Mac OS X Sicherheitsratgeber I: Innere Sicherheit

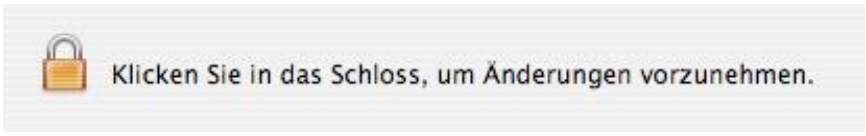
Wie macht man den Mac gegen unbefugten Zugriff sicher?

Mac OS X gilt als sicher. Das ist sicherlich auch seinem geringen Verbreitungsgrad zu verdanken, ein System, das nur 5 Prozent Marktanteil hat ist für Skript-Kiddies und andere Bösewichte, die es auf die Verursachung eines möglichst großen Schadens abgesehen haben, uninteressant.

So gibt es für das System bisher kaum Dialer, Trojaner und Viren. Und die, die es gibt, sind so selten, dass es wirklich ein Glücksfall wäre, wenn einer seinen Weg auf die Festplatte findet. Doch das heißt nicht, dass es sie niemals geben wird.

Mac OS X - aber sicher

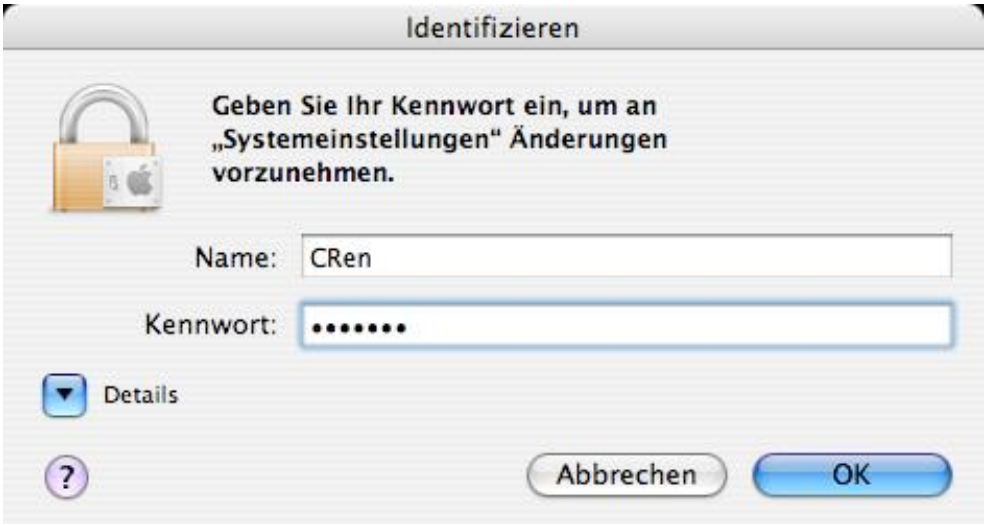
Mac OS X gilt als so sicher, dass sogar das FBI dazu übergegangen ist, Macs als Arbeitsplatzrechner einzusetzen. Doch nur die Tatsache, dass bösartige Programme so gut wie nicht verfügbar sind, gibt noch keine Garantie, dass vertrauliche Daten nicht doch ihren Weg in unbefugte Hände finden. Diese Serie soll zeigen, wie Mac OS X weitestgehend gegen Zugriff nicht berechtigter User abgedichtet werden kann.



Zuallererst sollte folgende Regel gelten: Genau wie jede andere komplexe Software kann es bei Mac OS X durchaus zu Sicherheitslücken kommen. Diese werden aber in der Regel recht schnell von Apple behoben. Daher sollte jeder Macuser mindestens einmal wöchentlich über die Software-Aktualisierung nach neuen Software-Updates schauen. So können eventuell entdeckte Lücken schnell geschlossen werden.

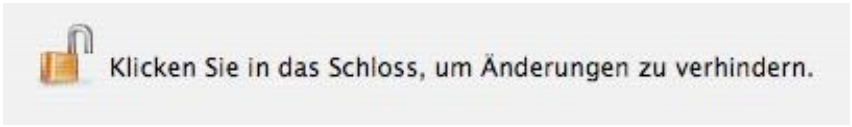
Teil 1: Das Einbruchs-Szenario

Doch neben der Bedrohung aus dem Internet gibt es natürlich auch das klassische Szenario des Datenklaus, nämlich den Diebstahl des Rechners bei einem Einbruch oder der schnelle Blick des konkurrierenden Mitarbeiters in der Firma. In beiden Fällen könnte auch bösartige Software auf dem Rechner installiert werden. Denn wie bei Windows hat der Haupt-User erstmal Admin-Zugriff auf das System, darf installieren, löschen und bearbeiten, was ihm lieb ist.



Schutzmaßnahme 1: Passwörter

Ab Werk verlangt OS X nur in den seltensten Fällen Passwörter, zum Beispiel bei der Installation Systemrelevanter Software wie Updates oder Unix-Tools. Um anderen den Zugriff zu erschweren, sollten die Systemeinstellungen bemüht werden (Programme-> Systemeinstellungen oder im Dock).

