



MARCELL DIETL

iPhone 3G

Schwierigkeitsgrad:



Apples iPhone ist eines der meist geliebten aber auch gehassten Mobiltelefone der letzten Jahre. Fanatiker loben es in den Himmel und Gegner kritisieren die Geschäftspolitik Apples bei jeder Gelegenheit. Was bietet das iPhone wirklich? Was ist gut, was eher schlecht?

Und wie sieht es mit dem Thema *Jailbreaking* aus? Diesen Fragen widmen wir uns im folgenden Artikel tiefergehend.

Der folgende Artikel behandelt das stark umworbene iPhone 3G von Apple und soll Ihnen als Leser eine Entscheidung zum oder gegen den Kauf erleichtern. Falls Sie nur daran interessiert sind zu sehen, was so *magisch* an diesem neuen Smartphone sein soll oder was die Gemeinde der Nutzer mit *Jailbreaking* meint, dann ist dieser Artikel dennoch für Sie interessant. Beginnen wir also ganz am Anfang: die Hardware.

Die Hardware des iPhone 3G

Besonders auffällig und von Apple immer wieder in den Vordergrund gestellt, ist das große Display des iPhones, welches über eine Multitouch -Technologie verfügt (es reagiert also nicht nur auf Berührungen mit einem, sondern auch auf gleichzeitige Berührungen mit mehreren Fingern). Der Bildschirm ist 3,5 Zoll groß und besteht aus 480 x 320 Pixeln. Ausgeliefert wird das iPhone 3G mit 8 und 16 GB Speicherkapazität und unterstützt zudem Funktechnologien wie HSDPA, GSM, UMTS etc. Die eingebaute Digitalkamera hat insgesamt 2 Megapixel und ist damit für Schnappschüsse ausreichend gut geeignet. Sie schwächelt jedoch nachts enorm und Bilder ohne ausreichend Helligkeit werden unsauber. Ein Blitz ist nicht inbegriffen, was einen leider stark abhängig

von den Lichtverhältnissen macht. Mit etwas weniger als 150 Gramm ist das iPhone leicht und wenig störend. Die relativ großen Ausmaße, welche durch den Bildschirm entstehen, stören jedoch den einen oder anderen beim ständigen Tragen des Smartphones in der Hosentasche. Mitgeliefert mit dem iPhone werden hochwertige Kopfhörer, ein USB Kabel, welches direkt an den Computer angeschlossen oder mit einem Steckdosenadapter verbunden werden kann. Handbücher, ein Reinigungstuch und andere Kleinigkeiten sind inbegriffen.

Erfahrungen beim Kauf

Will man ein iPhone (legal) in Deutschland erwerben, so führt kein Weg an einem T-Mobile Shop vorbei und auch nicht an dem damit einhergehenden Vertrag. Der meiner Meinung nach für den Normalnutzer am Besten geeignete Tarif nennt sich *Complete M* und ist auch der, welchen ich gewählt habe. Es sind 100 Freiminuten inbegriffen, 40 SMS und unbegrenzte Nutzung von WLAN und HSDPA. Sollte man sich für einen günstigeren Tarif entscheiden, ist diese Flatrate nicht enthalten, was ich für bedenklich halte, da beim iPhone schnell große Datenmengen anfallen durch Emails, Surfen, Internetradio hören und auch durch die Verbindungen, welche das iPhone zu Apples Servern in regelmäßigen Abständen herstellt. Nun zum Thema: Das iPhone kaufen! Um es in einem Wort zu sagen: Umständlich.

IN DIESEM ARTIKEL ERFAHREN SIE...

Grundlegende Information zum neuen iPhone;

Vorteile und Nachteile dieses Smartphones;

wie ein Jailbreak funktioniert, was er bietet und wo die Risiken liegen.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN...

Kein spezielles Vorwissen.

Als ich mich für einen Kauf entschied, stellte ich erstmal enttäuscht fest, dass es überall ausverkauft war und erfuhr durch Nachfragen, dass Apple nur 5000 von 35000 versprochenen iPhones bisher an Deutschland auslieferte. Mittlerweile sollte das nicht mehr der Fall sein und so wird vermutet, dass dies von Apple beabsichtigt gemacht wurde, um den Reiz, ein solches Gerät zu besitzen, noch zu erhöhen. Auf einer Warteliste mit über 80 Leuten erhielt ich komischerweise schon nach einer Woche von der Telekom einen Anruf, dass ich mein Gerät abholen könne. Also habe ich direkt am gleichen Abend den Shop aufgesucht und dann fing der Umstand an. Ich habe aufgehört zu zählen, wie viele Seiten die Verkäuferin ausfüllen musste an ihrem Terminal. Aber es waren einige. Bis endlich alles an Daten aufgenommen war, dauerte es fast eine volle Stunde. Ich bezahlte noch etwa 150 Euro für das iPhone und ging nach Hause, um es freizuschalten.

