ILLUSTRATION RICHARD DOWNS

Hinter Schloss und Riegel

Geben Sie Datendieben keine Chance! Wir zeigen, wie persönliche Daten geschützt werden können und wie sicher die Methoden sind.

● *von Beat Rüdt*

Auf einer Festplatte befinden sich viele persönliche Daten: die gesamte E-Mail-Korrespondenz, Briefe, Fotoalben, Ferienvideos, Tagebücher, aber auch Geschäftsberichte und andere vertrauliche Dokumente. Das macht den Computer interessant – z. B. für neugierige Kollegen oder gar für hinterlistige Spione und Datendiebe. Ist der PC ans Internet angeschlossen und unzureichend geschützt, haben diese besonders leichtes Spiel. Alle Daten werden kopiert, ohne dass es der Besitzer merkt.

Ärgerlich ist es aber auch, wenn bei einem Einbruch nicht nur der Familienschmuck, sondern noch das Notebook geklaut wird. Ohne Sicherheitsvorkehrungen hat ein Dieb sofort Zugriff auf sämtliche Dateien.

In diesem Artikel zeigen wir Ihnen daher Mittel und Wege, wie Sie Ihren PC oder Ihr Notebook vor Datenklau sichern. Dafür gibt es zwei verschiedene Ansätze: Einerseits verhindert ein Zugangsschutz, dass ein Datendieb das Betriebssystem überhaupt starten kann, andererseits werden die Dateien auf der Festplatte so abgelegt, dass sie – falls der Betriebssystemschutz geknackt wird – für Fremde nicht lesbar sind.

Wir haben die Tricks mit Windows 2000 und XP getestet und – sofern benötigt – mit Office 2000 und XP. Die Tipps eignen sich auch für Computer, die für mehrere Benutzer eingerichtet sind. Ohne Schutz haben nämlich alle Anwender Zugriff auf alle Dateien des Systems.

Die Schutzmechanismen werden in drei Sicherheitsstufen unterteilt:

- Die erste Stufe beinhaltet einfache Massnahmen, die im Betriebssystem bereits vorgesehen, aber nicht aktiviert sind.
- Die zweite Stufe zeigt aufwändigere Möglichkeiten innerhalb des Betriebssystems und Lösungen, die Zusatzprogramme voraussetzen.
- Die dritte Stufe schützt effizient, setzt aber fortgeschrittene PC-Kenntnisse voraus.

Sicherheitsstufe 1

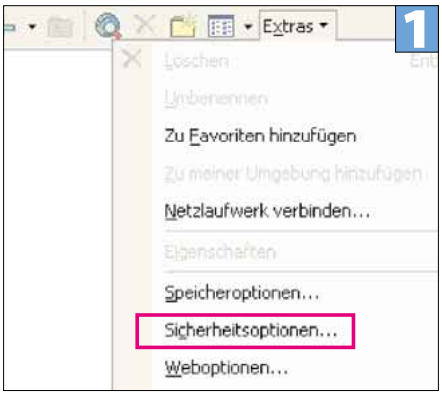
Office-Dateien mit Passwortschutz: Am einfachsten werden Daten mit einem Passwort vor fremden Blicken geschützt. In Word 2002 (in Office XP) ist das eine Option, die beim Speichervorgang aufgerufen wird. Klicken Sie auf DATEI/SPEICHERN UNTER und im folgenden Dialogfeld auf EXTRAS und dann SICHERHEITSOPTIONEN... (Word 2000: ALLGEMEINE OPTIONEN), **Screen 1**.

Das Fenster «Sicherheit» bietet nun zwei Möglichkeiten: je ein Kennwort zum Öffnen, **Screen 2**, **A**, und eines zum Bearbeiten der Datei, **B**.

