



Ist Ihr Mac wirklich gefeit gegen Spionage und Sabotage? Johannes Schuster deckt auf, was Neugierige auf Ihrem Mac alles entdecken können und wie Sie sich dagegen am besten schützen.

Security first

Spionage und Sabotage sind große Worte für das, was auch unter der Bezeichnung „kleine Geheimnisse auskundschaften“ oder „jemandem eins auswischen“ läuft und wovor so mancher Mac-User nicht ganz sicher ist. Darf Ihr Ehepartner wissen, wo Sie letzte Nacht gesurft sind oder welche Briefe Sie geschrieben haben? Dürfen Ihre Kinder alle Dokumente auf Ihrem Mac öffnen, ansehen oder gar löschen? Sollte Ihr Arbeitgeber erfahren, was Sie neben Ihrem Broterwerb noch am Bürocomputer tun oder von wann bis wann der Rechner läuft? Haben Sie nur liebe Arbeitskollegen, die Ihren Mac zwar manchmal benutzen, aber stets so hinterlassen, wie sie ihn vorgefunden haben - oder möchte Ihnen einer sogar gezielt schaden?

Wir wollen hier keine Panik verbreiten, schließlich sind Mac-Anwender ja meistens nette Menschen. Sie sollten jedoch zumindest wissen, was auf der Festplatte so alles über Sie zu erfahren ist. Und natürlich geben wir Ihnen auch gezielte Ratschläge, wie Sie ihre kleinen Geheimnisse bewahren können oder wie Sie Ihren Mac trotz Mitbenutzern arbeitsfähig erhalten.

Spionagefelder

Verräterische Dateien. Setzt sich jemand nach Ihnen an den Mac, so kann er ohne Probleme im Apple-Menü unter „Benutzte Dokumente“, „Benutzte Programme“ oder „Benutzte Server“ sehen, welche Aktionen Sie zuletzt am Rechner durchgeführt haben. Da es sich bei den Inhalten dieser Ordner um Aliase der Dokumente, Programme und Server handelt, lassen sie sich durch einen simplen Doppelklick starten, und das Infofenster gibt ihr Erstellungsdatum preis. Ist also etwas Geheimes unter den benutzten Sachen, sollten Sie das Alias vor dem Abschalten löschen oder so viele unauffällige Aktionen starten, bis nur noch harmlose Dokumente gelistet sind. Ganz sicher ist der geleerte Papierkorb allerdings nicht, da Programme wie die Norton Utilities sich auf das Reaktivieren gelöschter Dateien verstehen, doch dazu später mehr. Alternativ können Sie

natürlich auch die Speicherung im Kontrollfeld „Apple-Menü Optionen“ auf Null setzen. Anschließend steht Ihnen dann diese meist durchaus sinnvolle Einrichtung - wo hab ich den letzten Text nur gespeichert? - nicht mehr zur Verfügung.

Auch einige Programme wie Excel oder Word führen im Datei-Menü eine Liste der zuletzt benutzten Dokumente. Sie können diese Funktion meist in den Voreinstellungen auf Null setzen oder deaktivieren, alternativ können Sie entsprechend viele Dokumente öffnen, bis das gewünschte Objekt von der Liste verschwindet.

Natürlich können Sie jeder Datei über deren Attribute ansehen, wann sie erzeugt und wann zuletzt geändert wurde, nur ist es etwas mühsam, die gesamte Festplatte nach frischen Spuren abzusuchen. Das kann dem geübten Spion

Sicherheit

Mit diesem Heft starten wir eine dreiteilige Serie zum Thema Datensicherheit am Mac. In den nächsten Ausgaben lesen Sie mit Sicherheit:

