Informationen zum Thema Hacker

Software-Schwachstellen

'Errare humanum est' (' Irren ist menschlich.')
Marcus Tullius Cicero, römischer Staatsmann, Philosoph und Schriftsteller

'Irren ist menschlich, aber um etwas richtig zu versauen, braucht man einen Computer'
Paul Ehrlich

Zur Bezeichnung von Schwachstellen in Verbindung mit Computersicherheit wird in vielen verschiedenen Zusammenhängen häufig der englische Begriff 'Vulnerability' verwendet. (Im nachfolgenden Artikel verwenden wir diesen Begriff.)

Allgemein gesagt steht so eine Vulnerability im Zusammenhang mit der Verletzung eines Sicherheitsverfahrens und kann entweder mit einigen unzureichenden Regeln in der Struktur des Verfahrens oder mit einem Problem in der Sicherheitsoftware selbst zu tun haben, die der Seite, die das Sicherheitsverfahren anwendet, nicht bekannt sind. Es muss auch gesagt werden, dass theoretisch alle Computersysteme Schwachstellen haben - der Unterschied, ob sie praktisch ausgenutzt werden können oder nicht, liegt in den Kosten eines Angriffs.

Im weitesten Sinne steht der Begriff Vulnerability im Zusammenhang mit einem Verstoß gegen ein Sicherheitsverfahren. Die Ursache können unzureichende Sicherheitsregeln sein, oder es kann sein, dass es in der Software selbst ein Problem gibt. Theoretisch haben alle Computersysteme Schwachstellen; ob sie schwerwiegend sind oder nicht, hängt davon ab, ob sie benutzt werden, um dem System Schaden zuzufügen.

Es hat schon viele Versuche gegeben, den Begriff Vulnerability als Schwachstelle klar zu definieren und die zwei Bedeutungen zu trennen. MITRE, eine Forschungs- und Entwicklungsgruppe, die in den USA auf Bundesebene finanziert wird, konzentriert sich auf die Untersuchung und Lösung entscheidender Sicherheitsfragen. Die Gruppe hat die folgenden Definitionen erstellt:

Nach MITRE's CVE Terminology:

[...] ist eine universelle Vulnerability der Zustand in einem Computersystem (oder Systemsatz), der entweder:

- **einen Angreifer Befehle ausführen lässt wie ein Anwender, oder/und**
- **einen Angreifer auf Daten zugreifen lässt im Widerspruch zu festgelegten Zugangsbeschränkungen, oder/und**
- **einen Angreifer als Entität auftreten lässt, oder/und**
- **einen Angreifer eine DoS-Attacke (Verweigerung der Dienstleistung/Ablehnung) ausführen lässt.**

MITRE ist der Ansicht, dass eine Situation, wo ein Angriff durch ein fehlerhaftes oder unpassendes Sicherheits-verfahren ermöglicht wird, besser als 'Exposure' beschrieben werden sollte:

Eine Exposure ist ein Zustand in einem Computersystem (oder Systemsatz), der keine universelle Schwachstelle ist, der aber entweder:

- **einen Angreifer Informationen sammeln lässt, oder/und**
- **einen Angreifer Aktivitäten verbergen lässt, oder/und**
- **ein Leistungsmerkmal hat, das sich zwar wie erwartet verhält, aber leicht gefährdet werden kann, oder /und**
- **ein vorrangiger Eingangspunkt ist, an dem ein Angreifer versuchen könnte, Zugriff auf das System oder Daten zu erlangen, oder die nach einem sinnvollen Sicherheitsverfahren als Problem betrachtet wird.**

Wenn ein Eindringling versucht, unbefugt Zugang zu einem System zu erlangen, führt er gewöhnlich zunächst eine Routineabfrage (oder Untersuchung) des Ziels durch, erfaßt alle etwa wegen einer Sicherheitslücke ungeschützten Daten, und nutzt dann (mit Exploits) Fehler oder Schwachstellen des Sicherheitsverfahrens aus. Schwachstellen und Sicherheitslücken sind deshalb beides wichtige Punkte, die bei der Sicherung eines Systems gegen unbefugten Zugriff zu prüfen sind.

Beispiele und Beschreibungen verschiedener häufiger Schwachstellen

Microsoft Windows, das am häufigsten verwendete Betriebssystem auf Anlagen, die mit dem Internet verbunden sind, enthält mehrere schwerwiegende Schwachstellen. Die am meisten ausgenutzten befinden sich im IIS, MS-SQL, Internet Explorer, und in der Dateizugriffssteuerung und Nachrichtenverarbeitung des Betriebssystems selbst.

Eine Schwachstelle in IIS, die im Microsoft Security Bulletin MS01-033 genau dargestellt wird, ist eine der am meisten ausgebeuteten Windows-Schwachstellen überhaupt. Im Laufe der Jahre sind jede Menge Netzwerk-Würmer geschrieben worden, um diese Schwachstelle auszunutzen, unter anderem auch 'CodeRed'. CodeRed wurde am 17. Juli 2001 zum ersten Mal entdeckt und soll über 300.000 Ziele infiziert haben. Er führte bei sehr vielen Unternehmen zu einem Zusammenbruch und verursachte gewaltige finanzielle Verluste auf der ganzen Welt. Obwohl Microsoft zusammen mit dem Sicherheitsbulletin MS01-033 eine Direktkorrektur für die Schwachstelle herausgegeben hat, verbreiten sich einige Versionen des Wurms CodeRed noch immer im gesamten Internet.

Der Netz-Wurm Spida, der fast ein Jahr nach dem Auftauchen von CodeRed entdeckt wurde, nutzte für seine Verbreitung eine Sicherheitslücke in der MS-SQL Server-Software aus. Einige Standard-Installationen des MS-SQL Servers hatten für den 'SA' System-Account kein Passwort. Dadurch konnte jeder, der Netzzugang zum System hatte, beliebige Befehle ausführen. Beim Eindringen durch diese Sicherheitslücke konfiguriert der Wurm den 'Gast'-Account so, dass Datei-Mehrfachnutzung zugelassen wird und lädt sich dann selbst auf das Zielsystem. Danach benutzt es den selben Zugang über den passwortlosen MS-SQL 'SA' Account, um eine Kopie von sich selbst zu starten, und so die Infektion zu verbreiten.