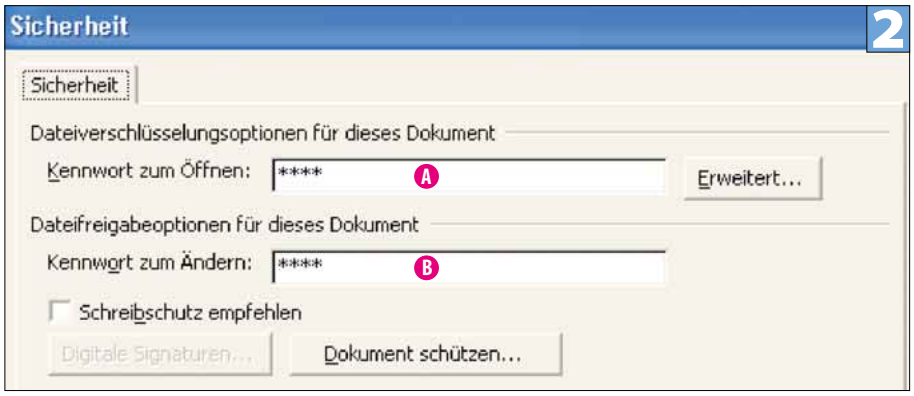
Nach einem Klick auf OK müssen Sie beide Kennwörter in einem Fenster nochmals bestätigen. Schliessen Sie den Speichervorgang ab mit einem Klick auf SPEICHERN im Fenster «Speichern unter».

In Zukunft muss das Passwort sowohl beim Öffnen wie auch fürs Bearbeiten des Dokumen-

Sicherer PC, sichere Daten



Verpassen Sie Office-Dateien ein Passwort.



Auf Wunsch wird das Passwort später beim Öffnen und beim Bearbeiten abgefragt.

tes eingegeben werden. Meistens dürfte es aber ausreichen, nur das erste Passwort zu setzen.

Bewertung: Eine unkomplizierte Methode, die wenig Zeitaufwand kostet, aber auch einfach auszutricksen ist. Zum Beispiel mit dem Programm Zip Cracker (**WEBCODE 24165**).

Zugang Betriebssystem: Windows XP und 2000 unterscheiden auf Wunsch verschiedene Benutzer. Jeder erhält einen eigenen Speicherort für persönliche Daten und E-Mail-Ordner und kann eigene Systemeinstellungen vornehmen, z. B. das Hintergrundbild ändern und private Ordner verwalten. Das ist praktisch, wenn mehrere Personen am selben PC arbeiten.

Den Benutzern sind unterschiedliche Rechte zugeteilt. Man unterscheidet Computeradministrator-Konten, mit denen alle Einstellungen und Zugriffe erlaubt sind, und eingeschränkte Konten. Deren Benutzer können neben den allgemein zugänglichen Bereichen auf dem PC nur ihre persönlichen Daten sehen und bearbeiten. Die dritte Variante ist ein Gastkonto, mit dem ein Zugriff auf persönliche Daten anderer Benutzer ebenfalls nicht möglich ist.

Damit niemand Ihre Einstellungen verändern kann oder auf Ihre Dateien zugreift, schützen Sie Ihren Benutzerzugang mit einem Kennwort. Eingestellt wird das unter START/SYSTEMSTEUERUNG/BENUTZERKONTEN. Sie sehen vor sich das Fenster «Benutzerkonten» und wählen Ihren Eintrag, **Screen 3**. Falls nur ein Benutzer eingerichtet ist, hat er die Rechte des Computeradministrators.

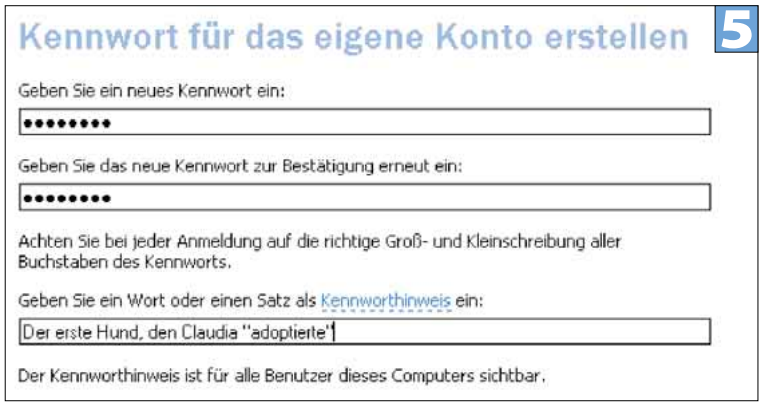
Ein Klick auf das Konto, das geändert werden soll, zeigt verschiedene Funktionen an. Wählen Sie «Kennwort erstellen», **Screen 4**.

Das Passwort ist zweimal einzugeben, um Tippfehlern vorzubeugen. Zudem können Sie einen Kennworthinweis hinterlegen – als Eselsbrücke, falls Sie das Passwort vergessen sollten, **Screen 5**.