10/99 xxxxxxxxxxxx

11/99 Risiko Internet
eine schöne zeile xxxxxx

12/99 Unfall, Ungeschick, Ungeziefer
eine schöne zeile cxxxxx



Auf CD-ROM: Das Rundum-sicher-Pack

Big Secret 4.2	25 Dollar
BlackWatch 1.4.1	Freeware
Blind Folder 1.0	Freeware
Burn 2.5	Freeware
Cache File Delete (CFD) 1.3	Freeware
Drop Stuff 5.1.2	30 Dollar
Enigma 2.8	20 Dollar
FileBuddy 5.3.1	40 Dollar
FileTyper 5.3.1	10 Dollar
Forgotit 1.0	15 Dollar
Keys Off, x.x	xxx
Kill Cache 3.0	5 Dollar
Lockout 1.3.3	15 Dollar
Mac Dim 2.2	Freeware
MM Extension Guards	
Nova, 3.1	20 Dollar
Password Please 1.0	Freeware
Password-Protect-Folders 1.4.810	Dollar
Quick Encrypt 3.0.3	25 Dollar
Quitter 1.5.2	15 Dollar
ResEdit 2.1.3	Freeware
Search and Rescue xx	xxx
Secret Folder 1.0	20 Dollar
Security Delete 1.0.3	Freeware
Sentry 4.0.3	10 Dollar
Sesame, 2.2 dt.	10 Dollar
Shift Key Suite	xx.xx
Spy 2.5.2	10 Dollar
Super Save xx	xx
TechTool 1.1.8	0? Free?
The Eraser 2.5.1	15 Dollar
The Mac Locksmith 2.3.0	10 Dollar

Kommerzieller Paßwortschutz

Disk Guard 1.8.6	
Hersteller: xxx	ca. 230 Mark
File Guard 3.2.3	
Hersteller: xxx	ca. 400 Mark
Hard Disk Toolkit 3.0.2	
Hersteller: FWB	ca. 300 Marl
Bezug: Fachhandel (klären, ob auch DG/ FG anderswo als Prisma)	

jedoch das Betriebssystem mit der Finden-Funktion - neuerdings Sherlock genannt - abnehmen. Die Suche läßt sich per Pulldown-Menü auf alle Objekte begrenzen, die im Zeitraum eines oder mehrerer Tage oder Wochen oder Monate erstellt respektive geändert wurden. Natürlich sind dabei auch eine Menge Nieten, wie System-Preferences oder -Dateien, jedoch auch alle frischen Texte und Bilder. Hier hilft nur eine Abschottung über ein paßwortschützendes Utility oder das Mitnehmen des Datenträgers. Zu den Möglichkeiten im einzelnen geben wir im folgenden noch Auskunft.

Leicht lassen sich manchmal in Dokumenten enthaltene Informationen über Programmversionen, Ursprungsrechner, vorherige Dateinamen oder versteckte Botschaften der Programmierer sichtbar machen. Texteditoren wie Word, RealView oder Can Opener reißen so gut wie alles auf: Probieren Sie es mal einem älteren Systemkoffer, und Sie erfahren die schockierende Wahrheit über die Schöpfer des Mac OS.

Internet Spuren. Ohne besondere kriminelle Energie kommt ein Wissbegieriger auch schnell an die von Ihnen zuletzt betrachteten Internetbilder heran. Ganze Seiten findet er natürlich, wenn er Ihre Bookmarks oder Favoriten noch einmal ansurft. Auch wenn Sie alle irgendwie verfänglichen Links beseitigt haben, kann der Schnüffler immer noch in den Cachedateien des Browsers lesen wie in einem offenen Buch. Er braucht nur im Systemordner das Preferences-Verzeichnis aufzusuchen, dort beispielsweise einen Ordner namens Netscape zu öffnen und die hier abgelegten Dateien auf ein Programm wie Photoshop oder GraphicConverter zu ziehen - schon sieht er den nackten Tatsachen ins Auge. Kill Cache oder CFD Cache File Delete löschen den Browser-Cache, so daß Sie nach jedem Surfvergnügen einen unkompromittierenden Mac hinterlassen. Zum Kapitel Internet wollen wir jedoch im nächsten Heft ausführlicher kommen.

Paßwortknacker. Natürlich gibt es im Internet auch Programme, die einen Paßwortschutz umgehen können. Offizieller Zweck ist es, dem Anwender zu helfen, falls dieser mal sein Paßwort vergessen hat. Benutzt werden diese kleinen Helfer jedoch eher für Dateien, deren Codewort man nie gewußt hat ... Beispiele hierfür sind etwa ein Password-Remover für ältere Stuffit-Dateien oder Cracks von FileMaker-Datenbanken bis Version 3, wie GoldViewer. Wir verbreiten solche Produkte nicht, noch geben wir hier weitere Tips dazu. Wir wollen die Braven und Gutgläubigen unter unseren Lesern nur aufklären - und ein wenig gruseln ;-).

Sicherheitslücken im lokalen Netzwerk. Einem weiteren Gefährdungspotential sind vernetzte Macs ausgesetzt, deren Festplatten auch von anderen Netzteilnehmern ausgespäht werden können, ohne daß diese sich dazu an Ihren Mac setzen müßten. Haben sie zum Beispiel File Sharing aktiviert, aber im zugehörigen Kontrollfeld kein Paßwort eingegeben, kann sich jeder im Netz unter Ihrem Benutzernamen auf Ihrem eingeschalteten Mac einloggen und dort alles ansehen oder kopieren. Natürlich mag es auch sein, daß Sie Ihr Paßwort - beabsichtigt oder nicht - weitergegeben oder leicht zugänglich notiert haben: Auch dann nützt es wenig.