Der Netz-Wurm Slammer, der Ende Januar 2003 entdeckt wurde, benutzte eine noch direktere Methode, um Windows-Systeme zu infizieren, die mit dem MS-SQL Server arbeiten: eine Schwachstelle mit einem Pufferüberlauf in einem der UDP-Paket-Unterprogramme. Da Slammer relativ klein war - 376 Bytes - und UDP benutzte, ein Kommunikationsprotokoll, das für die schnelle Übertragung von Daten entwickelt wurde, breitete er sich mit beinahe unglaublicher Geschwindigkeit aus. Manche schätzen, dass Slammer es in sage und schreibe 15 Minuten schaffte, sich in der ganzen Welt auszubreiten und ungefähr 75.000 Hauptrechner zu infizieren.

Diese drei berüchtigten Würmer benutzten Schwachstellen und Sicherheitslücken in Software, die mit verschiedenen Versionen von Microsoft Windows betrieben wird. Jedoch der Wurm Lovesan, der am 11. August 2003 entdeckt wurde, benutze für seine Verbreitung einen viel schwerwiegenderen Pufferüberlauf in einer Grundkomponente von Windows selbst. Diese Schwachstelle wird im Microsoft Microsoft Security Bulletin MS03-026 genau beschrieben.

Sasser, der Anfang Mai 2003 zum ersten Mal auftrat, nutzte eine andere Schwachstelle in einer Grundkomponente aus, und zwar dieses Mal im Local Security Authority Subsystem Service (LSASS). Informationen über die Schwachstelle wurden im Microsoft Security Bulletin MS04-011 veröffentlicht. Sasser breitete sich schnell aus und infizierte weltweit Millionen von Computern, mit enormen Kosten für die Wirtschaft. Viele Unternehmen und Institutionen waren auf Grund des Netzzusammenbruchs, den der Wurm verursachte, dazu gezwungen, ihren Betrieb zeitweilig einzustellen.

Es ist unvermeidlich, dass alle Betriebssysteme Schwachstellen und Sicherheitslücken enthalten, auf die Hacker und Virusschreiber abzielen können. Obwohl die Schwachstellen von Windows wegen der Anzahl der mit Windows laufenden Geräte die größte öffentliche Aufmerksamkeit erhalten, hat auch Unix seine schwachen Punkte.

Seit Jahren gehört die Dienstfunktion 'Finger' zu den beliebtesten Sicherheitslücken in der Welt von Unix. Dieser Dienst läßt jemanden außerhalb des Netzes sehen, welche User an einem bestimmten Gerät eingeloggt sind oder von wo aus Anwender auf den Computer zugreifen. Die Dienstfunktion 'Finger' ist zwar nützlich, aber sie legt auch eine Menge Informationen ungeschützt offen, die von Hackern genutzt werden können.

Hier eine Probe, so sieht ein fern abgefragter 'Finger'- Bericht aus:

```
Login     Name       Tty      Idle  Login Time   Office
Office Phone

xenon               pts/7   22:34  May 12 16:00 (chrome.chiba)

polly               pts/3      4d  May  8 14:21
```

```
cracker   DarkHacker pts/6      2d  May 10 11:58
```

Dies zeigt, dass wir aus dem Finger Server einige interessante Dinge über das ferne Gerät erfahren können: es sind drei User eingeloggt, aber zwei sind schon seit über zwei Tagen inaktiv, während der andere den Computer seit 22 Minuten verlassen hat. Die im Finger angezeigten Log-in-Namen kann man benutzen, um Kombinationen von Login/Passwort auszuprobieren. Das kann schnell zu einer Gefährdung des Systems führen, besonders wenn Anwender ihr Passwort auf der Grundlage ihres User-Namens aufgebaut haben, was eine relative übliche Praxis ist.

Die Dienstfunktion Finger legt nicht nur wichtige Informationen über den Server offen, auf dem sie läuft, sie ist auch schon das Ziel vieler Exploits gewesen, unter anderem des berühmten Netzwerk-Wurms, der von Robert Morris Jr geschrieben wurde, und der am 2. November 1988 ausgelöst wurde. Im modernen Unix-Vertrieb ist dieser Dienst deshalb meistens gesperrt.

Das Programm 'Sendmail', das ursprünglich von Eric Allman geschrieben wurde, ist ebenfalls ein weiteres beliebtes Ziel für Hacker. 'Sendmail' wurde für die Übertragung von E-Mail über das Internet entwickelt. Durch die große Anzahl von Betriebssystemen und Hardwarekonfigurationen, wuchs 'Sendmail' zu einem ziemlich komplexen Programm an, mit einer langen und berüchtigten Geschichte von schwerwiegenden Schwachstellen. Der Wurm von Morris nutzte für seine Verbreitung ein 'Sendmail'- Exploit aus sowie die 'Finger'- Schwachstelle.

Es gibt noch viele andere beliebte Exploits in der Unix-Welt, die Softwarepakete angreifen, wie zum Beispiel SSH, Apache, WU-FTPD, BIND, IMAP/POP3, verschiedene Teile der Kernroutinen, etc.

Die oben aufgeführten Exploits, Schwachstellen und Vorfälle heben eine wichtige Tatsache hervor. Während die Anzahl der Systeme, die mit IIS, MS-SQL oder sonstigen spezifischen Softwarepaketen laufen, sich in der Größenordnung von Hunderttausenden bewegt, liegt die Gesamtzahl der Systeme, die mit Windows laufen wahrscheinlich nahe an mehreren Hundert Millionen. Wenn all diese Geräte von einem Wurm oder von Hackern mit einem automatisierten Hacker-Tool angegriffen würden, so wäre das eine extrem schwere Bedrohung für die interne Struktur und Stabilität des Internets.