Nach einem Klick auf «Passwort erstellen» fragt Windows: «Möchten Sie Dateien und Ordner nur für die eigene Verwendung einschränken?», was mit einem Klick auf JA, NUR FÜR EIGENE VERWENDUNG beantwortet wird. Danach rechnet der Computer einige Minuten, bis die Rechte neu verteilt sind. Nun kann nur noch der Be- ▶

Einer der im System eingetragenen Benutzer ist gleichzeitig auch der Computeradministrator.

Die Option KENNWORT ERSTELLEN führt zur Passwort-Definition.



Die Eselsbrücke darf nur Ihnen helfen, ein vergessenes Passwort zu rekonstruieren.

▶ nutzer auf die Dateien zugreifen, der sich mit dem Passwort angemeldet hat.

Unter Windows 2000 ist die Funktion unter START/SYSTEMSTEUERUNG/BENUTZER UND KENNWÖRTER zu finden. Im Register BENUTZER wird ein Benutzer ausgewählt. Nach einem Klick auf den Button KENNWORT ÄNDERN erscheinen die Felder zum Eingeben des Passwortes. Jetzt hat nur noch der Administrator und der angemeldete Benutzer auf alle Dateien Zugriff, nicht aber andere Nutzer.

Sie können sogar noch weiter gehen und die Passworteingabe auch dann verlangen, wenn jemand versucht, den PC zu reaktivieren, nachdem sich der Bildschirmschoner eingeschaltet hat. Die Einstellung versteckt sich in der Systemsteuerung: Klicken Sie auf START/(EINSTELLUNGEN)/SYSTEMSTEUERUNG/ANZEIGE und anschliessend auf das Register BILDSCHIRMSCHONER. Aktivieren Sie das Kontrollkästchen KENNWORTEINGABE BEI REAKTIVIERUNG und schliessen Sie mit ÜBERNEHMEN ab, **Screen 6**.

Bewertung: Diese Methode schützt alle persönlichen Dateien. Andere Benutzer des Computers können nicht mehr darauf zugreifen. Allerdings gibt es auch für diesen Schutz Programme im Internet, die das Passwort knacken, z. B. Offline NT Password & Registry Editor (**WEBCODE 24166**).

Ein Hinweis für Notebook-Anwender: Falls Sie Ihr Gerät bei Nichtgebrauch meistens nur in den Ruhezustand versetzen, nützt ein passwortgeschütztes Benutzerkonto wenig. Es sei denn, Sie verabschieden sich jedes Mal mit START/ABMELDEN bzw. START/BEENDEN (Windows 2000) vom Betriebssystem, bevor Sie Ihr Notebook «zuklappen».

6 **Mit dieser Einstellung bedarf es des Windows-Passworts, um den Bildschirmschoner zu umgehen.**

7 **Ordner lassen sich mit diesem Häkchen verstecken.**

Daten verstecken: Ein Datendieb kommt nur an Dokumente, die er sieht. Deshalb ist wohl die einfachste Methode, sich zu schützen, Ordner mit sensiblem Inhalt unsichtbar zu machen. Die Funktion dafür versteckt sich im Kontextmenü EIGENSCHAFTEN, das bei einem Rechtsklick auf einen Ordner erscheint. Ist das Kontrollkästchen «Versteckt» markiert, ist der Ordner unsichtbar, **Screen 7**.

Bewertung: Unsichtbare Ordner lassen sich mit einer einfachen Einstellung wieder einblenden. Dies ist auch der Weg, den Benutzer wählen müssen, wenn sie ihre eigenen versteckten Ordner wieder anzeigen wollen. Im Windows-Explorer unter EXTRAS/ORDNEROPTIONEN im Register ANSICHT steht unter «Erweiterte Einstellungen» «Alle Dateien und Ordner anzeigen». Ist die Funktion aktiviert, sieht man auch die versteckten Ordner. Trotzdem lohnt sich dieser Trick: Was nicht auf dem Servierteller präsentiert wird, weckt zumindest kein Interesse.

Sicherheitsstufe 2

Anmeldung mit Benutzernamen und Passwort: In Windows XP werden nach dem Aufstarten die eingetragenen Benutzer angezeigt. Nur wer das Passwort eines Benutzers kennt, kommt weiter. Die Anmeldung am Computer kann aber so verändert werden, dass sowohl Benutzername und Passwort bei der Anmeldung abgefragt werden. Diese Kombination erschwert einem Hacker den Zugriff auf den Computer zusätzlich.