Etwas mehr kriminelle Energie braucht dann schon jemand, der sich kurz an Ihren Mac setzt und das File-Sharing-Paßwort ändert - dazu muß man das alte nicht kennen! - oder unter einem Fantasienamen einen neuen Benutzer mit allen Zugriffsrechten einrichtet. Dieser kann nun unauffällig von einem anderen Rechner lustig spionieren. Allerdings ist im ausgefahrenen Kontrollleistenmodul sofort erkennbar, ob jemand auf Ihrem Mac eingeloggt ist. Zudem ändern sich bei aktuellen Systemversionen die Icons der besuchten Ordner, und im Kontrollfeld „File Sharing Monitor“ erfahren Sie auch noch den gewählten Namen der Besucher und die frequentierten Ordner oder Volumes.

Spionage-Werkzeug

■ Softwares wie Super Save, das jeden Tastendruck registriert, oder Search and Rescue, das den Arbeitsspeicher ausliest, sollen eigentlich nach einem Absturz bei der Rekonstruktion der letzten Worte helfen, lassen sich natürlich aber auch bei einer versteckten Installation auf fremden Rechnern zur Spionage einsetzen.

Überraschend hilfreiche Programme wie Norton Utilities oder TechTool können nicht nur versehentlich Gelöschtes le-

sen, sondern auch absichtlich Beseitigtes. Außerdem holen sie sogar noch etwas von geschützten Volumes - dazu später mehr. Wollen Sie gelöschte Dateien endgültig vernichten, gibt es allerdings einige Möglichkeiten: Unbenutzte Blöcke der Festplatte löschen die Freewares Burn 2.5 und Security Delete 1.0.3, die Shareware The Eraser 2.5.1 oder auch Wipe Info, ein Bestandteil der Norton Utilities.

xxx xxxx xxxxxx xxxxx xxxxxxxxxxxx



Sabotagefelder

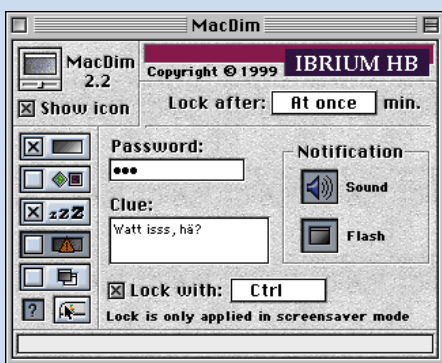
Vernichten oder Verändern. Der freie Zugang zu Ihrem Mac oder das oben benannte Fehlen oder Umgehen eines Paßworts für File Sharing kann nicht nur dem Auskundschaften Ihres Macs dienen, es lädt auch zu Späßen ein, die nur noch als übel zu bezeichnen sind: Löschen von wichtigen Dateien oder das Unbrauchbarmachen des Betriebssystems. Noch schlimmer das unauffällige Manipulieren von Daten oder das Einbauen von peinlichen Fehlern, die nicht Sie, sondern erst ein Kunde, Ihr Chef oder ein Kollege bemerkt und was natürlich ein schlechtes Licht auf sie wirft.

Natürlich kann Ihnen ein übelmeinender Zeitgenosse auch einen der wenigen in der Mac-Welt kursierenden Vi-

ren auf die Festplatte kopieren, dazu reicht sogar schon ein für File Sharing geöffnetes Postfach. Dazu mehr im dritten Teil dieser Serie. Etwas harmloser ist da noch das Zukleistern der Festplatte mit sinnlos duplizierten Daten, so daß Sie eventuell Probleme beim Speichern geöffneter Dokumente bekommen oder der Virtuelle Speicher beim nächsten Start nicht mehr läuft. Auf jeden Fall haben Sie den Ärger mit dem Aufräumen.

Üble Späße. Ein netter Spaß für alle nicht betroffenen Kollegen ist auch das Beenden von Programmen über das Netzwerk. Treffen Sie auf einen unbedarften Zeitgenossen, der bei aktiven „Programmverbindungen“ noch einen Gastzugang über File Sharing gewährt, lassen sich sämtliche geöffneten Programme mit der Shareware Quitter 1.5.2

Die Gegenmittel – damit Geheimes geheim bleibt



Geile zeile Xxxx xxxx xxxxxx x

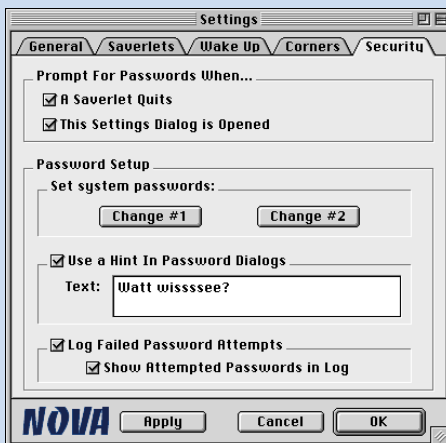
Bildschirmschoner mit Paßwortschutz.