Grundlegende Schwachstellen Statistik

Mit einem verbreiteten Netz von 'Honeypots' (Honigtöpfen), Computer mit spezieller Software zur Erfassung des Netzverkehrs, kann die Verteilung der beliebtesten Exploits und der gewöhnlich ausgenutzten Schwachstellen ganz einfach verfolgt werden. Daten, die aus einer angemessen großen Anzahl von Systemen zusammengetragen und nach ihrer Art, ihrem Ursprung und ihrem Zielort sortiert werden, bieten eine Statistik über die üblichsten Angriffe, die sichersten (oder unsichersten) geografischen Gebiete, und auch darüber, wie sich die Beliebtheit bestimmter Exploits mit der Zeit ändert.

Hier ist zum Beispiel die Liste der am meisten ausgenutzten Schwachstellen, die das Smallpot-Projekt für September 2004 zusammengetragen hat:

Vuln Name	Attack Count
Sasser worm FTPD server buffer overflow	290
Mydoom.A Backdoor execute exploit	260
Microsoft SQL Server SA password brute-force guessing	84
Dameware remote buffer overflow	64
Microsoft Knowledge Base Q313418 null password vulnerability	50
MS03-026 RPC Vulnerability	13
MS02-061 Elevation of Privilege in SQL Server	7
Mydoom.A Backdoor execute command	7
MS01-059 Unchecked Buffer in Universal Plug and Play service	4

Die am meisten ausgenutzten Schwachstellen, die das Smallpot-Projekt für September 2004 gemeldet hat

Das Institut SANS (SysAdmin, Audit, Network, Security) und das National Infrastructure Protection Center (NIPC) (Zentrum für den Schutz landesweiter Infrastruktur) beim FBI gibt ebenfalls jedes Jahr ein Dokument heraus, in dem die entscheidendsten Schwachstellen der Internetsicherheit aufgeführt sind.

Dies sind die Top 20 der Schwachstellen für 2004 von SANS:

Hauptangriffe auf Windows-Systeme

- W1 Web Servers & Services
- W2 Workstation Service
- W3 Windows Remote Access Services
- W4 Microsoft SQL Server (MSSQL)
- W5 Windows Authentication
- W6 Web Browsers
- W7 File-Sharing Applications
- W8 LSAS Exposures
- W9 Mail Client
- W10 Instant Messaging

Hauptangriffe auf UNIX-Systeme

- U1 BIND Domain Name System
- U2 Web Server
- U3 Authentication
- U4 Version Control Systems
- U5 Mail Transport Service
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layer (SSL)
- U8 Misconfiguration of Enterprise Services NIS/NFS
- U9 Databases
- U10 Kernel

Wie erkennt man eine Hacker-Attacke?

Die meisten Computerschwachstellen können auf unterschiedliche Weise ausgebeutet werden. Hacker können für ihre Angriffe einzelne spezielle Exploits, mehrere Exploits gleichzeitig, einen Konfigurationsfehler in einer Systemkomponente oder sogar ein Hintertürchen aus einer früheren Attacke nutzen.

Deshalb ist das Erkennen von Hacker-Attacken insbesondere für einen unerfahrenen Anwender keine leichte Aufgabe. Dieser Artikel enthält ein paar grundlegende Hinweise, wie man feststellt, ob ein Computer angegriffen wird oder ob die Sicherheit eines Systems geschädigt worden ist. Dabei ist zu bedenken, dass es genau wie bei Viren keine 100%ige Garantie gibt, dass man eine Hacker-Attacke so tatsächlich feststellt. Es ist jedoch gut möglich, dass Ihr System nach einem Angriff durch einen Hacker eine oder mehrere der folgenden Verhaltensweisen zeigt.

Windows-Geräte:

Verdächtig hoher abgehender Netztraffic. Wenn Sie in einem Einwählkonto sind oder ADSL verwenden und einen ungewöhnlich hohen abgehenden Datenverkehr bemerken (insbesondere wenn Ihr Computer gerade im Ruhezustand ist oder nicht gerade etwas verschickt), dann ist es möglich, dass Ihr Computer geschädigt worden ist. Es kann sein, dass Ihr Computer womöglich gerade zum Verschicken von Spam benutzt wird, oder von einem Netzwerkwurm, der sich gerade vervielfältigt und Kopien von sich verschickt. Für Kabelverbindungen ist das weniger relevant - es ist ziemlich üblich, dass es etwa die gleiche Menge abgehenden und ankommenden Datenverkehr gibt, selbst wenn Sie nichts anderes tun, als nur im Internet browsen oder Downloads machen.

Erhöhte Laufwerksaktivität oder verdächtig aussehende Dateien in den Hauptverzeichnissen von beliebigen Laufwerken. Wenn Hacker in ein System eingedrungen sind, führen viele von ihnen eine umfangreiche Suchabfrage nach interessanten Dokumenten oder Dateien durch, die Passwörter oder Logins für Bankkonten oder ePayment-Konten wie z.B. PayPal enthalten. Ebenso durchsuchen einige Würmer die Festplatte nach Dateien, die E-Mail-Adressen enthalten, um sie zur Weiterverbreitung zu benutzen. Wenn Ihnen im Zusammenhang mit verdächtigen Dateinamen in gemeinsamen Ordnern selbst im Ruhezustand des Systems eine beträchtliche Aktivität der Festplatte auffällt, so könnte das ein Zeichen für das Eindringen eines Hackers oder für eine Malware-Infektion sein.

Große Mengen an Datenpaketen, die von einer einzigen Adresse kommen und von einer persönlichen Firewall gestoppt werden. Wenn Hacker ein Ziel gefunden haben (z.B. den IP - Bereich einer Firma oder einen Pool von Kabelanwendern), lassen sie gewöhnlich automatische Suchprogramme ablaufen, die versuchen, mit den verschiedensten Exploits in das System einzubrechen. Wenn Sie eine persönliche Firewall einsetzen (ein Grundelement für den Schutz gegen Hacker-Attacken) und Ihnen auffällt, dass eine große Anzahl Datenpakete gestoppt wird, die von der selben Adresse kommen, dann ist das ein gutes Anzeichen dafür, dass Ihr Gerät gerade angegriffen wird. Die gute Nachricht dabei ist, dass Sie wahrscheinlich sicher sind, wenn Ihre persönliche Firewall diese Attacken meldet. Je nachdem, wie viele Dienste Sie zum Internet hin ungeschützt lassen, kann es jedoch sein, dass die persönliche Firewall Sie nicht gegen einen Angriff schützt, der direkt auf einen bestimmten FTP-Dienst gerichtet ist, der auf Ihrem System läuft und für alle zugänglich gemacht worden ist. In diesem Fall liegt die Lösung darin, den IP, von dem die Verletzung ausgeht, zeitweilig zu blockieren bis die Verbindungsversuche aufhören. Bei vielen persönlichen Firewalls und IDS-Systemen ist diese Möglichkeit eingebaut.

