Die Hacking Geschichte

Teil 2: Das Wählmodem

Bruce Nikkel

Bruce Nikkel Museumsführer
im Museum ENTER

Dies ist der zweite Teil einer vierteiligen Serie zur Geschichte des Computerhackings. Im Teil I wurde das Hacking der globalen Telefonzentralen beschrieben. Im Folgenden wird das Hacken der Heimcomputer, Modem und Einwählverbindungen erläutert.

Frühe Computernetzwerke nutzten die vorhandenen Sprachleitungen der Telefongesellschaften. Diese Kommunikation erforderte eine Umwandlung zwischen analogen Audiotönen und digitalen Datenbits unter Verwendung von Signalmodulation und Demodulation. Der Ursprung des Wortes «Modem» leitet sich aus diesem Prozess ab.

Die meisten Telefongesellschaften haben streng geregelt, welche Geräte an das Telefonnetz angeschlossen werden dürfen. Frühe «Akustikkoppler»-Modems verwendeten Audiotöne, um mit dem Mikrofon und dem Lautsprecher des Telefons zu kommunizieren. Dies war keine direkte elektrische Verbindung («Luftspalt») und erforderte keine Genehmigung der Telefongesellschaft, sodass Amateure ihre eigenen akustischen Kopplungsmodems bauen und verwenden konnten.

Modems, die direkt (elektrisch) mit dem Telefonsystem verbunden waren, waren viel schneller und hatten weniger Fehler als akustische Modems, für die jedoch

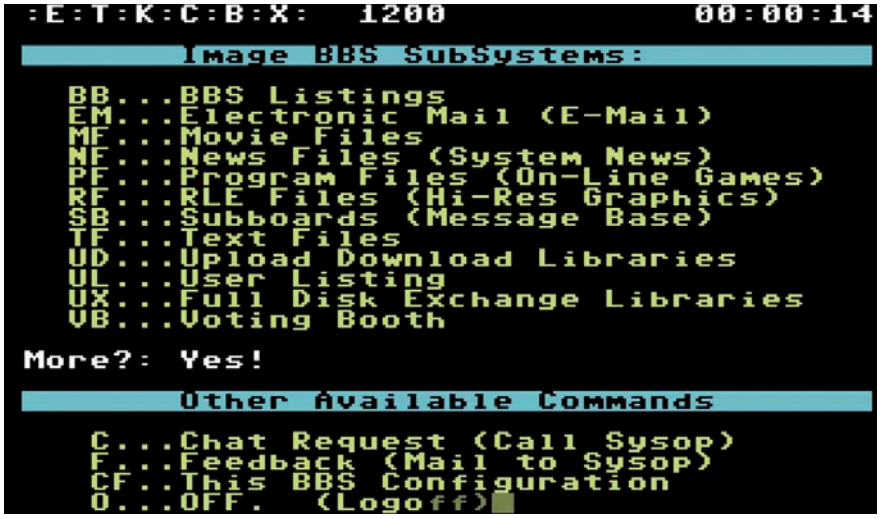
Kopplermodem und Telefon

eine Zertifizierung durch die Telefongesellschaft erforderlich war. Akustische Kopplermodems konnten auch mit Münztelefonen verwendet werden, bei denen kein direktes Kabel verfügbar war. Im Laufe der Zeit wurden direkt angeschlossene elektronische Modems billig und ersetzten die akustische Kopplertechnologie. Die Nutzung des öffentlichen Telefonnetzes für Computernetzwerke machte es Hackern leicht, diese auszunutzen.

Anfänglich wurden Einwählmodems verwendet, um Fernterminals mit Grossrechnern und Minicomputern zu verbinden, auf denen Unix oder andere Time-Sharing-Systeme liefen.

Terminals und Modems verwendeten eine spezielle Zeichenfolge, die als «Escape-Codes» oder «Escape-Sequenz» bezeichnet wurde, um die Sitzung und das Modem zu steuern. Escape-Sequenzen wurden verwendet, um spezielle Befehle für Dateiübertragungen, lokales Drucken, Konfiguration, Diagnose und andere Steuerfunktionen an das System oder das Modem zu senden. Escape-Sequenzen waren für Hacker besonders interessant, da sie mehr Kontrolle über ein System ermöglichten und dazu verwendet werden konnten, aus Programmen oder Menüsystemen auszubrechen, um auf Systembefehlsansagen und -shells zuzugreifen.