Ohne iTunes kein iPhone

Schon von der Verkäuferin wurde mir mitgeteilt, dass ich das iPhone über iTunes freischalten müsse. Das tat ich auch der Anleitung entsprechend. Dieser Schritt war sehr unkompliziert und dauerte nur wenige Minuten. Zwar könnte man argumentieren, dass nicht jeder über ein Windows oder Mac OS X System verfügt, aber die Wahrscheinlichkeit, dass sich diese Person dann ein iPhone kauft, ist gering. iTunes wird aber nicht nur benötigt, um das iPhone zu aktivieren, vielmehr ist es der Kernpunkt des Datenaustausches mit dem Gerät. Musik wird ausschließlich über iTunes übertragen, zudem lassen sich Kontakte im Adressbuch mit dem auf dem iPhone befindlichen Adressverzeichnis synchronisieren. Ohne iTunes macht das iPhone wenig Spaß und Sinn.

Was bedeutet Jailbreaking

Das iPhone bietet viele Funktionen, doch Apple hat eine strenge (und oftmals nicht nachvollziehbare) Geschäftspolitik und so lässt sich das iPhone nur um Programme und Funktionen erweitern, die Apple genehmigt und in seinen App Store aufnimmt. Anwendungen können auch nachträglich wieder entfernt

werden, sogar vom iPhone selbst (Wie dies funktioniert, dazu später mehr!). So ist zum Beispiel ein Direktzugriff auf das Dateisystem nicht möglich und genau

hier kommt der Begriff *Jailbreaking* ins Spiel. Mithilfe diverser Tools wie Pwnage, Quickpwn und Winpwn lässt sich die von Apple installierte Firmware



Abbildung 1. Der Startbildschirm von Pwnage



Abbildung 2. Pwnage baut die neue Firmware

durch eine gecrackte Version ersetzen. Hinzukommend wird ein Programm namens Cydia installiert, welches dem App Store ähnelt, mit dem Unterschied, dass alle Programme frei verfügbar sind und oftmals Funktionen bieten, welche von Apple so nicht vorgesehen waren. Eine der interessantesten Anwendungen ist das Terminal, welches Shellzugriff auf das iPhone ermöglicht, sowie die kürzlich erschienene Applikation *Backgrounder*, welche es erlaubt, Programme im Hintergrund weiterlaufen zu lassen (eine Funktion, über welche bisher nur die iPod Anwendung von Apple verfügte). Betrachten wir einmal, wie der Prozess des Jailbreakings abläuft (ausgeführt auf einem Mac OS X System mit Pwnage). Anmerkung: Ein iPhone, welches einem Jailbreak unterzogen wurde, verliert jegliche Garantie durch Apple!