Die Einstellung wird wie bei der Festlegung des Passwortes (siehe «Zugang Betriebssystem», S. 47) im Fenster «Benutzerkonten» eingestellt. Wählen Sie ART DER BENUTZERANMELDUNG ÄNDERN. Das Häkchen vor «Willkommensseite verwenden» ist zu entfernen, bevor Sie die Einstellung mit OPTIONEN ÜBERNEHMEN abschliessen. Beim nächsten Aufstarten des PCs werden Benutzername und Passwort verlangt.

Bewertung: Jetzt ist nicht mehr ersichtlich, wie viele verschiedene Benutzerkonten es gibt, und schon gar nicht, ob ein Gastkonto vorhanden ist, das ein Login ohne Passwort erlaubt. Leider ist beim Anmelden immer noch der Name des *letzten* Benutzers sichtbar, immerhin nicht mehr alle anderen Konten. (In Windows 2000 ist das übrigens standardmässig so.)

Daten verschlüsseln: Für das Verschlüsseln von Daten gibt es viele Programme, die teils gratis, teils gegen Bezahlung bezogen werden. Das bekannte, einfach zu bedienende PGP 8.0 haben wir im PCtip 2/2003 vorgestellt. Sie finden den Artikel auf der PCtip-Website: **http://www.pctip.ch/library/pdf/03/02/0240_pgp.pdf**.

Noch sicherer ist DriveCrypt, das Sie als Download auf der PCtip-Webseite finden (**WEBCODE 20076**). Das Programm kann 30 Tage kostenlos mit wenigen Einschränkungen auspro-

Tipps für noch mehr Sicherheit

Die Hardware professionell absichern

Schutz der Hardware

Viele der im Artikel vorgestellten Datensicherheitslösungen lassen sich überwinden, wenn man genug Zeit hat. Daher lohnt es sich für einen Dieb, das ganze Gerät abzuzügeln – was bei Notebooks besonders einfach ist – und erst später die Zugangsbarrieren zu knacken.

Lösung: Dagegen gibt es erstaunlicherweise auf dem Markt nur wenige Abhilfen. Allerdings sind viele Notebooks (und auch Flachbildschirme) mit einem kleinen Schlitz versehen. In diese Öffnung passen Schlösser verschiedener Hersteller. Ähnlich wie das Velo in der Stadt kann so der Computer «angekettet» werden. Ähnliche Lösungen existieren auch für Desktop-PCs.

Schutz der Laufwerke

Einige der beschriebenen Sicherheitsvorkehrungen lassen sich mit Hilfe einer Start-CD oder Start-Diskette umgehen.

Lösung: Das kann man nur verhindern, wenn der Zugang zum Laufwerk mit einem Laufwerksschloss versperrt wird. Das Schloss wird wie eine Diskette oder ein Zip in den Laufwerksschlitz gesteckt. Bei Laufwerken, bei denen die Medien in eine Schublade eingelegt werden (CD-ROM), wird das Schloss so angebracht, dass sich das Laufwerk nicht mehr öffnen kann.

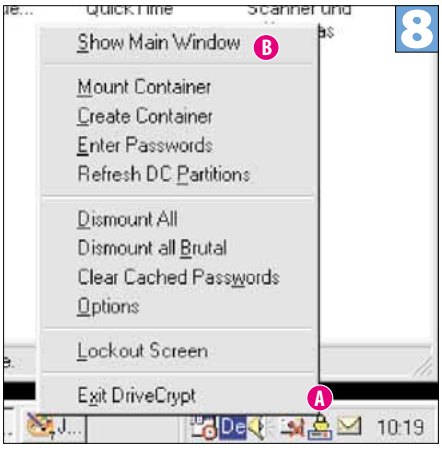
Schützt vor Diebstahl: das «Veloschloss» für Notebooks.

Ein Laufwerksschloss verhindert, dass Unbefugte den PC mit einer Diskette starten.