Für den Mac gibt es eine Reihe von Bildschirmschonern, die zum Teil auch den Rechner mit Kennwort vor dem Aufwecken schützen. So etwa die Programme MacDim 2.2 oder Lockout 1.3.3, die sich aber ganz einfach durch einen erzwungenen Neustart (Ctrl., Befehl, Einschalttaste) umgehen lassen. Gleiches gilt auch für Nova 3.1 und BlackWatch 1.4.1, die nach dem Zwangs-Boot zwar nicht die Daten verteidigen können, aber sich wenigstens mit einem Paßwort vor Deaktivierung schützen wollen. Nova merkt sich zusätzlich, wann es wer mit welchem Kennwort versucht hat. Gelöscht im Papierkorb mußten die beiden dann allerdings doch aufgeben. Insgesamt scheinen Screensaver doch nur harmlose Spione abschrecken zu kön-

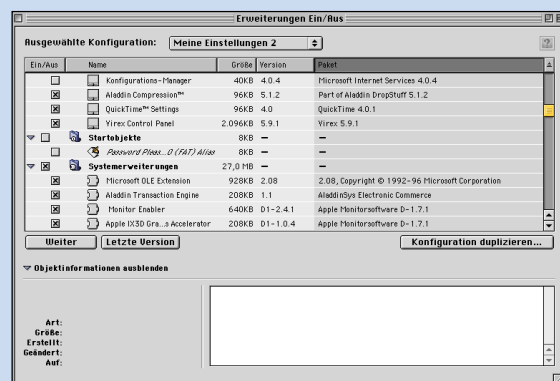
nen.

Paßwortschutz des kompletten Macs.

Einige Utilities versprechen nicht mehr und nicht weniger als den Paßwortschutz des gesamten Macs. Dazu gehört auch Keys Off 1.3, das in unserem Test allerdings gar nicht zum Arbeiten zu bewegen war und immer ein Paßwort haben wollte, welches wir nie eingegeben hatten. Shift Key Suite 1.0, das die Deaktivierung der Erweiterungen per Shift-Taste verhindern soll, lief nicht auf unserem G3/233 unter Mac OS 8.5.1. Das kleine Tool Password Please 1.0 läßt sich allein durch Halten der Leertaste und Deaktivieren des zugehörigen Alias in den Startobjekten umgehen. Bleibt die auch deutschsprachig verfügbare Software Sesame 2.2, die das Deaktivieren



Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x

nicht nur einsehen, sondern auch sang- und klanglos beenden! Der User hat keine Chance mehr, die geöffneten Dokumente des Programms zu speichern.

Fremdbenutzer-Willkür. Manchmal grenzt es schon an Sabotage, wenn Kollegen, Kinder oder Freunde in Ihrer Abwesenheit den Arbeits-Mac zu einem prima Spiele-Rechner umbauen: Sie finden nach Ihrer Rückkehr zahlreiche Einstellungen verändert, alte Erweiterungen abgeschaltet und zahlreiche neue installiert, den Systemordner überladen und die Festplatte mit reichlich Schlick gefüllt. Als Gegenmaßnahme bietet sich zunächst an, verschiedene Erweiterungs-Sets für jeden Benutzer oder Einsatzzweck im Kontrollfeld „Erweiterungen Ein/Aus“ anzulegen, die Sie mit unseren Extension Guards (auf CD) so-

der Erweiterungen durch einen Systempatch verhindert. Bei verschärften Sicherheitseinstellungen zeigt es sich schnell zickig und läßt bei falschen Kennwörtern nur noch die Wahl zwischen Neustart und Ausschalten. Fast wäre uns das Umgehen dieses Schutzes nicht gelungen, doch schließlich kamen wir ambitionierten Amateur-Hacker durch einen simplen Start von einer System-CD weiter: Wir hatten vollen Zugriff auf alle Dateien der Festplatte, Sesame hatte außerdem sein Passwort vergessen und wir konnten das Programm kaltschneuzig löschen. Falls Sie das CD-Laufwerk und sämtliche SCSI-Buchsen wirksam verkleben, scheint Sesame wirklich sicher.