Abbildung 3. Das Startlogo eines iPhones mit erfolgreichem Jailbreak

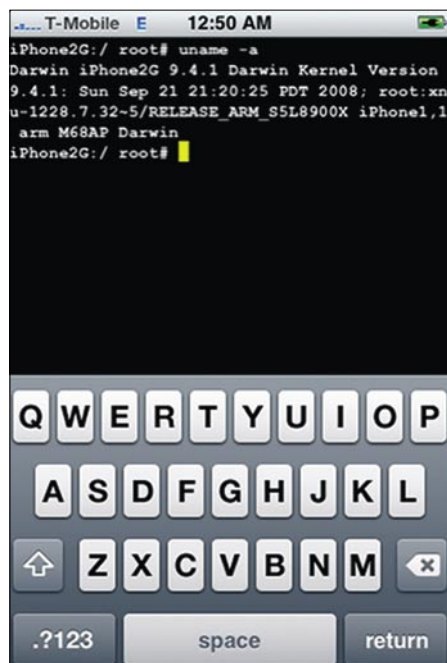


Abbildung 4. Die per Cydia installierte Terminal.app

Pwnage in Aktion

Denkbar simpel und einfach, wie man es von Macsoftware gewohnt ist, präsentiert sich das Programm Pwnage dem Nutzer beim Starten (siehe Abbildung 1). Man wählt das zu knackende Device aus und folgt den Anweisungen auf dem Bildschirm. Es gibt zwar genug Anleitungen im Internet, doch sind diese selten nötig. Die Firmware für das Apple iPhone ist zusammengefasst in einer IPSW Datei, welche man vorher in der richtigen Version von einem Apple Server herunterlädt. Dann übergibt man diese Datei dem Tool, ändert möglichst nichts an den Standardeinstellungen und sieht irgendwann einen Bildschirm, der einem mitteilt, dass die Firmware erstellt wird (siehe Abbildung 2). Dies kann bis zu 20 Minuten dauern. Anschließend wird man noch gefragt, ob dieses iPhone schonmal gecrackt wurde oder dies das erste Mal ist. Anschließend bringt man das iPhone in den sogenannten DFU (Device Firmware Upgrade) Mode, um die Firmware komplett zurückzusetzen. Dies

ist ein von Apple eingebautes Feature in iTunes, welches dazu gedacht ist das iPhone in seinen Auslieferungszustand zu versetzen, bietet sich jedoch ebenso an, um eine selbst erstellte Firmware einzuspielen. Dieser Vorgang kann auch wieder einige Minuten dauern. Ist alles erledigt, startet das iPhone neu und Sie sehen ein verändertes Bootimage (siehe Abbildung 3), welches das Logo des Pwnage Projektes darstellt. Zum Testen, ob alles geklappt hat, kann man zum Beispiel die Applikation *Terminal* installieren und ausprobieren (siehe Abbildung 4).

Backdoors und Bugs

Über die Zeit sind immer wieder Spekulationen über Backdoors im iPhone aufgetaucht und schließlich wurde man auch fündig, jedoch ist die Bezeichnung *Backdoor* meiner Meinung nach etwas unpassend. Das iPhone verbindet sich in bestimmten Abständen mit einer von Apple gehosteten Webseite, welche unter <https://iphone-services.apple.com/clbl/ unauthorizedApps> zu finden ist. Diese



Abbildung 5. Das Menü eines Plagiats aus China

Webseite enthält eine Liste namens `BlackListedApps`. Es ist also weniger eine Backdoor, welche es erlauben würde, Befehle auf dem iPhone auszuführen, als vielmehr eine Funktion unerwünschte Software zu entfernen. Offiziell soll diese Funktion gegen Malware genutzt werden, welche bestimmt bald folgen wird und wäre, wenn wirklich nur dafür eingesetzt, durchaus hilfreich und sinnvoll. Es lässt sich natürlich darüber streiten, ob es gut ist, so etwas einzubauen, aber der Hype um eine iPhone Backdoor, welcher im Internet zu finden war, war definitiv überspitzt. Die zweite Gefahr für den Nutzer sind die Bugs. Apple redet zwar von Sicherheit und stellt es als eine der wichtigsten Prioritäten dar, doch Bugs treten immer wieder auf, besonders dann, wenn es möglich ist, Third-Party-Applications (Software, die nicht von Apple selbst entwickelt wurde) zu installieren. Zu den bisher gefährlichsten Schwachstellen gehörten definitiv Möglichkeiten, Code durch den Browser Safari auszuführen als auch der im Internet viel diskutierte Fehler in der alten Firmware, welcher es erlaubte, durch einen einfachen Trick die Passworтеingabe zu umgehen.

Der Akku

Dieser Artikel wäre unvollständig, wenn nicht auch ein Absatz zu der Betriebsdauer auftauchen würde. Der Akku des iPhones ist leider sehr schnell leer. Bei einer aktiven Nutzung (zum Beispiel durch das Hören von Musik) hält der Akku keine fünf Stunden. Im Standby Modus dafür wiederum recht lange. Vorteil ist jedoch: der Akku lässt sich auch aufladen, indem man ihn an einen Computer anschließt. Zu bedenken ist auch: Der Akku wird noch schneller leer, wenn man viel Netzwerkaktivitäten verursacht. Zudem kann man gerade bei Third-Party-Applications nie sicher sein, ob die Entwickler wirklich so speicheroptimiert arbeiten, wie es Apple wünscht.