Fortgeschrittenere Modems hatten voll funktionsfähige Befehlssätze in ihrer Firmware und konnten mit komplexen «AT-Befehlen» (ursprünglich von der **Hayes-Modemfirma** erfunden) manipuliert werden. Hacker würden diese Funktion auch verwenden, um Ortsgespräche an Ferngesprächs-



Bulletin Board System (BBS)

nummern weiterzuleiten und den Zugriff auf Remotecomputersysteme zu ermöglichen.

Der Zugang zu grossen Unternehmen oder Netzwerken war entweder eingeschränkt oder teuer. Dies führte zur Verbreitung von kostenlosen Bulletin Board-Systemen (BBS), die von privaten «Sysops» oder Systembetreibern herausgegeben wurden. Jeder Computerfan mit einem Modem konnte ein BBS erstellen und die Nummer veröffentlichen (in lokalen Zeitungen, Computermagazinen oder anderen BBS). BBS waren textbasierte Systeme, die für Chat, Forumsdiskussionen, E-Mail, Spiele, Nachrichten, das Hoch- und Herunterladen von Dateien sowie für den Gateway-Zugriff auf andere BBS oder Netzwerke verwendet wurden.

Die BBS-Hacker-Szene umfasste das Teilen von «Warez» oder urheberrechtlich geschützter gehackter/geknackter Software, gestohlenen Kreditkarten und Ferngesprächskarten, gestohlenen Passwörtern und Zugangscodes sowie gestohlenen Quellcodes und Dokumentation. BBS waren auch eine beliebte Methode, um mit Viren infizierte Programme zu verbreiten.

Netzwerke von Computersystemen auf der ganzen Welt wurden ebenfalls immer beliebter. Einige Netzwerke waren kommerzielle Datenfernübertragungsanbieter wie **Compuserve** oder **AOL,** für die eine monatliche Gebühr für Dienste erhoben wurde. Nationale Telefon-/Postorganisationen erbrachten auch kommerzielle Dienste wie **Minitel** in Frankreich oder **BTX** (Bildschirmtext) in Deutschland. Nichtkommerzielle Netzwerke wie **FidoNet,** die BBS-Systeme aus der ganzen Welt miteinander verbanden, und **UUCPNET** verbanden Unix-Systeme über UUCP miteinander. Es gab auch regionale Netzwerke wie **MausNet** (http://maus.de) im deutschsprachigen Raum Europas. Diese basierten auf Datenfernübertragungstechnologie und das Hacken war grösstenteils nicht böswillig, um Zugriff auf Systeme zu erhalten oder andere


Französischer Minitel Terminal

Netzwerke (über Gateways) zu erkunden, sondern eher ein Spass, war interessant oder stellte eine Lernerfahrung dar.

Die Suche nach Computern mit Modems war eine Herausforderung, da die Telefonnummern nicht wie in einem Telefonbuch aufgeführt waren und die Telefongesellschaften nicht wussten, wer Modems an ihre Telefonleitungen angeschlossen hatte. Eine Technik namens «war-dialing» (Kriegswahl) wurde verwendet, um nach Computern mit Modems zu suchen, die mit dem Telefonnetz verbunden sind. Ein Computer wurde so programmiert, dass er jedes Telefon kontinuierlich aus einer Reihe von Nummern wählt (normalerweise eine Ortsvorwahl, um Gebühren für Ferngespräche zu vermeiden, oder eine Reihe von Nummern, die einem Unternehmen gehören). Wenn ein Mensch antwortete, legte der Computer auf und wählte die nächste Nummer in der Liste. Wenn ein Computer antwortete, wurde ein Modemträgersignal erkannt und die War-Dialer-Software speicherte die Telefonnummer und andere Verbindungsinformationen zur späteren Analyse. Das Wählen einer grossen Anzahl Nummern durch den War-Dialer konnte einige Tage dauern, aber am Ende hatte der Hacker eine Liste aller Computer, die den Anruf entgegengenommen hatten. Das Auffinden von Computermodems war interessant, da viele frühe Systeme keine Passwörter verwendeten und man brauchte für den Zugriff nur die Nummer zu kennen.

Andere Methoden zum Auffinden von Modemnummern und Passwörtern waren «Social Engineering» und «Dumpster Diving» (wie im letzten Artikel erwähnt).

War-dialing wurde im Film War Games verwendet

Beim Social Engineering (heute bei Cyberkriminellen sehr beliebt), werden Menschen getäuscht oder dazu verleitet, Dinge zu tun oder Informationen preiszugeben. Hacker haben verschiedene Personen in einem grossen Unternehmen angerufen oder besucht, die sich als andere Mitarbeiter oder technischer Support ausgeben. Sie hatten eine freundliche Unterhaltung mit einer plausiblen Geschichte und baten um Hilfe, um Telefonnummern und Passwörter von Computermodems zu finden.

