Mac OS X 10.3.4

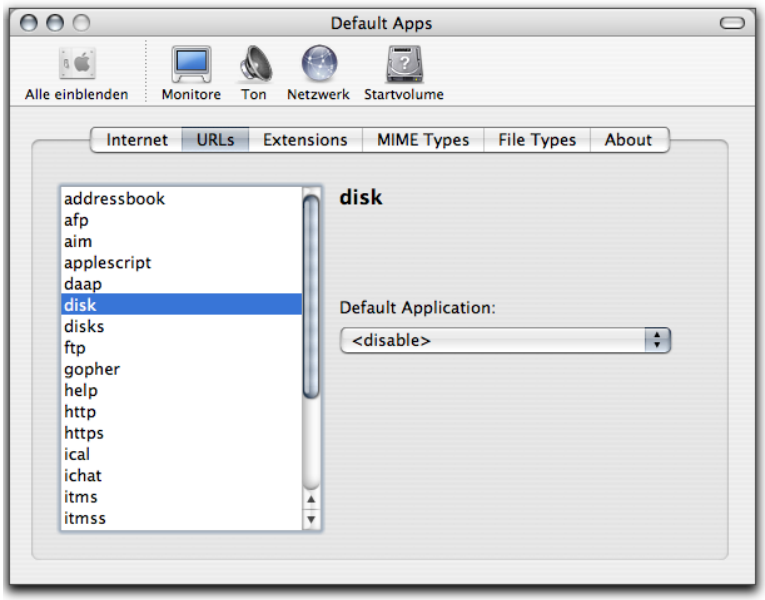
Seit kurzem ist ein Update auf Mac OS X 10.3.4 auf der Web-Seite von Apple erhältlich. Es gibt eine weniger umfangreiche Variante, mit der man Mac OS X 10.3.3 auf 10.3.4 bringt. Das deutlich größere **Combo-Update** lässt sich dagegen mit jeder Version von Mac OS X 10.3 verwenden. Wer einen Breitbandanschluss hat, sollte auf jeden Fall das Combo-Update aus dem Internet laden, da dieses erfahrungsgemäß weniger Probleme bereitet und man außerdem bei einer Neuinstallation von Mac OS X 10.3 anschließend nur ein Update installieren muss. Alternativ zum schnellen DSL-Anschluss kann man auch einen Teilnehmer von iMove.org in Anspruch nehmen, die anderen Anwendern die Software auf eine CD brennen.

Neue Funktionen gibt es kaum, Apple hat hauptsächlich Fehler behoben und außerdem das System in Sachen Geschwindigkeit noch etwas optimiert, so dass beispielsweise etliche Programme schneller starten als bisher. Hand angelegt haben die Programmierer unter anderem an die Programme Mail und Adressbuch. Neu ist in Mail die Möglichkeit, im Zip-Format komprimierte Anhänge zu speichern, ohne sie automatisch auspacken zu müssen. Eine weitere Neuerung zeigt sich in der iPod-Unterstützung: die neueren Geräte mit USB-2.0-Anschluss lassen sich nun auch am Mac über diese Verbindung nutzen. Apple empfiehlt aber weiterhin die Anbindung über Firewire, weil nur dann auch das gleichzeitige Laden der iPod-Batterie möglich ist. Verbessert wurde außerdem die Zusammenarbeit mit externen Laufwerken, die Übertragung von Videos von der Kamera auf ein Powerbook und das Ausdrucken von schattiertem Text. Mit Ausnahme des aktuellen Sicherheitsupdates vom 24. Mai sind im Update auf 10.3.4 auch alle vorherigen Sicherheitsupdates enthalten.

Sicherheitsprobleme

Vor kurzem ist bekannt geworden, dass in Mac OS X ein paar Sicherheitslöcher existieren, die es theoretisch ermöglichen, bei aktiver Internetverbindung einen Programmcode auf den Rechner zu übertragen, der sich dann ferngesteuert starten lässt und im Privatordner des aktiven Anwenders Daten löschen könnte. Eine Variante verwendet ein automatisch übertragenes und auf dem Schreibtisch von Safari aktiviertes **Disk Image** sowie das Programm **Help Viewer**, das dann das auf dem Disk Image eingeschleuste Script ausführt. Dieses Loch hat Apple mit dem Sicherheitsupdate 2004-05-24 gestopft, das eine neue Version des Help Viewers installiert, die Scripts nicht mehr automatisch starten kann. Man sollte dieses Sicherheitsupdate unbedingt installieren und außerdem in **Safari** die Option „Sichere" Dateien nach dem Laden öffnen in den Voreinstellungen ausschalten.

Auch das Update auf Mac OS X 10.3.4 schließt ein Loch nach draußen, über das sich theoretisch mit den Protokollen Telnet und ssh Programme auf dem Rechner ohne Zutun des Anwenders ausführen ließen. Ganz sind die potentiellen Angriffsmöglichkeiten damit aber noch nicht aus der Welt geschafft, da es immer noch theoretisch möglich wäre, ein Schadprogramm über das Internet auf den Rechner zu übertragen und dann ferngesteuert über einen **URI** (Uniform Resource Identifier) zu starten. Abhilfe schafft die Systemeinstellung RCDefaultApp 1.1.1, mit der man die entsprechenden URIs deaktiviert. Dazu installiert man die kostenlose Systemeinstellung, startet sie und begibt sich in die Abteilung URL. Dort stellt man für folgende URLs im Aufklappmenü <DISABLE> ein: AFP, DISK, DISKS und FTP.



(Mit Hilfe dieser Systemeinstellung lassen sich außerdem die Standardprogramme für Mail und Web einstellen, falls man andere Anwendungen als Safari und Mail benutzen möchte.)