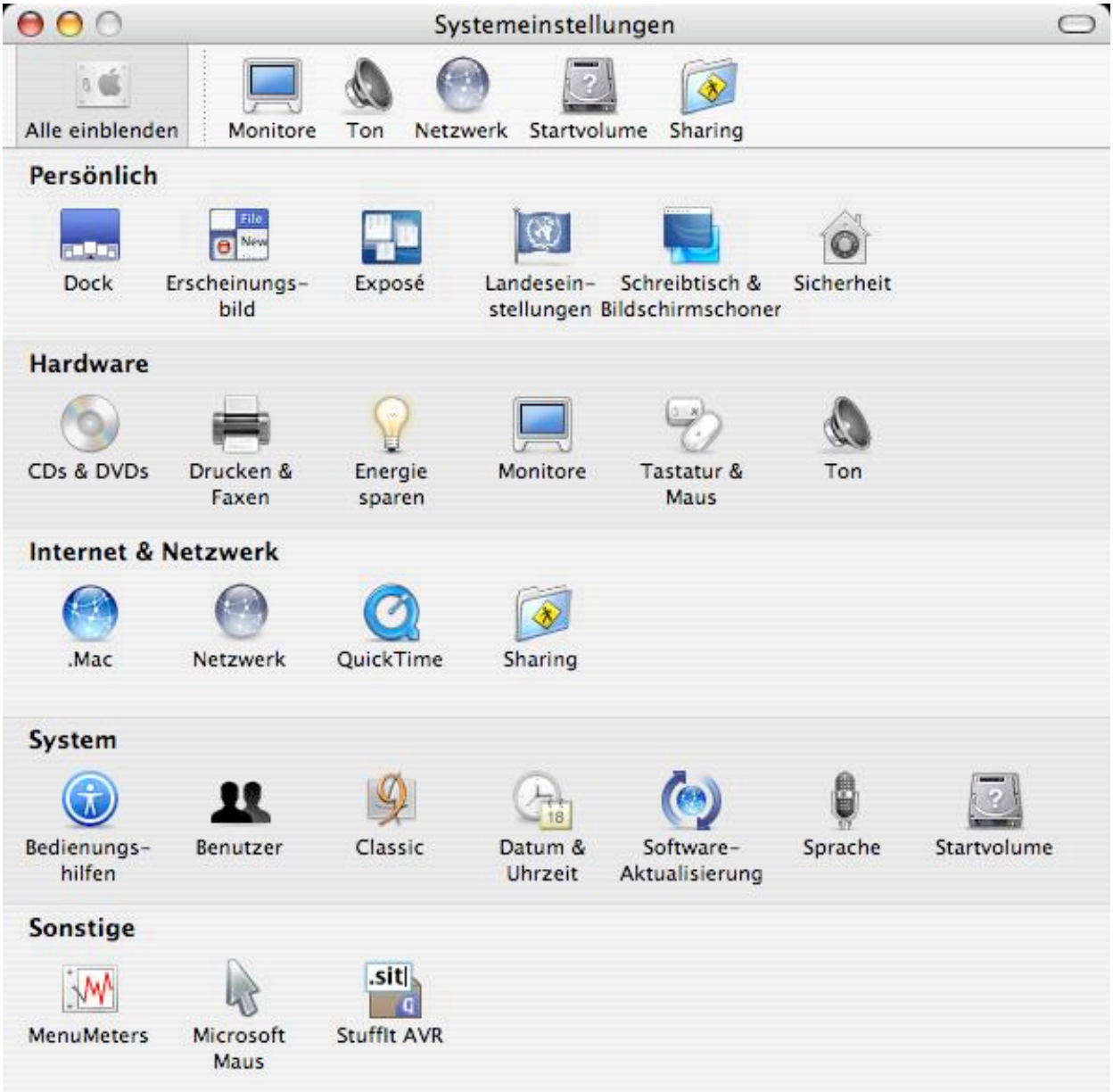


Bei der Installation wurde ein Admin-Kennwort angegeben. Dieses Admin-Kennwort wird verlangt, wenn systemrelevante Software installiert werden soll. Damit lässt sich, wenn man als Admin unterwegs ist, bereits einiges für die Sicherheit tun.

Mac OS X Sicherheitsratgeber I: Innere Sicherheit

Wie macht man den Mac gegen unbefugten Zugriff sicher?

Unter dem Punkt "Sicherheit" in den Systemeinstellungen findet sich der Punkt "Sicherheit". Der Punkt "Beim Beenden des Ruhezustandes oder Bildschirmschoners ein Kennwort verlangen" sorgt dafür, dass der Rechner nicht problemlos von Unbefugten aus dem Ruhezustand geweckt werden kann. Dazu muss der Ruhezustand natürlich aktiviert sein (Systemeinstellungen -> Energie sparen").



Automatische Anmeldung deaktivieren

"Automatisches Anmelden deaktiveren" verlangt beim Systemstart und beim Login ein Passwort. Durch diese Option lässt sich sicherstellen, dass ein Hard-Reset nicht den Zugang zum Rechner öffnet. Ganz nebenbei kann auch nicht jeder Nutzer auf jeden Benutzeraccount zugreifen, sondern nur auf den, für den er berechtigt ist.

"Für das Freigeben jeder geschützten Systemeinstellung ein Kennwort verlangen" macht die Systemeinstellungen dicht. Nach Aktivierung dieser Option können systemrelevante Funktionen wie die Sicherheitseinstellungen, die Benutzerverwaltung oder die Netzwerkeinstellungen nur noch mit dem Admin-Kennwort geöffnet werden. Wird diese Option deaktiviert, sind die anderen eher sinnlos, weil sie von jedem Benutzer verändert werden können.

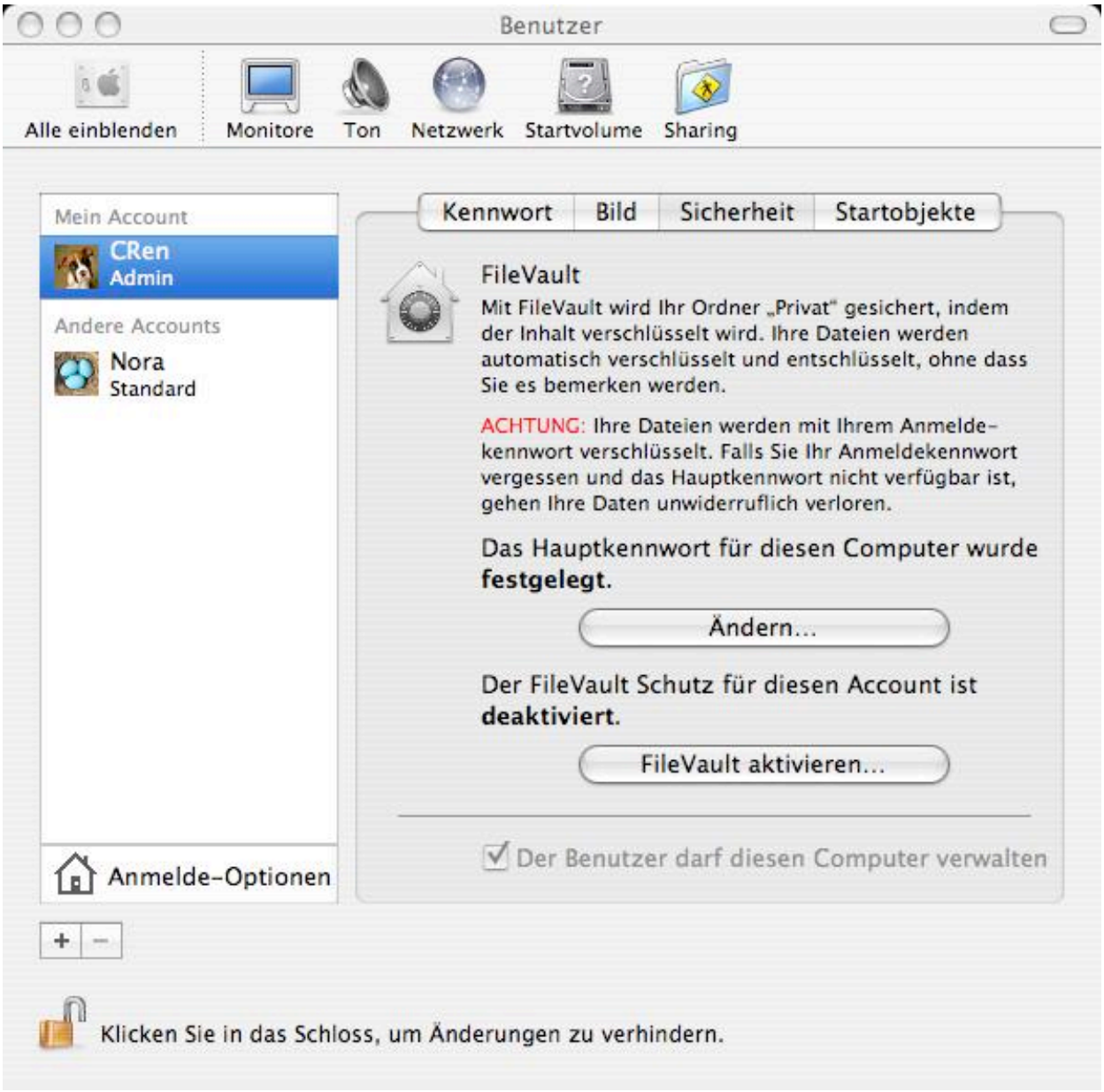
Kennwort-Schutz ist Dialer-Schutz

Durch den Kennwort-Schutz ist es, anders als bei Windows, sporadisch vorkommenden Dialern nicht möglich, sich ohne Wissen des Nutzers als Standard-Verbindung einzutragen. Denn selbst, wenn der User als Admin unterwegs ist, wird immer ein Passwort verlangt, wenn Änderungen in den Systemeinstellungen vorgenommen werden sollen.