Unsichtbar machen. Neben dem Ver-

gar vor Änderung schützen können. Was jedoch Zeichensätze, Preferences oder andere Systembestandteile angeht, helfen die Sets auch nicht weiter. Sie können diese allerdings komplett mit einem Etikett versehen und nachher bequem alle Eindringlinge durch Sherlock-Suche oder Sortieren nach Etikett in der Listendarstellung sammeln und ausmerzen.

Haben sie genügend Platz auf der Festplatte, ist das Sicherste jedoch die Aufteilung in unterschiedliche Volumes mit eigenen Systemen und eventuellem Paßwortschutz (siehe unten) oder Sie nutzen externe Fest-/Wechselplatten für Start und Betrieb. Falls Sie die Festplatte nicht mehr partitionieren können oder wollen, hilft auch der System-Switcher (which is what?).

stecken vertraulicher Dateien in Unterunterordnern ist das Unsichtbarmachen der Dokumente schon ein etwas besserer Schutz vor neugierigen Blicken. Allerdings zeigten sich in unserem Test einschlägiger Programme starke Sicherheitslücken, die auch ein talentierte rojähriger schnell herausfindet.

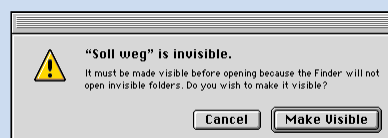
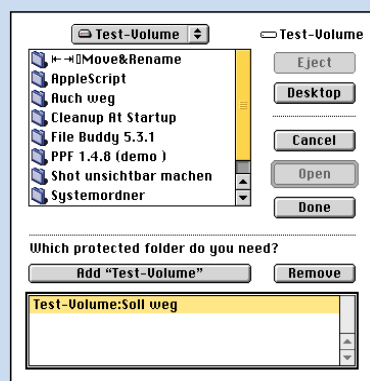
Zum Verstecken der Icons gibt es einige Tools: Die Freeware Blind Folder 1.0 sowie die Sharewares FileTyper 5.3.1 und Password-Protect-Folders 1.4.8 machen Objekte einfach per Drag-and-drop unsichtbar, während Big Secret 4.2 die Auswahl über ein Dialogfenster ermöglicht. Secret Folder 1.0 kann auch über das Ziehen der Dateien ins Programmfenster geführt werden. Bei Res Edit 2.1.3 und FileBuddy 5.3.1 müssen Sie die Attribute einer ausgewählten Datei im

Mac OS 9 - das neue Sicher

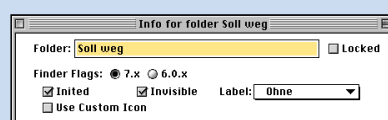
■ Wenn im Oktober Mac OS 9 herauskommt, wird erneut ein Feature aus der PC-Welt seinen Weg auf den Mac gefunden haben. Nachdem Mac OS 8 von Windows 95 bereits die Kontextmenüs für Mac-Anwender adaptiert hatte, wird Mac OS 9 diverse Sicherheitsfunktionen enthalten, die sich am ehesten mit Windows NT vergleichen lassen: das User-Login und die Möglichkeit, mehrere User zu verwalten. Der Anwender identifiziert sich beim Rechnerstart mit Benutzernamen und Passwort. Zugriffe auf das CD-ROM-Laufwerk und externe Speichermedien lassen sich ebenso unterbinden wie Zugang zu einem Drucker oder anderen Netzwerkfunktionen einschließlich Internet. Nach dem „Login“ bekommt man seinen Arbeitsplatz präsentiert, wie der Administrator ihn einrichtete. Insbesondere jüngere und verspielte Familienangehörige können nun keinen Schaden mehr anrichten, weil sie nicht unbedingt alle Dateien und Programme zu sehen bekommen. Enthält man ihnen zum Beispiel das Kontrollfeld „Datum & Uhrzeit“ vor, läßt sich nicht mal mehr an der Systemuhr drehen. In gewisser Weise dehnt Mac OS 9 die Zugriffsberechtigungen der Netzwerkfunktion File Sharing aus auf die lokale Festplatte. Nach der stillschweigenden Einstellung des Finder-Ersatzes At Ease würdigt Apple nunmehr wieder Sicherheitsaspekte auf Systemebene. Auch für Firmen ist Mac OS 9 daher interessant. Das kommende Sicherheitssystem sieht sogar vor, daß sich der Arbeitsplatz nach definierter Zeit der Abwesenheit selbständig verriegelt. Man kann also nicht mal kurz in der Mittagspause die E-Mails von Kollegen einsehen. **Sesam, öffne Dich!** Anstelle des eingetippten Passworts kann unter Mac OS 9 die Benutzererkennung anhand eines gesprochenen Satzes erfolgen. Apple nennt dies „Voice Authentication“, die Echtheitsprüfung per Spracherkennung. Das mnemonisch eingängige „Sesam, öffne Dich!“ wird jedoch nicht funktionieren - die Code-Phrase sollte rund doppelt so lang sein. Zudem muß man seinen Zugangscode mehrfach vorsprechen. Dafür soll die Sprachidentifizierung dann auch den Mac freigeben, wenn man mal erkältet ist, weil charakteristische Sprachmuster auch bei belegter Stimme gleich bleiben.

