So schützen Sie vertrauliche Daten

Streng geheim

Auch wenn kein absolut sicherer Schutz existiert: Es gibt nützliche Programme, die es Daten-Spionen erschweren, mit neugierigem Blick auf Ihrer Festplatte spazierenzugehen

Wer geheime Daten schützen wollte, mußte sich laut einem Experten vom Chaos Computer Club früher etwas umständlich behelfen: Einem Sklaven wurde die Nachricht auf den kahlrasierten Kopf tätowiert. Nachdem die Haare des Boten so lang gewachsen waren, daß nichts mehr zu erkennen war, machte er sich auf den Weg. Der Empfänger schnitt die Haare ab und konnte so die Mitteilung entziffern. Der Sklave wurde anschließend geköpft – sicher ist sicher.

Heute tun Sie sich da leichter: Eine Vielzahl von Programmen ermöglicht es Ihnen, auch ohne Blutvergießen vertrauliche Daten vor fremden Zugriff zu schützen. So läßt sich verhindern, daß nicht jeder, der Zugang zu Ihrem PC hat, Ihre persönlichen Dokumente einsehen und kopieren kann.

Grundsätzlich stehen Ihnen drei Wege offen, Ihre Daten vor fremden Blicken abzuschirmen. **Lösung 1: Zugangsschutz-Software.** Damit verhindern Sie, daß Benutzer unbefugt bestimmte Aktionen auf Ihrem PC ausführen. Die Palette reicht vom klassischen Zugangsschutz, der beim Start des PCs ein Paßwort abfragt, über den Kennwortschutz einzelner Programme bis hin zum Anlegen komplexer Benutzerprofile. Diese ermöglichen es Ihnen, zu bestimmen, was welcher Benutzer an Ihrem PC tun darf, welche Programme er einsetzen kann und welche Aktionen untersagt sind. Echten Datenschutz können solche Programme aber nicht leisten. Diese Sicherung ist für Computer-Freaks meist einfach zu umgehen. Außerdem: Wer das nötige Know-how besitzt, kann die Festplatte ausbauen und kopieren.

Lösung 2: Verschlüsselungs-Software. Für mehr Sicherheit sorgen Sie, indem Sie Ihre Daten verschlüsseln. Bei der Wahl des richtigen Kryptographie-Programms sollten Sie allerdings auf den eingesetzten → *Algorithmus* und seine → *Schlüssellänge* achten. Von diesen Faktoren hängt wesentlich ab, wie schnell eine Verschlüsselung geknackt werden kann – und davon, wieviel Rechenkapazität zum Knacken zur Verfügung steht. In einer Gemeinschaftsaktion haben Anfang 1998 circa 50.000 Computer aus aller Welt über das Internet in 39 Tagen eine Nachricht entschlüsselt, die mit dem → *DES*-Algorithmus (Schlüssellänge: 56 Bits) chif-

friert war. Mit jedem Bit, das der Schlüssel länger ist, verdoppelt sich die Zeit, die zum Knacken gebraucht wird.

Lösung 3: Kombination aus Zugangsschutz und Verschlüsselung. Damit schotten Sie Ihren PC vor unliebsamen Besuchern ab. Sollte jemand trotzdem eingedrungen sein, muß er erst die verschlüsselten Dateien knacken, bevor er Ihre Daten einsehen kann. Insgesamt erhöht sich der Datenschutz durch die Kombination aber nur minimal.

Beliebter Verschlüsselungs-Algorithmus: Blowfish. Mit einer variablen Schlüssellänge bis 448 Bits bietet der Algorithmus → *Blowfish* zur Zeit ein hohes Maß an Sicherheit. Ob Sie eine so starke Verschlüsselung benötigen, ist aber fraglich. Schließlich wird ein neugieriger Kollege nicht Zehntausende von PCs organisieren, nur um einmal einen Blick auf Ihre privaten Dateien zu werfen. Andererseits ist es ein gutes Gefühl, wenn die Daten besonders sicher geschützt sind. Zumindest so lange, bis die Leistungsfähigkeit handelsüblicher PCs so hoch ist, daß sie auch eine starke Verschlüsselung schnell knacken können.

Sichere Methode: Steganographie. Beim → *Steganographie*-Verfahren verhindert der Sender, daß jemand die Existenz der geheimen Datei überhaupt bemerkt. Wie beim Beispiel des kahlrasierten Sklaven wird sie versteckt. Bei der modernen PC-Steganographie wird eine vertrauliche Datei in einer Trägerdatei verborgen, etwa in einer BMP-Datei. Betrachtet jemand das digitale Bild in einer Bildbearbeitung, kann er nicht erkennen, daß darin eine Datei versteckt ist. Und selbst wenn: Viele Steganographie-Programme bieten eine Option zum zusätzlichen Verschlüsseln.

Verschlüsselungsprogramme im Test: Wir haben 13 Kryptographie-Programme auf ihre Leistungsfähigkeit geprüft. Worauf wir dabei geachtet haben, lesen Sie im Kasten „Datenschutzprogramme: Wie wir testen“ auf Seite 158. Wichtige Begriffe zum Thema erläutern wir im „Fachchinesisch: Datenschutzprogramme“ ab Seite 159. Wie sicher ein Kryptographie-Programm Ihre Daten auch verschlüsselt: Wenn Sie ein zu kurzes und zu einfaches Paßwort benutzen, machen Sie es Hackern unnötig leicht. Beachten Sie daher unsere Tips zur Paßwortwahl auf Seite 166.

DANIEL BEHRENS ▶

ENTSCHEIDUNGSHILFE: DATENSCHUTZ

WENN...	...DANN
Sie nur einzelne Dateien vor fremden Blicken schützen möchten,	...empfehlen wir die Freeware Norton Secret Stuff.
Sie Kryptographie-Neuling sind,	...erleichtert Ihnen Top Secret den Einstieg.
Sie mehrere Anwender an Ihrem PC arbeiten lassen,	...können Sie mit PC Lock 98 Benutzer-Restriktionen festlegen.
Sie ganz auf Nummer Sicher gehen möchten,	...verwenden Sie ein Steganographie-Programm wie Steganos.

DATENSCHUTZPROGRAMME: DIE PRODUKTE IM ÜBERBLICK

Produkt	System	Preis	Zugangsschutz	Verschlüsselung	Verwendete Algorithmen	Löschfunktion	Namensänderung	Kompression	Seite	
Blowfish Advanced 97	Win 95	30 Mark	nein	ja	Blowfish, Cobra 128, Gost, PC1, Triple-DES	ja	ja	ja	**158**	Auf Heft-CD
Encrypted Magic Folders (EMF)	Win 95	60 Dollar	nein	ja	Eigenentwicklung	nein	ja	nein	**159**	Auf Heft-CD
Face it PC	Win 95	189 Mark	ja	ja	DES	ja	nein	nein	**160**	
Norton Secret Stuff	Win 3.1x/ Win 95/NT	Freeware	nein	ja	Blowfish	nein	nein	ja	**162**	Auf Heft-CD
Norton Your Eyes Only	Win 95/NT	249 Mark	ja	ja	DES, RC4	ja	nein	nein	**162**	
Novastor Datasafe	Win 95/NT	99 Mark	nein	ja	Blowfish	ja	nein	ja	**163**	
PC Lock 98	Win 95	20 Dollar	ja	nein	entfällt	entfällt	entfällt	entfällt	**163**	Auf Heft-CD
PGP 5.5.3i	Win 95/NT	Freeware *	nein	ja	Cast, Idea, Triple-DES	ja	nein	nein	**164**	Auf Heft-CD
Private EXE	Win 95/NT	30 Dollar	ja	nein	entfällt	entfällt	entfällt	entfällt	**164**	Auf Heft-CD
PTS-Security Manager	Win 95/NT	40 Mark	nein	ja	DES	ja	nein	nein	**166**	
Safe House	Win 3.1x/ Win 95/NT	80 Dollar	nein	ja	Blowfish, DES	nein	nein	nein	**167**	Auf Heft-CD
Steganos	Win 95/NT	49 Mark	nein	ja	HWY1	ja	nein	ja	**167**	Auf Heft-CD
Top Secret	Win 95	40 Mark	nein	ja	RC4	ja	nein	nein	**168**	

