ZT IT-KOLUMNE

(Computer-)Hacker, was ist das?

Der Begriff Hacker bzw. Computerhacker wird oft in den Medien verwendet, wenn es um Eindringlinge in Computersysteme geht. Aber was steckt genau hinter diesem Begriff? Dieser Artikel gibt einen Überblick und beantwortet die Frage.

Auf Wikipedia findet man folgende Begriffsdefinition: „Hacker hat im technischen Bereich mehrere Bedeutungen. Das Wort wird alltagssprachlich gebraucht, um jemanden zu bezeichnen, der in Computersysteme eindringt und zugleich Teil einer entsprechenden Szene ist.“[1]
Im Gabler Wirtschaftslexikon steht Folgendes: „Das engl. ‚to hack‘ bedeutet: in etwas eindringen. In der Informatik gilt ein Hacker als Person, die Freude an Erstellung bzw. Veränderung von Software oder Hardware hat. Der Begriff wird im Zusammenhang mit Kriminal-

fällen für Personen verwendet, die solche Lücken in fremden Systemen unerlaubt für eigene, oft kriminelle Zwecke wie den Diebstahl von Informationen nützen. ‚Echtes‘ Hacking bedeutet: Einbruch in Computer bzw. Computernetze.“[2]
Beide Begriffsdefinitionen zeigen die alltagssprachliche Verwendung von ‚Hacker‘: Personen, die illegal in fremde Computersystem eindringen. Das ist natürlich nur die eine Seite. In diesem Artikel werde ich die anderen Aspekte und Bedeutungen im Einzelnen erklären.

Die Geschichte des „Computerhackings“

Der Begriff „Hacker“ wurde erstmals am berühmten amerikanischen „Massachusetts Institute of Technology (MIT)“ in den 60er-Jahren des letzten Jahrhunderts verwendet. Eine sehr engagierte Gruppe von jungen Studenten, die Modelle von Maschinen zum Zweck der Leistungssteigerung auseinander- und umbaute, nannte sich ‚Hacker‘. Hacker waren also ursprünglich begeisterte, engagierte und experimentierfreudige Technikfreaks. Der ‚Vater des Hackens‘ ist der amerikanische Amateurfunker John „Captain Crunch“ Draper. Er fand 1969 heraus, dass die Spielzeugpfeife, die den Frühstücksflocken von Cap’n Crunch als Werbegeschenk beilag, einen Ton mit einer Frequenz von 2.600 Hertz erzeugt. Diese Tonfrequenz wurde im Telefonnetz von dem amerikanischen Telefonunternehmen „AT&T“ verwendet, um Ferngespräche freizuschalten. Pfiff er nun mit der Spielzeugpfeife in den Telefonhörer, konnte er ganz kostenfrei Inlands- und auch Auslandsgespräche führen. Diesen Trick taufte Draper „Phreaking“, eine Wortkombination aus phone (Telefon) und freak (Außenseiter). Erst viel später sprach auch er von Hacken.
Die außergewöhnlichen und spektakulären Aktionen des „Captain Crunch“ bewegte andere begeisterte und bastelorientierte Informatiker dazu, den legendären „Homebrew Computer Club“ zu gründen. Die Mitglieder bauten einen der ersten Personal Computer „Altair 8800“ um und entwickelten diesen dann auch weiter. Unter ihnen waren auch Steve Wozniak und Steve Jobs, die 1976 Apple gründeten.
In den 80er-Jahren des letzten Jahrhunderts wurde durch den siebzehnjährigen „Kevin Poulsen“, der in das militärische Computernetz und Internet-Vorläufer „ARPANET“ eindrang, die Hackerszene dann auch der Öffentlichkeit ein wenig bekannter. 1983 kam dann der Science-Fiction-Film „Wargames – Kriegsspiele“ von John Badham in die Kinos. Der Spielfilm handelt von den Abenteuern eines jungen Hackers, der zufällig auf das Computersystem des amerikanischen Militärs zugreift und fast einen weltweiten Atomkrieg auslöst. Die Öffentlichkeit erhielt durch diesen Film zum ersten Mal einen Einblick in die fantastische und geheimnisvolle Welt der Computerhacker.
In den 80er-Jahren wurden auch die ersten Computerviren bekannt. 1988 verbreitete sich der Computerwurm Morris über das ARPANET auf Tausenden Computern. Sein Erfinder, Robert Tappan Morris, wurde zu einer dreijährigen Bewährungsstrafe und einer Geldstrafe von 10.000 Dollar verurteilt. Von diesem Zeitpunkt an wurden Hacker zu Bösewichten deklariert, die im besten Fall als verantwortungslose Jugendliche, im schlimmsten Fall als potenziell gefährliche Verbrecher angesehen wurden.
In den 90er-Jahren spaltete sich dann die Hackerszene. Auf der einen Seite stehen auch heute noch die „Black-Hats“, die aus kriminellen Beweggründen hacken, und auf der anderen die „White-Hats“, die keine bösen Absichten verfolgen und primär auf Sicherheitslücken in Computersystemen hinweisen wollen. Zwei nennenswerte und spektakuläre Hackerfälle prägten die 90er-Jahre. 1994 hackte sich der russische Mathematiker Vladimir Levin in das internationale Bankennetz SWIFT ein und machte die Citybank um 10 Millionen Dollar ärmer. Er wurde zu drei Jahren Gefängnis verurteilt. 1995 wurde Kevin Mitnick vom FBI verhaftet. Er war seit 1989 auf der Flucht und mehrerer Software-Diebstähle sowie des Eindringens in geschützte Systeme angeklagt. Der Schaden wurde auf über 80 Millionen Dollar bemessen. Mitnick wurde zu einer fünfjährigen Gefängnisstrafe verurteilt. Nach seiner Entlassung wurde ihm der Zugang zu Telefonen, Computern und Datennetzen verboten.
Mit Beginn des 21. Jahrhunderts ging es weiter mit der sogenannten „Cyberkriminalität“. Die entdeckungsfreudigen Bastlerfreaks versuchten erneut, die Grenzen der Technologie zu überschreiten oder wenigstens die von den Industriellen aufgebauten Hindernisse zu überwinden (Cracking). 2001 gelang es Jon Johansen alias „DVD Jon“, den DVD-Schutz zu umgehen und Filme zu kopieren. 2007 gelang George Francis Hotz der iPhone-Jailbreak zur Entsperrung des Geräts für die Software von anderen Anbietern als Apple. Ein anderer großer Trend war die Gründung von Aktivistengruppen, die Hackertechniken für ihre militanten politischen Zwecke nutzen. Ein Beispiel ist die Website „WikiLeaks“, auf der geheime Informationen veröffentlicht werden, ohne die Quellen anzugeben. Einer der Gründer von WikiLeaks ist Julian Assange, der früher unter dem Pseudonym „Mendax“ in der Hackergruppe „International Subversives“ tätig war. Diese Form des Computerhackens knüpft an den guten alten Bastlergeist der frühen Hacker an und verbindet diesen mit einem ideologischen Ziel.
Nach Einführung von Gesetzen zur Computerkriminalität begannen sich White-Hat-, Grey-Hat- und Black-Hat-Hacker voneinander abzugrenzen, abhängig von der Gesetzmäßigkeit ihrer Tätigkeiten.