Ihr speicherresidentes Antivirus-System meldet plötzlich, dass backdoors oder Trojaner entdeckt worden sind, selbst wenn Sie gar nichts ungewöhnliches getan haben. Obwohl Hacker-Attacken komplex und innovativ sein können, benutzen viele bekannte Trojaner oder Hintertürchen, um vollen Zugriff auf ein geschädigtes System zu erlangen. Wenn der speicherresidente Teil Ihres Antivirus Schutzes solche Malware entdeckt und meldet, kann das ein Anzeichen dafür sein, dass man auf Ihr System von außen zugreifen kann.

Unix-Geräte:

Verdächtige Dateinamen im Ordner /tmp. Viele Exploits im Unix-Bereich erstellen temporäre Dateien im Standardordner /tmp, die nach dem Eindringen in das System nicht immer gelöscht werden. Das gleiche gilt für einige Würmer, von denen man weiß, dass sie Unix-Systeme infizieren; sie rekompilieren sich im Ordner /tmp und benutzen ihn als 'Ruheposition'.

Änderungen in den Binärzeichen des Systems, wie z.B. 'login', 'telnet', 'ftp', 'finger' oder noch komplexere Daemons, 'sshd', 'ftpd' und ähnliches. Ein Hacker versucht nach dem Einbruch in ein System gewöhnlich den Zugriff dadurch zu sichern, dass er ein Hintertürchen in einen der Daemons einschmuggelt, die direkten Zugriff vom Internet aus haben, oder normale Dienstprogramme des Systems modifiziert, die für die Verbindung zu anderen Systemen verwendet werden. Die modifizierten Binärzeichen gehören gewöhnlich zu einem Rootkit und sind im allgemeinen gegen eine direkte einfache Prüfung 'getarnt'. Auf alle Fälle lohnt es sich, eine Datenbank mit Prüfsummen für jedes Dienstprogramm des Systems zu führen und sie periodisch zu überprüfen, und zwar off-line im Einzelplatzmodus.

Änderungen in den Dateien /etc/passwd, /etc/shadow, oder anderen Systemdateien im Ordner /etc. Manchmal kann durch Hacker-Attacken ein neuer User in /etc/passwd angelegt werden, der dann später aus der Ferne eingeloggt werden kann. Achten Sie auf verdächtige Namen für User in der Passwort-Datei und überwachen Sie alles, was neu hinzugefügt wird, besonders in einem System mit mehreren Anwendern.

Verdächtige Dienstleistungen, die in /etc/services hinzugefügt worden sind. Das Öffnen einer Hintertür in einem Unix System ist manchmal nur eine Sache von zwei zusätzlichen Textzeilen. Das wird erreicht durch Abänderungen in /etc/services sowie in /etc/ined.conf. Überwachen Sie die beiden Dateien genau auf eventuelle zusätzliche Eintragungen, die ein Anzeichen für ein Hintertürchen sein können, das an einen unbenutzten oder verdächtigen Port gebunden ist.

Eine Analyse der Hacker-Mentalität

Warum jemand Hacker wird, ist ein häufig diskutiertes Thema. Manche sagen, die Erklärung ist die gleiche, die man auch von Leuten hört, die Berge besteigen: 'weil es sie [Computer] gibt'. Andere behaupten, dass Hacker zu einer höheren Computersicherheit beitragen, weil sie Schwachstellen deutlich machen. Und schließlich gibt es noch die Erklärung, die man am häufigsten hört: kriminelle Absicht.

Was auch immer der Grund sein mag, so lange es Computer gibt, wird es auch Hacker geben - White Hats, Black Hats und Grey Hats. Und weil man nicht vorhersagen kann, welche Art von Angriff ('Neugier' gegenüber 'Böswilligkeit') Ihren Computer zuerst treffen wird, ist es immer am besten, auf das Schlimmste vorbereitet zu sein.

Die Wahrheit ist, dass innerhalb von Stunden nachdem ein Gerät an das Internet angeschlossen wird, jemand es mit einem automatischen Prüfmittel auf Schwachstellen abtastet und Möglichkeiten sucht, hinein zu gelangen. Das kann jemand sein, der nur neugierig ist und sehen möchte, was sich auf dem Gerät befindet, oder ein White Hat vom anderen Ende der Welt, der prüft, ob der Computer sicher ist. Natürlich würden Sie im richtigen Leben nicht wollen, dass ein vorbeikommender Fremder anhält und prüft, ob Ihr Haus oder Auto abgeschlossen ist, und wenn nicht, dass er hineingeht, sich umschaut, Ihr Hab und Gut durchkramt und einen Zettel hinterlässt, auf dem steht 'Hallo, ich war hier, Ihre Tür war offen, aber kümmern Sie sich nicht um mich und, übrigens, reparieren Sie Ihr Schloss.' Wenn man nicht will, dass das im eigenen Haus passiert, will man auch nicht, dass das im eigenen Computer passiert. Und es gibt auch keine Entschuldigung dafür, so etwas dem Computer von jemand anderem anzutun.

Vorsätzliches, kriminelles Hacken ist ganz offensichtlich noch schlimmer. In der Wirklichkeit bedeutet das, jemand kommt vorbei, bricht Ihr Schloss auf, geht hinein, stellt das Alarmsystem ab, stiehlt irgend etwas oder schmuggelt Abhörgeräte in Ihr Telefon ein oder Überwachungsgeräte in Ihr Wohnzimmer. Wenn das passiert, rufen Sie die Polizei, die schauen sich um, schreiben einen Bericht, und Sie warten, dass die Diebe gefasst werden.