* Nur für Privatanwender kostenlos; 69 Mark für kommerzielle Zwecke (Personal Edition mit zwei Lizenzen und technischem Support)

So schützen Sie vertrauliche Daten

BLOWFISH ADVANCED 97

Offen für eigene Algorithmen

Auf Heft-CD

Einzelne Dateien und ganze Verzeichnisse lassen sich mit Blowfish Advanced 97 für Windows 95 verschlüsseln. Wie der Name des Programms schon sagt, kommt dabei der Algorithmus → *Blowfish* zum Einsatz. Alternativ bietet die deutschsprachige Software vier weitere Methoden an: → *Cobra 128*, → *Gost*, → *PC1* und → *Triple-DES*. Als einziges der von uns getesteten Programme unterstützt Blowfish Advanced den UCDI-Standard (Universal Crypt Driver Interface). Dadurch lassen sich weitere Verschlüsselungs-Algorithmen in das Programm integrieren. Die erforderlichen UCDI-Treiber können Sie aus dem Internet herunterladen oder selbst programmieren – vorausgesetzt, Sie beherrschen etwa MS Visual C++ oder Borland Delphi.

Blowfish Advanced 97: Über den eingebauten Browser wählen Sie Dateien aus

Blowfish Advanced komprimiert auf Wunsch die ausgewählten Dateien vor dem Verschlüsseln. Zum Löschen der Originale bietet die Software vier Varianten an. In der sichersten Stufe werden die Originaldateien 35mal überschrieben. Für zusätzliche Sicherheit soll die Option „Dateinamen verbergen“ sorgen. Ist sie aktiviert, benennt das Programm die Dateien nach dem Verschlüsseln so um, daß niemand erkennen kann, worum es sich zuvor gehandelt hat. Blowfish Advanced besitzt einen eingebauten Dateimanager, in dem Sie die zu verschlüsselnden Dateien und Verzeichnisse auswählen. In einem Optionsfenster lassen sich dann das Paßwort und weitere Einstellungen definieren. Alternativ zum Paßwort können Sie eine „Keydisk“ erstellen. Nur mit dieser Diskette ist dann das Entschlüsseln der Dateien möglich.

DATENSCHUTZ-SOFTWARE

Blowfish Advanced 97

Markus Hahn, Nürtingen
http://blowfish.home.ml.org/
Shareware, Registrierung 30 Mark

⊕ **UCDI-Schnittstelle zum Importieren von Krypto-Algorithmen**
⊖ **kein Eintrag im Kontextmenü des Windows-Explorers**

Testurteil: Blowfish Advanced 97 bietet sichere Verschlüsselungs-Algorithmen. Das Verschlüsseln ist aber nur über den eingebauten Dateimanager möglich.

BEWERTUNG

Funktionsumfang	●●●●◐
Bedienung	●●●◐○
Sicherheit	●●●●●

DATENSCHUTZPROGRAMME: WIE WIR TESTEN

Funktionsumfang: Bei einem Verschlüsselungsprogramm ist der eingesetzte Algorithmus das Wichtigste. Pluspunkte gibt es, wenn mehrere Methoden verfügbar sind. Nach dem Verschlüsseln müssen die Originaldateien sicher vernichtet werden. Programme sollten diese Löschfunktion bieten. Eine sinnvolle Zusatzfunktion ist die Dateinamensverschleierung. Die Dateien werden nach dem Verschlüsseln so umbenannt, daß sich vom Dateinamen nicht mehr auf den Inhalt schließen läßt. Wenn Software die Daten zusätzlich komprimiert, wird sie ebenfalls höher bewertet. Software, die neben dem Verschlüsseln auch Zugangsschutz oder Restriktions-Möglichkeiten für andere Benutzer bietet, geben wir Pluspunkte. Reine Zugangsschutz-Programme bewerten wir danach, wie umfassend sich die Rechte für andere Benutzer einschränken lassen.

Bedienung: Die zu ver- und entschlüsselnden Dateien soll der Anwender möglichst schnell und einfach auswählen können. Positiv bewerten wir Programme, die einen Eintrag ins Kontextmenü des Windows-Explorers einfügen. So kann der Anwender direkt im Explorer Dateien markieren und mit der rechten Maustaste die Programmfunktionen ausführen. Andernfalls erwarten wir, daß sich Dateien zumindest per Drag & Drop auswählen und per Doppelklick entschlüsseln lassen. Die weitere Benutzerführung im Programm selbst sollte übersichtlich sein und sich an Windows-Standards orientieren.

Sicherheit: Bei der Bewertung der Sicherheit steht für uns im Vordergrund, wie schwer es ein fremder Benutzer hat, an Ihre Daten zu kommen. Die Höchstpunktzahl bekommt Software, die besonders lange Schlüssel (über 56 Bits) mit einem anerkannt sicheren Algorithmus (zum Beispiel Blowfish) verwendet. Programme wie Steganos, die die Existenz der verschlüsselten Dateien vertuschen, bekommen ebenfalls die Höchstwertung. Software aus den USA hat meist für internationale Benutzer wegen der strengen Exportrichtlinien eine maximale Schlüssellänge von 30 bis 40 Bits. Da auch dies für den privaten Einsatz noch einen sicheren Schutz bietet, bewerten wir solche Software mit „gut“.

Zugangsschutz-Programme können zwar Ihren PC gegen unbefugte Benutzung abschirmen, Ihre Daten liegen jedoch weiterhin unverschlüsselt auf der Festplatte. Ein Unbefugter hat es dadurch um ein Vielfaches leichter, an Ihre Daten zu kommen. Wir prüfen, ob schon nach einem Neustart ein voller Rechner-Zugriff möglich ist oder ob dazu eine Manipulation an Systemdateien nötig ist. Eine bessere Wertung bekommt ein Programm, wenn es bereits beim Booten nach dem Paßwort fragt und den Zugriff auf die Festplatte verhindert, auch wenn der Anwender eine Bootdiskette benutzt. Bei Software, die sowohl Verschlüsselung als auch Zugangsschutz bietet, zählen wir zum Ergebnis der Verschlüsselungs-Sicherheit einen halben Punkt dazu. Denn die Datensicherheit erhöht sich durch die Kombination beider Methoden nur minimal. ■

EMF

Verschlüsselt und versteckt

Auf Heft-CD

Die beste Verschlüsselung ist immer die, von der niemand etwas weiß. Nach diesem Prinzip arbeitet auch Encrypted Magic Folders (EMF). Die englischsprachige Shareware für Windows 95 verschlüsselt ganze Verzeichnisse und versteckt sie anschließend. Zum Verschlüsseln benutzt das Programm einen vom Hersteller selbstentwickelten Algorithmus mit variierendem Schlüssel. Auf Wunsch benennt die Software die codierten Dateien auch um.