Schlüsselring. Als zweites „Sesam, öffne Dich!“ bringt Mac OS 9 die Funktion namens KeyChain. Sie war ursprünglich schon für Mac OS 8.6 vorgesehen. KeyChain öffnet wie der Universalschlüssel des Hausmeisters alle Türen, die man sich mit dem jeweiligen Passwort öffnete. Gibt man zum Beispiel sein E-Mail-Paßwort ein, dann wird dieses dem KeyChain-Schlüsselring hinzugefügt. Die KeyChain-Funktion erkennt Passworteingaben für Terminplaner, Mail-Programme und Datenbanken sowie FileServer und sogar FTP-Server im Internet. Ein übergeordneter Code sichert wiederum den KeyChain. Für jeden Schlüssel auf dem Schlüsselring kann man angeben, ob dieser automatisch verwendet werden soll, wenn der KeyChain freigeschaltet ist. So bleiben etwa sensible Datenbanken trotzdem verschlossen. Vergleichbar mit dem „User-Login“ kann sich der KeyChain automatisch nach voreingestellter Zeit oder per Tastenkombination wieder verriegeln.

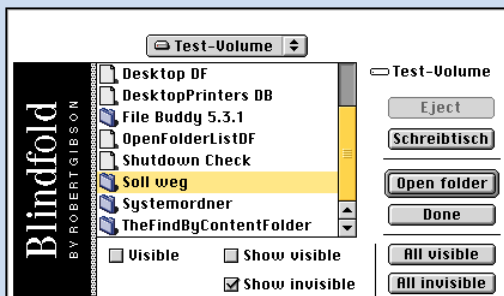
Verschlüsselung. Das vierte Sicherheitsfeature von Mac OS 9 kommt als Verschlüsselung für Dateien. Vergleichbar zu Drop-Stuff von Aladdin werden Dokumente komprimiert, aber zugleich auch verschlüsselt und mit einem Paßwort versehen. Selbstverständlich kann der Benutzer dieses Paßwort dem



Geile zeile Xxxx xxxx xxxxxx x



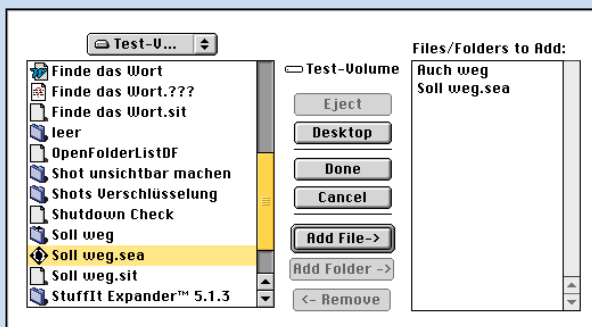
Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x

Informationsfenster ändern. Das Wieder-sichtbar-machen geschieht am einfachsten mit Big Secret, das eine Liste aller vom Programm versteckten Objekte führt. Ähnlich läuft es bei Secret Folder, allerdings können Sie damit immer nur einen Ordner tarnen. Bei allen anderen Programmen müssen Sie sich Namen und Ort des Objekts merken, um es zwischen allen anderen Dateien zu finden. Ausnahme ist nur File Buddy, das gezielt nach unsichtbaren Dateien fahnden kann (Menü Cleaning/Find Invisible Items) und sie nach einem Doppelklick und einer Warnmeldung wie-

der ins Reich der optischen Sinne zurückholt. Suchen können Sie unsichtbare Objekte übrigens auch mit der Finden-Funktion des Mac OS, indem Sie beim Klick auf „Name“, die Wahl taste gedrückt halten: Jetzt wird die Attributliste unter anderem um den Punkt „Sichtbarkeit“ ergänzt. Leider kann man vom Trefferfenster aus die Dateien weder öffnen noch sichtbar machen.

Große Gefahr von Verwirrung und Datenverlust besteht bei Blind Folder, da es ohne entsprechende Warnung Ordner ohne deren Inhalt sichtbar macht. Solange Sie nicht in den Preferences „Modify directory contents“ aktivieren, muß Datei für Datei einzeln zurückgeholt werden.