Der App Store

Wem die Standardanwendungen des iPhones nicht reichen, der kann den App Store nutzen, um weitere Programme herunterzuladen, die Auswahl ist sehr groß und von sinnfreien Spaßanwendungen bis hin zu teuren Businessanwendungen ist

so ziemlich alles dabei. Die Installation ist denkbar einfach und bezahlt wird über das iTunes Konto, welches man beim Aktivieren des iPhones registrieren musste. Bezahlung ist in Deutschland zum Beispiel per Bankeinzug über den Anbieter Click&Buy möglich. Hat man eine Applikation erworben, erscheint diese automatisch auf dem Bildschirm, kann jedoch wieder gelöscht werden. Möchte man sie erneut erwerben, muss man nicht erneut zahlen. Auch Updates sind umsonst inbegriffen. Die wohl bekannteste und am meisten für Schlagzeilen sorgende Applikation hieß *I am rich* und ließ ein rotes Symbol erscheinen. Für *günstige* 999 US Dollar. Sie wurde jedoch schnell wieder aus dem AppStore entfernt, man fragt sich jedoch, warum Apple überhaupt zugelassen hat, dass so etwas freigegeben wurde. Ein

Detail am App Store ist noch wichtig zu erwähnen: Programme, welche nur in dem amerikanischen Store zur Verfügung stehen, sind nicht auf einem deutschen iPhone installierbar. Versucht man es dennoch, erscheint eine Meldung und die Applikation wird wieder entfernt.

iPhone Development

Möchte man für das iPhone Programme schreiben, gibt es die Möglichkeit sich bei Apple das SDK (Software Development Kit) herunterzuladen mit speziellen Programmen und Dokumentationen. Alternativ kann man auch einen Vertrag abschließen, mit dem man weitere Möglichkeiten erhält, jedoch kostet dieser dementsprechend jedes Jahr Geld. So oder so muss man das Apple NDA (Non Disclosure Agreement) unterschreiben, welches man ohne zu



Abbildung 6. Gewellte Oberfläche bei einem Plagiat

übertreiben mit STFU (Shut The F*ck Up) zusammenfassen könnte, denn es enthält die klare Ansage an alle Entwickler, dass es nicht gestattet ist über das iPhone SDK und seine Funktionen zu diskutieren und wenn dagegen verstoßen wird, würde man mit Anwälten rechnen müssen. Dieses Verhalten verhindert auch, dass Bücher auf den Markt kommen, welche zeigen, wie man das SDK zum Entwickeln von Software für das iPhone einsetzt. Ein solches Buch ist zwar schon geschrieben, die Veröffentlichung wird jedoch von den Anwälten Apples verhindert. Als Beweis ein Auszug aus der Begrüßungsemail auf der Mailingliste von Apple zu diesem Thema: *Until an announcement is made otherwise, developers should be aware that the iPhone SDK is still under non-disclosure (section 5.3 of the iPhone Development Agreement). It can't be discussed here, or anywhere publicly.*

Plagiate aus China

Es ist nicht allzu überraschend, dass es Plagiate des iPhones gibt und dass diese aus China kommen. Über bestimmte Händler, kann man sich diese Geräte bestellen. Sie versprechen viel: Zwei Akkus werden mitgeliefert, es ist möglich das iPhone mit zwei SIM-Karten zu betreiben und eine Vertragsbindung mit T-Mobile ist nicht nötig. Doch das vermeintlich gute Angebot ist miserabel. Auf den ersten Blick sieht zwar alles, wie von Apple selbst hergestellt aus, doch das Apple Feeling hält genau bis zum ersten Einschalten des Gerätes, dann nämlich zeigt sich der billige Nachbau und die Lust am iPhone vergeht einem sehr schnell. Das Menü

lässt von Multitouch nur träumen (siehe Abbildung 1) und das Gehäuse ist gewellt und schlecht verarbeitet (siehe Abbildung 2). Ich kann nur jeden davor warnen, auf so etwas hereinzufallen. Wer einen Vertrag mit T-Mobile umgehen will, dem bleibt nur der Kauf eines SIM-UNlocked iPhones in einem Land wie Russland (zu einem preis von 23 000 Rubel, was ungefähr 600 Euro entspricht), jedoch ist auch hier Vorsicht geboten. Zwar lässt sich das iPhone mit jedem Anbieter wie ein normales Handy betreiben, jedoch sind die Datenmengen, welche Surfen und andere Netzwerkaktivitäten erzeugen, nicht zu unterschätzen und so kam mir von Bekannten schon zu Ohren, dass teilweise Rechnungen in Höhe von 1600 Euro nach einem Monat folgten. Da wäre ein iPhone von T-Mobile definitiv billiger gewesen (ca. 150 Euro + 24 Monate mal ca. 50 Euro = 1350 Euro).