Encrypted Magic Folders: Die Software verschlüsselt und versteckt Verzeichnisse

Das Programmfenster ist schlicht gehalten. Über den Button „Add" fügen Sie ein Verzeichnis zu einer Liste hinzu und legen anschließend fest, ob es nur verschlüsselt oder zusätzlich versteckt werden soll. Drag & Drop ist dabei nicht möglich. Beim Verlassen des Programms werden die gewählten Aktionen ausgeführt. Per Hotkey oder Start von EMF und anschließender Paßworteingabe werden die Verzeichnisse wieder freigegeben. Die Software bietet die Möglichkeit, mehrere Benutzerkonten einzurichten. Jeder zugelassene Benutzer kann damit seine eigenen Verzeichnisse schützen.

Der Hersteller weist selbst darauf hin, daß EMF Probleme mit dem DOS-Utility CHKDSK.EXE hat. Dies sieht die versteckten Verzeichnisse als ungenutzten Speicherplatz an und überschreibt unter Umständen die dort liegenden Dateien. Setzen Sie andere Festplatten-Utilities ein, rät der Hersteller, daß Sie zunächst die Kompatibilität prüfen. Wenngleich die Verschlüsselung von Encrypted Magic Folders nicht ohne weiteres zu knacken ist, lassen sich die versteckten Verzeichnisse ziemlich einfach sichtbar machen. Dazu muß der Aufruf von MF.EXE aus der AUTOEXEC.BAT entfernt werden.

DATENSCHUTZ-SOFTWARE

Encrypted Magic Folders

RSE Software, USA-Auburn
http://www.pc-magic.com
Shareware
Registrierung 60 Dollar

⊕ **Kombination von Verschlüsseln und Verstecken**
⊖ **versteckte Verzeichnisse zu einfach aufzuspüren**

Testurteil: Die Idee hinter dem Programm ist gut, die Umsetzung noch nicht perfekt.

BEWERTUNG

Funktionsumfang	●●●○○
Bedienung	●●●○○
Sicherheit	●●●○○

FACHCHINESISCH: DATENSCHUTZPROGRAMME (I)

Algorithmus

Bei der Datenverschlüsselung beschreibt der Algorithmus das Verfahren, mit dem die Daten codiert werden. Je ausgeklügelter dieser Algorithmus ist, desto sicherer ist die Verschlüsselung.

Asymmetrische Verschlüsselung

Jede Person besitzt bei dieser Methode der Verschlüsselung zwei zueinander gehörende Schlüssel: einen öffentlichen („Public Key") und einen privaten („Private Key"). Der Sender codiert seine Nachricht mit dem öffentlichen Schlüssel des Empfängers. Eine so verschlüsselte Nachricht läßt sich nur mit dem privaten Schlüssel des Empfängers wieder entschlüsseln. Pretty Good Privacy (PGP, Seite 164) ist eines der bekanntesten Programme, die nach diesem Verfahren arbeiten.

Blocklänge

Eine Datei wird in Blöcken verschlüsselt, deren Länge vom verwendeten → *Algorithmus* abhängt. Beim → *Blowfish*-Verfahren werden beispielsweise erst die ersten 64 Bits einer Datei codiert, dann die nächsten 64 Bits und so weiter.

Blowfish

Dieser sehr schnelle → *Algorithmus* bietet besonders bei 32-Bit-Prozessoren eine gute Leistung. Ein Vorteil von Blowfish ist seine variable → *Schlüssellänge* von 32 bis zu 448 Bits. Blowfish gilt als sehr sicher. Der Algorithmus wurde 1994 zum ersten Mal vorgestellt.

Cast

Cast arbeitet ähnlich wie → *DES*, ist aber zwei- bis dreimal schneller. Der → *Algorithmus* unterstützt variable → *Schlüssellängen* von 40 bis 128 Bits. Das bekannteste Programm, das Cast einsetzt, ist PGP (Seite 164). Der Algorithmus gilt als ziemlich sicher.

Cobra 128

Der relativ neue → *Algorithmus* aus dem Jahr 1996 gilt als Mutation von → *Blowfish* mit einigen Erweiterungstechniken. Ursprünglich wurde Cobra 128 als Chiffrierer mit 24 Verschlüsselungsrunden und einer → *Schlüssellänge* von 576 Bits entworfen. Durch seine offene Architektur kann er auf größere oder kleinere → *Blocklängen* erweitert beziehungsweise verkleinert werden.

DES

Der Data Encryption Standard wurde erstmals 1974 von der US-Regierung vorgestellt. In einer → *symmetrischen Verschlüsselung* werden Blöcke zu je 64 Bits mit einem 56-Bit-Schlüssel codiert. DES ist weitverbreitet, wurde allerdings schon einmal geknackt: In einer Gemeinschaftsaktion haben Anfang 1998 Zehntausende Computer in aller Welt über das Internet eine DES-chiffrierte Nachricht in mehreren Wochen entschlüsselt.

Gost

Dieser Algorithmus ist eine Entwicklung aus der früheren Sowjetunion und gilt als Gegenstück zum → *DES* aus der westlichen Welt. Obwohl Gost schon lange existiert, sind bis heute noch keine Schwächen bekannt. Seine → *Schlüssellänge* beträgt 256 Bits. ▶

So schützen Sie vertrauliche Daten

FACE IT PC

Gesichtskontrolle statt Paßwort

Face it PC für Windows 95 ist eine Kombination aus Zugangsschutz- und Verschlüsselungs-Software. Das besondere: Hier identifizieren Sie sich durch Ihr Gesicht. Dies geschieht mittels einer kleinen Kamera. In einem Lernprozeß erfaßt Face It die markanten Merkmale Ihres Gesichts. Wenn Sie Ihren PC verlassen, aktivieren Sie die Option „Lock Computer". Die englischsprachige Software sperrt daraufhin die Windows-Benutzung und scannt das Kamerabild nach Gesichtszügen ab. Sobald das Programm Sie erkennt, gibt es den Rechner wieder frei. Schwachpunkt: Mit einem Neustart läßt sich der Schutz umgehen. Sie können auch mehreren Benutzern den Zugang zu Ihrem PC per Gesichtserkennung erlauben. Restriktionen lassen sich allerdings nicht einstellen. Über die Log-Funktion sehen Sie, wer wann vor der Kamera gestanden hat.

Face it PC: Wenn das Gesicht stimmt, wird die PC-Benutzung freigegeben

Die Dateiverschlüsselung (→ *DES*-Verfahren) funktioniert ebenfalls per Gesichtserkennung. Die Erkennungsgenauigkeit war in unserem Test allerdings zwiespältig zu beurteilen: An einem Tag wurde unsere Testperson mit und ohne Brille einwandfrei innerhalb von 10 Sekunden erkannt. Am nächsten Tag dagegen brauchte Face it PC 30 Sekunden. Für den Fall, daß die Video-Erkennung nicht funktionieren sollte, drücken Sie <Esc> und geben ein vorher festgelegtes Paßwort ein. Damit wird die Gesichtserkennung umgangen – ein weiterer Schwachpunkt der Software. Zwar hätten Sie ohne eine solche Hintertür ein ziemliches Problem, wenn die Kamera nicht funktioniert. Der höhere Sicherheitsschutz, den die Software durch die Gesichtserkennung bietet, wird dadurch aber ad absurdum geführt.