Schutzmaßnahme 2: FileVault

Eine weitere Gefahr für die Daten auf dem Rechner liegt auf der Hardware-Seite. Jeder Mac kann durch das Drücken der Taste "T" beim Systemstart in den "Target Disc Mode" gebootet werden. Auf diese Weise kann der Mac über die Firewire-Schnittstelle wie eine externe Festplatte angesprochen werden, auch von Windows- oder Linux-Nutzern, sofern sie die nötigen Treiber für das Mac-Filesystem installiert haben.

Da diese Funktion fest in der Firmware implentiert ist, ist es unmöglich, dies zu verhindern. Ein Bösewicht könnte seinen Laptop mit einem Firewire-Kabel an den Mac klemmen, diesen im Target-Disc-Mode booten und auf diese Weise die Daten vom Rechner stehlen. Die Schutzmaßnahmen des Betriebssystems versagen hier, weil der Target-Disc-Mode vor dem Booten des Systems greift.



Sicherheitslücke Target-Disc-Mode

Um wenigstens zu verhindern, dass diese Daten im Klartext erscheinen, gibt es die Möglichkeit, die Daten im Benutzer-Ordner mit FileVault zu verschlüsseln. Dazu muss nur der Punkt "FileVault aktivieren" angeklickt werden und schon wird der Benutzerordner mit einem 128-Bit-Schlüssel verschlüsselt. Zwar kann der Bösewicht den Benutzerordner dann immer noch von dem Rechner klauen, die Chance, an die Daten innerhalb des Ordners zu kommen, verringert sich aber extrem.

Mac OS X Sicherheitsratgeber I: Innere Sicherheit

Wie macht man den Mac gegen unbefugten Zugriff sicher?

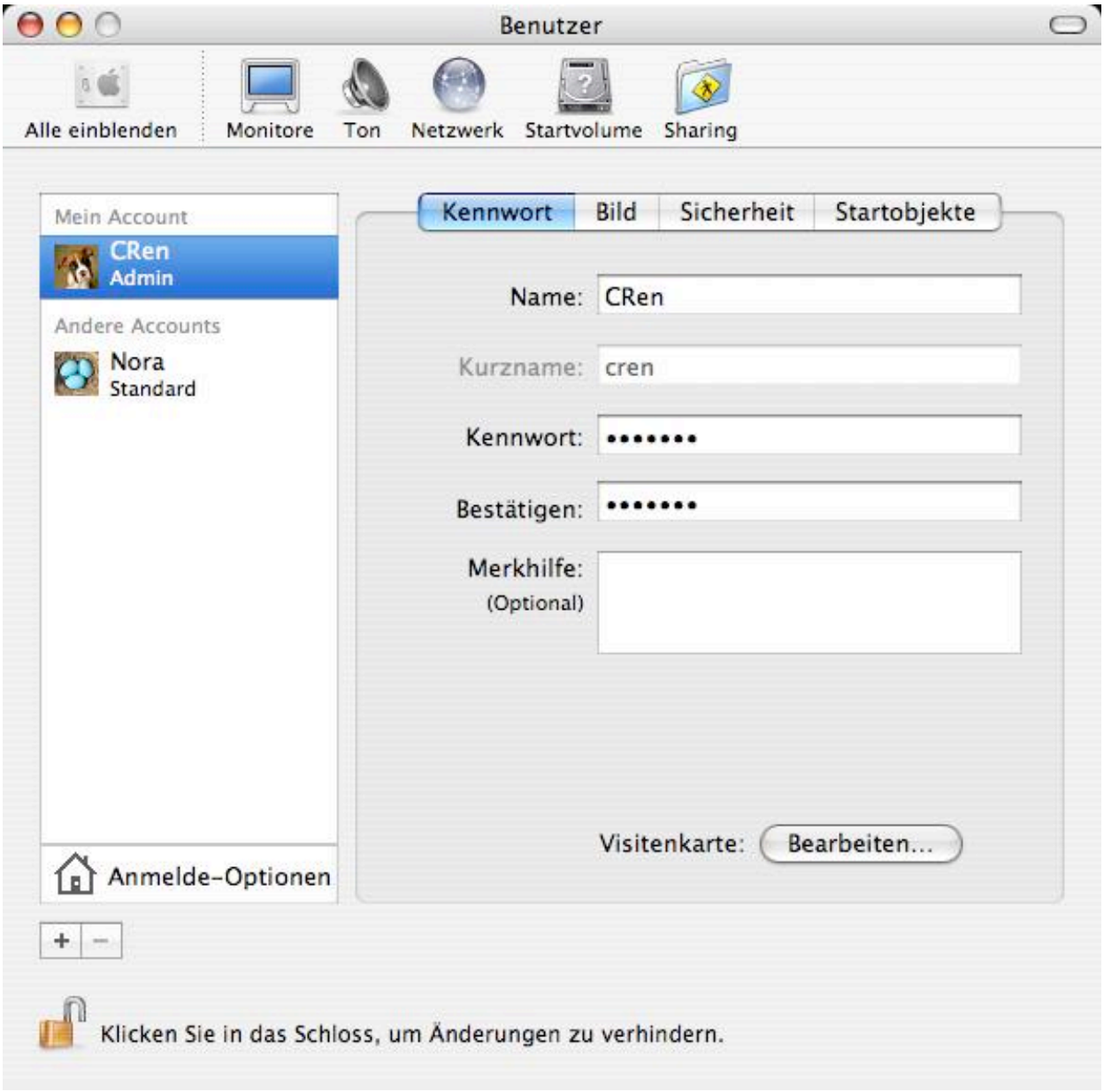
Leider ist der Einsatz von FileVault auf älteren Systemen nicht zu empfehlen, die Ver- und Entschlüsselung erfolgt in Echtzeit und ist dementsprechend träge. So wurde bereits von Performance-Einbußen um die 50 Prozent berichtet, realistisch ist aber ein Performance-Verlust von 10 - 20 Prozent.

Klartext-Sicherung empfohlen

Zudem sollte FileVault nur genutzt werden, wenn regelmässige Klartext-Backups der Daten erstellt werden. Sollte sich Mac OS X nämlich tatsächlich einmal aufgrund eines technischen Problemes verabschieden, kommt man über den für solche Fälle hilfreichen Target-Disc-Mode nicht mehr an die Daten heran. Die Sicherheitskopien allerdings sollten im Tresor gelagert werden, denn sonst macht FileVault wenig Sinn.

Schutzmaßnahme 3: Eingeschränkte Benutzer-Accounts

Wenn mehrere Benutzer an einem Rechner arbeiten, ist es hilfreich, die Benutzeraccounts zu beschränken. Mac OS X hat bereits ab Werk den aus Unix bekannten Root-User deaktiviert, selbst der Admin kann nicht ohne Tricks einfach in den Systemordnern herumfuhrwerken. Dennoch sollten Accounts für Kinder oder andere Nutzer des Systems tiefgehender beschränkt werden.



