzwischen entsorgt worden sei und wahrscheinlich auch keine Kopien der Software mehr vorhanden seien. Das Btx-System ist inzwischen Geschichte, es wurde später in den neuen Service Datex-J übernommen. Danach wurde Btx noch eine Zeit lang als Teil von T-Online weitergepflegt, 2007 wurde es endgültig abgeschaltet.

Zum Anlass des 30. Jubiläums hat die Wau Holland Stiftung zahlreiche Dokumente zum Btx-Hack auf ihrer Webseite zur Verfügung gestellt [https://www.wauland.de/de/hackerarchiv/1984-11-17_btx-hack.html] . Neben Pressemitteilungen, Briefwechseln und Zeitungsartikeln ist dort auch der originale BASIC-Code zu finden, mit dem der automatisierte Aufruf der Haspa-Seiten durchgeführt wurde. ■

Themenseiten:

CCC, Datensicherheit, Innovation & Forschung, Post, Software, Sparkasse, Unternehmen, Wauland, Wissen, Technologie, Applikationen, Internet