Beim Müllcontainertauchen (Dumpster diving oder trashing), haben Hacker den Müll des Unternehmens nach Computerausdrucken oder Telefonlisten des Unternehmens durchsucht, die möglicherweise Computermodemnummern, Kennwörter und andere technische Informationen enthalten. Um nicht erwischt zu werden, fand das Dumpster diving nachts statt, wenn die Büros geschlossen waren. Dies war in der Zeit, als Papierrecycling noch nicht üblich war und das Papier im Abfall landete.

Ein weiterer Angriff gegen Datenfernübertragungssysteme war «demon-dialing». Ein «Demon Dialer» war ein elektronisches Gerät (gesteuert durch DTMF-Töne), das an eine Telefonleitung oder ein Softwareprogramm angeschlossen war, das ein Modem steuert und wiederholt eine einzelne Nummer anruft. Dies wurde ursprünglich erstellt, um einen besetzten BBS oder ISP kontinuierlich zu wählen, bis eine Verbindung erfolgreich war. Hacker nutzten Dämonenwahl auch für DoS-Angriffe (Denial of Service) und Brute-Forcing-Zugriff.

Bei einem DoS-Angriff hielt man die Modems beschäftigt, sodass sich keine anderen Benutzer in den Dienst einwählen konnten. Wenn der Angreifer schneller wählen, auflegen und erneut wählen konnte, als der Anbieter die Modems neu initialisieren konnte, wurde ein erfolgreicher DoS erstellt.

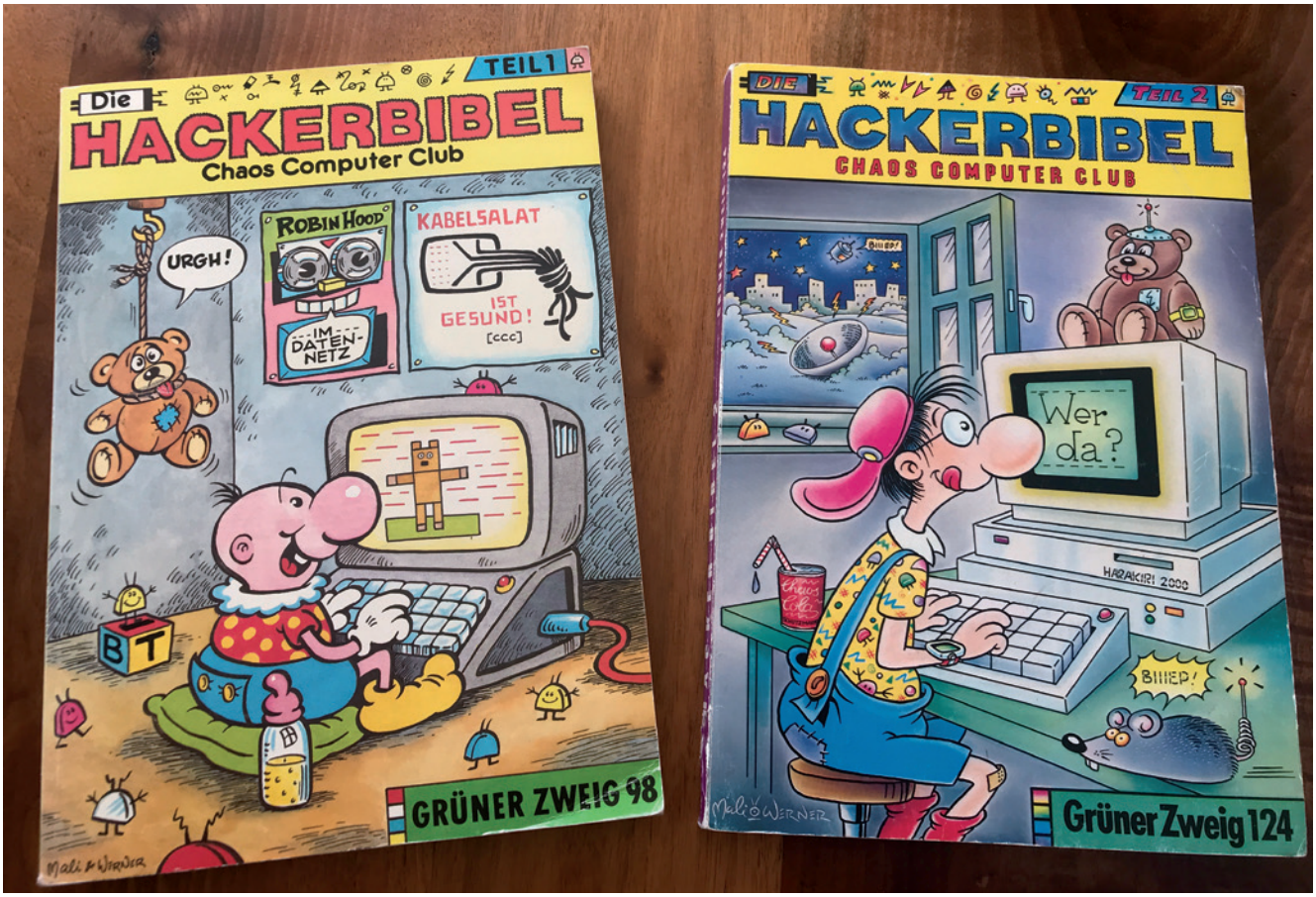
Eine andere Verwendung für demon-dialing bestand darin, wiederholt verschiedene Benutzernamen und Passwörter zu testen (Brute Force).