In der Computerwelt ist das leider ein seltener Luxus; der Täter kann weit, weit weg sein und Ihre vertraulichen Dateien herunterladen, während er in seiner privaten Villa sitzt oder an seinem riesigen Swimmingpool in der Sonne liegt, die er sich so schön mit gestohlenem Geld gebaut hat. Oder, in der Wirtschaft ziehen es viele große Unternehmen vor, Vorkommnisse mit Hackern überhaupt nicht bekannt zu geben, um ihr Firmen-Image zu schützen. Das bedeutet, dass die kriminellen Täter unbestraft bleiben.

Eine weitere Motivation für Hacker kann Vandalismus sein, oder digitale Graffiti, was man zusammenfassen kann als Einbruch in Systeme, um Zerstörung anzurichten. Die Verunstaltung von Websites ist eine sehr beliebte Form der digitalen Graffiti und es gibt einige Hacker-Gruppen, die sich ausschließlich auf diese Aufgabe konzentrieren. Genau wie in der physischen Welt außerhalb des Cyberspace, ist es eine mühsame Aufgabe, die Hooligans zu fangen, und lohnt oft den Aufwand nicht.

Wie das Hacken auch immer begründet ist, sei es 'um anderen zu helfen', 'die Sicherheit hoch zu halten', 'Vandalismus' oder 'kriminelle Absicht', es ist ein Phänomen, das tief in der Computerwelt verwurzelt ist, und wird wahrscheinlich nie aufhören. Es wird immer Leute geben, die unreif genug sind, öffentliche Ressourcen zu missbrauchen, selbst ernannte 'Robin Hoods' und Kriminelle, die sich in den dunklen Gassen des Cyberspace verstecken.

Historische Ereignisse im Hacker-Zusammenhang

Dezember 1947 - William Shockley erfindet den Transistor und führt seine Verwendung zum ersten Mal vor. Der erste Transistor bestand aus einem wirren Durcheinander von Drähten, Isolatoren und Germanium. Nach einer kürzlich von CNN's website durchgeführten Umfrage gilt der Transistor als die wichtigste Entdeckung der letzten 100 Jahre.

1964 - Thomas Kurtz und John Kemeny entwickeln BASIC, auch heute noch eine der beliebtesten Programmiersprachen.

1965 - Es sind schätzungsweise annähernd 20.000 Computersysteme in den Vereinigten Staaten im Einsatz. Die meisten davon wurden von International Business Machines (IBM) hergestellt.

1968 - Intel wird gegründet.

1969 - AMD wird gegründet.

1969 - Die Advanced Research Projects Agency (ARPA) entwickelt das ARPANET, den Vorläufer des Internet. Die ersten vier Knoten (Netzwerke) des ARPANET waren die University of California Los Angeles, University of California Santa Barbara, University of Utah und das Stanford Research Institute.

1969 - Intel kündigt 1K (1024 bytes) RAM Module an.

1969 - Ken Thompson und Dennis Ritchie beginnen die Arbeit an UNICS. Thompson schreibt die erste Version von UNICS in einem Monat auf einem Gerät mit 4KB aus 18-Bit-Wörtern. UNICS wird später in 'UNIX' umbenannt.

1969 - MIT wird zur Heimat der ersten Computer-Hacker, die damit anfangen, Software und Hardware abzuändern, damit sie besser und/oder schneller funktioniert.

1969 - Linus Torvalds wird in Helsinki geboren.

1970 - DEC führt den PDP-11 ein, eine der beliebtesten Computerausführungen überhaupt. Einige davon sind sogar heute noch in Gebrauch.

1971 - John Draper, alias 'Cap'n Crunch' zapft mit einer Spielzeugpfeife aus einer Müslischachtel Telefonsysteme an.

1971 - Für das Arpanet wird das erste E-Mail-Programm herausgebracht. Der Autor ist Ray Tomlinson, er trifft die Entscheidung, das Zeichen '@' als Trennung zwischen dem Usernamen und der Domainadresse einzusetzen.

1972 - Ritchie und Kerninghtam schreiben UNIX in C um, eine Programmiersprache, die im Hinblick auf Übertragbarkeit entwickelt wurde.

1972 - NCSA entwickelt das Tool 'Telnet'.

1973 - Gordon Moore, der Chairman von Intel, stellt das berühmte 'Moore Law' auf, das besagt, dass sich die Anzahl der Transistoren in CPUs alle18 Monate verdoppeln wird, ein Gesetzt, dass sich länger als 20 Jahre als zutreffend erweisen wird.

1973 - FTP wird eingeführt.

1974 - Stephen Bourne entwickelt die erste wesentliche Schale (Benutzeroberfläche) für UNIX, die 'Bourne Shell'.

1975 - Bill Gates und Paul Allen gründen Microsoft.

1976 - Der 21-jährige Bill Gates schreibt 'An Open Letter to Hobbyists', ein Dokument, in dem er Raubkopien von offenen Quellen und Software verurteilt.

1. April 1976 - Apple Computers wird gegründet.

1977 - Billy Joy schreibt BSD, ein weiteres UNIX-ähnliches Betriebssystem.

1979 - Microsoft erwirbt die Lizenz für den UNIX Quellcode von AT&T und entwickelt eine eigene Ausführung, 'Xenix'.

1981 - Das Domain Name System (DNS) wird geschaffen.

1981 - Microsoft erwirbt die Schutzrechte für das geistige Eigentum an DOS und nennt es MS-DOS.

1982 - Sun Microsystems wird gegründet. Sun wird berühmt für die SPARC Mikroprozessoren, Solaris, das Network File System (NFS) und Java.

1982 - Richard Stallman beginnt mit der Entwicklung einer freien Version von UNIX, die er 'GNU' nennt, eine rekursive Definition, die bedeutet 'GNU ist Nicht UNIX'.

1982 - William Gibson erfindet den Begriff 'Cyberspace'.

1982 - SMTP, das 'Simple Mail Transfer Protocol' wird veröffentlicht. SMTP ist gegenwärtig die am weitesten verbreitete Methode für den Austausch von Nachrichten im Internet.

1982 - Scott Fahlman erfindet das erste Emoticon, ' :) '.