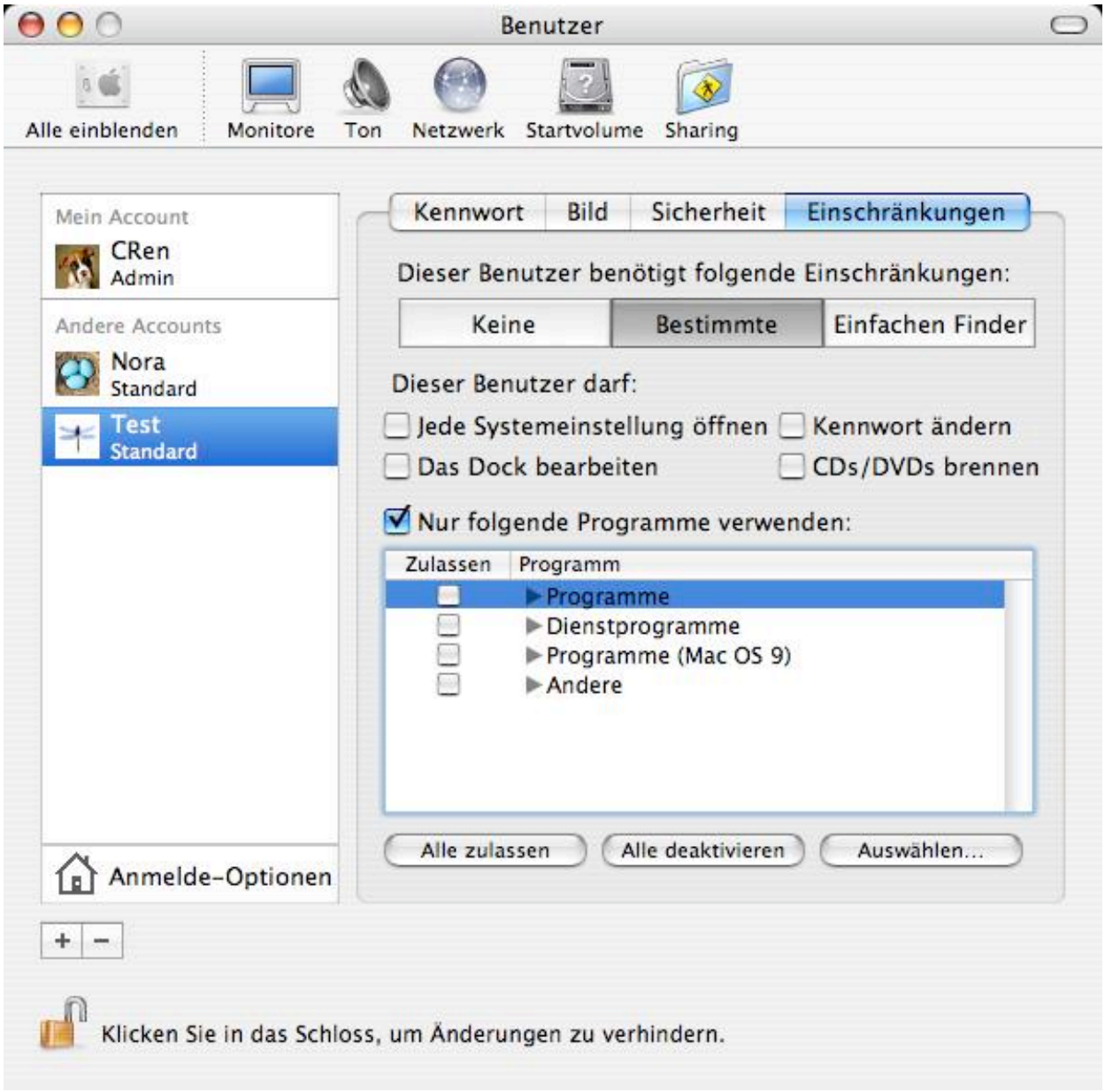
Dazu muss die die Benutzerverwaltung (Systemeinstellungen -> Benutzer) bemüht werden. Mit dem kleinen "+" unten links lässt sich ein neuer Nutzer samt Kennwort und Bildchen anlegen. Nun kann unter dem Tab "Sicherheit" wieder "FileVault" aktiviert werden.

Hauptkennwort festlegen

Zudem lässt sich ein Hauptkennwort für das System erstellen, dass dem Admin den Zugriff auf jeden Benutzer-Account sichert, zum Beispiel für den Fall, dass ein User sein Kennwort vergessen hat. Für eingeschränkte Benutzer darf keinesfalls der Punkt "Der Benutzer darf diesen Computer verwalten" aktiviert werden, über diesen Punkt werden nämlich Admin-Rechte vergeben.

Das Tab "Einschränkungen" bietet weitere Möglichkeiten, einem Benutzer die Rechte zu nehmen. Hier lässt sich der Account wahlweise ohne Beschränkungen, also als Hauptbenutzer oder mit bestimmten Beschränkungen erstellen. Ein Hauptbenutzer hat ähnliche Rechte wie ein Admin, darf also installieren und ausführen was er möchte, was nicht empfehlenswert ist.

Programmzugriff einschränken



Im Unterpunkt "Bestimmte" kann nun ausgewählt werden, ob der Benutzer für seinen Account die Systemeinstellungen und das Dock bearbeiten darf, ob er sein Kennwort ändern und Zugriff auf Wechseldatenträger erhalten soll. Zudem lässt sich der Zugriff auf Programme beschränken. Auf diese Weise kann der Admin genau bestimmen, welche Programme von welchem Nutzer gestartet werden dürfen.