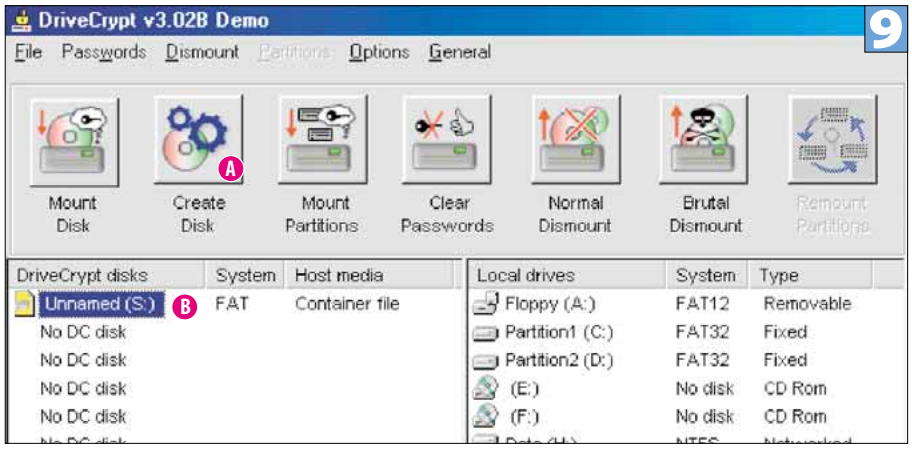
Erweiterte Verschlüsselung

Auf dem Markt sind auch verschiedene Sicherheitslösungen, die mit einer Kombination aus Soft- und Hardware Daten schützen. Meist sind es Verschlüsselungs-Programme, die Daten erst entschlüsseln, wenn auch eine bestimmte Hardware-Komponente vorhanden ist. Das kann eine PC-Card sein oder auch ein USB-Stick (Dongle), die eingeschoben bzw. eingesteckt sein müssen. Solche Lösungen gibt es entweder direkt von Computerherstellern, z. B. IBM, oder von spezialisierten Firmen, z. B. die CryptoCard von Infosys, http://www.infosys.com/.

Sicherer PC, sichere Daten



DriveCrypt: nach Installation in der Taskleiste



DriveCrypt: Die Programmoberfläche ist übersichtlich, aber in Englisch.

biert werden. Danach werden 49.95 Dollar fällig. Nachfolgend ein paar Tipps zu Installation und Gebrauch von DriveCrypt.

Nachdem Sie das Installations-Programm auf Ihren Rechner heruntergeladen haben, starten Sie die Installation mit einem Doppelklick auf die Datei. Klicken Sie beim Begrüssungsfenster auf NEXT, bei den Lizenzdetails auf YES, bei den Installationsdetails, den Konfigurationsoptionen und dem Benutzernamen jeweils auf NEXT. Am Schluss markieren Sie den Button «Yes I wish to restart my computer now» und klicken auf FINISH, um den Computer neu zu starten.

Nach dem Neustart finden Sie das DriveCrypt-Symbol in der Taskleiste, **Screen 8**, **A**. Mit einem Doppelklick auf das Symbol oder einem Rechtsklick, gefolgt von der Auswahl SHOW MAIN WINDOW, öffnen Sie das Haupt-Programm, **B**.

Im ersten Schritt wird ein so genannter Container erstellt, der Dateien verschlüsselt speichert. Ist der Container geöffnet, also das Passwort bereits eingegeben, wird er im Windows-Explorer wie eine Festplatte angezeigt und kann auch genauso verwendet werden. Ist der Container nicht aktiv, sieht man nur eine einzelne Datei, die sich nicht öffnen lässt.

Klicken Sie auf CREATE DISK, **Screen 9**, **A**, im ersten Fenster auf NEXT und bestimmen Sie dann die Grösse des Containers im Feld «[Size of Container File]», zum Beispiel 100 MB. Weiter gehts mit NEXT. Nun geben Sie bis zu vier verschiedene, mindestens achtstellige Passwörter ein. Je mehr Passwörter Sie verwenden, desto schwieriger wird das Knacken der verschlüsselten Dateien. Jedes Passwort wird sicherheitshalber zweimal eingegeben.

Im folgenden Fenster wird ein Zusatzschlüssel generiert. Das Programm verlangt vom Benutzer dazu ca. 100 Mal einen Klick auf den Button, der abwechselnd PICK und RANDOM anzeigt.

Diese Klick-Aktion garantiert, dass für Sie ein einmaliger, individueller Schlüssel generiert wird. Diesen benötigt das Programm – nebst den von Ihnen gewählten Passwörtern – beim Verschlüsseln Ihrer Daten im Container.

Erst danach geht es mit zwei Mal NEXT weiter. Nach einem Klick auf CREATE IT! wird das virtuelle Laufwerk erstellt, das auf die Container-Datei zeigt. Schliessen Sie mit FINISH ab. Jetzt sehen Sie im Programmfenster den Container, **Screen 9**, **B**.