Eine Liste mit gängigen Benutzernamen und Kennwörtern wurde mit einem Demon-Dialer Programm gegen das Datenfernübertragunssystem eines Unternehmens ausgeführt, um einen nicht autorisierten Zugriff zu versuchen.

Für zusätzliche Sicherheit verwendeten einige Organisationen eine Methode namens «dial-back»- oder «call-back»-Authentifizierung. Wenn ein Benutzer eine Verbindung zum Unternehmen herstellen wollte, rief er an, identifizierte sich und unterbrach den Anruf. Das Datenfernübertragungssystem des Unternehmens verfügte über eine vordefinierte Liste von Telefonnummern für autorisierte Benutzer und rief den identifizierten Benutzer zurück. Der Computer des Benutzers ging dann ans Telefon und baute die Verbindung auf.

Es gab eine einfache Möglichkeit, schlecht gestaltete Rückrufsysteme zu hacken. Wenn sich das angegriffene Modem weigerte, die Leitung zu unterbrechen, bemerk-

Eine Dämonen Wählbox



Chaos Computer Club Hacker Bibeln

ten einige Rückrufsysteme dies nicht und sendeten die Wählcodes (Impuls- oder DTMF-Töne) über die noch verbundene Telefonleitung. Ohne die Verbindung zu trennen, «antwortet» der Angreifer dem Wählmodem. Das Unternehmenssystem glaubt, dass die Rückwahl erfolgreich war, und eine nicht autorisierte Verbindung wird hergestellt.

Der Zugang zu Hacking-Tools und -Techniken begann mit beliebten Hacker-Ressourcen wie dem *Chaos Computer Club (CCC)*, dem *2600 Magazine*, dem *Phrack E-Zine* und anderen Online-Hacker-Communities zu wachsen.

In den 1970er und 1980er Jahren wurde der unbefugte Zugriff und das Eindringen in Computersysteme und Netzwerke über Modem für Systembesitzer problematisch. Dies führte in den meisten Ländern zu neuen Gesetzen für Computerbetrug und -missbrauch, um böswillige Hacking-Aktivitäten als kriminelle Handlung einzustufen. Diese Gesetze wurden im Zeitalter der Modemdatenfernübertragung geschaffen, sollten jedoch im Zuge des technologischen Wandels relevant bleiben.

Das Datenfernübertragungs-Modem ist heute grösstenteils verschwunden. Das Internet hat das BBS und andere Übertragungsnetzwerke ersetzt, Breitband und Glasfaser haben das Datenfernübertragungs-Internet ersetzt, sogar analoge Telefonleitungen sind veraltet und werden durch Voice-over-IP (VoIP) ersetzt.

Das Enter Museum in Solothurn verfügt über eine hervorragende Sammlung historischer Modems und Telekommunikationsgeräte und ich kann einen Besuch sehr empfehlen.

Quellen:

Chaos Computer Club:
https://www.ccc.de/

2600 Hacker Quarterly:
https://2600.com/

Phrack e-zine:
http://phrack.org/

Liste der über das Internet zugänglichen BBS-Systeme:
https://www.telnetbbsguide.com/

Der Artikel wurde von Florence Kunz übersetzt. Der englische Originalartikel befindet sich auf: https://digitalforensics.ch/nikkel20c.pdf

Original English version found here: https://digitalforensics.ch/nikkel20c.pdf