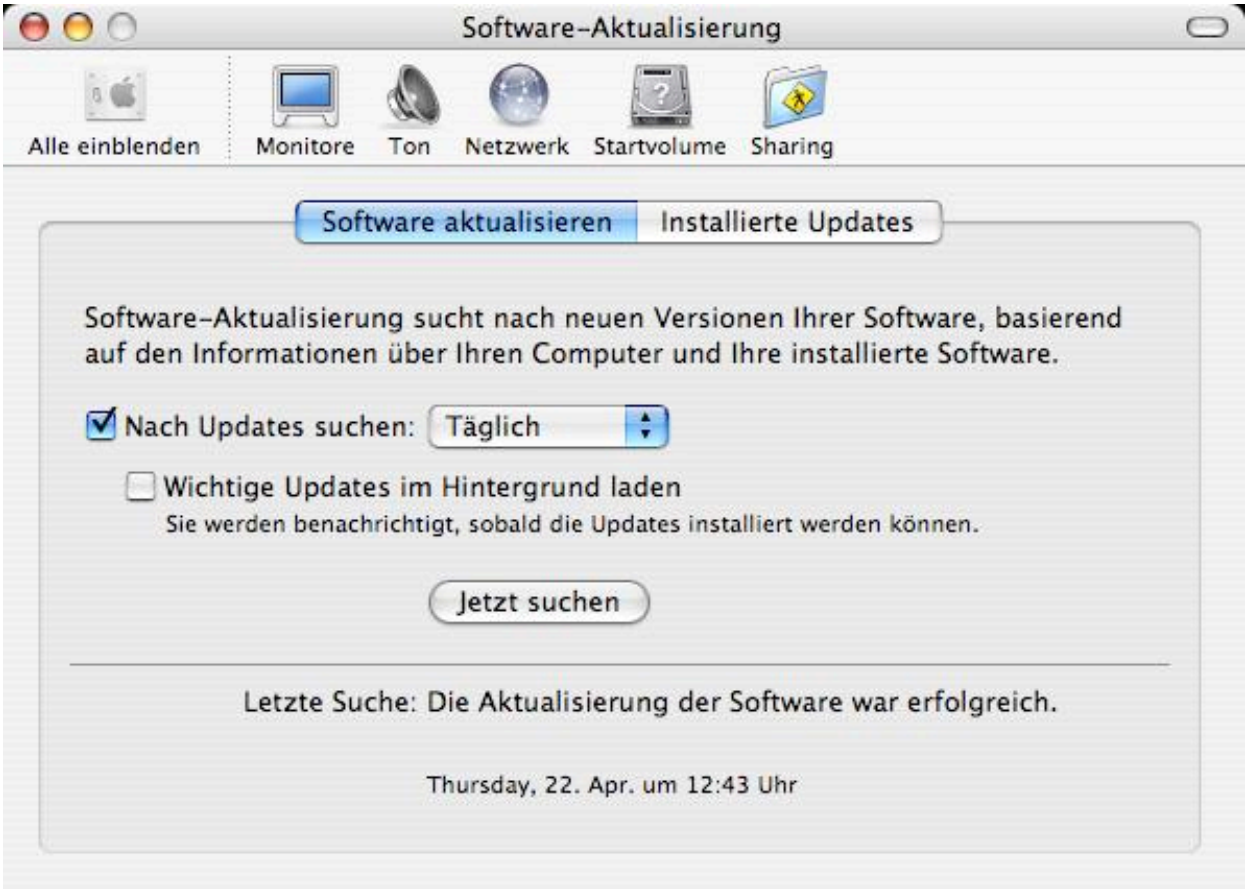
Mac OS X Sicherheitsratgeber I: Innere Sicherheit

Wie macht man den Mac gegen unbefugten Zugriff sicher?

Familienvätern gibt das die Möglichkeit, ihren Kindern den Vollzugriff auf die Office-Programme und Spiele zu geben, den Account aber ansonsten vollkommen abzudichten. Die meisten Programme für Mac OS X unterstützen übrigens diese Multiuser-Funktionalität, wodurch beispielsweise Word, Safari oder Mail für jeden Benutzer einen von den anderen Nutzern getrennten Account anlegt.

Unterordner verwenden

Eine weitere Möglichkeit, anderen den Zugriff auf bestimmte Programme zu verbieten ist übrigens die Installation von Software im Unterordner "Programme" des Admin-Accounts. Auf diese Weise kann nur der Herr über einen Account auf bestimmte Programme zugreifen. Umgekehrt werden Installationen von beschränkten Benutzern nicht im Programme-Ordner im Hauptverzeichnis, sondern innerhalb des jeweiligen Benutzerordners ausgeführt. So könnte der Kinder-Account sämtliche Spiele in diesem Ordner bereithalten, ohne dass das restliche System davon betroffen wäre.



Der letzte Tab im Einschränkungen-Menü erlaubt es zusätzlich, die Anzeige des Finders und des Docks einzuschränken. So können eingeschränkte Benutzeraccounts diese Programme nicht einmal sehen, geschweige denn ausführen.

Achtung, Anmeldeoption

Zuguterletzt sollte ein Blick auf den Punkt "Anmelde-Optionen" unten links geworfen werden. Dort muss der Punkt "Automatisch anmelden als" deaktiviert werden, ansonsten umgeht er nämlich die Anmelde-Optionen aus den Sicherheitseinstellungen.

Der schnelle Benutzerwechsel ist ebenfalls mit Vorsicht zu genießen. Er erlaubt, "mal schnell" den Account zu wechseln, um Töchterchen beispielsweise schnell ihre Mails checken zu lassen. Es gilt aber zu bedenken, dass durch

diese Option der andere Nutzer nicht wirklich abgemeldet ist, im Zweifelsfall kann ein Bösewicht auf diese Weise trotz eingeschränktem Account Zugriff auf sensible Daten bekommen.

Auftrag erfüllt

Insgesamt sollten die vertraulichen Daten auf dem Mac mit diesen Maßnahmen gegen den direkten Zugriff geschützt sein. Im zweiten Teil der Serie wird erklärt, wie sich Mac OS X mit Bordmitteln gegen die Gefahren des Internets absichern lässt.

Mac OS X Sicherheitsratgeber II: Äußere Sicherheit

Mac OS X im Netz dicht machen

Der moderne Mac ist als Internet-Computer konzipiert. Dadurch ist die Zeitspanne bis zum Erreichen des "Ich bin drin"-Moments auch oftmals wesentlich kürzer als bei Windows- oder Linux-Rechnern. Doch die nützliche Verbindung ins Internet bringt auch einige Gefahren mit sich. Diese lassen sich beim Mac allerdings, im Gegensatz zu den Mitbewerbern im Windows-Lager, mit Bordmitteln abstellen.

Im ersten Teil des Mac OS X Sicherheitsratgebers wurde der Mac gegen physische Attacken böswilliger Nutzer abgedichtet, der direkte Zugriff auf persönliche Daten wurde unterbunden. In diesem Teil der Serie soll der Mac nun gegen Angriffe aus dem Netzwerk, also auch dem Internet abgesichert werden. Dazu bedarf es allerdings erstmal ein wenig Theorie.

Die Sache mit dem Unix-Unterbau

Zuerst einmal sollte angemerkt werden, dass Mac OS X auf dem Open-Source-Unix "OpenDarwin" basiert. Dieses wiederum ist ein Ableger von FreeBSD. Da dieses System normalerweise auf Servern eingesetzt wird, erfüllt es entsprechend hohe Sicherheitsstandards. Dazu zählen unter anderem eine komplexe Rechteverwaltung und vollständige Unterstützung für Multitasking und mehrere Benutzer.

Kommandozeilen-Fetischisten können also im Zweifelsfall auch Unix-mässig über das Terminal (Programme -> Dienstprogramme ->Terminal) in den Funktionen herumpfuschen, wie es zum Beispiel auch bei Linux möglich ist - die Befehle sind ähnlich, oft sogar identisch. Die Aqua-Oberfläche des Betriebssystems ist quasi ein fest integrierter Aufsatz, der die Unix-Funktionen über ein schickes grafisches Benutzerinterface steuert.

Fummel-faule Macuser

Da Mac-User aber meist keinen Wert auf die Fummelei im Terminal legen, sondern den Mac wegen seiner einfachen Bedienung gewählt haben, soll die Kommandozeile hier außen vor bleiben. Stattdessen sollen die Einstellungen in der grafischen Benutzeroberfläche erklärt und Tipps zur Absicherung gegeben werden.

Übrigens: Mac OS X bringt nahezu alles mit, was nötig ist, um den Rechner im Netzwerk sicher zu machen. Die Unix-Wurzeln sind also unverkennbar. Aus diesem Grunde ist es auch, anders als bei Windows, nicht nötig, sich zusätzliche Tools von Drittanbietern wie Firewalls zu installieren, um einen Mac zu sichern. Mac OS X hat seine Firewall an Bord.