Die vier Basistechniken der Hacker

Die Computerhacker verwenden prinzipiell vier Basistechniken, die zu jedem Werkzeugkasten eines Hackers gehören:

1. Soziale Manipulation (Social Engineering)

Social Engineering gehört nicht zu den technischen Hilfsmitteln, um einen Angriff zu starten. Der Hacker verwendet hierbei Überzeugungsmethoden, um an Informationen von Menschen in Schlüsselpositionen zu kommen. Der Hacker benötigt also kein technisches Wissen. Es geht nicht darum, technische Sicherheitslücken aufzudecken, sondern menschliche. Betrug und Täuschung sind die wichtigsten Instrumente dieser Manipulationsstrategie. Beispiel: Ein Hacker ruft einen Systemadministrator an und gibt sich als Sicherheitsbeauftragter aus, um an entscheidende Systeminformationen zu gelangen. Der Erfolg dieser Methode ist demnach vom Überzeugungstalent des Hackers abhängig.

2. Defacement

Beim Defacement wird eine Webseite manipuliert, indem vom Besitzer der Webseite nicht genehmigte Inhalte hinzugefügt werden. Defacement (Verunstaltung bzw. Entstellung) wird von Hackern verwendet, um Machenschaften von Regierungen und Unternehmen schlecht zu machen. Um eine Webseite zu „verunstalten“, nutzt der Hacker eine Sicherheitslücke auf dem Webserver des Hostsystems aus (z. B. im Betriebssystem des Computers).