1983 - Das Internet wird durch Aufspaltung des Arpanet in separate militärische und zivile Netzwerke gegründet.

1983 - FidoNet wird von Tom Jennings entwickelt. FidoNet wird für die folgenden 10 Jahre zum weitest verbreiteten Informationsaustausch-Netzwerk der Welt, bis das Internet an seine Stelle tritt.

1983 - Kevin Poulsen, alias 'Dark Dante' wird für den Einbruch ins Arpanet verhaftet.

1984 - CISCO Systems wird gegründet.

1984 - Fred Cohen entwickelt die ersten PC-Viren und hat die Idee für den heute gängigen Begriff 'Computervirus'.

1984 - Andrew Tannenbaum entwickelt Minix, einen freien UNIX-Klon auf der Basis einer modularen Mikrokernarchitektur.

1984 - Bill Landreth, alias 'The Cracker', wird überführt, in Computersysteme eingebrochen zu sein und auf Computerdaten der NASA und des Verteidigungsministeriums zugegriffen zu haben.

1984 - Apple führt das Macintosh System 1.0 ein.

1985 - Richard Stallman gründet die Free Software Foundation.

1985 - 'Symbolics.com' wird als erster Domainname des Internets registriert.

1985 - Microsoft gibt 'Windows 1.0' für den Markt frei, für einen Verkaufspreis von $100.

1986 - Die USA verabschieden ein Gesetz über Computerbetrug und Computermissbrauch (Computer Fraud and Abuse Act).

1986 - 'Legion of Doom'-Mitglied Loyd Blankenship, alias 'The Mentor', wird verhaftet und veröffentlicht das inzwischen berühmte 'Hacker's Manifesto'.

1988 - Die CD-ROM wird erfunden.

1988 - IRC wird eingerichtet.

November 1988 - Robert Morris startet einen Internetwurm, der Tausende Systeme infiziert und durch einen Programmierfehler Computer im ganzen Land verstopft. Dieser Wurm wird als der Morris Worm bekannt.

1989 - In den CERN Laboratorien in der Schweiz wird das WWW entwickelt.

1990 - Das Arpanet wird abgebaut.

1990 - Kevin Poulsen dringt in ein Telefonsystem in LA ein und macht sich in einem Phone-in im Radio zum Gewinner eines Porsche 944.

1991 - PGP (Pretty Good Privacy), ein leistungsstarkes, freies Verschlüsselungsprogramm wird von Philip Zimmerman herausgebracht. Die Software wird schnell zum beliebtesten Verschlüsselungspaket der Welt.

1991 - Gerüchte tauchen auf um den Computervirus 'Michaelangelo', der so kodiert sein soll, dass er seinen zerstörerischen Inhalt am 6. März startet.

17. September 1991 - Linus Torvalds bringt die erste Version von Linux heraus.

1992 - Die Phone-Phreaker-Gruppe 'Masters of Deception' wird verhaftet auf Grund von Beweisen, die durch Abhören erlangt wurden.

1993 - Der Web-Browser Mosaic wird herausgebracht.

1993 - Microsoft bringt Windows NT heraus.

1993 - Die erste Version von FreeBSD wird herausgebracht.

23. März 1994 - Der 16-jährige Richard Pryce, alias 'Datastream Cowboy', wird verhaftet und des unbefugten Computerzugriffs angeklagt.

1994 - Vladimir Levin, ein russischer Mathematiker, hackt in die Citibank ein und stiehlt 10 Mio $.

1995 - Dan Farmer und Wietse Venema bringen SATAN heraus, einen automatischen Schwachstellen-Scanner, der ein beliebtes Hacker-Hilfsmittel wird.

1995 - Chris Lamprecht, alias 'Minor Threat', ist die erste Person überhaupt, die aus dem Internet verbannt wird.

1995 - Sun startet Java, eine Computer-Programmiersprache, die so gestaltet ist, dass sie in kompilierter Form über verschiedene Plattformen übertragen werden kann.

August 1995 - Microsoft Internet Explorer (IE) wird herausgebracht. IE wird der am meisten ausgebeutete Web-Browser der Geschichte und ein Lieblingsziel für Virusautoren und Hacker.

August 1995 - Windows 95 wird gestartet.

1996 - IBM bringt OS/2 Warp Version 4 heraus, ein leistungsstarkes Multitasking-Betriebssystem mit einem neuen User-Interface, als Entgegnung zum kurz vorher erschienen Windows 95 von Microsoft. Obwohl OS/2 zuverlässiger und stabiler ist, verliert es langsam an Boden und wird ein paar Jahre später ganz eingestellt.

1996 - ICQ, der erste Instant Messenger, wird herausgebracht.

1996 - Tim Lloyd schmuggelt eine Software-Zeitbombe bei Omega Engineering, einer Firma in New Jersey, ein. Die Attacke ist vernichtend: Schäden in Höhe von 12 Mio US$ und mehr als 80 Mitarbeiter verlieren ihren Job. Lloyd wird zu 41 Monaten Gefängnis verurteilt.

1997 - DVD Format Spezifikation veröffentlicht.

1998 - Zwei chinesische Hacker, Hao Jinglong und Hao Jingwen (Zwillingsbrüder), werden von einem Gericht in China für den Einbruch in das Computernetz einer Bank und Diebstahl von 720.000 Yuan (87.000$) zum Tode verurteilt.

18. März 1998 - Ehud Tenebaum, ein sehr produktiver Hacker alias 'The Analyzer', wird in Israel verhaftet für das Eindringen in viele profilierte Computernetze in den USA.

1998 - Virus CIH erscheint. CIH war der erste Virus, der einen Inhalt hatte, der den FLASH BIOS Speicher löscht, so dass Computersysteme nicht mehr gebootet werden können, womit der Irrglaube beendet war, dass 'Viren Hardware nicht schädigen können'.

26. März 1999 - Melissa erscheint.

2000 - Ein kanadischer jugendlicher Hacker, bekannt als 'Mafiaboy' führt eine DoS-Attacke durch und macht damit Yahoo, eBay, Amazon.com, CNN und einige andere Websites unzugänglich. Er wird später zu 8 Monaten in einer Jugendstrafanstalt verurteilt.