DATENSCHUTZ-SOFTWARE

Face it PC

Kronenberg, Bad Homburg
Info-Tel. 01805/177350, Fax 0130/177350; ***http://www.faceit.com***
189 Mark (mit PC-Kamera 389 Mark)

⊕ **Zugangsschutz kombiniert mit Dateiverschlüsselung**
⊖ **Technik der Gesichtserkennung noch nicht ausgereift**

Testurteil: Der Zugangsschutz läßt sich leicht umgehen – er sollte sich schon beim PC-Start aktivieren lassen.

BEWERTUNG

Funktionsumfang	●●●●○
Bedienung	●●●○○
Sicherheit	●●●●○

FACHCHINESISCH: DATENSCHUTZPROGRAMME (II)

Idea

Idea ist ein möglicher Ersatz für → *DES*. Der → *Algorithmus* arbeitet wie DES mit 64-Bit-Blöcken, benutzt aber einen 128-Bit-Schlüssel.

PC1

Dieser Algorithmus ist 100prozentig kompatibel zu → *RC4*. Das Programm Blowfish Advanced 97 (Seite 158) implementiert PC1 beziehungsweise RC4 mit einer → *Schlüssellänge* von 160 Bits.

Public-Key-Verschlüsselung

→ *Asymmetrische Verschlüsselung*

RC2, RC4, RC5

Die Verschlüsselungs-Algorithmen RC2 und RC4 bieten gegenüber → *DES* eine optional größere Sicherheit, denn die Länge der Schlüssel ist hier variabel. Für den Export aus den USA muß die Schlüssellänge jedoch auf 40 Bits beschränkt werden. Es gibt aber immerhin die Möglichkeit, eine zusätzliche, bis zu 40 Bit lange Zeichenkette an den Schlüssel anzuhängen. RC5 bietet eine → *Schlüssellänge* von 2048 Bits, darf allerdings nicht aus den USA exportiert werden.

Schlüssellänge

Mit dem Schlüssel, der normalerweise aus einem Paßwort generiert wird, werden die Daten codiert. Die → *Schlüssellänge* hängt ab vom verwendeten → *Algorithmus*. Je länger der Schlüssel ist, desto schwieriger ist es, die codierten Daten zu knacken.

Steganographie

Ein steganographisches Verfahren verheimlicht, daß geheime Daten existieren. Der Gedanke dahinter: Wo niemand geheime Daten vermutet, wird sie auch niemand suchen. Steganographie-Software versteckt die geheime Datei in einem anderen Dokument. Als sogenannte Trägerdateien dienen meist BMP-Bilder, WAV- oder Textdateien.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung dient ein identischer Schlüssel zum Codieren und Decodieren. Diese Variante setzen häufig Programme ein, die Daten verschlüsseln, die beim Anwender bleiben. Möchten Sie die codierte Datei jedoch weitergeben, muß dem Empfänger das Paßwort auf einem sicheren Übertragungsweg mitgeteilt werden. Da es neben dem Gespräch unter vier Augen keine wirklich sichere Methode gibt, wird dies zum Problem. Die Public-Key-Methode umgeht es (→ *Asymmetrische Verschlüsselung*).

Triple-DES

Dieser Algorithmus erhöht die Sicherheit des normalen → *DES*-Verfahrens, indem die Daten mit dreifacher → *Schlüssellänge* (168 Bits) verschlüsselt werden. ■

So schützen Sie vertrauliche Daten

NORTON SECRET STUFF

Unkompliziert und kostenlos

Auf Heft-CD

Als kleiner Bruder von Norton Your Eyes Only (siehe unten) kommt die englischsprachige Freeware Norton Secret Stuff daher. Mit ihr lassen sich mehrere Dateien auf einmal oder einzeln verschlüsseln. Das Programm läuft unter Windows 3.1x, 95 und NT. Unter Windows 95 und NT unterstützt Norton Secret Stuff lange Dateinamen. Ganze Verzeichnisbäume können Sie allerdings nicht verschlüsseln. Aus den Dateien (bis zu 2000 auf einmal) macht Norton Secret Stuff ein komprimiertes und codiertes Archiv. Die Software benutzt dazu den Algorithmus → *Blowfish*. Damit das Programm legal aus den USA exportiert werden darf, wurde die → *Schlüssellänge* aber auf magere 32 Bit beschränkt. Norton Secret Stuff akzeptiert Paßwörter mit einer Länge zwischen drei und fünfzehn Zeichen. Das verschlüsselte Archiv im DOS-Format ist selbstentpackend. Sie müssen es zum Entschlüsseln also nur doppelt anklicken und Ihr Paßwort eingeben.

Norton Secret Stuff: verschlüsselt Dateien mit dem Blowfish-Algorithmus

Dies hat aber den Nachteil, daß Sie nur alle Dateien insgesamt und nicht einzeln decodieren können. Weiterhin unpraktisch: Norton Secret Stuff bietet keine Möglichkeit, die Originaldateien zu vernichten. Dies müssen Sie nach dem Verschlüsseln manuell erledigen.

Die Auswahl der zu verschlüsselnden Dateien erfolgt ausschließlich im Programmfenster von Norton Secret Stuff. Sie klicken auf „Add“ und können im folgenden eine oder mehrere Dateien markieren. Drag & Drop oder die Auswahl der Dateien über das Kontextmenü des Windows-Explorers sind nicht möglich. Die englischsprachige Online-Hilfe ist nicht besonders ausführlich, enthält aber zumindest informative Tips.

DATENSCHUTZ-SOFTWARE

Norton Secret Stuff

Symantec, Ratingen
Info-Tel. 069/66410300, Fax 66410333
http://www.symantec.com/nss/
Freeware (nur im Internet erhältlich)

- ⊕ **kostenloses Utility ohne Funktions-Schnickschnack**
- ⊖ **keine Löschfunktion für die Originaldateien**

Testurteil: Secret Stuff ist praktisch für gelegentliches Verschlüsseln einzelner Dateien. Weitere Funktionen fehlen.

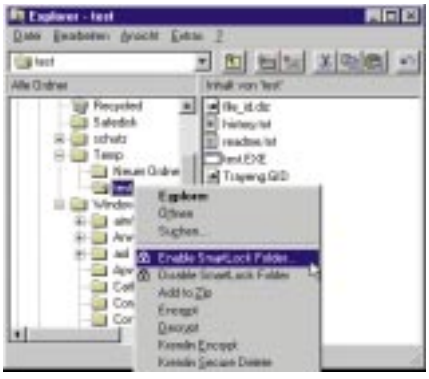
BEWERTUNG

Funktionsumfang	●●◐○○
Bedienung	●●●○○
Sicherheit	●●●●○

YOUR EYES ONLY

Zugangsschutz und Verschlüsselung

Eine Kombination aus Zugangsschutz und Dateiverschlüsselung bietet Symantec mit Norton Your Eyes Only für Windows 95 und NT. Den Zugangsschutz können Sie mit der englischsprachigen Software auf zwei Ebenen festlegen. Nur unter Windows 95 bietet das Programm „BootLock“. Diese Funktion verschlüsselt einige Systembereiche auf der Festplatte so, daß niemand auf die Platte zugreifen kann – auch nicht über eine Bootdiskette. Bei jedem Neustart des Computers fragt „BootLock“ zunächst nach Benutzernamen und Paßwort, bevor es die Festplatte freigibt und Windows startet. Wenn Sie diese mächtige Sicherheitsfunktion nicht einsetzen möchten, werden Sie erst beim Windows-Start aufgefordert, sich mit Ihrem Benutzernamen und Paßwort zu identifizieren.