Das Programm ordnet ihm einen Laufwerksbuchstaben zu, über den er mit dem Windows-Explorer erreicht wird. Sie können jetzt bereits Dateien auf dem virtuellen Laufwerk ablegen.

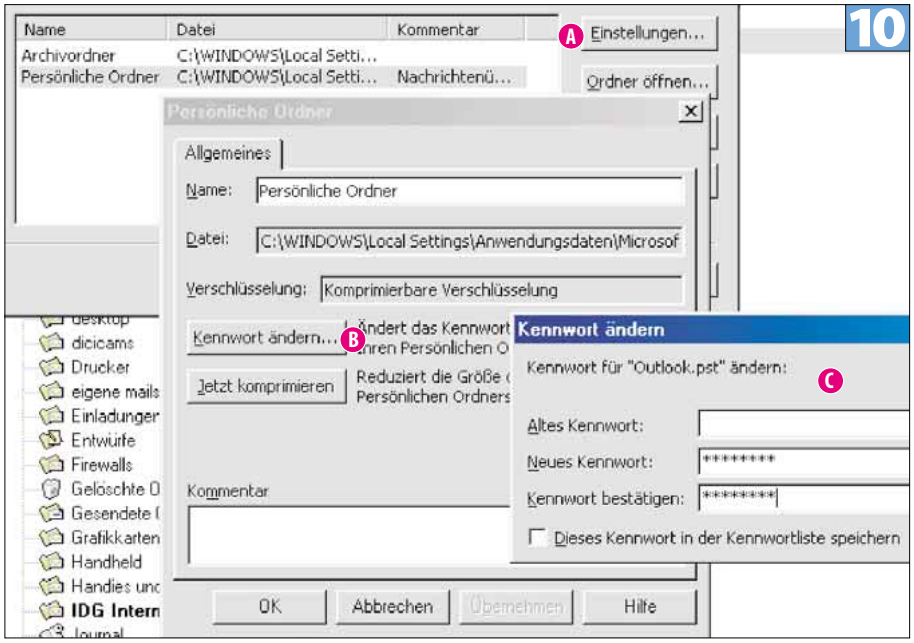
So einfach geht es übrigens nur direkt nach der Installation. Später müssen Sie die Container-Disks zuerst mit dem Passwort öffnen, bevor Sie sie benutzen können. Das geschieht mit einem Klick auf MOUNT DISK. Über ein Dialogfeld müssen Sie die Container-Datei angeben, die sich – sofern Sie die Installation wie oben beschrieben ausgeführt haben – direkt auf dem Laufwerk C:\ befindet. Wählen Sie die Datei Scramble.dcv, klicken Sie auf MOUNT, geben Sie die Passwörter ein und schliessen Sie mit OK ab. Das virtuelle Laufwerk kann wieder verwendet werden.

Bewertung: Dieses Programm ist einfach zu bedienen und schützt in der Vollversion effektiv. Es arbeitet mit bewährten Technologien und macht Ihre Daten für wenig Geld für Dritte unlesbar.

Mails schützen in Outlook: E-Mails enthalten oft vertrauliche Mitteilungen. Outlook erlaubt, die Dateien im Posteingang mit einem Kennwort vor fremden Blicken zu schützen. Die Einstellung ist unter DATEI/DATENDATEIVERWALTUNG versteckt.

Wählen Sie im Fenster «Outlook-Datendateien» den Eintrag «Persönliche Ordner» aus und klicken Sie auf EINSTELLUNGEN..., **Screen 10**, **A**, gefolgt von einem Klick auf KENNWORT ÄNDERN... im Fenstern «Persönliche Ordner», **B**. Dann legen Sie das Kennwort fest und bestätigen mit OK, **C**. Beim nächsten Start müssen Sie das Kennwort eingeben, bevor Sie Ihre Nachrichten sehen.

Bewertung: Diese Sicherung schützt vor einfachen Angriffen, kann aber natürlich auch mit geeigneten Programmen geknackt werden. Aber: Jede zusätzlich eingebaute Schwelle verzögert auch bei einem «Profi» den Datenklau. ▶



Auch Outlook kennt einen Schutz gegen neugierige Blicke.