Usability

Über die Usability des iPhones lässt sich wohl nicht allzu sehr streiten: Es ist super einfach zu bedienen und es benötigt keinerlei Anleitung. Wer ein Programm öffnen will, tippt das Symbol kurz an; will man es schließen, benutzt man den einzigen Knopf, der zur Verfügung steht – der Home-Button. Schaut man sich Fotos an, so kann man durch Drehen des iPhones deren Ausrichtung ändern. Zoomen geht durch das Benutzen zweier Finger. Zum Hineinzoomen bewegt man die Finger auseinander, zum Hinauszoomen bewegt man die Finger zueinander hin. Scrollen kann man durch das Bewegen mit dem Finger nach

oben oder unten. Um eine Webseite an einer bestimmten Stelle zu vergrößern, reicht das zweimalige Antippen des iPhones in einem kurzen Abstand oder die gleiche Methode, die auch bei den Fotos funktioniert. Dieses oftmalige Berühren des Displays erzeugt eine Menge Spuren der Finger, doch ist die Reinigung des iPhones mit einem Tuch sehr schnell erledigt. Jedoch sollten Sie mit Wasser vorsichtig sein, da das iPhone in Tests eine besondere Empfindlichkeit gegenüber diesem Element ergab.

Kaufen: Ja oder Nein?

Diese Frage ist pauschal nicht zu beantworten. Als User von Mac OS X, macht das iPhone natürlich enorm Spaß und man fühlt sich heimisch. Als normaler Anwender, der nur SMS schreiben und telefonieren will, lohnt sich diese Anschaffung gewiss nicht. Inwiefern das iPhone für die Wirtschaft geeignet ist, wird derzeit zwar noch diskutiert, aber dennoch haben sich schon große Konzerne für den konzernweiten Einsatz entschieden. Im Endeffekt bleibt es jedem selbst überlassen, ob er sich für dieses Gerät entscheidet. Für Personen, die gerne an etwas herumspielen und viele kleine Gimmicks schätzen, ist es definitiv eine gute Wahl. Dennoch gibt es günstigere Alternativen, die man durchaus in Betracht ziehen sollte. Ich hoffe, dass Ihnen dieser Artikel geholfen hat, einen Überblick über die verschiedenen Besonderheiten des iPhones zu gewinnen. Ansonsten empfehle ich, die weiterführenden Links in der Kategorie *Im Internet* durchzulesen.

Im Internet

- <http://wikee.phwn.org/> – Ein Wiki rund um das Hacken/Cracken eines iPhones;
- <http://blog.iphone-dev.org/> – Der Blog des iPhone Dev Teams ist der wichtigste Anlaufpunkt für Informationen rund um Jailbreaking;
- <http://www.t-mobile.de/iphone/> – Informationen zum Kauf des iPhones bei T-Mobile;
- <http://www.apple.com/de/iphone/> – Informationen rund um das iPhone 3G von Apple;
- <http://www.hackint0sh.org/> – Die bekannte Hakint0sh Community, welche sich mit Hacks rund um (Mac) OS X beschäftigt und auch HowTo's rund um das iPhone anbietet;
- <http://www.winpwn.com/> – Die WinPwn Projektseite zum Jailbreaken des iPhones auf Windows XP/Vista;
- http://de.wikipedia.org/wiki/Apple_iPhone – Ein sehr ausführlicher Artikel von Wikipedia mit vielen weiterführenden Links;
- <http://developer.apple.com/iphone/> – Das von Apple für Entwickler betriebene iPhone Dev Center.

Marcell Dietl

Der Autor beschäftigt sich seit einigen Jahren mit Computersicherheit und anderen Aspekten der Information Technology. Durch den Kauf eines iPhones ist nun auch sein Interesse an OS X Sicherheit gestiegen sowie an dem Thema der Mobile Device Malware. Seinen persönlichen Blog Wired-Security.net, auf dem auch mehrere Einträge zum Thema iPhone zu finden sind, betreibt er seit Anfang des Jahres. Kontakt mit dem Autor: skyouit@wired-security.net