2000 - Microsoft Corporation gibt zu, dass in ihr Computernetz eingebrochen wurde und die Codierung für mehrere kommende Versionen von Windows gestohlen wurde.

2000 - Das FBI verhaftet zwei russische Hacker, Alexei V. Ivanov and Vasiliy Gorshkov. Den Verhaftungen ging eine langwierige und komplexe Operation voraus, in deren Verlauf die Hacker zu einer 'Vorführung von Hackerfertigkeiten' in die USA gebracht wurden.

Juli 2001 - Der Wurm CodeRed erscheint. Er breitet sich schnell in der ganzen Welt aus und infiziert hunderttausend Computer in einigen Stunden.

2001 - Microsoft bringt Windows XP heraus.

18. Juli 2002 - Bill Gates verkündet die Initiative 'Trustworthy Computing', eine neue Richtung in der Strategie der Softwareentwicklung bei Microsoft, die zu mehr Sicherheit führen soll.

Oktober 2002 - Unbekannte Hacker starten einen Großangriff gegen 13 Hauptdomainserver des Internet. Das Ziel: die Adressenauflösung im gesamten Netz lahm zu legen.

2003 - Microsoft bringt den Windows Server 2003 heraus.

29. April 2003 - New Scotland Yard verhaftet Lynn Htun auf einer Londoner Computermesse, InfoSecurity Europe 2003. Lynn Htun soll unbefugten Zugriff auf viele große Computersysteme wie z.B. Symantec und SecurityFocus erlangt haben.

6. November 2003 - Microsoft verkündet einen Belohnungsfonds von 5 Mio US$. Das Geld soll erhalten, wer hilft, Hacker aufzuspüren, die es auf Anwendungen des Softwareriesen abgesehen haben.

7. Mai 2004 - Sven Jaschan, der Autor der Internetwürmer Netsky und Sasser, wird in Norddeutschland verhaftet.

September 2004 - IBM präsentiert einen Supercomputer, das schnellste Gerät der Welt. Seine Dauergeschwindigkeit beträgt 36 Billionen Operationen pro Sekunde.

Einige der größten Hacker

Dieser Abschnitt enthält kurze Informationen über einige der berühmtesten Hacker, sowohl Black Hats als auch White Hats. Die folgenden Personen sind aus den verschiedensten Gründen sehr bekannt: durch ihre Aktionen, gut oder böse, ihren Beitrag zur Entwicklung von Software und Technologie, oder ihre innovativen Methoden, Fertigkeiten und ihre Fähigkeit, kreativ zu denken.

Richard Stallman ist bekannt als der Vater freier Software. Als Stallman 1971 anfing, im Labor für künstliche Intelligenz bei MIT zu arbeiten, war er mit 'Geheimnisschutzvereinbarungen' und geschlossenen Programm-quellen konfrontiert, während er hackte und Systemtreiber 'auf traditionelle Weise' verbesserte. Nach einem interessanten Kampf um den Quellcode eines fehlerhaften Druckerprogramms gab Stallman seinen Job auf und wurde der lauteste Fürsprecher für freie Computersoftware und schuf dabei GNU und die Free Software Foundation.

Dennis Ritchie und Ken Thompson sind für zwei der größten Softwareentwicklungen des 20. Jahrhunderts berühmt: das Betriebssystem UNIX und die Programmiersprache C. Die beiden begannen ihre berufliche Laufbahn in den sechziger Jahren bei Bell Labs und revolutionierten die Computerwelt für immer mit ihren Ideen. Ken Thompson hat sich inzwischen aus der Computerwelt zurück gezogen, Dennis Ritchie ist noch bei Lucent Technology angestellt und arbeitet an einem neuen Betriebssystem, das von Unix abgeleitet ist und 'Plan9' heißt.

John Draper, alias 'Cap'n Crunch' ist berühmt für seine Fähigkeit, in Telefonsysteme einzudringen, und zwar mit nichts weiter als einer Pfeife aus einer Müslischachtel 'Cap'n Crunch' (daher der Spitzname). Außer als Vater des 'Phone Phreaking', ist John Draper auch noch berühmt dafür, dass er die vielleicht erste Textverarbeitung für IBM PCs geschrieben hat. Er leitet heute ein eigenes Sicherheitsunternehmen, entwickelt Antispam-Lösungen, vereitelt Hacker-Attacken und macht PCs sicher.

Robert Morris ist berühmt dafür, dass er 1988 den ersten Internetwurm entwickelt hat. Dieser hat Tausende Systeme infiziert und das Internet fast einen ganzen Tag praktisch zum Stillstand gebracht. Der 'Morris Worm' war vielleicht das erste vollkommen automatische Hackerwerkzeug und nutzte ein paar unkorrigierte Schwachstellen in Vax- und Sun-Computern aus.

Kevin Mitnick, womöglich der bekannteste Fall eines 'Black Hat', wurde bereits 1995 von dem Computerfachmann Tsutomu Shimomura erwischt.

Kevin Poulsen ist nach wie vor berühmt für sein Eindringen in das Telefonsystem von Los Angeles 1990. Dadurch konnte er der 102-te Anrufer in einer Radio-Telefonaktion werden und einen Porsche 944 gewinnen. Kevin Poulsen wurde schließlich gefasst und kam 3 Jahre ins Gefängnis. Er arbeitet jetzt als Kolumnist für das Online Sicherheitsmagazin 'SecurityFocus'.

Vladimir Levin, ein russischer Computerexperte, hackte sich in die Citibank und holte 10 Mio US$ heraus. Er wurde bereits 1995 von Interpol in Großbritannien verhaftet und zu 3 Jahren Gefängnis verurteilt und musste 240.015 US$ Schadenersatz zahlen.

Tsutomu Shimomura ist ein gutes Beispiel für einen 'White Hat'. Er arbeitete im Supercomputing Center in San Diego als Kevin Mitnick in sein Netzwerk einbrach und Informationen über Mobilfunktechnik und andere vertrauliche Daten klaute. Tsutomu startete die Verfolgung von Mitnick, die schließlich zu seiner Verhaftung führte.