Norton Your Eyes Only: Die Funktion „SmartLock“ verschlüsselt Verzeichnisse

Your Eyes Only ist Multiuser-fähig. Sie können also mehreren Anwendern den Zugriff auf Ihren PC gestatten. Jeder zugelassene Benutzer kann mit der Funktion „SmartLock“ seine privaten Verzeichnisse verschlüsseln. Dies geschieht über das Kontextmenü im Windows-Explorer. Sobald Sie neue Dateien in einem Ihrer geschützten Ordner speichern, werden diese automatisch codiert. Es stehen die Algorithmen → *DES* und → *RC4* zur Verfügung, jeweils in einer internationalen Version, die auf eine → *Schlüssellänge* von 40 Bits beschränkt ist. Nach dem Verschlüsseln werden die Originaldateien mit zweifachem Überschreiben sicher vernichtet. Als Administrator können Sie in einer Log-Datei sehen, welcher Benutzer zu welcher Zeit welches Programm gestartet hat.

DATENSCHUTZ-SOFTWARE

Norton Your Eyes Only

Symantec, Ratingen
Info-Tel. 069/66410300, Fax 66410333
http://www.symantec.de
249 Mark

- ⊕ **Kombination von Zugangsschutz und Verschlüsselung**
- ⊖ **kein Festlegen von Restriktionen auf Windows-Ebene**

Testurteil: Das Programm eignet sich für Benutzer, die den PC mit anderen teilen. Restriktions-Möglichkeiten fehlen.

BEWERTUNG

Funktionsumfang	●●●●○
Bedienung	●●●●○
Sicherheit	●●●●◐

NOVASTOR DATASAFE

Ein Tresor für Ihre Daten

Wie ein echter Tresor präsentiert sich das deutschsprachige Programm Datasafe (für Windows 95/NT) auf dem Bildschirm. Per Drag & Drop ziehen Sie Dateien in den virtuellen Safe und sperren ihn mit einem Paßwort ab. Die Software komprimiert daraufhin den Inhalt in einer einzelnen Datei und verschlüsselt diese mit dem → *Blowfish*-Algorithmus.

Novastor Datasafe: Die Benutzerführung orientiert sich an einem Tresor

Das Programm bietet aber nur eine → *Schlüssellänge* von 32 Bits. Die Originaldateien werden auf Wunsch durch einfaches Überschreiben gelöscht. Das Verschlüsseln ganzer Verzeichnisbäume unterstützt Datasafe nicht.

Zum Entschlüsseln wählen Sie im Programm die Safe-Datei aus und geben Ihr Paßwort ein. Die Software bietet allerdings keine Möglichkeit, die im Tresor abgelegten Dateien automatisch in ihr Ursprungsverzeichnis zurückzukopieren. Dies müssen Sie bei Bedarf manuell machen. Im Test erwies sich die Bedienung als unkomfortabel: Jedesmal, wenn wir den Inhalt des Tresors geändert hatten, wurden wir erneut nach einer Kombination zum „Verschließen" und einem Namen für die Safe-Datei gefragt. Punktabzug gab es auch, weil dieses Paßwort bei der Eingabe im Klartext auf dem Bildschirm angezeigt wird. Das erleichtert zwar die Eingabe, setzt aber voraus, daß Ihnen niemand dabei über die Schulter schaut.

Datasafe besitzt eine integrierte Update-Funktion, mit der Sie das Programm über das Internet automatisch auf den neuesten Stand bringen können. Für den Fall, daß Sie nicht zufrieden sind, gibt Novastor eine Geld-zurück-Garantie von 30 Tagen.

DATENSCHUTZ-SOFTWARE

Novastor Datasafe

Softline, Oberkirch
Tel. 07802/924222, Fax 924240
http://www.softline.de
99 Mark

⊕ **Blowfish-Algorithmus, mit Datenkompression**
⊖ **kein Verschlüsseln ganzer Verzeichnisbäume**

Testurteil: Die Bedienung von Datasafe soll durch die Tresor-Darstellung intuitiv sein. Sie ist aber eher umständlich.

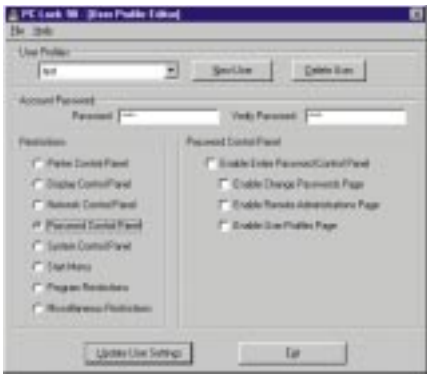
BEWERTUNG

Funktionsumfang	●●●○○
Bedienung	●●○○○
Sicherheit	●●●●○

PC LOCK 98

Schränkt die Benutzung von Win 95 ein Auf Heft-CD

PC Lock 98 ist ein Werkzeug, das den Zugriff auf Ihren PC in vielfältiger Weise beschränkt. Sie können festlegen, ob fremde Benutzer bestimmte Systemeinstellungen unter Windows 95 ändern dürfen. Dazu gehören etwa Drucker-, Grafik- und Netzwerkeinstellungen. Auch können der Suchen-Dialog, das Kommando „Ausführen" und sogar der Start-Button ausgeblendet werden. Wer Manipulationen verhindern will, sperrt den Zugriff auf die Windows-Registrierdatenbank. PC Lock wird automatisch beim Windows-Start geladen und fragt dabei Benutzernamen und Paßwort ab. Wenn Sie ohne korrekte Eingabe fortfahren, sperrt die Software den Computer mit den festgelegten Restriktionen.



PC Lock 98: Mit der Shareware können Sie Restriktionen für andere festlegen

PC Lock 98 bietet auch die Möglichkeit, Profile für mehrere Benutzer anzulegen, die Zugriff auf den PC haben dürfen. Dabei lassen sich pro Anwender die genannten Windows-Funktionen erlauben oder verbieten. Sie können für jeden Benutzer gezielt Anwendungen freigeben, die er einsetzen darf.

Wenn Sie als Adminstrator eingeloggt sind, können Sie mit Klick auf das PC-Lock-Icon in der Task-Leiste die Programmoptionen einstellen. Die Bedienung ist zwar recht übersichtlich, aber eine Online-Hilfe zur näheren Erklärung der englischsprachigen Optionen wäre doch wünschenswert.

Der Sicherheitsschutz von PC Lock 98 war auf Windows-Ebene in unseren Tests nicht zu knacken. Es gelang uns aber, durch einfaches Booten über eine Diskette an sämtliche Daten der Festplatte zu kommen.

DATENSCHUTZ-SOFTWARE

PC Lock 98

Russell Anderson, USA-Colorado Springs
http://software.pair.com/
Shareware
Registrierung 20 Dollar

⊕ **viele Möglichkeiten, Benutzer-Restriktionen festzulegen**
⊖ **Schutz nur auf Windows-Ebene, Zugriff auf Daten möglich**

Testurteil: Mit PC Lock 98 können Sie die Windows-Benutzung einschränken. Daten sind aber weiterhin zugänglich.