Schutzmaßnahme 1: Die Datei-Rechte

Unix-Systeme kommen von Haus aus mit einer höchst komplexen und sicheren Rechteverwaltung. Das verhindert einerseits, dass Angreifer den Root-Zugriff auf das System erhalten können, sorgt aber andererseits dafür, dass manche Dinge schlicht und einfach nicht möglich sind. Dazu zählen zum Beispiel die von Windows bekannten Datei-

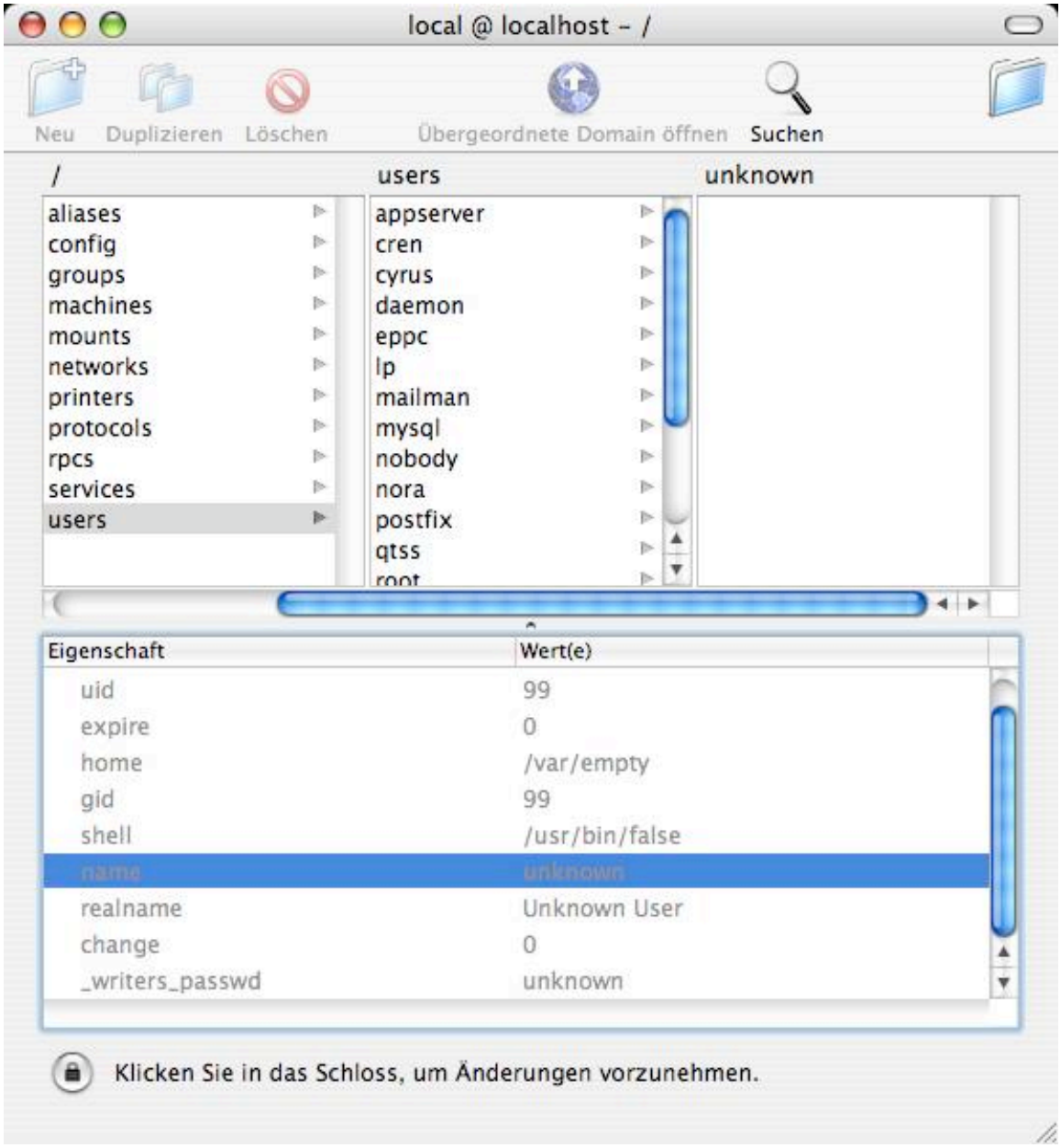
und Ordnerfreigaben.

Mac OS X Sicherheitsratgeber II: Äußere Sicherheit

Mac OS X im Netz dicht machen

Diese erlauben es Windows-Usern, einen beliebigen Ordner im Netzwerk freizugeben. Das ist im Netzwerkbetrieb sinnvoll, im Internet hingegen erlaubt es Angreifern hingegen im Zweifelsfall, Dateien auszulesen, die nicht für ihre Augen bestimmt sind. Bei extrem schlecht gesetzten Freigaben ist sogar der Vollzugriff über das System möglich.

Gott ist Root-User...



Mac OS X hingegen ist bereits ab Werk mit sicheren Freigaben bestückt. Zum Beispiel kann ein User aus dem Netz nur auf den Rechner zugreifen, wenn er die Zugangsdaten zu einem Account kennt. Allerdings kann dieser Nutzer sich dann ausschließlich in seinem Account bewegen. Es sei denn, er hat Admin- oder gar Root-Rechte.

Der Root-User ist in Unix-Systemen eine Art Gott. Er kann tun und lassen, was er möchte, Systemdateien ändern oder ersetzen, Benutzerkonten anlegen oder löschen und so das ganze System destabilisieren. Kommt das Passwort des Root-Nutzers in die falschen Hände, sind alle Sicherheitsmaßnahmen müßig.

...und wird deshalb ausgeschaltet

Dieser Problematik war sich auch Apple bewusst. Deshalb ist der Root-User auch standardmäßig deaktiviert. Zwar lässt er sich von einem Admin-Account aus über das Programm "Netinfo Manager" (Programme -> Dienstprogramme -> Netinfo Manager) wieder aktivieren. Sinnvoll ist das aber eigentlich nur, wenn viel mit den Unix-Funktionen gespielt oder in den für andere User als Root gesperrten Verzeichnissen gearbeitet werden soll.

Wenn ein Macuser mit einem anderen Macuser im Netzwerk Dateien austauschen will, kann er dies nicht wie bei Windows über die Freigabe eines Ordners machen. Stattdessen muss alles, auf das Zugriff erteilt werden soll, im "Öffentlich"-Ordner im Benutzerverzeichnis vorhanden sein. Das mag unkomfortabel erscheinen, ist aber ziemlich sicher.