Secret Folder und Password-Protect-Folder bieten zusätzlich einen Paßwortschutz an, allerdings schützt dieser nur das Programm selbst: Die Dateien lassen sich ohne Schwierigkeiten auch mit File Buddy wieder sichtbar machen. Haben Sie also wirklich vertrauliche Daten, sollten Sie es nicht bei dem Versteckspiel lassen, sondern eine der folgenden Si-

cherheitsmaßnahmen ergreifen.

Verschlüsselung. Natürlich können Sie auch einzelne Dateien und Ordner mit einem Paßwort schützen. Zum Beispiel erledigt die Shareware Drop Stuff 5.1.2 dies neben dem Komprimieren in angemessener Zeit, und Sie sparen auch noch Platz auf der Platte. Hierbei wird allerdings „nur“ nach Komprimierung ein Kennwort aufgesetzt. Die Shareware Enigma 2.8 verschlüsselt dagegen im eigentlichen Sinne und arbeitet um einiges schneller, packt die Daten dabei aber nicht dichter. Außerdem ist

das Handling von ganzen Ordnern etwas kompliziert, da erst ein „Valut“ genanntes Archiv erzeugt werden muß, bevor man einen Ordner hineinziehen kann. Das Auspacken ist mühselig in Einzelteilen vorzunehmen. Der Autor spricht von einer Verschlüsselung mit 32 Bit, registrierte Anwender kommen in den Genuß von 56 Bit Sicherheit. Wie sicher die Dateien wirklich gegen das Knacken sind, konnten wir leider nicht in einem vierwöchigen Hacker-Workshop klären - versuchen Sie es doch mal. ;-)

Auch Quick Encrypt 3.0.3 leistet ähnliches, allerdings ist es sehr langsam, das Handling ist nicht besonders intuitiv, und wir vermißten eine Möglichkeit, die Originale gleich löschen zu lassen. Wesentlich besser geht dieses Problem The MacLocksmith 2.3.0 an, das die Originale nicht nur löscht, sondern gleich auch überschreiben will. Denn hier wartet die große Gefahr der Enttarnung: Bei jeder Verschlüsselung muß die alte Datei gelesen und eine neue geschrieben werden. Auch nach dem Löschen des

Originals läßt sich dieses oft mit Helfern wie Norton UnErase lesen. Wir konnten allerdings in unserem Test mit den Norton Utilities bei keinem der Programme noch verwertbare Reste auf der Platte finden. Ein anderes Risiko besteht bei jeder Verschlüsselung durch Fehler beim Lesen, Kodieren oder Schreiben, die das Archiv unbrauchbar machen können. Außerdem dürfen Sie natürlich auch keine Sicherheitskopien, die Sie gegen Festplattencrashes absichern, ungeschützt herumliegen haben.

Alle genannten Programme sind in der Lage, selbstentpackende Archive zu kreieren, Sie können also auch verschlüsselte Dateien verschicken, der Adressat braucht nur noch das auf anderem Wege übermittelte Paßwort, das Programm muß bei ihm nicht vorhanden sein. Speziell für den E-Mail-Ver-sand sind Programme wie Private File von Aladdin, Phil Zimmermanns Pretty Good Privacy oder SafeMail von Highware entwickelt worden - im nächsten Teil gehen wir näher auf sie ein. Andere kommerzielle Verschlüsselungsprogramme wie die Power-On-Produkte DiskLock (ehemals Symantec) und On Guard waren nicht rechtzeitig zum Redaktionsschluß bei uns, es sollte jedoch auf unserer CD genügend geeignete Shareware zu finden sein.

Paßwortschutz für Volumes. Als sehr sicher gilt die Methode, eine Partition auf der Festplatte mit einem Paßwort zu versehen, allein zu diesem Zweck gibt es noch keine Shareware. Hard Disk Toolkit (3.0.2, etwa 300 Mark bei Prisma Express) erledigt diese Aufgabe auf allen Festplatten, die mit HDT formatiert sind, ohne Probleme, auch das reguläre Startvolume kann per Kennwort gesichert werden. Im Test konnten wir mit Norton Volume Recover jedoch zirka fünf Prozent der Dateien eines HDT-geschützten Volumes völlig intakt heraus-

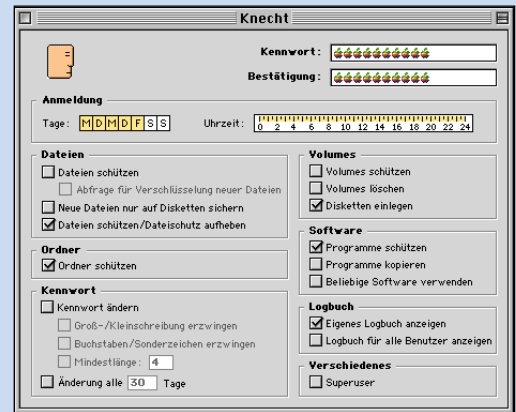
kopieren, so daß auch dieser Sicherheitsmechanismus durchfällt!