BEWERTUNG

Funktionsumfang	●●●◐○
Bedienung	●●●○○
Sicherheit	●●○○○

So schützen Sie vertrauliche Daten

PGP 5.5.3I

Verschlüsselt nicht nur E-Mails

Auf Heft-CD

Die englischsprachige Verschlüsselungs-Software PGP ist besonders unter Internet-Benutzern bekannt. Sie setzen das Programm häufig zum Verschlüsseln von E-Mails ein, da es nach dem → *Public-Key*-Verfahren arbeitet und mit → *Cast*, → *Idea* und → *Triple-DES* eine starke Verschlüsselung bietet. Weniger bekannt ist, daß sich die PGP-Versionen für Windows 95 und NT auch gut zum Verschlüsseln von lokalen Daten auf der Festplatte eignen. Das Programm besitzt sogar eine Option zum sicheren Löschen beliebiger Dateien. Während der Installation von PGP werden standardmäßig nach Eingabe eines Paßworts der private und der öffentliche Schlüssel generiert (→ *Asymmetrische Verschlüsselung*). Falls mehrere Benutzer auf Ihrem PC Dateien codieren möchten, können Sie über das Modul „PGPKeys“ weitere Schlüsselpaare erstellen. Dateien und Verzeichnisse (einschließlich aller Unterordner) lassen sich im Windows-Explorer per rechtem Mausklick zum Verschlüsseln auswählen. Im Kontextmenü klicken Sie dann auf „PGP, Encrypt“. In einem Dialogfenster läßt sich bestimmen, ob nur Sie oder auch andere Benutzer die Dateien wieder entschlüsseln können.

PGP 5.5.3i: Ein Assistent hilft beim Generieren des Schlüsselpaares

Zum Entschlüsseln klicken Sie die Dateien mit der Endung PGP an und geben Ihr Paßwort ein. Wenn Sie die Dateien nicht verändern, entfällt ein erneutes Codieren. Denn die verschlüsselten Dateien werden beim Entschlüsseln nicht gelöscht. Privatanwender bekommen eine kostenlose Version von PGP unter ***http://www.pgpi.com***. Wünschen Sie technischen Support oder möchten Sie das Programm geschäftlich nutzen, erwerben Sie die „Personal Edition“.

DATENSCHUTZ-SOFTWARE

PGP 5.5.3i

Network Associates, Germering
Tel. 089/8943560, Fax 89435699
http://www.nai.com
69 Mark (Personal Edition)

⊕ **sicheres Verschlüsseln durch Cast, Idea und Triple-DES**
⊖ **Public-Key-Verfahren fürs Verschlüsseln lokaler Daten überflüssig**

Testurteil: PGP ist der Standard zur E-Mail-Verschlüsselung, eignet sich aber auch dafür, lokale Daten zu schützen.

BEWERTUNG

Funktionsumfang	●●●○○
Bedienung	●●●◐○
Sicherheit	●●●●●

PRIVATE EXE

Paßwortschutz für Programme

Auf Heft-CD

Es ist nicht immer ein komplexer Zugangsschutz nötig. Mancher Anwender möchte einfach das Starten einiger Programme auf seinem Rechner unterbinden. Dafür eignet sich Private EXE für Windows 95/NT. Die englischsprachige Software schützt ausführbare Windows-Dateien vor unbefugtem Benutzen, indem sie eine Paßwortabfrage in die jeweilige EXE-Datei einbaut. Private EXE kommt dabei gleichermaßen mit Windows-3.x- und Windows-95-Programmen zurecht.

Im Programmfenster wählt der Benutzer die zu schützende EXE-Datei aus. Nach der Eingabe des gewünschten Paßworts (bis zu 16 Zeichen lang) modifiziert die Software die Datei. Beim nächsten Start des nun geschützten Programms erscheint eine Dialogbox, die zum Eintippen des Paßworts auffordert. Nur bei korrekter Eingabe startet das Programm wie gewohnt.

Private EXE: Die Software verhindert den Start von Windows-Programmen

Nachdem Private EXE den Paßwort-Schutz an den Anfang der Programmdatei gesetzt hat, speichert es die Originaldatei unter einem anderen Namen. Es empfiehlt sich, das Original zu löschen, sobald feststeht, daß die Paßwort-geschützte Version fehlerfrei funktioniert. Ansonsten könnte ein Fremder die Software durch einfaches Umbenennen dieser Backup-Datei auch ohne Paßwort zum Laufen bringen. Eine solche Löschfunktion bietet Private EXE selbst jedoch nicht.

Der Anwender sollte die Installationsdisketten oder -CDs der geschützten Programme sicher verwahren. Denn bei einer Neuinstallation werden alle Dateien durch die Originale ersetzt, also auch die geschützten EXE-Dateien.

DATENSCHUTZ-SOFTWARE

Private EXE

Midstream, USA-San Bruno
http://www.midstream.com
Shareware
Registrierung 30 Dollar

⊕ **einfacher Zugangsschutz für einzelne Programme**
⊖ **Schutz durch Neuinstallation der Anwendungen leicht zu knacken**

Testurteil: Private EXE verhindert den unbefugten Start von Programmen. Der Schutz läßt sich aber aushebeln.

BEWERTUNG

Funktionsumfang	●●○○○
Bedienung	●●●◐○
Sicherheit	●●○○○

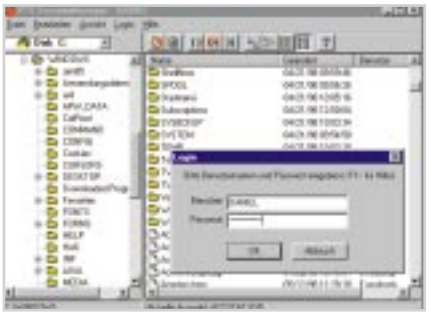
▶

So schützen Sie vertrauliche Daten

PTS-SECURITY MANAGER

Multiuser-fähiger Verschlüssler

„Kinderleichtes Verschlüsseln von Dateien und Verzeichnissen“ verspricht der deutschsprachige PTS-Security Manager für Windows 95/NT. „Kinderleicht“ ist jedoch übertrieben: Die Dateiauswahl per Kontextmenü im Windows-Explorer wird von der Software ebensowenig unterstützt wie Drag & Drop. Dateien und Verzeichnisse zur Verschlüsselung auswählen kann der Anwender lediglich in dem eigenen Dateimanager des Security Managers. Die Bedienung des Dateimanagers ist zunächst gewöhnungsbedürftig. Die Funktion der Icons, mit denen Sie das Ver- oder Entschlüsseln starten, läßt sich durch deren Motive nur schwer erahnen. Immerhin: Neben jeder Datei wird angezeigt, ob sie für jedermann zugänglich ist oder welcher Benutzer sie verschlüsselt hat.



PTS-Security Manager: Mehrere Benutzer können eigene Dateien codieren

Der PTS-Security Manager bietet die Möglichkeit, ganze Verzeichnisbäume auf einmal zu codieren. Bei der Methode hat der Benutzer aber keine Wahl: Das Programm offeriert nur den → *DES*-Algorithmus. Die Originaldateien werden durch einfaches Überschreiben gelöscht. Die codierten Dateien selbst benennt die Software aber nicht um. Im Programmfenster des Security Managers erscheinen sie zwar deutlich markiert. Im Windows-Explorer merkt man aber erst nach dem Aufrufen der Dateien, daß sie codiert sind. Der PTS-Security Manager verfügt auch nicht über eine Kompressionsfunktion.

Praktisch fanden wir die Multiuser-Option. Mehrere Benutzer können mit eigenem Login-Namen und Paßwort ihre persönlichen Daten verschlüsseln. Diese Zugangsdaten werden bei jedem Programmstart neu abgefragt.