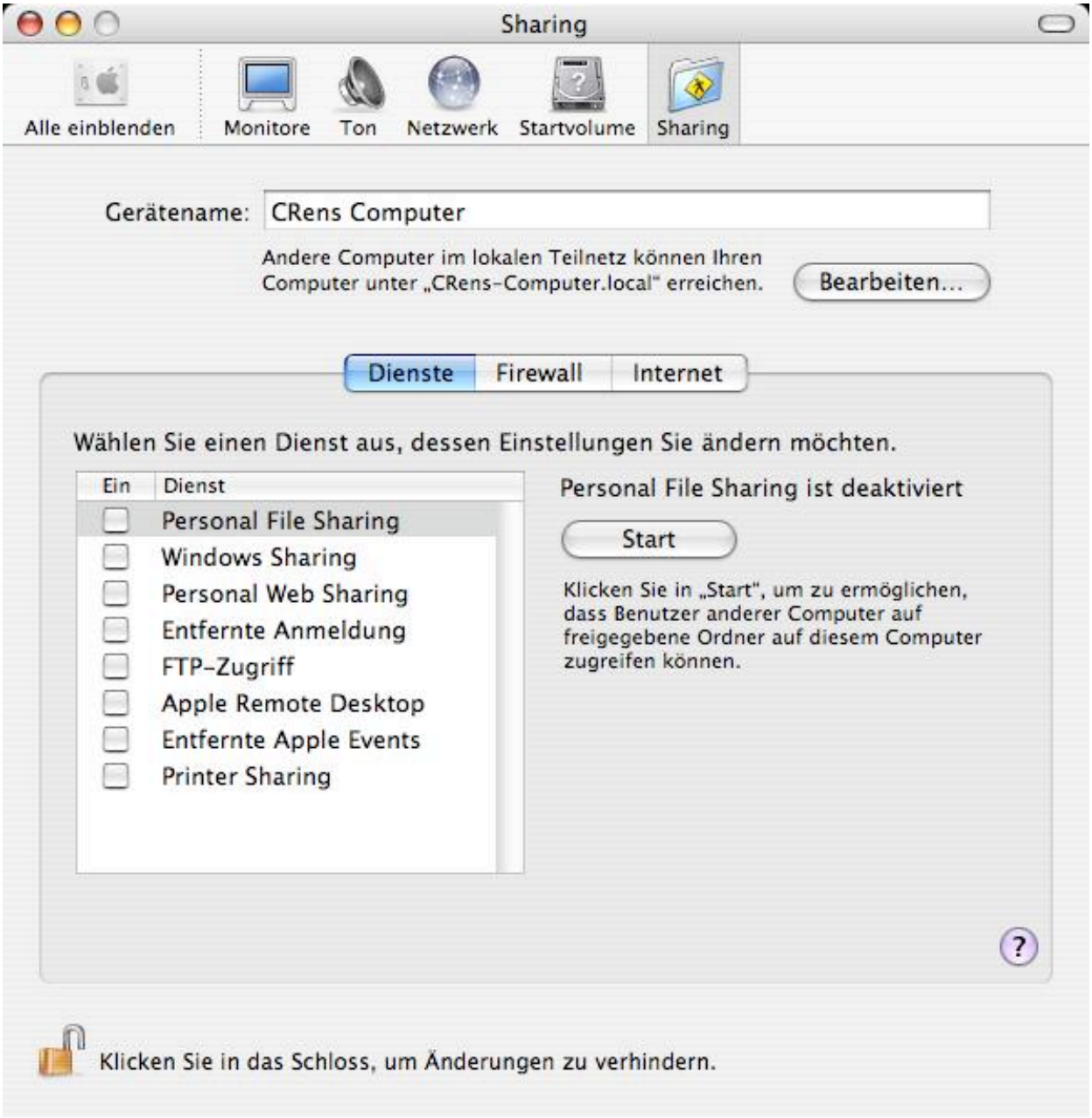
Schutzmaßnahme 2: Nicht benötigte Dienste deaktivieren

Unter "Sharing" (Systemeinstellungen -> Sharing) versteckt Apple alle für das Netzwerk relevanten Sicherheitseinstellungen. Hier können Dienste eingestellt werden, auf die Nutzer von außen auf dem Mac zugreifen dürfen, hier können Firewall und Internet-Sharing aktiviert werden.

Mac OS X Sicherheitsratgeber II: Äußere Sicherheit

Mac OS X im Netz dicht machen

In der Registerkarte "Dienste" gilt: Je weniger Häkchen, desto weniger potenzielle Sicherheitslücken.



Kleine Dienste-Kunde

- *Personal File Sharing* wird benötigt, um den Ordner "Öffentlich" im Netzwerk freizugeben.
- *Windows-Sharing* gibt den Rechner zusätzlich in Windows-Netzwerken frei. Ohne diese Option kann nur von anderen Macs oder Unix-Systemen im Netzwerk auf den Rechner zugegriffen werden.
- *Personal Web Sharing* macht den Rechner zum Apache Web-Server. Websites können lokal installiert und im Internet freigegeben werden. Die Option ist natürlich nur bei Rechnern mit Flatrate sinnvoll.
- *Entfernte Anmeldung* sorgt dafür, dass Benutzer auch von anderen Rechnern aus auf den Mac zugreifen können, wenn Sie Accountdaten haben.
- *FTP-Zugriff* verwandelt den Rechner in einen FTP-Server, ebenfalls nur sinnvoll, wenn der Rechner als solcher

genutzt werden soll. Achtung: Der FTP-Dienst ist nötig, um die FTP-Funktionalität des Finders zu nutzen.
- *Apple Remote Desktop* ermöglicht es anderen Benutzern, den Rechner über Apples Remote Desktop Tool über das Netz fernzusteuern. Diese Funktion ist verwandt mit VNC, der Remote-Nutzer sieht den Desktop des PCs und kann diesen komplett mit der Maus steuern.
- *Entfernte Apple Events* erlaubt es Programmen, andere Programme aufzurufen oder Dateien an sie zu übergeben. Was im Rechner selbst vollkommen sinnvoll ist, kann über das Netzwerk gefährlich werden.
- *Printer-Sharing* gibt die angeschlossenen Drucker im Netzwerk frei.

Im Firmen- oder Hausnetz machen all diese Dienste durchaus Sinn. So kann ein normaler Desktop-Mac gleichzeitig als Webs-, Print- und Fileserver tätig werden, während an ihm gearbeitet wird. Im Kontakt mit dem Internet sollte aber genau überlegt werden, welche Dienste benötigt werden und welche nicht, denn jede von ihnen bürgt eine potentielle Sicherheitslücke.

Schutzmaßnahme 3: Firewall nutzen

Genau wie im Dienste-Tab öffnet ein Häkchen im Firewall-Tab ein mögliches Loch. Die Logik ist etwas schwierig, normalerweise sollte man meinen, dass die Markierung eines Port-Bereichs diesen schließt. Dem ist aber nicht so: Dort, wo Häkchen sind, stehen die Türen sperrangelweit offen. Die Firewall sichert also erstmal komplett ab, offen ist nur, was im Port-Fenster markiert wurde.

Der Einsatz der Firewall ist mit Vorsicht zu genießen. Jede überflüssige Überwachung kann Rechenzeit kosten und bei zu paranoidem Einsatz die im Dienste-Tab ausgewählten Funktionen aushebeln. Zusätzlich kann es passieren, dass einige Programme nach Aktivierung nicht mehr ordentlich funktionieren.

Vordefinierte Regeln

Apple liefert bereits einige vordefinierte Regeln mit, die für die entsprechenden Dienste aufgesetzt sind. Weitere Ausnahmen lassen sich über den Button "Neu" definieren. Da die Regelvergabe invertiert ist, kann man dabei nichts falsch machen, stellt ein Programm den Dienst ein, kann man ihm den nötigen Port mit einer Regel frei machen. Umgekehrt werden die Ports dann natürlich auch für den Zugriff von Außen geöffnet.