Linus Torvalds ist bekannt als der Vater von Linux, dem beliebtesten auf Unix basierenden Betriebssystem, das heute in Gebrauch ist. Linus begann mit seiner Arbeit an einem neuen Betriebssystem 1991 und übernahm einige umstrittene Technologien für sein Projekt, nämlich das Konzept der freien Software und das System der öffentlichen Lizenz von GNU. Außerdem ist er bekannt für seine frühen Dispute mit Andrew Tannenbaum, dem Autor von Minix, das für Linus die Inspirationsquelle für das Projekt eines Betriebssystems war.

Hacker und das Gesetz

Da es Computerhacker schon seit mindestens drei Jahrzehnten gibt, haben Regierungen viel Zeit gehabt, Gesetzte über Computerkriminalität zu erarbeiten und zu verabschieden. Im Moment haben fast alle entwickelten Länder in der einen oder anderen Form Gesetze gegen Hacker oder Gesetzgebung zu Datendiebstahl oder Datenbeschädigung, die zur strafrechtlichen Verfolgung von Computerkriminalität angewendet werden können. Es gibt Bestrebungen, diese Gesetze noch zu verschärfen, was manchmal Proteste von Gruppen hervorruft, die das Recht auf Informationsfreiheit unterstützen.

In den letzen Jahren hat es viele Verurteilungen für Hacker und für unbefugten Datenzugriff gegeben. Hier sind einige davon:

> Kevin Mitnick ist wahrscheinlich einer der berühmtesten Fälle eines Hackers, der geschnappt wurde. Mitnick wurde am 15. Februar 1995 vom FBI in Raleigh, North Carolina, verhaftet, nachdem der Computerexperte Tsutomu Shimomura es geschafft hatte, ihn bis in sein Versteck aufzuspüren. Nachdem Mitnick sich zu den meisten Anklagepunkten, die gegen ihn vorgebracht wurden, schuldig bekannte, wurde er zu 46 Monaten Gefängnis und drei Jahren Bewährung verurteilt. Zusätzlich wurde er zu weiteren 22 Monaten für den Verstoß gegen Bewährungsauflagen und zu zusätzlichen Zahlungen verurteilt. Er wurde schließlich am 21. Januar 2000 aus dem Gefängnis entlassen.
>
> Pierre-Guy Lavoie, ein 22-jähriger kanadischer Hacker, wurde zu 12 Monaten gemeinnütziger Arbeit und 12 Monaten Bewährung verurteilt für betrügerische Benutzung von Computer-Passwörtern zur Verübung von Computer-Straftaten. Er wurde nach kanadischem Recht verurteilt.
>
> Thomas Michael Whitehead, 38, aus Boca Raton, Florida, war die erste Person, die nach dem Digital Millennium Copyright Act (DMCA) schuldig gesprochen wurde. Seine Strafverfolgung war Teil des vom Generalstaatsanwalt zum Thema Computer-Hacker und geistiges Eigentum eingesetzten Programms und ihm wurde vorgeworfen, Hardware zu verkaufen, die dazu verwendet werden konnte, Satellitenfernsehen von DirecTV illegal zu empfangen.
>
> Serge Humpich, ein 36-jähriger Ingenieur, wurde von der 13. Strafkammer zu einer 10-monatigen Haftstrafe verurteilt, die zur Bewährung ausgesetzt wurde. Außerdem musste er 12.000 Francs (ca. ?1,200) Geldstrafe und einen symbolischen Schadenersatz von 1 Franc an 'Groupement des Cartes Bancaires' zahlen.
>
> Am 10. Oktober 2001 wurde Vasiliy Gorshkov, Alter 26, aus Cheljabinsk, Russland, in 20 Anklagepunkten der Verschwörung, der Computerkriminalität, und des Betrugs gegen das Speakeasy Network in Seattle, Washington, die Nara Bank in Los Angeles, Kalifornien, die Central National Bank in Waco, Texas; sowie die Firma für Online-Zahlungen PayPal in Palo Alto, Kalifornien, schuldig gesprochen.
>
> Am 1. Juli 2003 wurde Oleg Zezev, alias "Alex," Staatsbürger von Kasachstan, von einem Bundesgericht in Manhattan zu mehr als 4 Jahren (51 Monate) Gefängnis verurteilt, nachdem er der ihm vorgeworfenen verbrecherischen Erpressung und des Computer-Hackens überführt war.
>
> Mateias Calin, ein rumänischer Hacker wurde zusammen mit fünf amerikanischen Staatsbürgern von einer Federal Grand Jury der Verschwörung zu einem Diebstahl von Computerausrüstungen im Wert von mehr als 10 Mio $ von Ingram Micro in Santa Ana, Kalifornien, dem größten Technologievertrieb der Welt, überführt. Mateias und sein Netzwerk warten noch auf das Urteil für diese Straftaten, wobei bis zu 90 Jahre Gefängnis herauskommen können.

Die obige Liste ist einfach eine kurze Übersicht, die illustriert, wie die Gesetzgebung zur Computerkriminalität in der ganzen Welt gegen Hacker oder allgemein zur Verurteilung von Cyberkriminalität angewendet wird. Es gibt einige Fälle, wo jemand fälschlich wegen Computerkriminalität verurteilt worden ist. Es gibt auch zahlreiche Fälle, wo Hacker immer noch die Freiheit genießen, obwohl ihr Name und ihre Identität bekannt ist. Die Zahl solcher Fälle wird jedoch Tag für Tag kleiner.

Computerkriminalität ist nichts vorübergehendes. Sie gehört zur Wirklichkeit des 21. Jahrhunderts und die weite Verbreitung des Internets und die unsicheren Systeme, die es mit sich bringt, haben die Reichweite der Computerkriminalität vergrößert. Mit ausreichend hochentwickelter Gesetzgebung und mehr internationalen Verträgen zur Cyberkriminalität, wie sie auch schon verabschiedet werden, bewegt sich die Welt hoffentlich in die richtige Richtung mit dem langfristigen Ziel, mehr Sicherheit und Gesetzlichkeit im Cyberspace zu erreichen.

Quelle: http://www.viruslist.com/de/hackers/info?chapter=153349525