DATENSCHUTZ-SOFTWARE

PTS-Security Manager

Hilchner Daten & Medien, Neuss
Tel. 02131/34940, Fax 349499
http://www.hilchner.de
40 Mark

- **eigener Login-Name und Paßwortschutz für mehrere Benutzer**
- **gewöhnungsbedürftige Benutzerführung, nur DES-Verschlüsselung**

Testurteil: Der Security Manager eignet sich zum privaten Einsatz. Die Benutzerführung ist gewöhnungsbedürftig.

BEWERTUNG

Funktionsumfang	●●●○○
Bedienung	●●◐○○
Sicherheit	●●●●○

10 TIPS: SO FINDEN SIE DAS RICHTIGE PASSWORT

Die beste Verschlüsselung nützt nichts, wenn Sie Fehler bei der Wahl Ihres Paßworts machen. Wir sagen Ihnen, was Sie beachten sollten.

1. Benutzen Sie keinesfalls Paßwörter, die sich leicht erraten lassen. Also nicht Ihren Namen, Ihr Geburtsdatum oder den Namen Ihrer Partnerin oder Ihres Partners.

2. Verwenden Sie möglichst lange Paßwörter. Denn je mehr Zeichen ein Kennwort besitzt, um so schwieriger ist es zu knacken. Mindestens sechs Zeichen sollte es haben.

3. Bauen Sie Ziffern und Zeichen wie Komma und Doppelpunkt oder einen Leerschritt ein: Beispiel: „12hack,er“. So erschweren Sie es Crack-Programmen, durch bloßes Ausprobieren vieler Paßwörter ans Ziel zu kommen.

4. Noch schwerer machen Sie es Crack-Programmen, wenn Sie sinnlose Kennwörter benutzen, etwa „KTGEBG_hjk jku“. Diese lassen sich allerdings schlecht merken.

5. Sinnlose Paßwörter lassen sich leichter einprägen, wenn Sie sich als Eselsbrücke der Anfangsbuchstaben eines Sprichworts oder einer Redewendung bedienen. Zum Beispiel: „WHNLLHN“ für „Was Hänschen nicht lernt, lernt Hans nimmermehr“.

6. Bauen Sie absichtlich Schreibfehler in Ihr Paßwort ein, etwa „PC-WÄLD“ statt „PC-WELT“.

7. Viele Anwendungen unterscheiden bei der Paßwortabfrage zwischen der Groß- und Kleinschreibung. Nutzen Sie dies und variieren Sie nach Lust und Laune. Aus „WHNLLHN“ in Tip 5 wird so beispielsweise „WHnllHn“.

8. Benutzen Sie möglichst für jede Anwendung ein anderes Kennwort.

9. Gewöhnen Sie sich an, Ihr Paßwort regelmäßig zu ändern. Denn falls Ihnen doch einmal jemand bei der Eingabe über die Schulter geschaut hat, verhindern Sie auf diese Weise weiteren Mißbrauch.

10. Auch wenn Ihr Programm eine Option zum Speichern eines Paßworts bietet: Aktivieren Sie sie nicht. Der Preis für die Bequemlichkeit ist, daß es irgendwo auf Ihrer Festplatte gespeichert wird, im schlimmsten Fall unverschlüsselt. ■

Paßwort speichern: Auch wenn Programme diese Möglichkeit bieten, sollten Sie sie nicht aktivieren (Tip 10)

SAFE HOUSE

Richtet verschlüsseltes Laufwerk ein

Auf Heft-CD

Arbeiten Sie mit mehreren verschlüsselten Verzeichnissen oder Dateien, ist es mühselig, diese bei jedem Programmstart einzeln zu entschlüsseln und vor dem Herunterfahren des Computers wieder zu verschlüsseln. Die englischsprachige Software Safe House (für Windows 3.1x/95/NT) bietet dafür eine Lösung: Sie erstellt für diesen Zweck ein virtuelles Laufwerk. Alles, was Sie darauf speichern, wird automatisch verschlüsselt und erst in dem Moment freigegeben, wenn Sie mit einem Programm darauf zugreifen. Beim Herunterfahren des Computers wird die Zuordnung der virtuellen Festplatte aufgelöst. Beim nächsten Windows-Start fragt die Software Sie nach dem vorher festgelegten Paßwort, bevor Sie wieder auf die Daten zugreifen können.

Safe House: Die Shareware erstellt ein virtuelles verschlüsseltes Laufwerk

Ein virtuelles Laufwerk anzulegen geht recht einfach von der Hand: In einer Dialogbox geben Sie an, welche Speicherkapazität das neue Laufwerk haben soll (1 KB bis 2 GB) und wo das Image (die Datei, die alle Daten des Laufwerks beinhaltet) auf der Festplatte gespeichert wird. Anschließend wählen Sie den Verschlüsselungs-Algorithmus. Hier stehen die internationalen Versionen von → *Blowfish* (→ *Schlüssellänge*: 32 Bits) und → *DES* (40 Bits) zur Verfügung. Safe House erstellt die Image-Datei sowie einen neuen Laufwerksbuchstaben unter Windows. Mit der neuen virtuellen Festplatte können Sie nun wie mit einer normalen arbeiten. Ihre geheimen Dateien verschieben Sie einfach dorthin. Safe House bietet jedoch keine Möglichkeit, die Originaldateien auf der Festplatte zu vernichten. Auch eine Möglichkeit zur Kompression der Image-Datei fehlt.

DATENSCHUTZ-SOFTWARE

Safe House

PC Dynamics, USA-Westlake Village
http://www.pcdynamics.com/SafeHouse/
Shareware
Registrierung 80 Dollar

⊕ **automatisches Ver- und Entschlüsseln**
⊖ **keine Löschfunktion, keine Datenkompression**

Testurteil: Safe House ist praktisch, wenn Sie viele verschiedene Verzeichnisse häufig ver- und entschlüsseln.

BEWERTUNG

Funktionsumfang	●●●○○
Bedienung	●●●○○
Sicherheit	●●●●○

STEGANOS

Versteckt geheime Daten in Bildern

Auf Heft-CD

Eines der ersten deutschsprachigen Programme für → *Steganographie* ist Steganos für Windows 95/NT. Das Programm beherrscht das Verstecken von Dateien in Grafik- (BMP, DIB), Klang- (WAV, VOC), HTML- und Ascii-Dateien. Zur optimalen Sicherheit kann die Software die geheimen Dateien zuvor mit dem HWY1-Algorithmus (→ *RC4*-kompatibel) verschlüsseln. Zusätzlich ist Datenkompression möglich. Zum unwiderruflichen Löschen überschreibt Steganos die Originaldateien mit Zufallswerten. Mit dem mitgelieferten „Shredder" können Sie diese sichere Löschmethode auch anstelle des Windows-Papierkorbs benutzen.

Steganos: Ein Assistent hilft Ihnen beim Verstecken Ihrer Daten

Die Bedienung von Steganos ist einfach: Ein Assistent führt Sie Schritt für Schritt zum Ziel. Zunächst werden Sie nach der Quelldatei gefragt. Sie können festlegen, ob die Datei nur versteckt, nur verschlüsselt oder versteckt und verschlüsselt werden soll. Nach der Wahl eines Paßworts verlangt Steganos den Namen der Trägerdatei. Sollte diese zu klein sein, um die Quelldatei aufzunehmen, bekommen Sie einen entsprechenden Warnhinweis angezeigt. Allerdings gibt Steganos keine Auskunft darüber, wie groß die Trägerdatei sein muß. Bei unserem Test haben wir nur durch langwieriges Probieren eine passende Datei gefunden. Das kombinierte Verstecken und Verschlüsseln bietet einen hohen Sicherheitsschutz. Denn der Trägerdatei ist es nicht anzumerken, daß sie eine weitere Datei in sich trägt. Und selbst wenn jemand die Steganographie entdeckt, benötigt er immer noch das Paßwort, um an die geheimen Daten heranzukommen.