Anders als die XP-Firewall arbeitet die Firewall von Mac OS X in beide Richtungen, sie kann Netzwerkkommunikation komplett unterbinden. Auf diese Weise werden Trojaner, Spyware und vergleichbare Übeltäter einfach, aber effizient ausgesperrt, da sie eine Regel bräuchten, um nach Hause zu telefonieren. Allerdings sendet Adware oft auf dem HTTP-Port, der von der Firewall nicht gesichert wird.

Mac OS X Sicherheitsratgeber II: Äußere Sicherheit

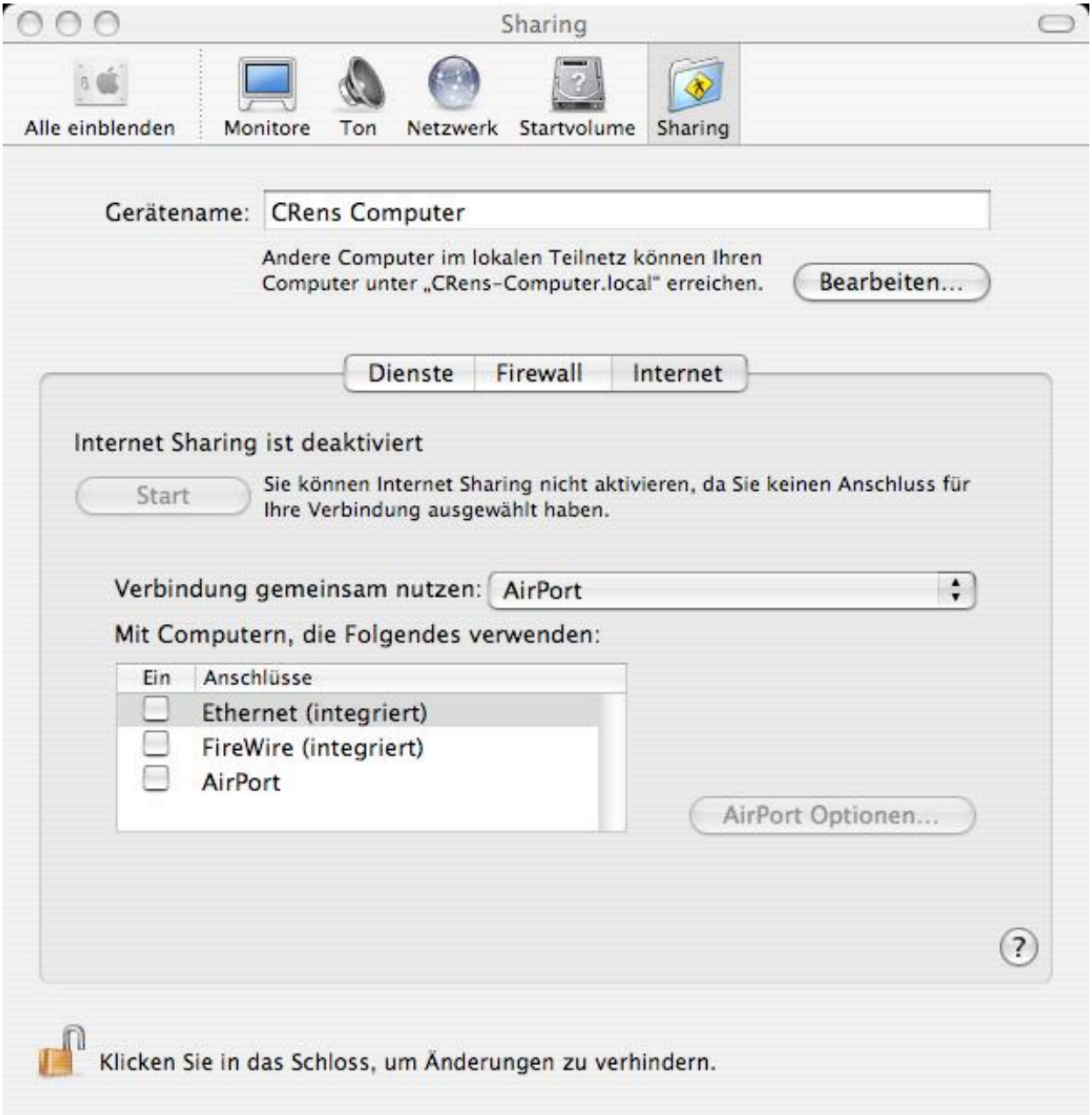
Mac OS X im Netz dicht machen

Schutzmaßnahme 4: Kostenfalle Internet-Sharing

Internet-Sharing ist eine feine Sache. Auf diesem Wege können mehrere Rechner ans Internet geklemmt werden, während nur eine Verbindung besteht. Der Mac wird damit zu Router und gibt die Internet-Anfragen an den Provider weiter. Diese Funktion ist besonders sinnvoll, wenn keine WLAN-Station vorhanden ist oder die einzige Telefonbuchse von mehreren Rechnern im Netz benutzt werden soll.

Allerdings gibt es auch hier ein Problem, insbesondere bei mobilen Rechnern. Ist nämlich bei einem Mac mit Airport die Verbindungsfreigabe aktiviert, kann ein wildfremder anderer User die Verbindung nutzen. Einzige Voraussetzung: Er hat ebenfalls WLAN. Das mag auf den ersten Blick albern sein, da über WLAN ja jeder ins Netz kann.

Besonders bei WLAN gefährlich



Spätestens aber, wenn es wie zum Beispiel bei der Telekom käufliche WLAN-Accounts gibt, kann es unangenehm werden, da ein Wildfremder ohne zu zahlen den Account mitbenutzen kann. Falls dann noch nach Volumen abgerechnet wird, kann es schnell teuer werden.

Wenn alle Dienste und die Firewall korrekt eingestellt und Benutzeraccounts mit den nötigen Rechten versehen sind, ist der Mac sicher im Netz unterwegs. Alles, was noch fehlt, ist ein Virenscanner, doch den kann man sich normalerweise getrost sparen, da es kaum nennenswerte Viren für Mac OS X gibt.

Fremdanbieter-Tools sinnlos

Überhaupt sind Tools von Fremdanbietern wie Norton bestenfalls Placebos, mit Bordmitteln lässt sich die Sicherheitsproblematik oft besser, effizienter und vor allem günstiger lösen. Diese Tatsache scheint sich inzwischen auch herumgesprochen zu haben, wieso sonst hätte Norton trotz steigender Mac-Verkaufszahlen seine Entwicklungsarbeit für Mac OS eingestellt?

Eines darf allerdings nicht vergessen werden: Programmierfehler können scheunentorgroße Sicherheitslücken aufstoßen. Aus diesem Grunde sollte mindestens einmal wöchentlich ein Blick in die Software-Aktualisierung geworfen werden. Diese Lücken betreffen zwar meist eher professionelle Anwender als Privatnutzer, doch sollte die Gefahr durch ungerichtete DoS-Attacken oder ähnliches nicht unterschätzt werden. Und wenn durch den Absturz nur die Arbeit einiger Stunden vernichtet wird.