Sicherer PC, sichere Daten

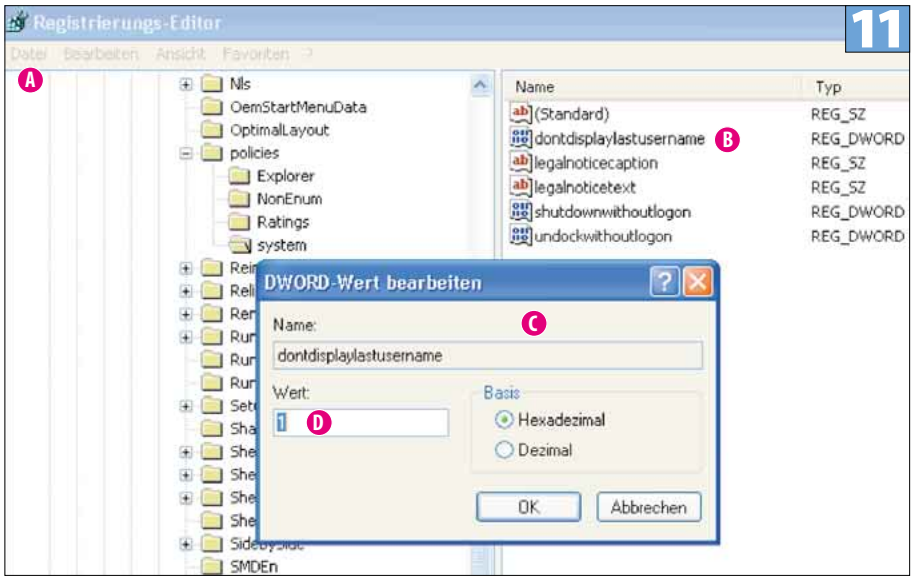
Sicherheitsstufe 3

Anmeldung mit Benutzername und Passwort: In Sicherheitsstufe 2 haben wir bemängelt, dass bei der Anmeldung von Windows 2000 und XP der Name des letzten Benutzers automatisch angezeigt wird. Damit das nicht geschieht, müssen Sie einen Registry-Eintrag verändern.

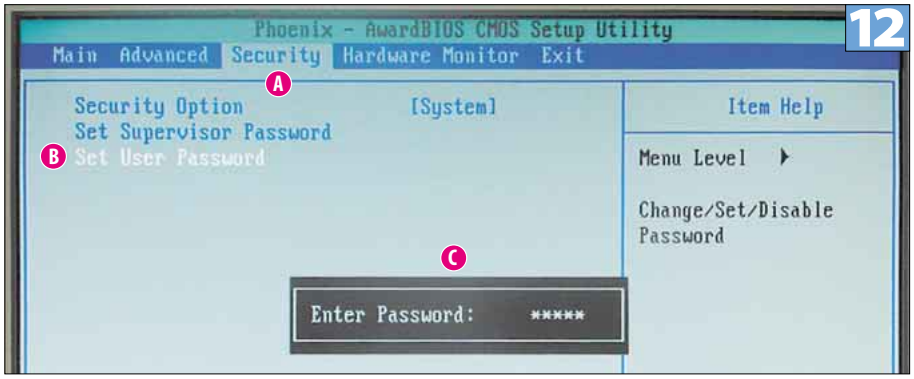
Ein Klick auf START/AUSFÜHREN öffnet das Fenster «Ausführen». Schreiben Sie «regedit» in das Feld hinter «Öffnen» und klicken Sie auf OK. Das Ändern von Einträgen in der Registry ist heikel. Legen Sie deshalb mit DATEI/EXPORTIEREN, **Screen 11**, A, von der aktuellen, unveränderten Version ein Backup an: Wählen Sie einen geeigneten Speicherort (z. B. den Ordner «Eigene Dateien»), geben Sie dem Backup einen passenden Namen (z. B. «registry_alt.reg») und schliessen Sie die Eingabe mit SPEICHERN ab.

Klicken Sie sich wie folgt durch die Verzeichnisstruktur (linker Teil im Fenster): ARBEITSPLATZ/HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/CURRENTVERSION/POLICIES/SYSTEM. Ein Rechtsklick auf den Eintrag DONTDISPLAYLASTUSERNAME, **Screen 11**, B, zeigt das Kontextmenü. Klicken Sie auf ÄNDERN, um das Fenster «DWORD-Wert bearbeiten» zu öffnen, C. Setzen Sie den Wert von «0» auf «1», D. Nach einem Neustart wird der Benutzername im Login-Fenster nicht mehr angezeigt.

Bewertung: Von den zwei Identifikationsmerkmalen Benutzername und Passwort wird endlich keines mehr angezeigt. So muss ein Hacker beides erraten. Wenn die Wörter gut gewählt sind, lässt sich das System nur noch schwer knacken.