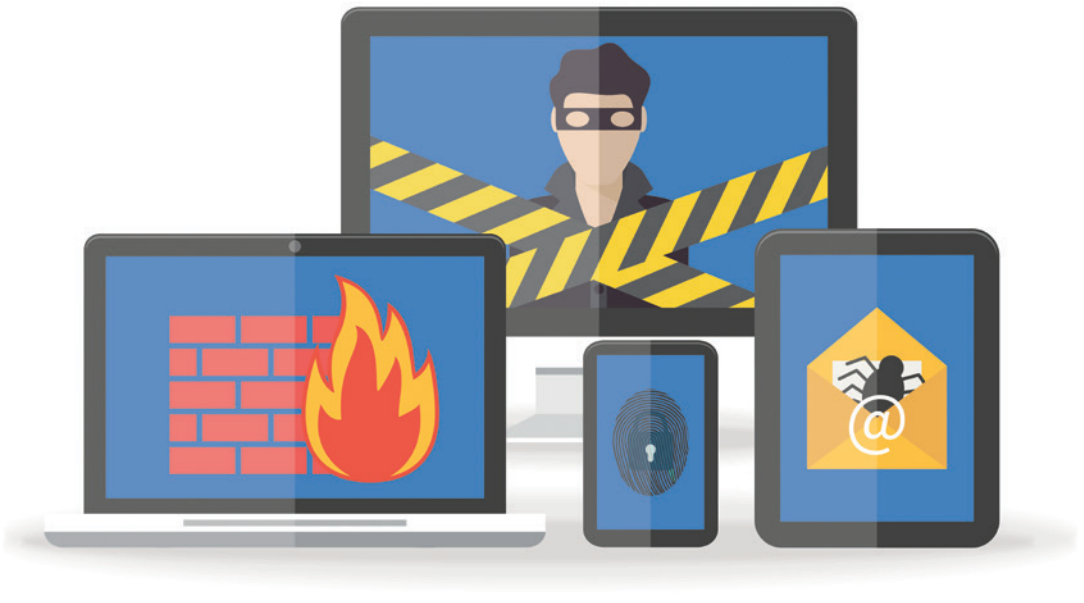
3. Verteilte Dienstblockade (DDoS)

Mit einem DDoS-Angriff (Distributed Denial of Service) wird ein Dienst überlastet und nicht mehr erreichbar gemach. Typische Ziele solcher Angriffe sind Webserver für Webseiten. Werden diese überlastet, können die Webseiten nicht mehr erreicht werden. Schlecht geschützte Computersysteme werden zu-

erst mit einem bösartigen Programmcode infiziert, zum Beispiel in Form von Spam-Mails. Dies geschieht verdeckt im Hintergrund. Das Ziel eines Hackers ist es, alle notwendigen Tools zu installieren, um später den Angriff starten zu können. Sind erst einmal viele Rechner infiziert, kann dann der Hacker eine gleichzeitige Attacke aller Computersysteme starten. Das Ergebnis ist das Zusammenbrechen der Zielserver als Folge von einer Anfrageflut.

4. Pufferüberlauf

Das Prinzip eines Pufferüberlauf-Angriffs (Buffer Overflow) besteht darin, einen Fehler in einer von einem Entwickler programmierten Software zu verursachen, das dann den Systemschutz angreift. Ein Puffer ist ein temporärer Speicherbereich (im Hauptspeicher RAM) einer Software. Ein Überlauf entsteht, wenn dem Bereich mehr Daten zugeordnet werden als er aufnehmen kann. Ergebnis: Im Programm tritt ein Fehler auf. Der Hacker nutzt den Fehler, um seinen eigenen böswilligen Code vom geschwächten Programm ausführen zu lassen. Meistens sind Webbrowser das Ziel von Pufferüberläufen. Der Fehler wird ausgelöst, wenn eine Spam-Mail geöffnet oder im Internet eine kontaminierte Seite aufgerufen wird.



© Ira Yapanda/Shutterstock.com

Hacking im deutschen Strafgesetz

Der § 202c des deutschen Strafgesetzbuches (Vorbereiten des Ausspähens und Abfangens von Daten, der sog. „Hackerparagraf“) stellt die Beschaffung und die Verbreitung von Zugangscodes zu zugangsgeschützten Daten sowie die Herstellung und den Gebrauch von Werkzeugen, die diesem Zweck dienen, als Vorbereitung einer Straftat unter Strafe.

Ausblick

In der Zukunft werden immer mehr Dinge miteinander vernetzt werden (Internet der Dinge). Dabei wird die Sicherheit der Daten und Systeme eine entscheidende Rolle spielen. Hacker mit böswilligen Gedanken werden selbstverständlich versuchen, in die vernetzten Systeme einzudringen, um Schaden anzurichten. Viele Sicherheits- und Software-Unternehmen werden aber auch Hacker engagieren, die die Sicherheit der Systeme genau analysieren und die Schwachstellen herausfinden, um die Systeme dann sicherer zu gestalten. Es wird im Internet, wie im wahren Leben, immer zwei Lager geben: Die guten Hacker und die bösen Hacker, und die Industrie wird höchstwahrscheinlich weiterhin den Hackern hinterherrennen. Die Hackerszene wird sich jedoch warm anziehen müssen, denn die Technologien werden immer komplexer und dadurch schwieriger zu verstehen sein. Aber auch für die Menschen, die einfach nur die vernetzten Systeme verwenden, heißt es in der Zukunft, sich mit den möglichen Technologien zu beschäftigen. Das ist die wichtigste Voraussetzung, um gegen böswillige Angriffe gewappnet zu sein. Es bleibt auf jeden Fall spannend und man darf gespannt sein, wie und wohin sich die Hackerszene entwickeln wird. ZT

Infos zum Autor

Literatur

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung & Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de