Zusätzlich gibt es bei HDT für jedes Volume noch drei Verschlüsselungsstufen, die allerdings einen sehr, sehr zeitaufwendigen Prozeß in Gang setzen, der nicht immer zu einem guten Abschluß kommt. Hersteller FWB warnt deshalb zu Recht davor und mahnt ein vorheriges Backup an. Unsere Daten waren gleich beim ersten Versuch komplett weg, selbst die Norton Utilities konnte sie nicht retten. :- (Das unbrauchbar gewordenen Volume reparierte Norton allerdings wieder.

Erwähnt werden sollen hier auch die Iomega-Tools, die Zip- und Jaz-Medien mit einem Paßwort schützen. Zusätzlich können Sie die Disks ja noch in den Tresor packen. :-)

Auch DiskGuard (1.8.6 dt, etwa 230 Mark bei Prisma Express) von Highware schützt Volumes zuverlässig. Zusätzlich übernimmt es noch andere Aufgaben wie Bildschirmschoner, die Verwaltung verschiedener Nutzungsrechte für mehrere User, die Verschlüsselung einzelner Ordner und sogar einen Kennwortschutz für den ganzen Mac. Zudem ist es in deutsch und kommt auch mit Apple-formatierten Platten klar. Der große Bruder FileGuard (3.2.3 dt., 400 Mark bei Prisma Express) beherrscht zusätzlich die Registrierung fast aller Aktivitäten auf dem Mac, automatische Verschlüsselung nach Benutzung einer Datei, Blockade von CD- und Disketten-Laufwerk und Löschen durch Überschreiben. Damit bietet das Programm einen wirklich idealen Rundumschutz vor allem und jedem, aber leider auch vor sich selbst, wenn es hart kommt. Vergessen Sie nämlich ihr Master-Paßwort oder wird Ihr Betriebssystem mal richtig zerschossen, kommen auch Sie nicht mehr an Ihre Daten.

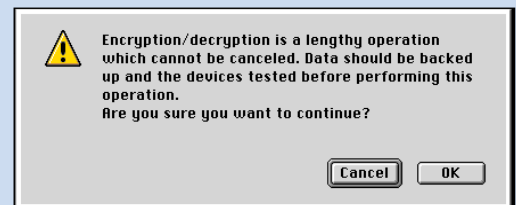
xxxx
xxxxxxxxxxxxxxxxxx



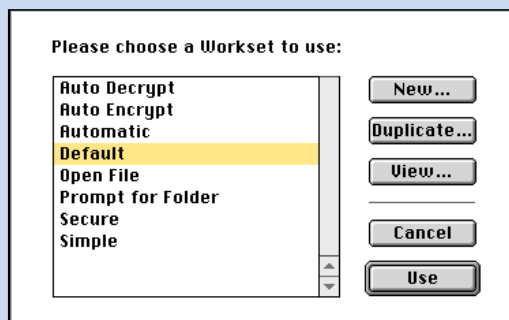
Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x



Geile zeile Xxxx xxxx xxxxxx x

Gegenspionage

■ Ganz hilflos muß man sich und seinen Mac den neugierigen Blicken der anderen also nicht aussetzen, es gibt offenbar doch funktionierenden Schutz, wie unser Überblick gezeigt hat. Wollen Sie allerdings nicht nur Ihre Daten in Sicherheit bringen, sondern vielleicht noch etwas über den Spion erfahren, geben wir Ihnen hier noch einige Tips zur Gegenspionage. Das Programm Sentry 4.0.3 zeichnet alle Rechnerstarts auf, während Spy 2.5.2 sämtliche Programmaktivitäten registriert. Die Sharewareversion von TechTool 1.1.8 kann die Betriebsstunden Ihres Macs zählen: Verdächtig, wenn über Nacht einige hinzukommen. Forgotit 1.0 speichert alle Paßwörter zentral in einer kleinen Datenbank, die wiederum nur mit Paßwort zugänglich ist, und hilft damit gegen Ihre vielleicht größte Angst: sich selbst auszusperrern und die Kennwörter zu vergessen!