Ein Eingriff in die Registry bringt Windows mehr Vorsicht bei.



Das BIOS-Passwort ist die allererste Zugangssperre beim Aufstarten.

Zugang Computer: Einige der bisher vorgestellten Möglichkeiten können einfach umgangen werden, indem der Computer mit einer Diskette statt von der Harddisk aufgestartet wird. Zum Glück kann man über das BIOS eine Passwortschranke errichten, die eine Authentifizierung verlangt, noch bevor irgendetwas anderes geschieht.

Wer Einstellungen im BIOS vornehmen will, muss gleich nach dem Aufstarten bei den meisten PCs die Taste *F2*, *DEL* oder *ESC* drücken. Welche es ist, steht einerseits in der Betriebsanleitung des Computers, andererseits weist der PC beim Aufstartvorgang darauf hin («Setup»). Da es verschiedene BIOS-Versionen verschiedener Hersteller gibt, ist die folgende Anleitung nur als Beispiel zu verstehen. Der Vorgang ist zwar immer gleich, die Namen der Menüpunkte ebenso wie die Menüstruktur können jedoch abweichen.

Achtung: Im BIOS funktioniert die Maus nicht, man navigiert mit den *Pfeiltasten*, *ESC* und *Enter*. Wählen Sie zuerst den Menüpunkt «Security», **Screen 12**, A. Steuern Sie zu «Set User Password», B, und drücken Sie *Enter*. Nun werden Sie aufgefordert, ein Passwort einzugeben («Enter Password:», C).

Danach müssen Sie die Eingabe bestätigen («Confirm Password»), um sicherzustellen, dass Sie sich beim ersten Mal nicht vertippt haben. Navigieren Sie zu «Exit» und wählen Sie «Exit and Save». Beim nächsten Aufstarten wird der PC das Passwort abfragen, noch bevor das System aufstartet und auf ein Laufwerk zugreift.

Bewertung: Diese Methode ist sehr sicher. Man kann die Abfrage fast nur umgehen, indem man den Computer aufschraubt und die Hardware manipuliert. Dennoch: Profis finden auch hier Tools, die zumindest bei einigen BIOS-Varianten die Passwörter knacken, siehe PCtip 7/2003 (**http://www.pctip.ch/library/pdf/2003/07/0740tric.pdf**).

Fazit: Keine der hier vorgestellten Lösungen ist hundertprozentig sicher. Die absolute Sicherheit, so wie sie manche Hersteller versprechen, gibt es nicht. Aber: Je mehr Möglichkeiten kombiniert werden, desto besser sind Ihre persönlichen Daten vor unbefugten Zugriffen geschützt. Beachten Sie deshalb auch die beiden Boxen «Die Hardware professionell absichern», S. 48, und «Artikel zum Thema Sicherheit», links.

Lesestoff

Artikel zum Thema Sicherheit

Passwörter

Bei der Wahl eines guten Passwortes müssten zwei Kriterien erfüllt sein: Es soll aus einer Zahlen-/Buchstaben-Kombination bestehen, die nicht zu erraten und trotzdem einfach zu merken ist. Strategien für die Wahl eines guten Passwortes beschreibt der PCtip in der Ausgabe 3/2003 im Artikel «Geheime Schlüssel» ab S. 42, http://www.pctip.ch/library/pdf/03/03/0342pass.pdf.

Daten sichern

Falls die Daten doch einmal verloren gehen, muss eine Sicherheitskopie vorhanden sein. Wie man ein effizientes Backup macht, ist im PCtip 2/2003 in «Daten bergen» ab S. 54 beschrieben (http://www.pctip.ch/library/pdf/2003/02/0254Back.pdf). Welche Laufwerke sich dafür eignen, konnten Sie in der letzten Ausgabe 8/2003 im Artikel «Sicher sichern» ab S. 60 lesen.

Sicheres Internet

Am fiesesten ist der Datenklau via Internet. Der Inhalt einer Festplatte stiehlt ein Profi-Hacker, ohne dass der Besitzer es merkt. Aber auch dagegen kann man sich effizient schützen. Mehr dazu stand im PCtip 12/2002 ab Seite 26 im Artikel «Der Feind liest mit» (http://www.pctip.ch/library/pdf/2002/12/1226safe.pdf) oder in diesem Heft ab Seite 24.