DATENSCHUTZ-SOFTWARE

Steganos

JDS-Software, Varel
Tel. 04451/959195, Fax 959196
http://www.demcom.com/deutsch/steganos/
Shareware, Registrierung 49 Mark

⊕ **wirkungsvoller Datenschutz durch Verschlüsseln und Verstecken**
⊖ **nur einzelne Dateien chiffrierbar, keine Auswahl der Kryptomethode**

Testurteil: Sensible Daten lassen sich mit Steganos sicher verwahren. Der Algorithmus läßt sich aber nicht wählen.

BEWERTUNG

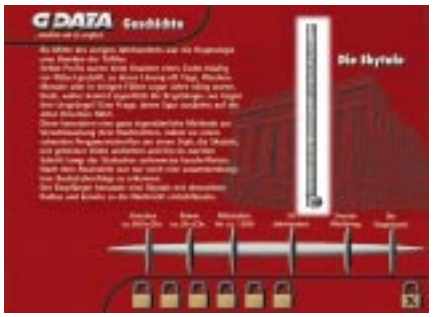
Funktionsumfang	●●●◐○
Bedienung	●●●◐○
Sicherheit	●●●●●

So schützen Sie vertrauliche Daten

TOP SECRET

Mit 160 Bits Schlüssellänge

Mit dem →*RC4*-Algorithmus (→*Schlüssellänge*: 160 Bits) verschlüsselt das deutschsprachige Top Secret Dateien und Verzeichnisstrukturen. Gelöscht werden die Originaldateien durch einfaches Überschreiben. Top Secret für Win 95 komprimiert die verschlüsselten Dateien allerdings nicht. Sie können festlegen, daß Ihr Paßwort für eine bestimmte Zeit im Speicher bleibt. Innerhalb dieser Zeit können Sie Dateien ohne erneute Paßworteingabe ver- und entschlüsseln. Diese Bequemlichkeit ist jedoch nur anzuraten, wenn Sie sicher sind, daß Sie Ihren PC während dieser Zeit nicht verlassen.



Top Secret: In einer Multimedia-Show erfahren Sie Hintergründiges

Die Bedienung von Top Secret ist unkompliziert. Nach der Installation fordert Sie die Software auf, Ihr Paßwort zu definieren, und fügt einen Eintrag ins Kontextmenü des Windows-Explorers hinzu. Nach einem rechten Mausklick können Sie dann Dateien und Verzeichnisse zum Verschlüsseln auswählen. Um den Vorgang zu starten, müssen Sie allerdings erst das Paßwort eingeben, das Sie bei der Installation vergeben haben. So verhindern Sie, daß jemand unbefugt Ihre Daten codiert. Der Nachteil dabei: Sie haben keine Möglichkeit, für jede zu verschlüsselnde Datei ein eigenes Paßwort festzulegen. Es läßt sich nur global ändern.

Das Entschlüsseln funktioniert nach dem gleichen Prinzip, alternativ auch über einen Doppelklick.

Für Einsteiger interessant sind die zusätzlichen Informationen, die sich noch auf der Installations-CD befinden. In einer interaktiven Präsentation erfahren Sie Wissenswertes zur Geschichte der Kryptologie und zu verschiedenen Verschlüsselungstechniken.

DATENSCHUTZ-SOFTWARE

Top Secret

G-Data, Bochum
Tel. 0234/9762110, Fax 9762299
http://www.gdata.de
40 Mark

⊕ **einfache Bedienung über das Kontextmenü**
⊖ **keine Kompression der Dateien, nur ein Paßwort verwendbar**

Testurteil: Durch die Präsentation und die einfache Bedienung eignet sich Top Secret gut für Kryptographie-Einsteiger.

BEWERTUNG

Funktionsumfang	●●●○○
Bedienung	●●●●○
Sicherheit	●●●●●

■

TIPS: DATEN SCHÜTZEN OHNE ZUSATZ-SOFTWARE

Um Ihre persönlichen Daten geheimzuhalten, brauchen Sie nicht unbedingt ein spezielles Kryptographie-Programm. Eine gewisse Sicherheit bietet Ihnen auch die Software, die Sie ohnehin auf Ihrem Rechner installiert haben, sowie die PC-Hardware selbst. Aber beachten Sie: Die hier vorgestellten Methoden sind teilweise leicht zu knacken und schützen nur vor spontaner Neugier, etwa eines Kollegen.

OFFICE-PAKETE

Alle neueren Versionen der Office-Pakete ermöglichen es, Ihre Dateien mit einem Paßwort zu versehen. Unter **Microsoft Office** (Word, Excel und Access) aktivieren Sie den Schutz, indem Sie den Befehl „Datei, Speichern unter" wählen und auf „Optionen" klicken. Dort können Sie ein Schreibschutz- und ein Schreib-/Lesekennwort festlegen. Die zweite Option schützt das Dokument vor jeglichem Zugriff, die erste verhindert nur das unbefugte Ändern der Datei.

In **Star Office** von Stardivision setzen Sie bei „Speichern unter" ein Häkchen vor „Paßwort" und klicken auf den Button „Speichern". Analog verfahren Sie in der **Wordperfect Suite** von Corel. Der Paßwortschutz der Office-Pakete ist allerdings nicht besonders sicher. Im Internet kursieren Programme, mit denen sich der Schutz teilweise leicht knacken läßt.

BILDSCHIRMSCHONER

Dem Windows-95-Screensaver können Sie ein Paßwort zuweisen. Sobald der Schoner aktiv ist und jemand den PC benutzen möchte, fordert Windows dessen Eingabe, bevor der Desktop wieder sichtbar wird. Das Paßwort können Sie im Start-Menü über „Einstellungen, Systemsteuerung, Anzeige, Bildschirmschoner" festlegen. Durch einen einfachen Neustart des Computers läßt sich dieser Schutz aber aushebeln. Wie in unserem „Tip des Monats" auf Seite 183 in dieser Ausgabe beschrieben, gibt es auch Tools, die das Kennwort im Klartext ausgeben.

BIOS-PASSWORT

Besseren Schutz bietet das Bios-Paßwort. Haben Sie es einmal eingerichtet, wird es beim Einschalten und bei jedem Neustart des PCs abgefragt. Ein Umgehen des Schutzes ist nur möglich, wenn Master-Paßwörter existieren und durch Öffnen des PCs bei Manipulation der Hauptplatine (siehe „Die Paßwort-Falle", PC-WELT 10/97, Seite 62). So richten Sie das Bios-Paßwort ein: Drücken Sie nach dem Einschalten des PCs mehrmals auf <Entf>. Je nach Hersteller kann auch eine Tastenkombination das Bios-Menü aufrufen. Suchen Sie nach dem Punkt „Paßwort" oder „Security". Dort können Sie Ihr Paßwort festlegen. Beim Award-Bios müssen Sie unter „Bios Features Setup, Security Option" noch einstellen, daß das Paßwort beim Systemstart abgefragt werden soll.

KOMPRESSIONSPROGRAMME

Fast jeder Packer erlaubt es, das Entpacken eines Archivs mit einem Paßwort zu schützen. Bei ARJ legen Sie beim Packen mit dem Schalter -g ein Kennwort fest, zum Beispiel „arj a -g<Paßwort> <Archivname>". Bei Pkzip verwenden Sie dazu den Schalter -s. ■